aws

管理者ガイド

Amazon WorkMail

Version 1.0

Amazon WorkMail: 管理者ガイド

Table of Contents

Amazon とは WorkMail

Amazon WorkMail は、既存のデスクトップおよびモバイル E メールクライアントをサポートする、安全でマネージド型のビジネス E メールおよびカレンダーサービスです。Amazon WorkMail ユーザーは、Microsoft Outlook、ブラウザ、またはネイティブの iOS および Android E メールアプリケーションを使用して、E メール、連絡先、カレンダーにアクセスできます。Amazon を既存の社内ディレクトリ WorkMail と統合して、データを暗号化するキーと、データの保存場所の両方を制御できます。

サポートされている AWS リージョンとエンドポイントのリストについては、AWS のリージョンとエンドポイントを参照してください。

トピック

Amazon WorkMail システム要件

Amazon WorkMail 管理者から Amazon WorkMail アカウントにサインインするように求められたら、Amazon WorkMail ウェブクライアントを使用してサインインできます。

Amazon は、Exchange ActiveSync プロトコルをサポートするすべての主要なモバイルデバイスとオペレーティングシステム WorkMail でも動作します。これらのデバイスは、iPad、iPhone、Android、Windows Phone などです。macOS のユーザーは、Amazon WorkMail アカウントをメール、カレンダー、連絡先アプリに追加できます。

Amazon では、以下のオペレーティングシステムバージョン WorkMail がサポートされています。

- Windows – Windows 7 SP1 以降
- MacOS – MacOS 10.12 (Sierra) 以降
- Android — アンドロ 5.0 以降
- iPhone – iOS 5 以降

- Windows phone – Windows 8.1 以降
- Blackberry - Blackberry OS 10.3.3.3216

有効な Microsoft Outlook ライセンスをお持ちの場合は、以下のバージョンの Microsoft Outlook WorkMail を使用して Amazon にアクセスできます。

- Outlook 2013 以降
- Outlook 2013 Click-to-Run 以降
- Outlook for Mac 2016 以降

Amazon WorkMail ウェブクライアントには、次のブラウザバージョンを使用してアクセスできます。

- Google Chrome – バージョン 22 以降
- Mozilla Firefox – バージョン 27 以降
- Safari – バージョン 7 以降
- Internet Explorer – バージョン 11
- Microsoft Edge

任意の IMAP クライアント WorkMail で Amazon を使用することもできます。

Amazon の WorkMail 概念

Amazon WorkMail を理解し使用するために重要な用語と概念を以下に示します。

組織

Amazon のテナント設定 WorkMail。

エイリアス

組織を識別するグローバルに一意の名前。エイリアスは、Amazon WorkMail ウェブアプリケーション (https://*alias* .awsapps.com/mail) にアクセスするために使用されます。

ドメイン

E メールアドレスの @ 記号の後に付くウェブアドレス。E メールを受信して組織のメールボックスに配信するドメインを追加できます。

メールドメインをテストする

ドメインはセットアップ時に自動的に設定され、Amazon のテストに使用できます WorkMail。テストメールドメインは *alias*.awsapps.com であり、独自のドメインを設定しない場合はデフォルトのドメインとして使用されます。テストメールドメインには、さまざまな制限があります。詳細については、「Amazon WorkMail クォータ」を参照してください。

ディレクトリ

CC で作成された AWS Simple AD、AWS Managed AD、または AD Connector。Amazon WorkMail Quick Setup を使用して組織を作成すると、 WorkMail ディレクトリが作成されます。に WorkMail ディレクトリを表示することはできませんAWS Directory Service。

ユーザー

AWS Directory Service で作成されたユーザー。ユーザーは ユーザー または REMOTE_USER ロールで作成できます。ユーザーが ユーザー で有効になると、アクセスする独自のメールボックスを受け取ります。ユーザーが無効化されると、Amazon にアクセスできなくなります WorkMail。

REMOTE_USER ロールを使用して作成および有効化されたユーザーは、アドレス帳に一覧表示されますが、Amazon のメールボックスは取得されません WorkMail。REMOTE_USER は Amazon の外部でメールボックスをホストできます WorkMail が、Amazon WorkMail アドレス帳にはメールボックスを持つ他のユーザーとして表示され、互いのカレンダーを検索して空き時間情報を検索できます。

グループ

AWS Directory Service で使用されるグループ。グループは、Amazon のディストリビューションリストまたはセキュリティグループとして使用できます WorkMail。グループには独自のメールボックスはありません。

リソース

リソースは、Amazon WorkMail ユーザーが予約できる会議室または機器リソースを表します。

モバイルデバイスポリシー

モバイルデバイスのセキュリティの機能と動作を制御するさまざまな IT ポリシールール。

AWS の関連サービス

以下の サービスが Amazon とともに使用されます WorkMail。

- AWS Directory Service— Amazon を既存の AWS Simple AD、 AWS Managed AD、または AD Connector WorkMail と統合できます。にディレクトリAWS Directory Serviceを作成し、このディレクトリ WorkMail に対して Amazon を有効にします。この統合を設定したら、既存のディレクトリ内のユーザーの WorkMail リストから Amazon を有効にするユーザーを選択し、ユーザーは既存の Active Directory 認証情報を使用してログインできます。詳細については、AWS Directory Service 管理ガイドを参照してください。
- Amazon Simple Email Service — Amazon WorkMail は Amazon SES を使用してすべての送信 E メールを送信します。テストメールのドメインとお客様のドメインは、Amazon SES コンソールで管理できます。Amazon から送信される送信 E メールにはコストはかかりません WorkMail。詳細については、Amazon Simple Email Service デベロッパーガイドを参照してください。
- AWS Identity and Access Management — AWS Management Console ではユーザー名とパスワードが要求されます。これでリソースへのアクセス許可があるかどうかをサービスが判断できます。AWS アカウントの認証情報を使用して AWS にアクセスしないことをお勧めします。AWS アカウントの認証情報はいかなる方法でも取り消したり、制限したりできないためです。代わりに、IAM ユーザーを作成し、管理アクセス権限のある IAM グループにそのユーザーを追加することをお勧めします。その結果、IAM ユーザーの認証情報を使用してコンソールにアクセスすることになります。

  AWS にサインアップしたけれど、自身の IAM ユーザーをまだ作成していない場合は、IAM コンソールを使用して作成できます。詳細については、IAM ユーザーガイドの個々の IAM ユーザーを作成するを参照してください。
- AWS Key Management Service— Amazon WorkMail は、顧客データの暗号化AWS KMSのためにと統合されています。キーの管理は、AWS KMS コンソールから行うことができます。詳細については、AWS Key Management Service デベロッパーガイド の AWS Key Management Service とは何でしょうか を参照してください。

Amazon の WorkMail 料金

Amazon では WorkMail、前払い料金やコミットメントはありません。アクティブなユーザーアカウントに対してのみ料金が発生します。料金の詳細については、料金表を参照してください。

Amazon WorkMail リソース

このサービスを利用する際に役立つ関連リソースは次のとおりです。

- クラスとワークショップ – AWS のスキルを磨き、実践的な経験を得るために役立つセルフペースラボに加えて、ロールベースのコースと特別コースへのリンクです。
- AWS デベロッパーセンター – チュートリアルの検索、ツールのダウンロード、AWS デベロッパーイベントの確認を行います。
- AWS デベロッパーツール - AWS アプリケーションを開発および管理するためのデベロッパーツール、SDK、IDE ツールキット、およびコマンドラインツールへのリンクです。
- ご利用開始のためのリソースセンター — AWS アカウント をセットアップする方法、AWS コミュニティに参加する方法、最初のアプリケーションを起動する方法を説明します。
- ハンズオンチュートリアル – step-by-step チュートリアルに従って、 で最初のアプリケーションを起動しますAWS。
- AWS ホワイトペーパー – アーキテクチャ、セキュリティ、エコノミクスなどのトピックについて、AWS のソリューションアーキテクトや他の技術エキスパートが記述した AWS の技術ホワイトペーパーの包括的なリストへのリンクです。
- AWS Support センター – AWS Support のケースを作成して管理するためのハブです。フォーラム、技術上のよくある質問、サービスヘルスステータス、AWS Trusted Advisor など、他の役立つリソースへのリンクも含まれています。
- AWS Support – クラウドでのアプリケーションの構築と実行に役立つ one-on-one、高速対応サポートチャネルAWS Supportである に関する情報のメインウェブページです。
- お問い合わせ - AWS の請求、アカウント、イベント、不正使用、その他の問題などに関するお問い合わせの受付窓口です。
- AWS サイトの利用規約 – 当社の著作権、商標、お客様のアカウント、ライセンス、サイトへのアクセス、その他のトピックに関する詳細情報。

前提条件

Amazon WorkMail 管理者として行動するには、AWS アカウントが必要です。まだ AWS にサインアップしていない場合は、次のタスクを行い、セットアップを終了します。

トピック

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

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

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティのベストプラクティスとして、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 サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] を選んで、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理できます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、 を保護し AWS アカウントのルートユーザー、 を有効にして AWS IAM Identity Center、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。

のセキュリティ保護 AWS アカウントのルートユーザー

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

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドの「ルートユーザーとしてサインインする」を参照してください。
2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、「IAM ユーザーガイド」の AWS アカウント 「ルートユーザーの仮想 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。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。
2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

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

管理アクセス権を持つユーザーとしてサインインする

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

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

追加のユーザーにアクセス権を割り当てる

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

手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。

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

   手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの参加」を参照してください。

Amazon のアクセス許可を IAM ユーザーに付与する WorkMail

デフォルトでは、IAM ユーザーには Amazon WorkMail リソースを管理するアクセス許可はありません。AWS 管理ポリシー (AmazonWorkMailFullAccess または AmazonWorkMailReadOnlyAccess) をアタッチするか、IAM ユーザーにそれらのアクセス許可を明示的に付与するカスタマー管理ポリシーを作成する必要があります。次に、そのような許可が必要な 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。詳細については、「Amazon の Identity and Access Management WorkMail」を参照してください。

Amazon のセキュリティ WorkMail

のクラウドセキュリティが最優先事項 AWS 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からメリットを得られます。

セキュリティは、 AWS とユーザーの間で共有される責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ — AWS クラウドで AWS サービスを実行するインフラストラクチャを保護する AWS 責任があります。 AWS また、 では、安全に使用できるサービスも提供しています。AWS コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。Amazon 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 WorkMail、「コンプライアンスAWS プログラムによる対象範囲内のサービス」を参照してください。
- クラウドのセキュリティ — お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、Amazon の使用時に責任共有モデルを適用する方法を理解するのに役立ちます WorkMail。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 WorkMail ように Amazon を設定する方法について説明します。また、Amazon WorkMail リソースのモニタリングや保護に役立つ他の 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 でのデータ保護 WorkMail
- Amazon の Identity and Access Management WorkMail
- AWS Amazon 管理ポリシー WorkMail
- Amazon WorkMail のサービスリンクロールの使用
- Amazon でのロギングとモニタリング WorkMail
- Amazon のコンプライアンス検証 WorkMail
- Amazon の耐障害性 WorkMail
- Amazon のインフラストラクチャセキュリティ WorkMail

Amazon でのデータ保護 WorkMail

責任 AWS 共有モデル、Amazon のデータ保護に適用されます WorkMail。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービス のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された「AWS 責任共有モデルおよび GDPR」のブログ記事を参照してください。

データ保護の目的で、 認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須であり TLS 1.3 がお勧めです。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、コンソール、API、WorkMail または AWS のサービス SDK を使用して Amazon AWS CLIまたは他の を操作する場合も同様です。 AWS SDKs 名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

Amazon が WorkMail を使用する方法 AWS KMS

Amazon は、メッセージがディスクに書き込まれる前に、すべての Amazon WorkMail 組織のメールボックス内のすべてのメッセージを WorkMail 透過的に暗号化し、ユーザーがメッセージにアクセス

するときにメッセージを透過的に復号します。暗号化は無効にできません。メッセージを保護する暗号化キーを保護するために、Amazon WorkMail は AWS Key Management Service () と統合されていますAWS KMS。

Amazon には、ユーザーが署名付きまたは暗号化された E メールを送信できるようにするオプション WorkMail もあります。この暗号化機能は AWS KMSを使用していません。詳細については、「署名または暗号化された E メールの有効化」を参照してください。

トピック

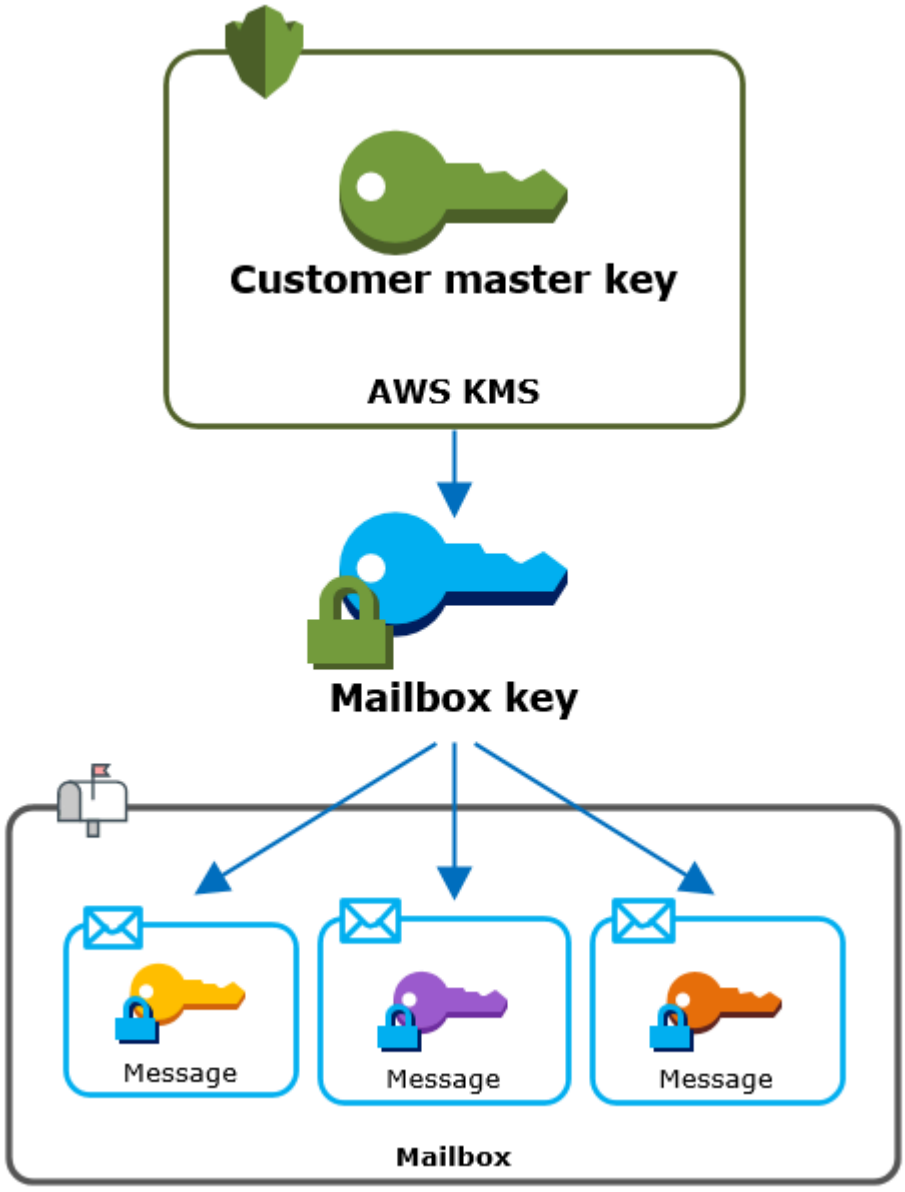
- Amazon WorkMail 暗号化
- CMK の使用の許可
- Amazon WorkMail 暗号化コンテキスト
- との Amazon WorkMail インタラクションのモニタリング AWS KMS

Amazon WorkMail 暗号化

Amazon では WorkMail、各組織には、組織内のユーザーごとに 1 つずつ、複数のメールボックスを含めることができます。E メール、カレンダーの項目などのすべてのメッセージはユーザーのメールボックスに保存されます。

Amazon WorkMail 組織内のメールボックスの内容を保護するために、Amazon はすべてのメールボックスメッセージをディスクに書き込む前に WorkMail 暗号化します。お客様から提供された情報がプレーンテキストで保存されることはありません。

各メッセージは、一意のデータ暗号化キーで暗号化されます。メッセージキーは、そのメールボックスでのみ使用される一意の暗号化キーであるメールボックスキーで保護されています。メールボックスキーは、 が暗号化 AWS KMS されずに を残さない組織の AWS KMS カスタマーマスターキー (CMK) で暗号化されます。次の図では、 AWS KMSにおける、暗号化されたメッセージ、暗号化されたメッセージキー、暗号化されたメールボックスキー、組織の CMK の関係を示しています。



組織の CMK を設定する

Amazon WorkMail 組織を作成するときに、組織の AWS KMS カスタマーマスターキー (CMK) を選択するオプションがあります。この CMK は組織内のすべてのメールボックスキーを保護します。

Amazon のデフォルトの AWS 管理の CMK を選択するか WorkMail、所有および管理している既存のカスタマー管理の CMK を選択できます。詳細については、AWS Key Management Service デベロッパーガイドのカスタマーマスターキー (CMK) を参照してください。各組織に同じ CMK を使用するか異なる CMK を使用するかを選択できますが、一度選択した CMK を変更することはできません。

> **Important**
>
> Amazon は、対称 CMKsのみ WorkMail をサポートします。非対称 CMK を使用することはできません。CMK が対称か非対称かを判断する方法については、AWS Key Management Service デベロッパーガイドの対称と非対称 CMK の識別を参照してください。

組織の CMK を検索するには、 への呼び出しを記録する AWS CloudTrail ログエントリを使用します AWS KMS。

各メールボックスの一意の暗号化キー

メールボックスを作成すると、Amazon は、メールボックスキー と呼ばれるメールボックスの一意の 256 ビット Advanced Encryption Standard (AES) 対称暗号化キーを、 の外部で WorkMail 生成します AWS KMS。Amazon WorkMail はメールボックスキーを使用して、メールボックス内の各メッセージの暗号化キーを保護します。

メールボックスキーを保護するために、Amazon は AWS KMS を WorkMail 呼び出して、組織の CMK でメールボックスキーを暗号化します。その後、メールボックスのメタデータに暗号化されたメールボックスキーを保存します。

> **Note**
>
> Amazon WorkMail は、対称メールボックス暗号化キーを使用してメッセージキーを保護します。以前は、Amazon WorkMail は各メールボックスを非対称キーペアで保護していました。パブリックキーを使用して各メッセージキーを暗号化し、プライベートキーで復号していました。プライベートメールボックスキーは組織の CMK で保護されていました。古いメールボックスは非対称メールボックスkey pair を使用している場合があります。この変更により、メールボックスやそのメッセージのセキュリティに影響が生じることはありません。

各メッセージを暗号化する。

ユーザーがメールボックスにメッセージを追加すると、Amazon は の外部でメッセージの一意の 256 ビット AES 対称暗号化キー WorkMail を生成します AWS KMS。このメッセージキーを使用してメッセージを暗号化します。Amazon はメールボックスキーでメッセージキーを WorkMail 暗号化し、暗号化されたメッセージキーをメッセージとともに保存します。次に、組織の CMK でメールボックスキーを暗号化します。

新しいメールボックスの作成

Amazon がメールボックス WorkMail を作成すると、次のプロセスを使用して、暗号化されたメッセージを保持するメールボックスを準備します。

- Amazon は、AWS KMS の外部でメールボックスの一意の 256 ビット AES 対称暗号化キー WorkMail を生成します。
- Amazon は AWS KMS Encrypt オペレーションを WorkMail 呼び出します。メールボックスキーと組織のカスタマーマスターキー (CMK) の識別子を渡します。 は、CMK で暗号化されたメールボックスキーの暗号文 AWS KMS を返します。
- Amazon は、暗号化されたメールボックスキーをメールボックスメタデータとともに WorkMail 保存します。

メールボックスメッセージの暗号化

メッセージを暗号化するために、Amazon は次のプロセス WorkMail を使用します。

1. Amazon は、メッセージの一意の 256 ビット AES 対称キー WorkMail を生成します。プレーンテキストメッセージキーと Advanced Encryption Standard (AES) アルゴリズムを使用して、 の外部でメッセージを暗号化します AWS KMS。
2. メールボックスキーでメッセージキーを保護するには、Amazon は常に暗号化された形式で保存されているメールボックスキーを復号 WorkMail する必要があります。

   Amazon は AWS KMS Decrypt オペレーションを WorkMail 呼び出し、暗号化されたメールボックスキーを渡します。 は、組織の CMK AWS KMS を使用してメールボックスキーを復号し、プレーンテキストのメールボックスキーを Amazon に返します WorkMail。
3. Amazon WorkMail は、プレーンテキストのメールボックスキーと Advanced Encryption Standard (AES) アルゴリズムを使用して、 の外部でメッセージキーを暗号化します AWS KMS。
4. Amazon WorkMail は、暗号化されたメッセージキーを暗号化されたメッセージのメタデータに保存して、復号化できるようにします。

メールボックスメッセージの復号

メッセージを復号するために、Amazon は次のプロセス WorkMail を使用します。

1. Amazon AWS KMS は Decrypt オペレーションを WorkMail 呼び出し、暗号化されたメールボックスキーを渡します。 は組織の CMK AWS KMS を使用してメールボックスキーを復号し、プレーンテキストのメールボックスキーを Amazon に返します WorkMail。

2. Amazon WorkMail は、プレーンテキストのメールボックスキーと Advanced Encryption Standard (AES) アルゴリズムを使用して、暗号化されたメッセージキーを の外部で復号化します AWS KMS。
3. Amazon WorkMail は、プレーンテキストのメッセージキーを使用して暗号化されたメッセージを復号します。

メールボックスキーのキャッシュ

パフォーマンスを向上させ、 への呼び出しを最小限に抑えるために AWS KMS、Amazon は各クライアントの各プレーンテキストのメールボックスキーを最大 1 分間ローカルに WorkMail キャッシュします。キャッシュ期間の終了時に、メールボックスキーは削除されます。キャッシュ期間中にそのクライアントのメールボックスキーが必要な場合、Amazon は を呼び出す代わりにキャッシュからキーを取得 WorkMail できます AWS KMS。メールボックスキーはキャッシュで保護されており、プレーンテキストでディスクに書き込まれることはありません。

CMK の使用の許可

Amazon が暗号化オペレーションでカスタマーマスターキー (CMK) WorkMail を使用する場合、Amazon はメールボックス管理者に代わって動作します。

ユーザーに代わってシークレットに AWS KMS カスタマーマスターキー (CMK) を使用するには、管理者に次のアクセス許可が必要です。IAM ポリシーまたはキーポリシーで、これらの必要なアクセス許可を指定できます。

- `kms:Encrypt`
- `kms:Decrypt`
- `kms:CreateGrant`

CMK を Amazon から発信されたリクエストにのみ使用できるようにするには WorkMail、kms:ViaService 条件キーを `workmail.<region>.amazonaws.com`値とともに使用できます。

また、暗号化オペレーションに CMK を使用する条件として、暗号化コンテキストでキーまたは値を使用することもできます。例えば、IAM またはキーポリシードキュメントで文字列条件演算子を使用したり、許可で許可制約を使用したりできます。

AWS 管理 CMK のキーポリシー

Amazon 用 AWS マネージド CMK のキーポリシーは、Amazon がユーザーに代わってリクエスト WorkMail を行った場合にのみ、指定されたオペレーションに CMK を使用するアクセス許可をユーザーに WorkMail 付与します。このキーポリシーでは、ユーザーが CMK を直接使用することは許可されません。

このキーポリシーは、すべての AWS 管理キーと同様に、サービスによって確立されます。キーポリシーは変更できませんが、いつでも表示できます。詳細については、AWS Key Management Service デベロッパーガイドのキーポリシーの表示を参照してください。

このキーポリシーのポリシーステートメントには次の効果があります

- アカウントとリージョンのユーザーが CMK を暗号化オペレーションに使用したり、権限を作成したりできるようにします。ただし、リクエストがユーザーに代わって Amazon から送信された場合に限り WorkMail ます。`kms:ViaService` 条件キーで、この制限を適用します。
- AWS アカウントが CMK プロパティの表示と許可の取り消しをユーザーに許可する IAM ポリシーを作成できるようにします。

以下は、Amazon 用 AWS マネージド CMK の例のキーポリシーです WorkMail。

```
{
  "Version" : "2012-10-17",
  "Id" : "auto-workmail-1",
  "Statement" : [ {
    "Sid" : "Allow access through WorkMail for all principals in the account that are
 authorized to use WorkMail",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "*"
    },
    "Action" : [ "kms:Decrypt", "kms:CreateGrant", "kms:ReEncrypt*", "kms:DescribeKey",
 "kms:Encrypt" ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "kms:ViaService" : "workmail.us-east-1.amazonaws.com",
        "kms:CallerAccount" : "111122223333"
      }
    }
  }, {
    "Sid" : "Allow direct access to key metadata to the account",
    "Effect" : "Allow",
```

```
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : [ "kms:Describe*", "kms:List*", "kms:Get*", "kms:RevokeGrant" ],
    "Resource" : "*"
  } ]
}
```

許可を使用した Amazon の認証 WorkMail

キーポリシーに加えて、Amazon WorkMail は権限を使用して、各組織の CMK にアクセス許可を追加します。アカウントの CMK に対する許可を表示するには、 ListGrantsオペレーションを使用します。

Amazon WorkMail は権限を使用して、組織の CMK に次のアクセス許可を追加します。

- Amazon がメールボックスキーを暗号化 WorkMail できるようにするアクセス`kms:Encrypt`許可を追加します。
- Amazon が CMK を使用してメールボックスキーを復号 WorkMail できるようにする`kms:Decrypt`アクセス許可を追加します。Amazon では、メールボックスメッセージを読み取るリクエストは、メッセージを読み取るユーザーのセキュリティコンテキストを使用するため、このアクセス許可をグラントに WorkMail 要求します。リクエストは AWS アカウントの認証情報を使用しません。組織の CMK を選択すると、Amazon はこの許可 WorkMail を作成します。

権限を作成するために、Amazon は組織を作成したユーザーCreateGrantに代わって を WorkMail 呼び出します。権限付与を作成するアクセス許可はキーポリシーから付与されます。このポリシーは、Amazon `CreateGrant`が承認されたユーザーに代わってリクエスト WorkMail を行うときに、アカウントのユーザーが組織の CMK で を呼び出すことを許可します。

キーポリシーでは、アカウントルートが AWS マネージドキーの許可を取り消すことも許可します。ただし、許可を取り消すと、Amazon WorkMail はメールボックス内の暗号化されたデータを復号化できません。

Amazon WorkMail 暗号化コンテキスト

暗号化コンテキストは、任意のシークレットデータを含まない、一連のキーと値のペアです。データを暗号化するリクエストに暗号化コンテキストを含めると、 は暗号化コンテキストを暗号化されたデータに AWS KMS 暗号的にバインドします。データを復号するには、同じ暗号化コンテキストに渡す必要があります。詳しくは、AWS Key Management Service デベロッパーガイドの Encryption context を参照してください。

Amazon は、すべての暗号化オペレーションで同じ AWS KMS 暗号化コンテキスト形式 WorkMail を使用します。暗号化コンテキストを使用して、AWS CloudTrail などの監査レコードやログで、暗号化オペレーションを確認できます。また、ポリシーと許可で認可の条件として確認することもできます。

への Encrypt および Decrypt リクエストでは AWS KMS、Amazon はキーが `aws:workmail:arn`で値が組織の Amazon リソースネーム (ARN) である暗号化コンテキスト WorkMail を使用します。

```
"aws:workmail:arn":"arn:aws:workmail:region:account ID:organization/organization-ID"
```

例えば、次の暗号化コンテキストには欧州 (アイルランド) (`eu-west-1`) リージョンの組織の ARN のサンプルが含まれています。

```
"aws:workmail:arn":"arn:aws:workmail:eu-west-1:111122223333:organization/m-
a123b4c5de678fg9h0ij1k2lm234no56"
```

との Amazon WorkMail インタラクションのモニタリング AWS KMS

AWS CloudTrail および Amazon CloudWatch Logs を使用して、Amazon が AWS KMS ユーザーに代わって WorkMail に送信するリクエストを追跡できます。

暗号化

メールボックスを作成すると、Amazon WorkMail はメールボックスキーを生成し、 AWS KMS を呼び出してメールボックスキーを暗号化します。Amazon は、プレーンテキストのメールボックスキーと Amazon WorkMail 組織の CMK の識別子 AWS KMS を使用して Encrypt リクエストを WorkMail に送信します。

`Encrypt` 演算を記録するイベントは、次のようなサンプルイベントになります。ユーザーは Amazon WorkMail サービスです。パラメータには、CMK ID (`keyId`) と Amazon WorkMail 組織の暗号化コンテキストが含まれます。Amazon はメールボックスキー WorkMail も渡しますが、ログには記録されません CloudTrail 。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "workmail.eu-west-1.amazonaws.com"
    },
    "eventTime": "2019-02-19T10:01:09Z",
    "eventSource": "kms.amazonaws.com",
```

```
    "eventName": "Encrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "workmail.eu-west-1.amazonaws.com",
    "userAgent": "workmail.eu-west-1.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:workmail:arn": "arn:aws:workmail:eu-west-1:111122223333:organization/
m-a123b4c5de678fg9h0ij1k2lm234no56"
        },
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d"
    },
    "responseElements": null,
    "requestID": "76e96b96-7e24-4faf-a2d6-08ded2eaf63c",
    "eventID": "d5a59c18-128a-4082-aa5b-729f7734626a",
    "readOnly": true,
    "resources": [
        {
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "accountId": "111122223333",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "sharedEventID": "d08e60f1-097e-4a00-b7e9-10bc3872d50c"
}
```

Decrypt

メールボックスメッセージを追加、表示、または削除すると、Amazon はメールボックスキーを復号するように AWS KMS に WorkMail 要求します。Amazon は、暗号化されたメールボックスキーと Amazon WorkMail 組織の CMK の識別子を使用して、Decrypt リクエストを WorkMail に送信します。 AWS KMS

Decrypt 演算を記録するイベントは、次のようなサンプルイベントになります。ユーザーは Amazon WorkMail サービスです。パラメータには、ログに記録されない暗号化されたメールボックスキー (暗号文 BLOB として) と、Amazon WorkMail organization. AWS KMS の暗号化コンテキストが含まれます。 は、暗号文から CMK の ID を取得します。

```
{
```

```
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "workmail.eu-west-1.amazonaws.com"
    },
    "eventTime": "2019-02-20T11:51:10Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "workmail.eu-west-1.amazonaws.com",
    "userAgent": "workmail.eu-west-1.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:workmail:arn": "arn:aws:workmail:eu-west-1:111122223333:organization/
m-a123b4c5de678fg9h0ij1k2lm234no56"
        }
    },
    "responseElements": null,
    "requestID": "4a32dda1-34d9-4100-9718-674b8e0782c9",
    "eventID": "ea9fd966-98e9-4b7b-b377-6e5a397a71de",
    "readOnly": true,
    "resources": [
        {
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "accountId": "111122223333",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "sharedEventID": "241e1e5b-ff64-427a-a5b3-7949164d0214"
}
```

Amazon の Identity and Access Management WorkMail

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

トピック

対象者

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

サービスユーザー – ジョブを実行するために Amazon WorkMail サービスを使用する場合、管理者から必要な認証情報とアクセス許可が与えられます。さらに多くの Amazon WorkMail 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解しておくと、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、 WorkMail「」を参照してくださいAmazon WorkMail アイデンティティとアクセスのトラブルシューティング。

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

IAM 管理者 – IAM 管理者は、Amazon 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 WorkMail。IAM で使用できる Amazon WorkMail アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon WorkMail アイデンティティベースのポリシーの例。

アイデンティティを使用した認証

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

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center （ 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 の認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 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。へのサインインの詳細については AWS、「 ユーザーガイド」の「 にサインインする方法 AWS アカウントAWS サインイン 」を参照してください。

AWS プログラムで にアクセスする場合、 は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。 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リクエストを自分で署名する方法の詳細については、IAM ユーザーガイドの API AWS リクエストの署名を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 AWS では、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「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。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての AWS のサービス およびリソースへの完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID 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サインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、IAM ユーザーガイドの「ルートユーザー認証情報が必要なタスク」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内の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、一時認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アク

セスキーをローテーションすることをお勧めします。詳細については、IAM ユーザーガイド の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

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

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時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、特定のアクセス許可 AWS アカウント を持つ 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 AWS Management Console ことで、 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、 または AWS API AWS CLI 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:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションの詳細については、「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 Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM 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 ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。

- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (ロールをプロキシとして使用する代わりに) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスのロールとリソースベースのポリシーの違いについては、IAM ユーザーガイドの「IAM でのクロスアカウントリソースアクセス」を参照してください。
- クロスサービスアクセス — 一部の は、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) — IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。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、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールの許可を表示できますが、編集することはできません。
- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。 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

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

管理者は 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んなリソースにどんな条件でアクションを実行できるかということです。

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

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

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザー、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 権限ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベース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ています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロン

ポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「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、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

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

アクセスコントロールリスト (ACL)

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

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

その他のポリシータイプ

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

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベース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) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境

界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。

- サービスコントロールポリシー (SCPs) – SCPs は、 の組織または組織単位 (OU) に対する最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、 AWS アカウント ビジネスが所有する複数の をグループ化して一元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、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、AWS Organizations ユーザーガイドの「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ションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

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

Amazon と IAM WorkMail 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 WorkMail、Amazon で使用できる IAM 機能を理解しておく必要があります WorkMail。Amazon WorkMail およびその他の AWS のサービスが IAM と連携する方法の概要を把握するには、「IAM ユーザーガイド」の「IAM AWS と連携する のサービス」を参照してください。

トピック

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

Amazon WorkMail 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、許可または拒否するアクションとリソース、アクションを許可または拒否する条件を指定できます。Amazon は、特定のアクション、リソース、および条件キー WorkMail をサポートしています。JSON ポリシーで使用するすべての要素については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素のリファレンス」を参照してください。

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んなリソースにどんな条件でアクションを実行できるかということです。

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

このアクションは、関連付けられたオペレーションを実行するための権限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は、アクションの前にプレフィックス WorkMail を使用しますworkmail:。例えば、Amazon WorkMail ListUsers API オペレーションを使用してユーザーのリストを取得するアクセス許可を付与するには、ポリシーに workmail:ListUsersアクションを含めます。ポリシーステートメントには、Action または NotAction 要素を含める必要があります。Amazon WorkMail は、このサービスで実行できるタスクを記述する独自のアクションのセットを定義します。

単一ステートメントに複数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": [
      "workmail:ListUsers",
      "workmail:DeleteUser"
```

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、List 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": "workmail:List*"
```

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

リソース

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どのような条件でアクションを実行できるかということです。

Resource JSON ポリシー要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

Amazon WorkMail は、Amazon WorkMail 組織のリソースレベルのアクセス許可をサポートしています。

Amazon WorkMail 組織リソースには、次の ARN があります。

```
arn:aws:workmail:${Region}:${Account}:organization/${OrganizationId}
```

ARN の形式の詳細については、「Amazon リソースネーム (ARNs AWS 「サービス名前空間」を参照してください。

例えば、ステートメントで m-n1pq2345678r901st2u3vx45x6789yza 組織を指定するには、次の ARN を使用します。

```
"Resource": "arn:aws:workmail:us-east-1:111122223333:organization/m-
n1pq2345678r901st2u3vx45x6789yza"
```

特定のアカウントに属するすべての組織を指定するには、ワイルドカード (*) を使用します。

```
"Resource": "arn:aws:workmail:us-east-1:111122223333:organization/*"
```

リソースを作成するためのアクションなど、一部の Amazon WorkMail アクションは、特定のリソースで実行できません。このような場合は、ワイルドカード *を使用する必要があります。

```
"Resource": "*"
```

Amazon WorkMail リソースタイプとその ARNs」の「Amazon で定義されるリソース WorkMail」を参照してください。 各リソースの ARN に指定できるアクションについては、「Amazon のアクション、リソース、および条件キー WorkMail」を参照してください。

条件キー

Amazon では、以下のグローバル条件キー WorkMail がサポートされています。

- aws:CurrentTime
- aws:EpochTime
- aws:MultiFactorAuthAge
- aws:MultiFactorAuthPresent
- aws:PrincipalOrgID
- aws:PrincipalArn
- aws:RequestedRegion
- aws:SecureTransport
- aws:UserAgent

次のポリシー例では、AWS リージョンの MFA 認証された IAM プリンシパルからのみ Amazon eu-west-1 WorkMail コンソールへのアクセスを許可します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ses:Describe*",
                "ses:Get*",
                "workmail:Describe*",
                "workmail:Get*",
                "workmail:List*",
                "workmail:Search*",
```

```
                "lambda:ListFunctions",
                "iam:ListRoles",
                "logs:DescribeLogGroups",
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                },
                "Bool": {
                    "aws:MultiFactorAuthPresent": true
                }
            }
        }
    ]
}
```

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。

workmail:ImpersonationRoleId は、Amazon でサポートされている唯一のサービス固有の条件キーです WorkMail。

次のポリシーの例では、特定の WorkMail 組織となりすましロールAssumeImpersonationRoleに対するアクションの範囲を絞り込みます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workmail:AssumeImpersonationRole"
      ],
      "Resource": "arn:aws:workmail:us-east-1:111122223333:organization/m-
n1pq2345678r901st2u3vx45x6789yza",
      "Condition": {
        "StringEquals": {
          "workmail:ImpersonationRoleId":"12345678-1234-1234-1234-123456789012"
        }
```

```
      }
    }
  ]
}
```

例

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

Amazon WorkMail リソースベースのポリシー

Amazon WorkMail 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 WorkMail タグに基づく認可

Amazon WorkMail リソースにタグをアタッチするか、Amazon へのリクエストでタグを渡すことができます WorkMail。タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。Amazon WorkMail リソースのタグ付けの詳細については、「」を参照してください組織へのタグ付け。

Amazon WorkMail 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 での一時的な認証情報の使用 WorkMail

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する、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やGetFederationトークン などの AWS STS API オペレーションを呼び出します。

Amazon WorkMail は、一時的な認証情報の使用をサポートしています。

サービスリンクロール

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

Amazon WorkMail は、サービスにリンクされたロールをサポートしています。Amazon WorkMail のサービスにリンクされたロールの作成または管理の詳細については、「」を参照してくださいAmazon WorkMail のサービスリンクロールの使用。

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、サービスがお客様に代わって他のサービスのリソースにアクセスし、アクションを完了することが許可されます。サービスロールは、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 管理者は、このロールの権限を変更できます。ただし、それにより、サービスの機能が損なわれる場合があります。

Amazon WorkMail はサービスロールをサポートしています。

Amazon WorkMail 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 ユーザーとロールには Amazon WorkMail 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 Management Console AWS CLI、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、ユーザーとロールに必要な、指定されたリソースで特定の API オペレーションを実行する権限をユーザーとロールに付与する IAM ポリシーを作成する必要があります。続いて、管理者はそれらの権限が必要な IAM ユーザーまたはグループにそのポリシーをアタッチする必要があります。

これらの JSON ポリシードキュメント例を使用して IAM の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「JSON タブでのポリシーの作成」を参照してください。

トピック

- ポリシーのベストプラクティス
- Amazon WorkMail コンソールの使用
- ユーザーが自分の許可を表示できるようにする
- Amazon WorkMail 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

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが Amazon WorkMail リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに

料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

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

Amazon WorkMail コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 AWS アカウント内の Amazon WorkMail リソースの詳細を一覧表示および表示できます。最小限必要な許可よりも厳しく制限されたアイデンティティベースポリシーを作成すると、そのポリシーを添付したエンティティ (IAM ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

これらのエンティティが引き続き Amazon WorkMail コンソールを使用できるようにするには、エンティティに次の AWS 管理ポリシーAmazonWorkMailFull「アクセス」もアタッチします。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

AmazonWorkMailFullアクセスポリシーは、IAM ユーザーに Amazon WorkMail リソースへのフルアクセスを付与します。このポリシーにより、ユーザーはすべての Amazon WorkMail、 AWS Key Management Service、Amazon Simple Email Service、および AWS Directory Service オペレーションにアクセスできます。これには、Amazon がユーザーに代わって実行 WorkMail する必要があるいくつかの Amazon EC2 オペレーションも含まれます。E メールイベントのログ記録logs、および Amazon WorkMail コンソールでのメトリクスの表示には、 および アクセスcloudwatch許可が必要です。監査ログ記録では、 CloudWatch ログ、Amazon S3、Amazon Data FireHose を使用して を保存しますlogs。詳細については、「Amazon でのロギングとモニタリング WorkMail」を参照してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "WorkMailAdministration",
      "Effect": "Allow",
      "Action": [
        "ds:AuthorizeApplication",
        "ds:CheckAlias",
        "ds:CreateAlias",
        "ds:CreateDirectory",
        "ds:CreateIdentityPoolDirectory",
        "ds:DeleteDirectory",
        "ds:DescribeDirectories",
        "ds:GetDirectoryLimits",
        "ds:ListAuthorizedApplications",
        "ds:UnauthorizeApplication",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
```

```
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteVpc",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "route53:ChangeResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53:GetHostedZone",
        "route53domains:CheckDomainAvailability",
        "route53domains:ListDomains",
        "ses:*",
        "workmail:*",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:DeleteDeliveryDestination",
        "logs:DeleteDeliveryDestinationPolicy",
        "logs:DescribeDeliveryDestinations",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:PutDeliveryDestination",
        "logs:PutDeliveryDestinationPolicy",
        "logs:CreateDelivery",
        "logs:DeleteDelivery",
        "logs:DescribeDeliveries",
        "logs:GetDelivery",
        "logs:DeleteDeliverySource",
        "logs:DescribeDeliverySources",
        "logs:GetDeliverySource",
        "logs:PutDeliverySource",
```

```
            "logs:DescribeResourcePolicies",
            "cloudwatch:GetMetricData",
            "firehose:DescribeDeliveryStream",
            "firehose:ListDeliveryStreams",
            "s3:ListAllMyBuckets"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AuditLogDeliveryThroughCWLogs",
        "Effect": "Allow",
        "Action": [
            "firehose:TagDeliveryStream",
            "logs:PutResourcePolicy",
            "s3:GetBucketPolicy",
            "s3:PutBucketPolicy"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:CalledViaLast": "logs.amazonaws.com"
            }
        }
    },
    {
        "Sid": "InboundOutboundEmailEventsLink",
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "iam:AWSServiceName": "events.workmail.amazonaws.com"
            }
        }
    },
    {
        "Sid": "AuditLoggingLink",
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "iam:AWSServiceName": "delivery.logs.amazonaws.com"
            }
```

```
        }
    },
    {
        "Sid": "InboundOutboundEmailEventsUnlink",
        "Effect": "Allow",
        "Action": [
            "iam:DeleteServiceLinkedRole",
            "iam:GetServiceLinkedRoleDeletionStatus"
        ],
        "Resource": "arn:aws:iam::*:role/aws-service-role/
events.workmail.amazonaws.com/AWSServiceRoleForAmazonWorkMailEvents*"
    },
    {
        "Sid": "InboundOutboundEmailEventsAuth",
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::*:role/*workmail*",
        "Condition": {
            "StringLike": {
                "iam:PassedToService": "events.workmail.amazonaws.com"
            }
        }
    }
  ]
}
```

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

ユーザーが自分の許可を表示できるようにする

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
```

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

Amazon WorkMail リソースへの読み取り専用アクセスをユーザーに許可する

次のポリシーステートメントは、IAM ユーザーに Amazon WorkMail 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、AWS 管理ポリシー と同じレベルのアクセスを許可しますAmazonWorkMailReadOnlyAccess。どちらのポリシーも、ユーザーにすべての Amazon WorkMail `Describe` オペレーションへのアクセスを許可します。 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 `DescribeDirectories`オペレーションへのアクセスが必要です。設定済みドメインに関する情報を取得するには、Amazon SES サービスへのアクセスが必要です。使用済み暗号化キーに関する情報を取得するには、 へのアクセス AWS Key Management Service が必要です。Amazon WorkMail コンソールで E メールイベントのログ記録とメトリクスの表示を行うには、 `logs`および アクセス`cloudwatch`許可が必要です。監査ログ記録では、 CloudWatch ログ、Amazon S3、Amazon Data FireHose を使用して を保存します`logs`。詳細については、「Amazon でのロギングとモニタリング WorkMail」を参照してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "WorkMailReadOnly",
      "Effect": "Allow",
      "Action": [
        "ses:Describe*",
        "ses:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "lambda:ListFunctions",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:DescribeDeliveryDestinations",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliverySources",
        "logs:GetDelivery",
        "logs:GetDeliverySource",
        "cloudwatch:GetMetricData"
      ],
      "Resource": "*"
    }
  ]
}
```

Amazon WorkMail アイデンティティとアクセスのトラブルシューティング

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

トピック

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

Amazon でアクションを実行する権限がない WorkMail

がアクションを実行する権限がないと AWS Management Console 通知した場合は、管理者に連絡してサポートを依頼する必要があります。担当の管理者はお客様のユーザー名とパスワードを発行した人です。

以下の例のエラーは、mateojackson IAM ユーザーがコンソールを使用して、グループの詳細を表示しようとしているが、workmail:DescribeGroup アクセス許可がない場合に発生します。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workmail:DescribeGroup on resource: group
```

この場合、Mateo は、workmail:DescribeGroup アクションを使用して group リソースへのアクセスが許可されるように、管理者にポリシーの更新を依頼します。

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、ポリシーを更新して Amazon にロールを渡すことができるようにする必要があります WorkMail。

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

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

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

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

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

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

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

詳細については、以下を参照してください:

- Amazon がこれらの機能 WorkMail をサポートしているかどうかを確認するには、「」を参照してくださいAmazon と IAM WorkMail の連携方法。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティー に提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイドの外部認証されたユーザーへのアクセスの提供 (ID フェデレーション) 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 でのクロスアカウントリソースアクセス」を参照してください。

AWS Amazon 管理ポリシー WorkMail

ユーザー、グループ、ロールにアクセス権限を追加するには、 AWS 自分でポリシーを記述するよりも管理ポリシーを使用する方が簡単です。チームに必要な許可のみを提供する IAM カスタマーマネージドポリシーを作成するには、時間と専門知識が必要です。すぐに始めるには、 AWS 管理ポリシーをご利用ください。これらのポリシーは、一般的なユースケースをターゲット範囲に含めており、 AWS アカウントで利用できます。 AWS 管理ポリシーの詳細については、IAM ユーザーガイドの「AWS 管理ポリシー」を参照してください。

AWS AWS サービスは管理ポリシーを維持および更新します。 AWS 管理ポリシーの権限は変更できません。サービスでは、新しい機能を利用できるようにするために、 AWS マネージドポリシーに権限が追加されることがあります。この種類の更新は、ポリシーがアタッチされている、すべてのアイデンティティ (ユーザー、グループおよびロール) に影響を与えます。新しい機能が立ち上げられた

場合や、新しいオペレーションが使用可能になった場合に、各サービスが AWS マネージドポリシーを更新する可能性が最も高くなります。 AWS サービスは管理ポリシーから権限を削除しないため、ポリシーを更新しても既存の権限が損なわれることはありません。

さらに、 AWS 複数のサービスにまたがるジョブ機能の管理ポリシーもサポートされます。たとえば、ReadOnlyAccess AWS AWS 管理ポリシーはすべてのサービスとリソースへの読み取り専用アクセスを提供します。サービスが新しい機能を起動すると、 AWS 新しい操作やリソースに対する読み取り専用権限が追加されます。ジョブ機能のポリシーの一覧および詳細については、「IAM ユーザーガイド」の「AWS のジョブ機能のマネージドポリシー」を参照してください。

AWS 管理ポリシー: AmazonWorkMailFullAccess

`AmazonWorkMailFullAccess` ポリシーは IAM ID にアタッチできます。このポリシーは、Amazon WorkMail へのフルアクセスを許可する権限を付与します。

このポリシーの権限を確認するには、AmazonWorkMailFullAccessのを参照してください AWS Management Console。

AWS 管理ポリシー: AmazonWorkMailReadOnlyAccess

`AmazonWorkMailReadOnlyAccess` ポリシーは IAM ID にアタッチできます。このポリシーは、Amazon WorkMail への読み取り専用アクセスを許可するアクセス権限を付与します。

このポリシーの権限を確認するには、AmazonWorkMailReadOnlyAccess AWS Management Consoleのを参照してください。

AWS 管理ポリシー: AmazonWorkMailEventsServiceRolePolicy

このポリシーは、Amazon AmazonWorkMailEvents AWS WorkMail イベントによって使用または管理されるサービスとリソースへのアクセスを許可するという名前のサービスにリンクされたロールにアタッチされます。詳細については、「Amazon WorkMail のサービスリンクロールの使用」を参照してください。

Amazon WorkMail AWS による管理ポリシーの更新

WorkMail このサービスが変更の追跡を開始して以降の Amazon AWS の管理ポリシーの更新に関する詳細を表示します。

変更	説明	日付
AWS 管理ポリシーの更新 — 既存のポリシーへの更新	Amazon `AmazonWorkMailReadOnlyAccess` `AmazonWorkMailFullAccess` WorkMail が監査ログをサポートするようにおよび権限が更新されました。更新されたアクセス権限の詳細については、「Amazon WorkMail アイデンティティベースのポリシーの例」を、監査ログについては「」を参照してください監査ログを有効にする。	2024 年 2 月 14 日
Amazon WorkMail が変更の追跡を開始しました	Amazon WorkMail AWS は管理ポリシーの変更の追跡を開始しました。	2021 年 3 月 1 日

Amazon WorkMail のサービスリンクロールの使用

Amazon WorkMail は、AWS Identity and Access Management (IAM) サービスリンクロールを使用しています。サービスにリンクされたロールは、Amazon WorkMail に直接リンクされた特殊な IAM ロールです。サービスリンクロールは Amazon WorkMail によって事前に定義されており、サービスがユーザーに代わって AWS のその他サービスを呼び出すために必要なすべての許可が含まれています。

必要な許可を手動で追加する必要がないため、サービスリンクロールは Amazon WorkMail のセットアップを容易にします。サービスリンクロールの許可は Amazon WorkMail が定義し、別段の定義がない限り、Amazon WorkMail のみがそのロールを引き受けることができます。定義された許可には信頼ポリシーと許可ポリシーが含まれ、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスリンクロールは、関連する リソースを削除した後でしか削除できません。これは、リソースにアクセスするための許可を誤って削除できないため、Amazon WorkMail リソースを保護します。

サービスリンクロールをサポートする他のサービスについては、IAM と連携する AWS のサービスでサービスリンクロール列がはいになっているサービスを検索してください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、リンクのある [Yes] (はい) をクリックします。

Amazon WorkMail のサービスリンクロール許可

Amazon WorkMail では、AmazonWorkMailEvents という名前のサービスリンクロールを使用します。Amazon WorkMail は、このサービスリンクロールを使用して、CloudWatch によってログ記録された E メールイベントのモニタリングなど、Amazon WorkMail イベントによって使用または管理される AWS のサービスとリソースにアクセスできます。Amazon WorkMail の E メールのイベントのログ記録の有効化の詳細については、E メールイベントロギングを有効にする を参照してください。

AmazonWorkMailEvents サービスリンクロールは、ロールの引き受けについて以下のサービスを信頼します。

- `events.workmail.amazonaws.com`

ロールのアクセス許可ポリシーは、指定したリソースに対して以下のアクションを実行することを Amazon WorkMail に許可します。

- アクション: `all AWS resources` 上の `logs:CreateLogGroup`
- アクション: `all AWS resources` 上で `logs:CreateLogStream`
- アクション: `logs:PutLogEvents` 上で `all AWS resources`

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。詳細については、IAM ユーザーガイドのサービスにリンクされたロールのアクセス許可を参照してください。

Amazon WorkMail のサービスリンクロールの作成

サービスにリンクされたロールを手動で作成する必要はありません。Amazon WorkMail イベントログを有効にして Amazon WorkMail コンソールでデフォルト設定を使用すると、Amazon WorkMail によってサービスリンクロールが作成されます。

このサービスにリンクされたロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。Amazon WorkMail イベントログを有効にしてデフォルト設定を使用すると、Amazon WorkMail によってサービスリンクロールが作成されます。

Amazon WorkMail のサービスリンクロールの編集

Amazon WorkMail では、AmazonWorkMailEvents サービスリンクロールを編集することはできません。サービスにリンクされたロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、IAM ユーザーガイドのサービスにリンクされたロールの編集を参照してください。

Amazon WorkMail のサービスリンクロールの削除

サービスにリンクされたロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、積極的にモニタリングまたは保守されていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスにリンクされたロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースを削除しようとしているときに Amazon WorkMail サービスがロールを使用している場合は、削除が失敗する可能性があります。失敗した場合は、数分待ってから操作を再試行してください。

AmazonWorkMailEvents によって使用されている Amazon WorkMail リソースを削除するには

1. Amazon WorkMail イベントのログ記録を無効にします。
   a. Amazon WorkMail コンソール (https://console.aws.amazon.com/workmail/) を開きます。

      必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 全般のリファレンス」の「 のリージョンとエンドポイント」を参照してください。
   b. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
   c. ナビゲーションペインで、[組織の設定]、[モニタリング] の順に選択します。
   d. [ログ設定] で、[編集] を選択します。

e. メールイベントを有効化スライダーをオフの位置に移動します。

f. [保存] を選択します。

2. Amazon CloudWatch ロググループを削除します。

a. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。

b. [Logs] (ログ) を選択します。

c. [Log Groups] (ロググループ) で、削除するロググループを選択します。

d. [Actions] (アクション) で、[Delete log group] (ロググループを削除する) を選択します。

e. [Yes, Delete] (はい、削除します) を選択します。

IAM を使用してサービスリンクロールを手動で削除するには

IAM コンソール、AWS CLI、または AWS API を使用して、AmazonWorkMailEvents サービスリンクロールを削除します。詳細については、IAM ユーザーガイドのサービスにリンクされたロールの削除を参照してください。

Amazon WorkMail のサービスリンクロールがサポートされるリージョン

Amazon WorkMail は、このサービスを利用できるすべてのリージョンでサービスリンクロールの使用をサポートします。詳細については、Amazon WorkMail リージョンとエンドポイントを参照してください。

Amazon でのロギングとモニタリング WorkMail

E メールと口グを監視および監査することは、Amazon WorkMail 組織の健全性を維持するために重要です。Amazon は次の 2 WorkMail 種類のモニタリングをサポートしています。

- イベントロギング — 組織の E メール送信アクティビティを監視することで、ドメインの評判を守ることができます。モニタリングは送受信された E メールを追跡するのにも役立ちます。E メールイベントログを有効にする方法の詳細については、E メールイベントロギングを有効にする を参照してください。
- 監査ログ — 監査ログを使用して、メールボックスへのユーザーのアクセスの監視、疑わしいアクティビティの監査、アクセス制御と可用性プロバイダーの構成のデバッグなど、Amazon WorkMail 組織の使用状況に関する詳細情報を取得できます。詳細については、「監査ログを有効にする」を参照してください。

AWS には WorkMail、Amazon を監視したり、問題が発生した場合に報告したり、必要に応じて自動アクションを実行したりするための以下の監視ツールが用意されています。

- Amazon は、 CloudWatch AWS AWS お客様のリソースとお客様が実行するアプリケーションをリアルタイムで監視します。たとえば、Amazon の E メールイベントロギングを有効にすると WorkMail、組織で送受信された E CloudWatch メールを追跡できます。 WorkMail での Amazon のモニタリングの詳細については CloudWatch、を参照してください CloudWatch メトリクスによる Amazon WorkMail のモニタリング。詳細については CloudWatch、Amazon CloudWatch ユーザーガイドを参照してください。
- Amazon CloudWatch Logs を使用すると、Amazon WorkMail コンソールで E WorkMail メールと監査ログが有効になっている場合に、Amazon の E メールイベントと監査ログを監視、保存、アクセスできます。 CloudWatch ログはログファイル内の情報を監視でき、ログデータを耐久性の高いストレージにアーカイブできます。 CloudWatch Logs を使用して Amazon WorkMail メッセージを追跡する方法の詳細については、「」E メールイベントロギングを有効にする と「」を参照してください監査ログを有効にする。 CloudWatch ログの詳細については、Amazon CloudWatch Logs ユーザーガイドを参照してください。
- AWS CloudTrailは、お客様によって、またはお客様に代わって行われた API 呼び出しと関連イベントをキャプチャし AWS アカウント、指定した Amazon S3 バケットにログファイルを配信します。どのユーザーとアカウント AWS、呼び出しが行われたソース IP アドレス、呼び出しがいつ発生したかを特定できます。詳細については、「 WorkMail での Amazon API 呼び出しのロギング AWS CloudTrail」を参照してください。
- Amazon S3 では、費用対効果の高い方法で Amazon WorkMail イベントを保存し、アクセスできます。Amazon S3 にはイベントデータのライフサイクルを管理するメカニズムが用意されており、古いイベントの自動削除を設定したり、Amazon S3 Glacier への自動アーカイブを設定したりできます。Amazon S3 の配信は、監査ロギングイベントでのみ使用できることに注意してください。Amazon S3 の詳細については、「Amazon S3 ユーザーガイド」を参照してください。
- Amazon Data Firehose を使用すると、Amazon Simple Storage Service (Amazon S3)、Amazon Redshift、Amazon Service、Amazon OpenSearch Service、Amazon OpenSearch Serverless、Splunk などの他の AWS サービスや、Datadog、Dynatrace、MongoDB、New Relic、Coralogix、Elastic など、サポートされているサードパーティのサービスプロバイダーが所有するカスタム HTTP エンドポイントまたは HTTP エンドポイントにイベントデータをストリーミングできます。 LogicMonitorFirehose への配信は、監査ログイベントでのみ使用できます。Firehose の詳細については、Amazon Data Firehose 開発者ガイドを参照してください。

トピック

- CloudWatch メトリクスによる Amazon WorkMail のモニタリング
- Amazon WorkMail E メールイベントログのモニタリング
- Amazon WorkMail 監査ログのモニタリング
- Amazon CloudWatch でインサイトを利用する WorkMail
- WorkMail での Amazon API 呼び出しのロギング AWS CloudTrail
- E メールイベントロギングを有効にする
- 監査ログを有効にする

CloudWatch メトリクスによる Amazon WorkMail のモニタリング

WorkMail を使用してAmazonを監視できます。これにより CloudWatch、未加工のデータが収集され、読み取り可能でほぼリアルタイムのメトリックスに変換されます。無料のメトリックスは 15 か月間保存されるため、履歴情報にアクセスしてウェブアプリケーションやサービスのパフォーマンスを確認できます。また、特定のしきい値をモニタリングするアラームを設定し、しきい値に達したときに通知を送信したりアクションを実行したりできます。詳細については、Amazon CloudWatch ユーザーガイドを参照してください。

CloudWatch Amazon ンの指標 WorkMail

Amazon は、 WorkMail CloudWatch以下のメトリックスとディメンション情報をに送信します。

`AWS/WorkMail` 名前空間には、次のメトリクスが含まれます。

メトリクス	説明
`OrganizationEmailReceived`	Amazon WorkMail 組織が受信した E メールの数。1 通の E メールが組織内の 10 人の受信者に宛てられた場合、`OrganizationEmailReceived` その数は 1 件です。 単位: カウント
`MailboxEmailDelivered`	Amazon WorkMail 組織内の個々のメールボックスに配信された E メールの数。1 通の E メールが組織内の 10 人の受信者に正常に配信された場合、`MailboxEmailDelivered` その数は 10 になります。

メトリクス	説明
	単位: カウント
IncomingEmailBounced	フルメールボックスが原因で返送された受信メールの数。このメトリクスは、意図された受信者ごとにカウントされます。たとえば、組織内の 10 人の受信者に 1 通のメールが送信され、そのうちの 2 人の受信者のメールボックスがいっぱいになり、バウンス応答があった場合、その数は 2 件になります。IncomingEmailBounced 単位: カウント
OutgoingEmailBounced	配信できなかった送信メールの数。このメトリクスは、意図された受信者ごとにカウントされます。たとえば、1 通のメールが 10 人の受信者に送信され、2 通のメールが配信されなかった場合、OutgoingEmailBounced　件数は 2 件になります。 単位: カウント
OutgoingEmailSent	Amazon WorkMail 組織から正常に送信された E メールの数。このメトリクスは、正常に送信された E メールの受信者ごとにカウントされます。たとえば、1 通の E メールが10人の受信者に送信され、その E メールが8人の受信者に正常に配信された場合、OutgoingEmailSent　の数は8です。 単位: カウント

メトリクス	説明
AuthenticationFailure	このメトリックスは認証試行回数をカウントします。認証が成功すると 0 回になり、認証に失敗したときの数は 1 になります。Sumこの統計情報を使用して、認証に失敗した回数を監視します。Sample countこの統計を使用して認証イベントの総数を監視します。Averageこの統計を使用して、認証イベントの失敗と成功の比率を監視します。 単位: カウント
AccessDenied	このメトリックは、アクセス制御評価の数をカウントします。アクセス制御によってアクションが拒否された場合の数は 1 で、アクションが許可された場合の数は 0 です。Sum統計を使用して拒否されたアクションの量を監視し、Sample count統計を使用して試行されたアクションの総数を監視し、Average統計を使用して許可されたアクションと拒否されたアクションの比率を監視します。 単位: カウント
ActionDenied	この指標は、メールボックスデータに対してアクションがあった場合にカウントされます。アクションが拒否された場合の数は 1 で、アクションが許可された場合の数は 0 です。Sum統計を使用して拒否されたメールボックスアクションの量を監視し、Sample count試行されたメールボックスアクションの総数を監視するには統計を使用し、Average許可されたアクションと拒否されたアクションの比率を監視するには統計を使用してください。 単位: カウント

メトリクス	説明
AvailabilityProviderFailure	このメトリックスは、Amazon WorkMail が外部ソースからカレンダーの空き状況を取得するために実行する可用性プロバイダーのリクエストごとにカウントされます。アベイラビリティプロバイダの詳細については、『Amazon WorkMail 管理者ガイド』を参照してください。

Amazon WorkMail E メールイベントログのモニタリング

Amazon WorkMail 組織の E メールイベントロギングを有効にすると、Amazon WorkMail CloudWatch はを使用してメールイベントを記録します。E メールのイベントログ記録をオンにすることの詳細については、E メールイベントロギングを有効にする を参照してください。

次の表は、Amazon WorkMail が ログに記録するイベント CloudWatch、イベントが送信されるタイミング、およびイベントフィールドの内容を示しています。

ORGANIZATION_EMAIL_RECEIVED

このイベントは、Amazon WorkMail 組織がメールメッセージを受信すると記録されます。

フィールド	説明
受信者	メッセージの意図された受信者です。
送信者	別のユーザーの代理で E メールメッセージを送信したユーザーの E メールアドレス。このフィールドは、E メールが別のユーザーの代理で送信されたときにのみ設定されます。
送信元	[From] (送信元) アドレス。通常、メッセージを送信したユーザーの E メールアドレスです。ユーザーがメッセージを別のユーザーとして送信したか別のユーザーの代理で送信した場合、この フィールドは、実際の送信者の E メールアドレスではなく、E メールの名目上の送信者

フィールド	説明
	であるユーザーの E メールアドレスを返します。
subject	E メールメッセージの件名です。
messageId	SMTP メッセージ IDです。
spamVerdict	メッセージが Amazon SES によってスパムとしてマークされているかどうかを示します。詳細については、Amazon Simple Email Service デベロッパーガイドの Amazon SES E メール受信の通知の内容を参照してください。
dkimVerdict	DomainKeys 識別メール (DKIM) チェックに合格したかどうかを示します。詳細については、Amazon Simple Email Service デベロッパーガイドの Amazon SES E メール受信の通知の内容を参照してください。
dmarcVerdict	ドメインベースのメッセージ認証、報告、および適合 (DMARC) チェックに合格したかどうかを示します。詳細については、Amazon Simple Email Service デベロッパーガイドの Amazon SES E メール受信の通知の内容を参照してください。
dmarcPolicy	dmarcVerdict フィールドに「FAIL」が含まれている場合にのみ表示されます。DMARC チェックが失敗した場合に、E メールに対して実行するアクションを示します (NONE、QUARANTINE、または REJECT)。これは、送信側の E メールドメインの所有者によって設定されます。

フィールド	説明
spfVerdict	送信者ポリシーフレームワーク (SPF) チェックに合格したかどうかを示します。詳細については、Amazon Simple Email Service デベロッパーガイドの Amazon SES E メール受信の通知の内容を参照してください。
messageTimestamp	メッセージがいつ受信されたかを示します。

MAILBOX_EMAIL_DELIVERED

このイベントは、組織内のメールボックスにメッセージが配信されたときに記録されます。これは、メッセージが配信されるメールボックスごとに 1 回記録されるため、単一の ORGANIZATION_EMAIL_RECEIVED イベントによって複数の MAILBOX_EMAIL_DELIVERED イベントが発生する可能性があります。

フィールド	説明
受取人	メッセージが配信されるメールボックスです。
フォルダ	メッセージが配置されているメールボックスフォルダです。

RULE_APPLIED

このイベントは、受信メッセージまたは送信メッセージがメールフロールールを開始すると記録されます。

フィールド	説明
ruleName	ルールの名前。
ruleType	適用されるルールのタイプ (インバウンドルール、アウトバウンドルール、またはメールボックスルール)。インバウンドルールとアウトバウンドルールは Amazon WorkMail 組織に適用

フィールド	説明
	されます。メールボックスルールは、指定されたメールボックスにのみ適用されます。詳細については、「E メールフローの管理」を参照してください。
ruleActions	ルールに基づいて取られたアクションです。メッセージの受信者が異なれば、返送された E メールや正常に配信された E メールなど、さまざまなアクションが発生する可能性があります。
targetFolder	Move または Copy MAILBOX_RULE の対象となる保存先フォルダ。
targetRecipient	Forward または Redirect MAILBOX_RULE の対象となる受取人。

JOURNALING_INITIATED

このイベントは、Amazon が組織管理者が指定したジャーナリングアドレスに E WorkMail メールを送信したときに記録されます。組織に対してジャーナリングが設定されている場合にのみ送信されます。詳細については、「Amazon WorkMail での E メールジャーナリングの使用」を参照してください。

フィールド	説明
journalingAddress	ジャーナリングメッセージの送信先の E メールアドレスです。

INCOMING_EMAIL_BOUNCED

このイベントは、受信メッセージをターゲット受信者に配信できないときに記録されます。E メールは、完全なターゲットメールボックスなど、さまざまな理由でバウンスする可能性があります。システムは、バウンスメールになった受信者ごとに 1 回記録します。たとえば、受信メッ

セージが 3 人の受信者宛てで、そのうちの 2 人がフルメールボックスを持っている場合、2 つの INCOMING_EMAIL_BOUNCED イベントが記録されます。

フィールド	説明
bouncedRecipient	Amazon WorkMail がメッセージをバウンスした対象受信者。

OUTGOING_EMAIL_SUBMITTED

このイベントは、組織内のユーザーが送信用の E メールメッセージを送信したときに記録されます。これはメッセージがAmazonから送信される前に記録されるため WorkMail、このイベントではメールが正常に配信されたかどうかはわかりません。

フィールド	説明
受信者	送信者によって指定されたメッセージの受信者です。宛先、CC、および BCC 行のすべての受信者を含みます。
送信者	別のユーザーの代理で E メールメッセージを送信したユーザーの E メールアドレス。このフィールドは、E メールが別のユーザーの代理で送信されたときにのみ設定されます。
送信元	[From] (送信元) アドレス。通常、メッセージを送信したユーザーの E メールアドレスです。ユーザーがメッセージを別のユーザーとして送信したか別のユーザーの代理で送信した場合、この フィールドは、実際の送信者の E メールアドレスではなく、E メールの名目上の送信者であるユーザーの E メールアドレスを返します。
subject	E メールメッセージの件名です。

OUTGOING_EMAIL_SENT

このイベントは、送信 E メールがターゲット受信者に正常に配信されたときに記録されます。これは成功した受信者ごとに1回記録されるため、単一の OUTGOING_EMAIL_SUBMITTED で複数の OUTGOING_EMAIL_SENT エントリが発生する可能性があります。

フィールド	説明
受取人	E メールが正常に配信された受信者です。
送信者	別のユーザーの代理で E メールメッセージを送信したユーザーの E メールアドレス。このフィールドは、E メールが別のユーザーの代理で送信されたときにのみ設定されます。
送信元	[From] (送信元) アドレス。通常、メッセージを送信したユーザーの E メールアドレスです。ユーザーがメッセージを別のユーザーとして送信したか別のユーザーの代理で送信した場合、この フィールドは、実際の送信者の E メールアドレスではなく、E メールの名目上の送信者であるユーザーの E メールアドレスを返します。
messageId	SMTP メッセージ IDです。

OUTGOING_EMAIL_BOUNCED

このイベントは、発信メッセージをターゲット受信者に配信できないときに記録されます。E メールは、完全なターゲットメールボックスなど、さまざまな理由でバウンスする可能性があります。システムは、バウンスメールになる受信者ごとにバウンスを記録します。たとえば、送信メッセージが 3 人の受信者に宛てられ、そのうちの 2 人がフルメールボックスを持っている場合、2 つの OUTGOING_EMAIL_BOUNCED イベントが記録されます。

フィールド	説明
bouncedRecipient	送信先メールサーバーがメッセージを送信した受信者です。

DMARC_POLICY_APPLIED

このイベントは、組織に送信された E メールに DMARC ポリシーが適用されたときに記録されます。

フィールド	説明
送信元	[From] (送信元) アドレス。通常、メッセージを送信したユーザーの E メールアドレスです。ユーザーがメッセージを別のユーザーとして送信したか別のユーザーの代理で送信した場合、この フィールドは、実際の送信者の E メールアドレスではなく、E メールの名目上の送信者であるユーザーの E メールアドレスを返します。
受信者	メッセージの意図された受信者です。
ポリシー	適用された DMARC ポリシー。DMARC チェックが失敗したときに E メールで実行するアクション (NONE、QUARANTINE、または REJECT) を示します。これは、ORGANIZATION_EMAIL_RECEIVED イベントの dmarcPolicy フィールドと同じです。

Amazon WorkMail 監査ログのモニタリング

監査ログを使用して、Amazon WorkMail 組織のメールボックスへのアクセスを監視できます。Amazon は 4 WorkMail 種類の監査イベントをログに記録し、 CloudWatch これらのイベントはログ、Amazon S3、または Amazon Firehouse に公開できます。監査ログを使用して、組織のメールボックスに対するユーザー操作、認証試行、アクセスコントロールルールの評価を監視し、外部システムへの可用性プロバイダー呼び出しを実行できます。監査ログの設定については、を参照してください監査ログを有効にする。

以下のセクションでは WorkMail、Amazon が記録する監査イベント、イベントが送信されるタイミング、およびイベントフィールドに関する情報について説明します。

メールボックスのアクセスログ

メールボックスアクセスイベントは、どのメールボックスオブジェクトに対して実行された (または試行された) かに関する情報を提供します。メールボックス内のアイテムまたはフォルダーに対して操作を実行しようとするたびに、メールボックスアクセスイベントが生成されます。これらのイベントは、メールボックスデータへのアクセスを監査するのに役立ちます。

フィールド	説明
event_timestamp	イベントが発生した日時 (UNIX エポックからのミリ秒単位)。
request_id	リクエストを一意に識別する ID。
「組織」_arn	認証されたユーザーが属する & Amazon WorkMail 組織の ARN。
user_id	認証されたユーザーの ID。
インパーソネーター ID	インパーソネーターの ID。リクエストに偽装機能が使用された場合にのみ表示されます。
protocol	使用したプロトコル。プロトコルにはAutoDiscover 、、、、EWSIMAP、WindowsOutlook 、ActiveSync 、SMTP、WebMailIncomingEmail 、またはを使用できますOutgoingEmail 。
ソース_IP	リクエストのソース IP アドレス。
user_agent	リクエストを行ったユーザーエージェント。
アクション	オブジェクトに対して実行されたアクション。、、、read、、、read_hierarchy 、read_summary 、read_attachment 、read_permissions 、create、update、update_permissions 、update_re

フィールド	説明
	ad_state 、delete、submit_email_for_sending 、abort_sending_email 、movemove_tocopy、copy_toまたはのいずれかです。
owner_id	アクションの対象となるオブジェクトを所有するユーザーの ID。
object_type	オブジェクトタイプ。フォルダー、メッセージ、添付のいずれかです。
item_id	イベントの件名であるメッセージ、またはイベントの件名である添付ファイルを含むメッセージを一意に識別する ID。
folder_path	処理対象のフォルダーのパス、または処理対象のアイテムを含むフォルダーのパス。
folder_id	イベントの対象となるフォルダー、またはイベントの対象となるオブジェクトを含むフォルダーを一意に識別する ID。
添付ファイル:パス	影響を受ける添付ファイルへの表示名のパス。
アクション許可済み	アクションが許可されたかどうか。true でも false でもかまいません。

アクセス制御ログ

アクセス制御イベントは、アクセス制御ルールが評価されるたびに生成されます。これらのログは、禁止されているアクセスを監査したり、アクセス制御設定をデバッグしたりするのに役立ちます。

フィールド	説明
event_timestamp	イベントが発生した日時 (Unix エポックからのミリ秒単位)。
request_id	リクエストを一意に識別する ID。
「組織」_arn	WorkMail 認証されたユーザーが属する組織の ARN。
user_id	認証されたユーザーの ID。
インパーソネーター ID	インパーソネーターの ID。リクエストに偽装機能が使用された場合にのみ表示されます。
protocol	使用したプロトコル。、、、AutoDiscover 、、、EWS、IMAPWindowsOutlook ActiveSync SMTPWebMailIncomingEmail 、またはのいずれでもかまいません。OutgoingEmail
source_ip	リクエストのソース IP アドレス。
scope	ルールの適用範囲。、AccessControl DeviceAccessControl 、またはのいずれでもかまいませんImpersonationAccessControl 。
ルールID	一致したアクセスコントロールルールの ID。一致するルールがない場合、rule_id は使用できません。
アクセス権限付与	アクセスが許可されたかどうか。true でも false でもかまいません。

認証ログ

認証イベントには、認証試行に関する情報が含まれます。

> **Note**
>
> Amazon WorkMail WebMail アプリケーションによる認証イベントでは、認証イベントは生成されません。

フィールド	説明
event_timestamp	イベントが発生した日時 (Unix エポックからのミリ秒単位)。
request_id	リクエストを一意に識別する ID。
「組織」_arn	WorkMail 認証されたユーザーが属する組織の ARN。
user_id	認証されたユーザーの ID。
ユーザー	認証を試みたユーザー名。
protocol	使用したプロトコル。、、AutoDiscover 、、、EWS、IMAP、WindowsOutlook ActiveSync SMTPWebMailIncomingEmail 、またはのいずれでもかまいませんOutgoingEmail 。
source_ip	リクエストのソース IP アドレス。
user_agent	リクエストを行ったユーザーエージェント。
method	認証メソッド。現在、basic のみがサポートされています。
認証成功	認証が成功したかどうか。真でも偽でもかまいません。
認証に失敗した理由	認証が失敗した理由。認証に失敗した場合にのみ表示されます。

アベイラビリティプロバイダーのログ

可用性プロバイダーイベントは、Amazon がお客様に代わって、 WorkMail設定した可用性プロバイダーに対して行う可用性リクエストごとに生成されます。これらのイベントは、アベイラビリティープロバイダーの設定をデバッグするのに役立ちます。

フィールド	説明
event_timestamp	イベントが発生した日時 (Unix エポックからのミリ秒単位)。
request_id	リクエストを一意に識別する ID。
「組織」_arn	WorkMail 認証されたユーザーが属する組織の ARN。
user_id	認証されたユーザーの ID。
type	呼び出される可用性プロバイダーのタイプ。使用できるのは:または。EWS LAMBDA
ドメイン	アベイラビリティを取得するドメイン。
関数_arn	タイプが LAMBDA の場合、呼び出された Lambda の ARN。それ以外の場合、このフィールドは存在しません。
ews_endpoint	EWS エンドポイントのタイプは EWS です。それ以外の場合、このフィールドは表示されません。
error_message	障害の原因を説明するメッセージ。リクエストが成功した場合、このフィールドは表示されません。
アベイラビリティーイベント_成功	空き状況リクエストが正常に処理されたかどうか。

Amazon CloudWatch でインサイトを利用する WorkMail

Amazon WorkMail コンソールで E メールイベントロギングをオンにするか、Logs CloudWatch への監査ログ配信を有効にした場合は、Amazon CloudWatch Logs Insights を使用してイベントログをクエリできます。E メールのイベントログ記録をオンにすることの詳細については、E メールイベントロギングを有効にする を参照してください。 CloudWatch ログインサイトの詳細については、Amazon Logs ユーザーガイドの「 CloudWatch CloudWatch ログインサイトによるログデータの分析」を参照してください。

以下の例は、一般的な E CloudWatch メールイベントについてログをクエリする方法を示しています。 CloudWatch これらのクエリはコンソールで実行します。これらのクエリの実行方法については、Amazon CloudWatch Logs ユーザーガイドの「チュートリアル:サンプルクエリの実行と変更」を参照してください。

Example ユーザー B がユーザー A から送信された E メールを受信しなかった理由をご覧ください。

次のコード例は、タイムスタンプ順にソートされた、ユーザー A からユーザー B に送信された送信メールを照会する方法を示しています。

```
fields @timestamp, traceId

| sort @timestamp asc
| filter (event.from like /(?i)userA@example.com/
and event.eventName = "OUTGOING_EMAIL_SUBMITTED"
and event.recipients.0 like /(?i)userB@example.com/)
```

これは送信されたメッセージとトレース ID を返します。次のコード例のトレース ID を使用して、送信メッセージのイベントログを照会します。

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter traceId = "$TRACEID"
```

これにより、E メールメッセージ ID と E メールイベントが返されます。OUTGOING_EMAIL_SENT は E メールが送信されたことを示します。OUTGOING_EMAIL_BOUNCED は、Eメールがバウンスしたことを示します。E メールが受信されたかどうかを確認するには、次のコード例のメッセージ ID を使用して照会します。

```
fields @timestamp, event.eventName
```

```
| sort @timestamp asc
| filter event.messageId like "$MESSAGEID"
```

メッセージ ID は同じなので、受信したメッセージも返されるはずです。次のコード例のトレース ID を使用して、配信を照会します。

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter traceId = "$TRACEID"
```

これにより、配信アクションと適用可能なすべてのルールアクションが返されます。

Example ユーザーまたはドメインから受信したメールをすべて表示する

次のコード例では、指定されたユーザーから受信したすべてのメールを照会する方法を示しています。

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter (event.from like /(?i)user@example.com/ and event.eventName =
 "ORGANIZATION_EMAIL_RECEIVED")
```

次のコード例は、指定したドメインから受信したすべてのメールを照会する方法を示しています。

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter (event.from like "example.com" and event.eventName =
 "ORGANIZATION_EMAIL_RECEIVED")
```

Example バウンスメールの送信者を確認する

次のコード例では、バウンスした送信メールを照会する方法を示し、バウンスの理由も返します。

```
fields @timestamp, event.destination, event.reason
| sort @timestamp desc
| filter event.eventName = "OUTGOING_EMAIL_BOUNCED"
```

次のコード例は、バウンスした受信メールをクエリする方法を示しています。また、バウンスされた受信者のメールアドレスとバウンスの理由も返されます。

```
fields @timestamp, event.bouncedRecipient.emailAddress, event.bouncedRecipient.reason,
 event.bouncedRecipient.status
| sort @timestamp desc
| filter event.eventName = "INCOMING_EMAIL_BOUNCED"
```

Example どのドメインがスパムを送信しているかを確認します。

次のコード例では、スパムを受信している組織内の受信者を照会する方法を示しています。

```
stats count(*) as c by event.recipients.0
| filter (event.eventName = "ORGANIZATION_EMAIL_RECEIVED" and event.spamVerdict =
 "FAIL")
| sort c desc
```

次のコード例では、スパムメールの送信者を照会する方法を示しています。

```
fields @timestamp, event.recipients.0, event.sender, event.from
| sort @timestamp asc
| filter (event.spamVerdict = "FAIL")
```

Example メールが受信者の迷惑メールフォルダに送信された理由を確認する

次のコード例では、件名でフィルタリングされた、スパムとして識別された E メールを照会する方法を示しています。

```
fields @timestamp, event.recipients.0, event.spamVerdict, event.spfVerdict,
 event.dkimVerdict, event.dmarcVerdict
| sort @timestamp asc
| filter event.subject like /(?i)$SUBJECT/ and event.eventName =
 "ORGANIZATION_EMAIL_RECEIVED"
```

E メールトレース ID で照会して、E メールのすべてのイベントを確認することもできます。

Example メールフロールールに一致するメールを表示する

次のコード例では、アウトバウンド Eメールフロールールに一致した E メールを照会する方法を示しています。

```
fields @timestamp, event.ruleName, event.ruleActions.0.action
| sort @timestamp desc
| filter event.ruleType = "OUTBOUND_RULE"
```

次のコード例では、受信 E メールフロールールに一致した E メールを照会する方法を示しています。

```
fields @timestamp, event.ruleName, event.ruleActions.0.action,
 event.ruleActions.0.recipients.0
| sort @timestamp desc
| filter event.ruleType = "INBOUND_RULE"
```

Example 組織が送受信したメールの数を確認する

次のコード例では、組織内の各受信者が受信した E メールの数を照会する方法を示しています。

```
stats count(*) as c by event.recipient
| filter event.eventName = "MAILBOX_EMAIL_DELIVERED"
| sort c desc
```

次のコード例は、組織内の各送信者によって送信された E メールの数を照会する方法を示しています。

```
stats count(*) as c by event.from
| filter event.eventName = "OUTGOING_EMAIL_SUBMITTED"
| sort c desc
```

WorkMail での Amazon API 呼び出しのロギング AWS CloudTrail

Amazon WorkMail は AWS CloudTrail、Amazon AWS のサービス 内のユーザー、ロール、 WorkMail またはによって実行されたアクションの記録を提供するサービスと統合されています。 CloudTrail Amazon WorkMail 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む、Amazon のすべての WorkMail API WorkMail 呼び出しをイベントとしてキャプチャします。証跡を作成すると、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 WorkMail。証跡を設定しなくても、 CloudTrail コンソールの [イベント履歴] に最新のイベントが表示されます。によって収集された情報を使用して CloudTrail、Amazonに対して行われたリクエスト WorkMail、リクエストが行われたIPアドレス、リクエストの実行者、リクエストの実行日時、その他の詳細を判断できます。

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

のAmazon WorkMail 情報 CloudTrail

CloudTrail AWS アカウント アカウントを作成すると、で有効になります。Amazon でアクティビティが発生すると WorkMail、 CloudTrail AWS のサービス そのアクティビティはイベント履歴の他のイベントとともにイベントに記録されます。で最近のイベントを表示、検索、ダウンロードできます AWS アカウント。詳細については、「 CloudTrail イベント履歴によるイベントの表示」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 WorkMail、証跡を作成する必要があります。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、コンソールで証跡を作成するときに、証跡がすべての AWS 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、 AWS CloudTrail ログに収集されたイベントデータをさらに分析して処理するように他のサービスを設定することもできます。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 サポート対象のサービスとインテグレーション
- の Amazon SNS 通知の設定 CloudTrail
- CloudTrail 複数のリージョンからのログファイルの受信、 CloudTrail および複数のアカウントからのログファイルの受信

Amazon WorkMail CloudTrail のすべてのアクションは記録され、Amazon WorkMail API リファレンスに記載されています。たとえば、、および `GetRawMessageContent` API オペレーションを呼び出すと`CreateUserCreateAlias`、 CloudTrailログファイルにエントリが生成されます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。同一性情報は次の判断に役立ちます。

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

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

Amazon WorkMail ログファイルエントリについて

トレイルは、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 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、特定の順序で表示されることはありません。

次の例は、Amazon WorkMail API CloudTrail `CreateUser` からのアクションを示すログエントリを示しています。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T17:49:59Z",
  "eventSource": "workmail.amazonaws.com",
  "eventName": "CreateUser",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-
Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "name": "janedoe",
    "displayName": "Jane Doe",
    "organizationId": "m-5b1c980000EXAMPLE"
  },
  "responseElements": {
    "userId": "a3a9176d-EXAMPLE"
  },
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```

次の例は、Amazon WorkMail API CloudTrail `CreateAlias` からのアクションを示すログエントリを示しています。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T18:13:44Z",
  "eventSource": "workmail.amazonaws.com",
  "eventName": "CreateAlias",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-
Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "alias": "aliasjamesdoe@testofconsole.awsapps.com",
    "organizationId": "m-5b1c980000EXAMPLE"
    "entityId": "a3a9176d-EXAMPLE"
  },
  "responseElements": null,
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```

次の例は、Amazon WorkMail メッセージフロー API CloudTrail `GetRawMessageContent` からのアクションを示すログエントリを示しています。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T18:13:44Z",
  "eventSource": "workmailMessageFlow.amazonaws.com",
  "eventName": "GetRawMessageContent",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-
Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "messageId": "123A4A5A-67B8-90C1-D23E-45FG67H890J1"
  },
  "responseElements": null,
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```

E メールイベントロギングを有効にする

組織の E メールメッセージを追跡するには、Amazon WorkMail コンソールで E メールイベントロギングを有効にします。E メールイベントロギングでは、 AWS Identity and Access Management サービスにリンクされたロール (SLR) を使用して、E メールイベントログを Amazon に公開する権限を付与します。 CloudWatchIAM サービスにリンクされたロールの詳細については、Amazon WorkMail のサービスリンクロールの使用 を参照してください。

CloudWatch イベントログでは、 CloudWatch 検索ツールとメトリックスを使用してメッセージを追跡し、E メールの問題のトラブルシューティングを行うことができます。Amazon WorkMail が送信するイベントログの詳細については CloudWatch、を参照してくださいAmazon WorkMail E メールイベントログのモニタリング。 CloudWatch ログの詳細については、Amazon CloudWatch Logs ユーザーガイドを参照してください。

トピック

- E メールイベントログ記録をオンにする
- E メールイベントログ記録用のカスタムのロググループと IAM ロールの作成
- E メールイベントログ記録をオフにする
- サービス間での不分別な代理処理の防止

E メールイベントログ記録をオンにする

デフォルト設定の Amazon を使用してメールイベントロギングをオンにすると、次のことが起こります WorkMail。

- AWS Identity and Access Management サービスにリンクされたロールを作成します —。`AmazonWorkMailEvents`
- CloudWatch ロググループを作成します —。`/aws/workmail/emailevents/`*`organization-alias`*
- CloudWatch ログの保存期間を 30 日間に設定します。

E メールイベントのログ記録をオンにするには

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

   必要に応じて、 AWS リージョンを変更してください。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで [ログ設定] を選択します。
4. [メールフローログ設定] タブを選択します。
5. [メールフローログ設定] セクションで [編集] を選択します。
6. [メールイベントを有効にする] スライダーを [オン] の位置に移動します。
7. 次のいずれかを行います。
   - (推奨)「デフォルト設定を使う」を選択します。
   - (オプション) [デフォルト設定を使用する] のチェックボックスをオフにし、[送信先ロググループ] と [IAM ロール] を選択します。

   > **Note**
   >
   > AWS CLIを使用してロググループと カスタム IAMロールをすでに作成している場合にのみ、このオプションを選択してください。詳細については、「E メールイベントログ記録用のカスタムのロググループと IAM ロールの作成」を参照してください。

8. [WorkMail この設定を使用してアカウントにログを公開することをAmazonに許可します] を選択します。
9. [保存] を選択します。

E メールイベントログ記録用のカスタムのロググループと IAM ロールの作成

Amazon の E メールイベントロギングを有効にする場合は、デフォルト設定を使用することをお勧めします WorkMail。カスタムモニタリング設定が必要な場合は、を使用して E メールイベントロギング専用のロググループとカスタム IAM ロールを作成できます。 AWS CLI

E メールイベントログ記録用のカスタムのロググループと IAM ロールを作成するには

1. AWS CLI 次のコマンドを使用して、Amazon AWS WorkMail 組織と同じリージョンにロググループを作成します。詳細については、『AWS CLI コマンドリファレンス』create-log-groupのを参照してください。

```
aws --region us-east-1 logs create-log-group --log-group-name workmail-monitoring
```

2. 以下のポリシーを含むファイルを作成します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "events.workmail.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

3. AWS CLI 次のコマンドを使用して IAM ロールを作成し、このファイルをロールポリシードキュメントとして添付します。詳細については、「AWS CLI コマンドリファレンス」の create-role を参照してください。

```
aws iam create-role --role-name workmail-monitoring-role --assume-role-policy-
document file://trustpolicyforworkmail.json
```

> **Note**
>
> WorkMailFullAccess管理ポリシーユーザーの場合は、workmailロール名にこの用語を含める必要があります。この管理ポリシーでは、名前に workmail を含むロールを使用して E メールイベントログ記録を設定することのみが許可されます。詳細については、『IAM ユーザーガイド』の「 AWS サービスにロールを渡すためのアクセス権限をユーザーに付与する」を参照してください。

4. 前のステップで作成した IAM ロールのポリシーを含むファイルを作成します。最低でも、このポリシーではそのロールに、ログストリームを作成するためのアクセス許可と、ステップ 1 で作成したロググループにログイベントを追加するためのアクセス許可を付与する必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:us-east-1:111122223333:log-group:workmail-
monitoring*"
        }
    ]
}
```

5. AWS CLI 以下のコマンドを使用して、ポリシーファイルを IAM ロールにアタッチします。詳細については、『AWS CLI コマンドリファレンス』put-role-policyのを参照してください。

```
aws iam put-role-policy --role-name workmail-monitoring-role --policy-
name workmail-permissions --policy-document file://rolepolicy.json
```

E メールイベントログ記録をオフにする

Amazon WorkMail コンソールから E メールイベントのログ記録をオフにします。E メールイベントロギングを使用する必要がなくなった場合は、 CloudWatch 関連するロググループとサービスにリン

クされたロールも削除することをお勧めします。詳細については、「Amazon WorkMail のサービスリンクロールの削除」を参照してください。

E メールイベントのログ記録を無効にするには

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

   必要に応じて、 AWS リージョンを変更してください。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで、[モニタリング] を選択します。
4. [設定] セクションで、[編集] を選択します。
5. [メールイベントを有効にする] スライダーをオフの位置に移動します。
6. [保存] を選択します。

サービス間での不分別な代理処理の防止

混乱した代理問題は、アクションを実行するためのアクセス許可を持たないエンティティが、より特権のあるエンティティにアクションの実行を強制できてしまう場合に生じる、セキュリティ上の問題です。では AWS、サービス間のなりすましによって、混乱した代理人問題が発生する可能性があります。サービス間でのなりすましは、あるサービス (呼び出し元サービス) が、別のサービス (呼び出し対象サービス) を呼び出すときに発生する可能性があります。

呼び出し元サービスを操作して、その権限を利用して、他の方法ではアクセス権限がないはずだった他の顧客のリソースを操作する可能性があります。

これを防ぐために、 AWS は、アカウント内のリソースへのアクセスを許可されているサービスプリンシパルを使用するすべてのサービスのデータを保護するのに役立つツールを提供しています。

aws:SourceArnaws:SourceAccountリソースポリシーでおよびグローバル条件コンテキストキーを使用して、 CloudWatch Logs と Amazon S3 がログを生成しているサービスに付与するアクセス権限を制限することをお勧めします。グローバル条件コンテキストキーを両方使用する場合、同じポリシーステートメントで値を使用する場合は同じアカウント ID を使用する必要があります。

aws:SourceArn の値は、ログを生成している配信リソースの ARN でなければなりません。

混乱した代理問題から保護するための最も効果的な方法は、リソースの完全な ARN を指定して aws:SourceArn グローバル条件コンテキストキーを使用することです。リソースの ARN 全

体が不明または複数のリソースを指定する場合、ARN の未知部分にワイルドカード *が付いた aws:SourceArn グローバルコンテキスト条件キー を使用します。

監査ログを有効にする

監査ログを使用して、Amazon WorkMail 組織の使用状況に関する詳細情報を取得できます。監査ログは、メールボックスへのユーザーのアクセスの監視、不審なアクティビティの監査、アクセス制御と可用性プロバイダーの構成のデバッグに使用できます。

> **Note**
>
> AmazonWorkMailFullAccess管理ポリシーには、ログ配信の管理に必要な権限がすべて含まれているわけではありません。このポリシーを使用して管理する場合は WorkMail、ログ配信の設定に使用するプリンシパル (引き受けたロールなど) にも必要な権限がすべてあることを確認してください。

Amazon WorkMail では、監査ログの配信先として、 CloudWatch ログ、Amazon S3、Amazon Data Firehose という 3 つの宛先をサポートしています。詳細については、Amazon CloudWatch Logs ユーザーガイドの「追加の権限を必要とするロギング [V2]」を参照してください。

追加の権限を必要とする [V2] の「ロギング」に記載されている権限に加えて、Amazon WorkMail ではログ配信を設定するための追加の権限が必要です。workmail:AllowVendedLogDeliveryForResource

作業ログ配信は次の 3 つの要素で構成されます。

- DeliverySource、ログを送信する 1 つまたは複数のリソースを表す論理オブジェクト。Amazon にとっては WorkMail、Amazon WorkMail 組織です。
- A はDeliveryDestination、実際の配送先を表す論理オブジェクトです。
- デリバリー:配信元と配信先を接続します。

Amazon WorkMail と送信先間の口グ配信を設定するには、次の操作を行います。

- で配信元を作成しますPutDeliverySource。
- で配信先を作成しますPutDeliveryDestination。

- ログをクロスアカウントに配信する場合は、PutDeliveryDestinationPolicy宛先アカウントでを使用して IAM ポリシーを宛先に割り当てる必要があります。このポリシーは、アカウント A の配信元からアカウント B の配信先への配信の作成を許可します。
- を使用してCreateDelivery、1 つの配信元と 1 つの配信先だけを組み合わせて配信を作成します。

以下のセクションでは、各送信先へのログ配信を設定するためにサインインするときに必要な権限の詳細を説明します。これらの権限は、サインインに使用する IAM ロールに付与できます。

> **Important**
> ログ生成リソースを削除した後は、ログ配信リソースを削除する責任があります。

ログ生成リソースを削除した後でログ配信リソースを削除するには、次の手順に従います。

1. オペレーションを使用してデリバリーを削除します。DeleteDelivery
2. DeliverySourceDeleteDeliverySourceオペレーションを使用して削除します。
3. DeliveryDestinationDeliverySource削除したばかりの関連付けがこの特定の目的にのみ使用されている場合はDeliverySource、DeleteDeliveryDestinationsオペレーションを使用して削除できます。

Amazon WorkMail コンソールを使用して監査ログを設定する

Amazon WorkMail コンソールで監査ログを設定できます。

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

   必要に応じて、 AWS リージョンを変更してください。コンソールウィンドウ上部のバーで [Select a Region] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. [ログ設定] を選択します。
4. 「監査ログ設定」タブを選択します。
5. 適切なウィジェットを使用して、必要なログタイプの配信を設定します。
6. [保存] を選択します。

ログは Logs に送信されます。 CloudWatch

ユーザーアクセス許可

Logs CloudWatch にログを送信できるようにするには、次の権限でログインする必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:GetDelivery",
                "logs:GetDeliverySource",
                "logs:PutDeliveryDestination",
                "logs:GetDeliveryDestinationPolicy",
                "logs:DeleteDeliverySource",
                "logs:PutDeliveryDestinationPolicy",
                "logs:CreateDelivery",
                "logs:GetDeliveryDestination",
                "logs:PutDeliverySource",
                "logs:DeleteDeliveryDestination",
                "logs:DeleteDeliveryDestinationPolicy",
                "logs:DeleteDelivery"
            ],
            "Resource": [
                "arn:aws:logs:region:account-id:delivery:*",
                "arn:aws:logs:region:account-id:delivery-source:*",
                "arn:aws:logs:region:account-id:delivery-destination:*"
            ]
        },
        {
            "Sid": "ListAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeDeliveryDestinations",
                "logs:DescribeDeliverySources",
                "logs:DescribeDeliveries",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
```

```
            "Sid": "AllowUpdatesToResourcePolicyCWL",
            "Effect": "Allow",
            "Action": [
                "logs:PutResourcePolicy",
                "logs:DescribeResourcePolicies",
                "logs:DescribeLogGroups"
            ],
            "Resource": [
                "arn:aws:logs:region:account-id:*"
            ]
        }
        {
            "Sid":"AllowLogDeliveryForWorkMail",
            "Effect":"Allow",
            "Action":[
                "workmail:AllowVendedLogDeliveryForResource"
            ],
            "Resource":[
                "arn:aws:workmail:region:account-id:organization/organization-id"
            ]
        }
    ]
}
```

ロググループのリソースポリシー

ログが送信されているロググループには、特定のアクセス許可が含まれるリソースポリシーが必要です。ロググループに現在リソースポリシーがなく、ロギングを設定しているユーザーがそのロググループに対するlogs:PutResourcePolicy、logs:DescribeResourcePolicies、logs:DescribeLogGroups権限を持っている場合、ログをログに送信し始めると、 AWS そのロググループに対して以下のポリシーが自動的に作成されます。 CloudWatch

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"AWSLogDeliveryWrite20150319",
            "Effect":"Allow",
            "Principal":{
                "Service":[
                    "delivery.logs.amazonaws.com"
                ]
```

```
            },
            "Action":[
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource":[
                "arn:aws:logs:region:account-id:log-group:my-log-group:log-stream:*"
            ],
            "Condition":{
                "StringEquals":{
                    "aws:SourceAccount":[
                        "account-id"
                    ]
                },
                "ArnLike":{
                    "aws:SourceArn":[
                        "arn:aws:logs:region:account-id:*"
                    ]
                }
            }
        }
    ]
}
```

ロググループリソースポリシーのサイズ制限に関する考慮事項

これらのサービスは、ログの送信先となる各ロググループをリソースポリシーに記載する必要があります。 CloudWatch ログリソースポリシーは 5,120 文字に制限されています。多数のロググループにログを送信するサービスでは、この制限に達する可能性があります。

これを軽減するために、 CloudWatch Logs はログを送信するサービスが使用するリソースポリシーのサイズを監視します。ポリシーが 5,120 文字のサイズ制限に近づいていることを検出すると、/aws/vendedlogs/*そのサービスのリソースポリシーで CloudWatch Logs が自動的に有効になります。その後、/aws/vendedlogs/ で始まる名前のロググループをこれらのサービスからのログの送信先として使用し始めることができます。

Amazon S3 に送信されたログ

ユーザーアクセス許可

Amazon S3 へのログ送信を有効にするには、次のアクセス許可でサインインする必要があります。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:GetDelivery",
                "logs:GetDeliverySource",
                "logs:PutDeliveryDestination",
                "logs:GetDeliveryDestinationPolicy",
                "logs:DeleteDeliverySource",
                "logs:PutDeliveryDestinationPolicy",
                "logs:CreateDelivery",
                "logs:GetDeliveryDestination",
                "logs:PutDeliverySource",
                "logs:DeleteDeliveryDestination",
                "logs:DeleteDeliveryDestinationPolicy",
                "logs:DeleteDelivery"
            ],
            "Resource": [
                "arn:aws:logs:region:account-id:delivery:*",
                "arn:aws:logs:region:account-id:delivery-source:*",
                "arn:aws:logs:region:account-id:delivery-destination:*"
            ]
        },
        {
            "Sid": "ListAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeDeliveryDestinations",
                "logs:DescribeDeliverySources",
                "logs:DescribeDeliveries",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUpdatesToResourcePolicyS3",
            "Effect": "Allow",
            "Action": [
                "s3:PutBucketPolicy",
                "s3:GetBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::bucket-name"
```

```
        }
          {
            "Sid":"AllowLogDeliveryForWorkMail",
            "Effect":"Allow",
            "Action":[
                "workmail:AllowVendedLogDeliveryForResource"
            ],
            "Resource":[
                "arn:aws:workmail:region:account-id:organization/organization-id"
            ]
        }
    ]
}
```

ログが送信されている S3 バケットには、特定のアクセス許可が含まれるリソースポリシーが必要です。バケットに現在リソースポリシーがなく、S3:PutBucketPolicyロギングを設定しているユーザーがバケットに対する権限を持っている場合は、Amazon S3 にログを送信し始めると、 AWS そのバケットに対して以下のポリシーが自動的に作成されます。S3:GetBucketPolicy

```
{
    "Version":"2012-10-17",
    "Id":"AWSLogDeliveryWrite20150319",
    "Statement":[
        {
            "Sid":"AWSLogDeliveryAclCheck",
            "Effect":"Allow",
            "Principal":{
                "Service":"delivery.logs.amazonaws.com"
            },
            "Action":"s3:GetBucketAcl",
            "Resource":"arn:aws:s3:::my-bucket",
            "Condition":{
                "StringEquals":{
                    "aws:SourceAccount":[
                        "account-id"
                    ]
                },
                "ArnLike":{
                    "aws:SourceArn":[
                        "arn:aws:logs:region:account-id:delivery-source:*"
                    ]
                }
            }
```

```
        },
        {
            "Sid":"AWSLogDeliveryWrite",
            "Effect":"Allow",
            "Principal":{
                "Service":"delivery.logs.amazonaws.com"
            },
            "Action":"s3:PutObject",
            "Resource":"arn:aws:s3:::my-bucket/AWSLogs/account-id/*",
            "Condition":{
                "StringEquals":{
                    "s3:x-amz-acl":"bucket-owner-full-control",
                    "aws:SourceAccount":[
                        "account-id"
                    ]
                },
                "ArnLike":{
                    "aws:SourceArn":[
                        "arn:aws:logs:region:account-id:delivery-source:*"
                    ]
                }
            }
        }
    ]
}
```

前のポリシーでは、このバケットにログを配信する対象となるアカウント ID のリストを指定しました。aws:SourceAccountaws:SourceArn には、ログを生成するリソースの ARN のリストを arn:aws:logs:*source-region*:*source-account-id*:* の形式で指定します。

バケットにリソースポリシーがあっても、そのポリシーに前のポリシーに示されたステートメントが含まれておらず、S3:PutBucketPolicyロギングを設定しているユーザーがそのバケットに対する権限を持っている場合、そのステートメントはバケットのリソースポリシーに追加されます。S3:GetBucketPolicy

> **Note**
>
> AWS CloudTrail s3:ListBucketアクセス権限が付与されていないと、AccessDeniedエラーが表示されることがあります。delivery.logs.amazonaws.com CloudTrail ログにこのようなエラーが記録されないようにするには、s3:ListBucketにアクセス許可を付与する必要がありますdelivery.logs.amazonaws.com。また、Conditions3:GetBucketAcl前述のバケットポリシーで設定した権限に示されて

いるパラメータも含める必要があります。これを効率化するために、新しいものを作成する代わりにStatement、AWSLogDeliveryAclCheckを直接に更新することもできます。“Action”: [“s3:GetBucketAcl”, “s3:ListBucket”]

Amazon S3 バケットのサーバー側の暗号化

Amazon S3 で管理されたキーによるサーバー側の暗号化 (SSE-S3) またはに格納されているキーによるサーバー側の暗号化 (SSE-KMS) のいずれかを有効にすることで、Amazon S3 バケットのデータを保護できます。 AWS KMS AWS Key Management Service 詳細については、「サーバー側の暗号化を使用したデータの保護」を参照してください。

SSE-S3 を選択した場合、追加の設定は必要ありません。Amazon S3 が暗号化キーを処理します。

> **Warning**
>
> SSE-KMS を選択する場合は、カスタマー管理のキーを使用する必要があります。このシナリオではの使用はサポートされていないためです。 AWS マネージドキー AWS マネージドキーを使用して暗号化を設定すると、ログは判読できない形式で配信されます。

AWS KMS カスタマー管理キーを使用する場合、バケット暗号化を有効にするときにカスタマー管理キーの Amazon リソースネーム (ARN) を指定できます。ログ配信アカウントが S3 バケットに書き込めるように、(S3 バケットのバケットポリシーではなく) カスタマー管理キーのキーポリシーに以下を追加してください。

このシナリオではマネージドキーの使用はサポートされていないため、SSE-KMS を選択する場合は、 AWS カスタマー管理キーを使用する必要があります。 AWS KMS カスタマー管理キーを使用する場合、バケット暗号化を有効にするときにカスタマー管理キーの Amazon リソースネーム (ARN) を指定できます。ログ配信アカウントが S3 バケットに書き込めるように、(S3 バケットのバケットポリシーではなく) カスタマー管理キーのキーポリシーに以下を追加してください。

```
{
    "Sid":"Allow Logs Delivery to use the key",
    "Effect":"Allow",
    "Principal":{
        "Service":[
            "delivery.logs.amazonaws.com"
        ]
    },
```

```
    "Action":[
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource":"*",
    "Condition":{
        "StringEquals":{
            "aws:SourceAccount":[
                "account-id"
            ]
        },
        "ArnLike":{
            "aws:SourceArn":[
                "arn:aws:logs:region:account-id:delivery-source:*"
            ]
        }
    }
}
```

にはaws:SourceAccount、このバケットにログを配信するアカウント ID のリストを指定します。aws:SourceArn には、ログを生成するリソースの ARN のリストを arn:aws:logs:*source-region*:*source-account-id*:* の形式で指定します。

Firehose に送信されたログ

ユーザーアクセス許可

Firehose へのログ送信を有効にするには、次の権限でログインする必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:GetDelivery",
                "logs:GetDeliverySource",
                "logs:PutDeliveryDestination",
                "logs:GetDeliveryDestinationPolicy",
```

```
                "logs:DeleteDeliverySource",
                "logs:PutDeliveryDestinationPolicy",
                "logs:CreateDelivery",
                "logs:GetDeliveryDestination",
                "logs:PutDeliverySource",
                "logs:DeleteDeliveryDestination",
                "logs:DeleteDeliveryDestinationPolicy",
                "logs:DeleteDelivery"
            ],
            "Resource": [
                "arn:aws:logs:region:account-id:delivery:*",
                "arn:aws:logs:region:account-id:delivery-source:*",
                "arn:aws:logs:region:account-id:delivery-destination:*"
            ]
        },
        {
            "Sid": "ListAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeDeliveryDestinations",
                "logs:DescribeDeliverySources",
                "logs:DescribeDeliveries",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUpdatesToResourcePolicyFH",
            "Effect": "Allow",
            "Action": [
                "firehose:TagDeliveryStream"
            ],
            "Resource": [
                "arn:aws:firehose:region:account-id:deliverystream/*"
            ]
        },
        {
            "Sid": "CreateServiceLinkedRole",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::account-id:role/aws-service-role/
delivery.logs.amazonaws.com/AWSServiceRoleForLogDelivery"
```

```
        }
           {
            "Sid":"AllowLogDeliveryForWorkMail",
            "Effect":"Allow",
            "Action":[
                "workmail:AllowVendedLogDeliveryForResource"
            ],
            "Resource":[
                "arn:aws:workmail:region:account-id:organization/organization-id"
            ]
        }
    ]
}
```

リソースのアクセス許可のために使用される IAM ロール

Firehose はリソースポリシーを使用しないため、これらのログを Firehose に送信するように設定するときに IAM AWS ロールを使用します。 AWS という名前のサービスにリンクされたロールを作成します。AWSServiceRoleForLogDeliveryこのサービスリンクロールには、以下のアクセス許可が含まれます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "firehose:PutRecord",
                "firehose:PutRecordBatch",
                "firehose:ListTagsForDeliveryStream"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/LogDeliveryEnabled": "true"
                }
            },
            "Effect": "Allow"
        }
    ]
}
```

このサービスにリンクされたロールは、LogDeliveryEnabledタグがに設定されているすべての Firehose 配信ストリームにアクセス権限を付与します。true AWS ロギングを設定すると、このタグが宛先配信ストリームに付与されます。

このサービスリンクロールには、delivery.logs.amazonaws.com サービスプリンシパルが必要なサービスリンクロールを引き受けることを可能にする信頼ポリシーもあります。以下がその信頼ポリシーです。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

コンソール固有の権限

前のセクションに挙げた権限に加えて、API ではなくコンソールを使用してログ配信を設定する場合は、以下の権限も必要です。

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"AllowLogDeliveryActions",
            "Effect":"Allow",
            "Action":[
                "firehose:DescribeDeliveryStream",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource":[
                "arn:aws:logs:region:account-id:log-group:*",
                "arn:aws:firehose:region:account-id:deliverystream/*",
                "arn:aws:s3:::*"
            ]
```

```
        },
        {
            "Sid":"ListAccessForDeliveryDestinations",
            "Effect":"Allow",
            "Action":[
                "logs:DescribeLogGroups",
                "firehose:ListDeliveryStreams",
                "s3:ListAllMyBuckets"
            ],
            "Resource":"*"
        }
    ]
}
```

Amazon のコンプライアンス検証 WorkMail

サードパーティーの監査者は、複数の コンプライアンスプログラム WorkMail の一環として Amazon のセキュリティと AWS コンプライアンスを評価します。これには、SOC、ISO、および C5 が含まれます。

特定のコンプライアンスプログラムの対象となる 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。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「<shared id="AWS"/> Artifact のレポートのダウンロード」をご参照ください。

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

- 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 にデプロイする手順について説明します AWS。
- AWS コンプライアンスリソース — このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS Config – この AWS サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。

- AWS Security Hub – この AWS サービスは、 内のセキュリティ状態を包括的に把握 AWS し、セキュリティ業界標準とベストプラクティスへの準拠を確認するのに役立ちます。

Amazon の耐障害性 WorkMail

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

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

Amazon WorkMail は、 AWS グローバルインフラストラクチャに加えて、データの耐障害性とバックアップのニーズをサポートするのに役立ついくつかの機能を提供しています。

Amazon のインフラストラクチャセキュリティ WorkMail

> **Note**
>
> Amazon は Transport Layer Security (TLS) 1.0 および 1.1 のサポート WorkMail を終了しました。TLS 1.0 または 1.1 を使用している場合は、TLS バージョンを 1.2 にアップグレードする必要があります。詳細については、「TLS 1.2」を参照して、すべての AWS API エンドポイントの最小 TLS プロトコルレベルにしてください。

マネージドサービスである Amazon WorkMail は グローバル AWS ネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「 Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

が AWS 公開した API コールを使用して、ネットワーク WorkMail 経由で Amazon にアクセスします。クライアントは以下をサポートする必要があります:

- Transport Layer Security (TLS)。TLS 1.2 は必須で TLS 1.3 がお勧めです。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

Amazon の開始方法 WorkMail

を完了すると前提条件、Amazon の使用を開始する準備が整います WorkMail。詳細については、「Amazon の開始方法 WorkMail」を参照してください。

既存のメールボックスの Amazon への移行 WorkMail、Microsoft Exchange との相互運用性、Amazon WorkMail クォータの詳細については、以下のセクションを参照してください。

トピック

Amazon の開始方法 WorkMail

新しい Amazon WorkMail ユーザーでも、Amazon または WorkDocs Amazon の既存のユーザーでも WorkSpaces、次のステップ WorkMail を実行して Amazon の使用を開始します。

> **Note**
>
> 使用開始の前に 前提条件 を完了させます。

トピック

ステップ 1: Amazon WorkMail コンソールにサインインする

ユーザーを追加し、そのアカウントとメールボックスを管理する前に、Amazon WorkMail コンソールにサインインする必要があります。

Amazon WorkMail コンソールにサインインするには

1. https://console.aws.amazon.com/workmail/ で Amazon WorkMail コンソールを開きます。
2. 必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。リージョンの詳細については、Amazon Web Services 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。

ステップ 2: Amazon WorkMail サイトを設定する

1. Amazon WorkMail コンソールにサインインしたら、組織を設定し、ドメインを追加します。Amazon WorkMail 組織専用のドメインを使用することをお勧めします。詳細については、「組織の作成 と ドメインの追加」を参照してください。
2. (オプション) Amazon が提供する無料のテストドメインを使用することを選択できます WorkMail。この操作を選択した場合は、ステップ 4 に進みます。

> **Note**
>
> テストドメインの形式は *alias*.awsapps.com です。作業を進めるときは、テスト ドメインはテストにのみ使用する必要があることに注意してください。本番環境にはテストドメインを使用しないでください。また、Amazon WorkMail 組織には少なくとも 1 人の有効なユーザーが必要です。有効なユーザーがない場合、ドメインは他のお客様による登録と使用が可能になります。

3. 外部ドメインを使用する場合は、適切なテキスト (TXT) レコードとメール交換 (MX) レコードをドメインネームシステム (DNS) サービスに追加してドメインを検証します。TXT レコードを使用すると DNS にメモを入力できます。MX レコードは、受信メールサーバーを指定します。ドメイ

ンを組織のデフォルトとして設定してください。詳細については、ドメインの検証 および デフォルトのドメインの選択 を参照してください。

4. 新しいユーザーを作成するか、Amazon の既存のディレクトリユーザーを有効にします WorkMail。詳細については、「ユーザーの追加」を参照してください。
5. (オプション) 既存の Microsoft Exchange メールボックスがある場合は、それらを Amazon に移行します WorkMail。詳細については、「Amazon への移行 WorkMail」を参照してください。

Amazon WorkMail サイトの設定が完了したら、ウェブアプリケーションの URL WorkMail を使用して Amazon にアクセスできます。

Amazon WorkMail ウェブアプリケーションの URL を見つけるには

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

   必要に応じて AWS リージョンを変更します。これを行うには、検索ボックスの右側にある [リージョンの選択] リストを開き、目的のリージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。

   [組織設定] ページが表示され、[ユーザーログイン] に URL が表示されます。URL は https://*alias* .awsapps.com/mail という形式をとります。

ステップ 3: Amazon WorkMail ユーザーアクセスを設定する

以下のオプションから選択して、Amazon WorkMail ユーザーアクセスを設定します。

- Microsoft Outlook クライアントを使用して、既存のデスクトップクライアントからユーザーアクセスを設定します。詳細については、「Microsoft Outlook を Amazon WorkMail アカウントに接続する」を参照してください。
- Kindle、Android、iPad、または iPhone などのモバイルデバイスからユーザーアクセスを設定できます。詳細については、モバイルデバイスの開始方法を参照してください。
- ユーザーアクセスを設定するには、インターネットメールアクセスプロトコル (IMAP) プロトコルと互換性のあるクライアントソフトウェアを使用してください。詳細については、「IMAP クライアントを Amazon WorkMail アカウントに接続する」を参照してください。

その他の リソース

- Amazon への移行 WorkMail
- Amazon WorkMail と Microsoft Exchange 間の相互運用性
- Amazon WorkMail クォータ

Amazon への移行 WorkMail

Microsoft Exchange、Microsoft Office 365、G Suite Basic (以前の Google Apps for Work)、およびその他のプラットフォーム WorkMail から Amazon に移行するには、当社のパートナーのいずれかを使用します。パートナーの詳細については、「Amazon WorkMail の機能」を参照してください。

トピック

- ステップ 1: Amazon でユーザーを作成または有効にする WorkMail
- ステップ 2: Amazon に移行する WorkMail
- ステップ 3: Amazon への移行を完了する WorkMail

ステップ 1: Amazon でユーザーを作成または有効にする WorkMail

ユーザーを移行する前に、Amazon にユーザーを追加してメールボックス WorkMail をプロビジョニングする必要があります。詳細については、「ユーザーの追加」を参照してください。

ステップ 2: Amazon に移行する WorkMail

任意のAWS移行パートナーと連携して Amazon に移行できます WorkMail。これらのプロバイダーの詳細については、「Amazon WorkMail の機能」を参照してください。

メールボックスを移行するには、移行管理者となる専用の Amazon WorkMail ユーザーを作成します。次の手順では、組織内のすべてのメールボックスにアクセスするアクセス許可を、このユーザーに付与します。

移行管理者を作成するには

1. 次のいずれかを行います:

    - Amazon WorkMail コンソールで、移行管理者となる新しいユーザーを作成します。詳細については、「ユーザーの追加」を参照してください。

- Active Directory で、移行管理者となる新しいユーザーを作成し、Amazon のユーザーを有効にします WorkMail。詳細については、「ユーザーの有効化」を参照してください。

2. Amazon WorkMail コンソールのナビゲーションペインで、Organizations を選択し、組織の名前を選択します。
3. [組織の設定]、[移行]、[編集]の順に選択します。
4. [移行を有効化] スライダーを [オン] の位置に移動します。
5. 移行管理者を開き、ユーザーを選択します。
6. [保存] を選択します。

ステップ 3: Amazon への移行を完了する WorkMail

E メールアカウントを Amazon に移行したら WorkMail、DNS レコードを検証し、デスクトップクライアントとモバイルクライアントを設定できます。

Amazon への移行を完了するには WorkMail

1. すべての DNS レコードが更新され、Amazon を指していることを確認します WorkMail。必要な DNS レコードの詳細については、ドメインの追加 を参照してください。

> **Note**
>
> DNS レコードの更新処理には数時間かかる場合があります。MX レコード変更中に移行元のメールボックスに新しい項目が表示された場合は、移行ツールを再び実行して、DNS レコードを更新してから新しい項目を移行することができます。

2. Amazon を使用するようにデスクトップまたはモバイルクライアントを設定する方法の詳細については WorkMail、「Amazon WorkMail ユーザーガイド」の「Microsoft Outlook を Amazon WorkMail アカウントに接続する」を参照してください。

Amazon WorkMail と Microsoft Exchange 間の相互運用性

Amazon WorkMail と Microsoft Exchange Server 間の相互運用性により、メールボックスを Amazon に移行したり WorkMail、会社のメールボックスのサブセット WorkMail に Amazon を使用したりするときに、ユーザーの中断を最小限に抑えることができます。

この相互運用性により、どちらの環境のメールボックスにも同じ企業ドメインを使用することができます。これにより、ユーザーはカレンダーの空き時間ステータス情報を双方向に共有して会議をスケジュールできます。

前提条件

Microsoft Exchange を使用して相互運用性を実現するには、以下を実行します。

- Amazon で少なくとも 1 人のユーザーが有効になっていることを確認します。これは、Microsoft Exchange WorkMail の可用性設定を構成するために必要です。ユーザーを有効にするには、ユーザーの E メールルーティングを有効にする の手順に従います。
- アクティブディレクトリ (AD) Connector をセットアップします。オンプレミスディレクトリに AD Connector をセットアップすると、ユーザーは既存の社内認証情報を引き続き使用できます。詳細については、「AD Connector を作成し、Amazon をオンプレミスディレクトリ WorkMail と統合する」を参照してください。
- Amazon WorkMail 組織をセットアップします。設定した AD Connector を使用する Amazon WorkMail 組織を作成します。
- 企業ドメインを Amazon WorkMail 組織に追加し、Amazon WorkMail コンソールで検証します。それ以外の場合、このエイリアスに送信される E メールはバウンスします。詳細については、ドメインの使用を参照してください。
- メールボックスを Amazon に移行します WorkMail。ユーザーはメールボックスをオンプレミス環境から Amazon に移行できます WorkMail。詳細については、「既存のユーザーを有効にする」および「Amazon への移行 WorkMail」を参照してください。

> **Note**
>
> Amazon を指すように DNS レコードを更新しないでください WorkMail。これにより、2 つの環境間で相互運用性が必要とされる限り、Microsoft Exchange は受信メールのプライマリサーバーとして維持されます。

- アクティブディレクトリのユーザープリンシパル名 (UPN) が、ユーザーのプライマリ SMTP アドレスと一致していることを確認します。

Amazon WorkMail は Microsoft Exchange の Exchange Web Services (EWS) URL に HTTPS リクエストを行い、カレンダーの空き時間情報を取得します。

EWS ベースの可用性プロバイダーの場合、Amazon WorkMail は Microsoft Exchange の Exchange Web Services (EWS) URL に HTTPS リクエストを行い、カレンダーの空き時間情報を取得します。したがって、以下の前提条件は EWS ベースのアベイラビリティプロバイダーにのみ適用されます。

- 該当するファイアウォール設定が、インターネットからアクセスできるようにセットアップされていることを確認します。HTTPS リクエストのデフォルトポートは、ポート 443 です。
- Amazon WorkMail は、有効な認証機関 (CA) によって署名された証明書が Microsoft Exchange 環境で利用可能な場合にのみ、Microsoft Exchange の EWS URL に対して成功した HTTPS リクエストを行うことができます。詳細については、Microsoft Exchange ドキュメントウェブサイトの認定権限の Exchange Server 証明書リクエストを作成するを参照してください。
- Microsoft Exchange の EWS で [Basic Authentication] (基本的な認証) を有効にする必要があります。詳細については、Microsoft MVP アワードプログラムのブログの仮想ディレクトリ: Exchange 2013 を参照してください。

ドメインを追加してメールボックスを有効にする

企業ドメインを Amazon に追加して、E メールアドレスで使用できる WorkMail ようにします。Amazon に追加されたドメインが検証されていることを確認し、ユーザーとグループ WorkMail が Amazon にメールボックスをプロビジョニングできるようにします WorkMail。相互運用性モード WorkMail の場合、Amazon でリソースを有効にすることはできません。相互運用性モードを無効に WorkMail した後、Amazon でリソースを再作成する必要があります。ただし、相互運用性モード中は、以前と同様、会議を設定できます。Microsoft Exchange のリソースは、常に Amazon のユーザータブに表示されます WorkMail。

- 詳細については、ドメインの追加、既存ユーザーの有効化、および既存グループの有効化を参照してください。

> **Note**
>
> Microsoft Exchange との相互運用性を確保するために、Amazon レコードを指すように DNS WorkMail レコードを更新しないでください。2 つの環境間で相互運用性が必要とされる限り、Microsoft Exchange は受信メールのプライマリサーバーとして維持されます。

相互運用性を有効にする

Amazon WorkMail 組織を作成していない場合は、パブリック API を使用して、相互運用モードを有効にした新しい WorkMail 組織を作成できます。

AD Connector が Active Directory にリンクされた Amazon WorkMail 組織がすでにあり、Microsoft Exchange も持っている場合は、AWS サポートに連絡して、既存の Amazon WorkMail 組織で Microsoft Exchange の相互運用性を有効にするためのサポートを依頼してください。

Microsoft Exchange と Amazon でサービスアカウントを作成する WorkMail

> **Note**
>
> Exchange がカスタム可用性プロバイダーのバックエンドとして使用されていない場合は、Exchange でサービスアカウントを作成する必要はありません。

カレンダーの空き時間情報にアクセスするには、Microsoft Exchange と Amazon の両方でサービスアカウントを作成します WorkMail。Microsoft Exchange のサービスアカウントは、Microsoft Exchange のユーザーを指し、他の Exchange ユーザーのカレンダーの空き時間情報にアクセスすることができます。アクセス権はデフォルトで付与されています。それで、特別なアクセス許可は必要ありません。

同様に、Amazon WorkMail サービスアカウントは、他の Amazon ユーザーのカレンダーの空き時間情報 WorkMail にアクセスできる Amazon のすべての WorkMail ユーザーです。この許可もデフォルトで付与されます。Amazon WorkMail を AD Connector WorkMail とディレクトリに統合するには、オンプレミスディレクトリに Amazon ユーザーを作成し WorkMail、Amazon のそのユーザーを有効にする必要があります。

相互運用性モードの制約事項

組織が相互運用モードにの場合は、Exchange 管理センターを使用してすべてのユーザー、グループ、リソースを管理する必要があります。Amazon WorkMail ユーザーとグループを有効にするには、 を使用しますAWS Management Console。詳細については、既存ユーザーを有効にするおよび既存グループを有効にするを参照してください。

Amazon のユーザーまたはグループを有効にする場合 WorkMail、それらのユーザーおよびグループの E メールアドレスまたはエイリアスを編集することはできません。また、Exchange 管理者セン

ターから設定する必要があります。Amazon は 4 時間ごとにディレクトリの変更を WorkMail 同期します。

相互運用性モード WorkMail の場合、Amazon でリソースを作成または有効にすることはできません。ただし、Exchange リソースはすべて Amazon WorkMail アドレス帳で利用でき、通常どおり会議をスケジュールするために使用できます。

Amazon での可用性設定の構成 WorkMail

外部システムのクエリ WorkMail 、カレンダー機能の提供、カレンダーの空き時間情報の取得を有効にするには、Amazon の可用性設定を構成します。Amazon は、リモートシステムから空き時間情報を取得する 2 つのモード WorkMail をサポートしています。

- Exchange Web Services (EWS) — この設定では、Amazon WorkMail は EWS プロトコルを使用して Exchange サーバーまたは別の WorkMail 組織に可用性情報をクエリします。これは最も単純な構成ですが、Exchange サーバーの EWS エンドポイントにパブリックインターネット経由でアクセスできる必要があります。
- カスタムアベイラビリティプロバイダー (CAP) — この設定では、管理者は AWS Lambda 関数を設定して、特定の E メールドメインのユーザー可用性情報を取得できます。E メールサーバープラットフォームに応じて、Amazon で CAP を使用すると、次の利点 WorkMail があります。
  - のファイアウォールを開かなくても、内部 EWS からユーザーの可用性を確保できます WorkMail。
  - Google Workspace (以前は G Suite と呼ばれていました) などの Exchange や ES 以外のシステムからもユーザーの可用性を確保できます。

トピック

- EWS ベースのアベイラビリティプロバイダを設定します。
- カスタムアベイラビリティプロバイダーの設定
- カスタムアベイラビリティプロバイダー Lambda 関数の構築

EWS ベースのアベイラビリティプロバイダを設定します。

コンソール上で EWS ベースの可用性設定を構成するには、次の手順を実行してください

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

必要に応じて AWS リージョンを変更します。これを行うには、検索ボックスの右側にある [リージョンの選択] リストを開き、目的のリージョンを選択します。詳細については、「Amazon Web Services 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。

2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで [組織の設定] を選択し、[相互運用性] タブを選択します。
4. [可用性設定を追加] を選択し、次の情報を入力します。
   - タイプ — [EWS] を選択します。
   - ドメイン — がこの設定を使用して可用性情報のクエリ WorkMail を試みるドメイン。
   - EWS URL — Amazon WorkMail はこの URL を EWS エンドポイントにクエリします。このガイドの「EWS URL の取得」セクションを参照してください。
   - ユーザーの E メールアドレス — EWS エンドポイントへの認証に が WorkMail 使用するユーザーの E メールアドレス。
   - パスワード — WorkMail が EWS エンドポイントへの認証に使用するパスワード。
5. [保存] を選択します。

ODBC URL の取得

Microsoft Outlook を使用して Exchange 用の EWS URL を取得するには、次の手順を実行します。

1. Exchange 環境のユーザーで Windows の Microsoft Outlook にログインします。
2. [Ctrl] キーを押したまま、タスクバーの Microsoft Outlook アイコンのコンテキスト (右クリック) メニューを開きます。
3. E メールのテスト AutoConfigurationを選択します。
4. Microsoft Exchange ユーザーの E メールアドレスとパスワードを入力し、[Test] (テスト) を選択します。
5. 結果ウィンドウから、[Availability Service URL] の値をコピーします。

を使用して交換用の EWS URL を取得するには PowerShell、 PowerShell プロンプトで次のコマンドを実行します。

```
Get-WebServicesVirtualDirectory |Select name, *url* | fl
```

Amazon の EWS URL を取得するには WorkMail、まず Amazon WorkMail エンドポイントとクォータ で EWS ドメインを見つけます。EWS URL `https://"EWS domain"/EWS/Exchange.asmx` を入力し、「EWS ドメイン」をご自身の EWS ドメインに置き換えます。

カスタムアベイラビリティプロバイダーの設定

カスタムアベイラビリティプロバイダー (CAP) を設定するには、次の手順を実行してください

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

   必要に応じて AWS リージョンを変更します。これを行うには、検索ボックスの右側にある [リージョンを選択] リストを開き、目的のリージョンを選択します。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションパネルで、[組織の設定]、[相互運用性] の順に選択します。
4. [可用性設定を追加] を選択し、次の情報を入力します。

   - タイプ — CAP Lambda を選択します。
   - ドメイン — がこの設定を使用して可用性情報のクエリ WorkMail を試みるドメイン。
   - ARN — 可用性情報を提供する Lambda 関数の ARN。

CAP Lambda 関数を構築するには、カスタムアベイラビリティプロバイダー Lambda 関数の構築を参照してください。

カスタムアベイラビリティプロバイダー Lambda 関数の構築

カスタムアベイラビリティプロバイダー (CAP) は、明確に定義された JSON スキーマで記述された JSON ベースのリクエスト/レスポンスプロトコルで設定されます。Lambda 関数はリクエストを解析し、有効なレスポンスを返します。

トピック

- リクエストとレスポンスの要素
- アクセス権の付与
- CAP Lambda 関数 WorkMail を使用した Amazon の例

リクエストとレスポンスの要素

リクエストの要素

以下は、Amazon WorkMail ユーザーの CAP を設定するために使用されるリクエストの例です。

```
{
    "requester": {
        "email": "user1@internal.example.com",
        "userName": "user1",
        "organization": "m-0123456789abcdef0123456789abcdef",
        "userId": "S-1-5-18",
        "origin": "127.0.0.1"
    },
    "mailboxes": [
        "user2@external.example.com",
        "unknown@internal.example.com"
    ],
    "window": {
        "startDate": "2021-05-04T00:00:00.000Z",
        "endDate": "2021-05-06T00:00:00.000Z"
    }
}
```

リクエストは、リクエスタ、メールボックス、ウィンドウの 3 つのセクションで構成されています。これらについては、本ガイドの次のリクエスタ、メールボックス、Windowの各セクションで説明しています。

リクエスタ

リクエスタセクションには、Amazon への元のリクエストを行ったユーザーに関する情報が表示されます WorkMail。CAP はこの情報を使用してプロバイダーの行動を変更します。たとえば、このデータを使用してバックエンドのアベイラビリティプロバイダーの同じユーザーになりすましたり、特定の詳細を応答から省略したりできます。

フィールド	説明	必須
Email	リクエスタのメインメールアドレス。	はい
Username	リクエスタのユーザー名。	はい

フィールド	説明	必須
Organization	リクエスタの組織 ID。	はい
UserID	リクエスタ ID。	はい
Origin	リクエスタの リモートアドレス。	いいえ
Bearer	将来の利用のために予約されています。	いいえ

メールボックス

メールボックスセクションには、空き状況情報を要求するユーザーの電子メールアドレスのコンマ区切りリストが含まれます。

Window

ウィンドウセクションには、可用性情報を要求する時間枠が含まれます。startDate、endDateともも UTC で指定され、RFC 3339 に従ってフォーマットされています。イベントが切り捨てられることは想定されていません。つまり、定義したイベントより前に開始されたイベントはStartDate、元の開始位置が使用されます。

レスポンス要素

Amazon WorkMail は、CAP Lambda 関数からレスポンスを取得するまで 25 秒間待機します。25 秒後、Amazon WorkMail は関数が失敗したと見なし、EWS GetUserAvailability レスポンス内の関連するメールボックスに障害を生成します。これにより、 GetUserAvailability オペレーション全体が失敗することはありません。

以下は、このセクションの冒頭で定義した構成からの応答例です。

```
{
    "mailboxes": [{
        "mailbox": "user2@external.example.com",
        "events": [{
            "startTime": "2021-05-03T23:00:00.000Z",
            "endTime": "2021-05-04T03:00:00.000Z",
            "busyType": "BUSY"|"FREE"|"TENTATIVE",
            "details": {  // optional
```

```
                "subject": "Late meeting",
                "location": "Chime",
                "instanceType": "SINGLE_INSTANCE"|"RECURRING_INSTANCE"|"EXCEPTION",
                "isMeeting": true,
                "isReminderSet": true,
                "isPrivate": false
            }
        }],
        "workingHours": {
            "timezone": {
                "name": "W. Europe Standard Time"
                "bias": 60,
                "standardTime": {  // optional (not needed for fixed offsets)
                    "offset": 60,
                    "time": "02:00:00",
                    "month":
 "JAN"|"FEB"|"MAR"|"APR"|"JUN"|"JUL"|"AUG"|"SEP"|"OCT"|"NOV"|"DEC",
                    "week": "FIRST"|"SECOND"|"THIRD"|"FOURTH"|"LAST",
                    "dayOfWeek": "SUN"|"MON"|"TUE"|"WED"|"THU"|"FRI"|"SAT"
                },
                "daylightTime": {  // optional (not needed for fixed offsets)
                    "offset": 0,
                    "time": "03:00:00",
                    "month":
 "JAN"|"FEB"|"MAR"|"APR"|"JUN"|"JUL"|"AUG"|"SEP"|"OCT"|"NOV"|"DEC",
                    "week": "FIRST"|"SECOND"|"THIRD"|"FOURTH"|"LAST",
                    "dayOfWeek": "SUN"|"MON"|"TUE"|"WED"|"THU"|"FRI"|"SAT"
                },
            },
            "workingPeriods":[{
                "startMinutes": 480,
                "endMinutes": 1040,
                "days": ["SUN"|"MON"|"TUE"|"WED"|"THU"|"FRI"|"SAT"]
            }]
        }
    },{
        "mailbox": "unknown@internal.example.com",
        "error": "MailboxNotFound"
    }]
}
```

レスポンスは、メールボックスのリストで構成される 1 つのメールボックスセクションで構成されます。可用性が正常に取得された各メールボックスは、「メールボックス」、「イベント」、「稼働

時間」の 3 つのセクションで構成されています。アベイラビリティプロバイダーがメールボックスの空き時間情報を取得できなかった場合、セクションはメールボックスとエラーの 2 つのセクションで構成されます。これらについては、本ガイドの次のメールボックス、イベント、稼働時間、タイムゾーン、作業期間、エラーの各セクションで説明しています。

メールボックス

メールボックスセクションは、リクエストのメールボックスセクションにあるユーザーのメールアドレスです。

イベント

イベントセクションは、リクエストされたウィンドウで発生するイベントのリストです。各イベントは、次のパラメータで定義されます。

フィールド	説明	必須
`startTime`	イベントの開始時刻は UTC で、RFC 3339 に従ってフォーマットされています。	はい
`endTime`	イベントの終了時刻は UTC で、RFC 3339 に従ってフォーマットされています。	はい
`busyType`	イベントのビジータイプ。`Busy`、`Free`、または `Tentative` のいずれかを設定できます。	はい
`details`	イベントの詳細	いいえ
`details.subject`	イベントの件名	はい
`details.location`	イベントの場所。	はい
`details.instanceType`	イベントのインスタンスタイプ。`Single_Instance` 、`Recurring_Instance` 、または	はい

フィールド	説明	必須
	Exception のいずれかを設定できます。	
details.isMeeting	イベントに出席者がいるかどうかを示すブール値。	はい
details.isReminderSet	イベントにリマインダーが設定されているかどうかを示すブール値。	はい
details.isPrivate	イベントが非公開に設定されているかどうかを示すブール値。	はい

稼働時間

WorkingHours セクションには、メールボックス所有者の勤務時間に関する情報が含まれています。これには、タイムゾーンと稼働期間の 2 つのセクションがあります。

タイムゾーン

タイムゾーン サブセクションには、メールボックス所有者のタイムゾーンが記述されています。リクエスタが別のタイムゾーンで働いている場合は、ユーザーの勤務時間を正しく表示することが重要です。アベイラビリティプロバイダーは、名前を使用するのではなく、タイムゾーンを明示的に記述する必要があります。標準化されたタイムゾーンの説明を使用すると、タイムゾーンの不一致を防ぐことができます。

フィールド	説明	必須
name	タイムゾーンの名前。	はい
bias	GMT からのデフォルトオフセット (単位：分)。	はい
standardTime	指定されたタイムゾーンの標準時間の開始。	いいえ

フィールド	説明	必須
daylightTime	指定したタイムゾーンの夏時間の開始。	いいえ

との両方を定義するかdaylightTime、standardTime両方を省略する必要があります。standardTimeand daylightTime オブジェクトのフィールドは以下のとおりです。

フィールド	説明	許可された値
offset	デフォルトオフセットを基準にしたオフセット (単位：分)。	該当なし
time	標準時間と夏時間の切り替えが行われる時刻。hh:mm:ssとして指定します。	該当なし
month	標準時間と夏時間の切り替えが行われる月。	JAN,FEB, MAR, APR, JUN, JUL, AUG, SEP, OCT, NOV, DEC
week	指定した月のうち、標準時間と夏時間の切り替えが行われる週。	FIRST, SECOND, THIRD, FOURTH, LAST
dayOfWeek	指定した週のうち、標準時間と夏時間の切り替えが行われる日。	SUN, MON, TUE, WED, THU, FRI, SAT

作業期間

WorkingPeriodsセクションには、1つ以上の作業期間オブジェクトが含まれています。各期間は、1日以上の稼働日の開始と終了を定義します。

フィールド	説明	許可された値
startMinutes	1 日の開始時刻を午前 0 時から分単位で表したものです。	該当なし
endMinutes	1 日の終了時間を午前 0 時からの分単位で表したものです。	該当なし
days	この期間が適用される日。	SUN, MON, TUE, WED, THU, FRI, SAT

エラー

エラー フィールドには任意のエラーメッセージを格納できます。次の表は、既知のコードと EWS エラーコードのマッピングを示しています。その他のメッセージはすべてにマップされます。ERROR_FREE_BUSY_GENERATION_FAILED

値	EWS エラーコード
MailboxNotFound	ERROR_MAIL_RECIPIENT_NOT_FOUND
ErrorAvailabilityConfigNotFound	ERROR_AVAILABILITY_CONFIG_NOT_FOUND
ErrorServerBusy	ERROR_SERVER_BUSY
ErrorTimeoutExpired	ERROR_TIMEOUT_EXPIRED
ErrorFreeBusyGenerationFailed	ERROR_FREE_BUSY_GENERATION_FAILED
ErrorResponseSchemaValidation	ERROR_RESPONSE_SCHEMA_VALIDATION

アクセス権の付与

AWS Command Line Interface（AWS CLI）から、次のコマンドを実行します。このコマンドは、CAP を解析する Lambda 関数にリソースポリシーを追加します。この関数により、Amazon WorkMail 可用性サービスは Lambda 関数を呼び出すことができます。

```
aws lambda add-permission \
    --region LAMBDA_REGION \
    --function-name CAP_FUNCTION_NAME \
    --statement-id AllowWorkMail \
    --action "lambda:InvokeFunction" \
    --principal availability.workmail.WM_REGION.amazonaws.com \
    --source-account WM_ACCOUNT_ID \
    --source-arn arn:aws:workmail:WM_REGION:WM_ACCOUNT_ID:organization/ORGANIZATION_ID
```

コマンドでは、以下のパラメータを指定された場所に追加します。

- *LAMBDA_REGION — CAP Lambda* がデプロイされているリージョンの名前。例えば、us-east-1 です。
- *CAP_FUNCTION_NAME* — CAP Lambda 関数の名前。

> **Note**
>
> これには、CAP Lambda 関数の名前、エイリアス、ARN の一部または全部を使用できます。

- *WM_REGION* — Amazon WorkMail 組織が Lambda 関数を呼び出すリージョンの名前。

> **Note**
>
> CAP で使用できるのは次のリージョンのみです。
>
> - 米国東部 (バージニア北部)
> - 米国西部 (オレゴン)
> - 欧州 (アイルランド)

- *WM_ACCOUNT_ID* — 組織アカウントの ID。
- *ORGANIZATION_ID* — CAP Lambda を呼び出す組織の ID。Org ID: m-934ebb9eb57145d0a6cab566ca81a21fなど

> **Note**
>
> *LAMBDA_REGION* と *WM_REGION* は、クロスリージョン呼び出しが必要な場合にのみ異なります。クロスリージョン呼び出しが不要な場合も同様です。

CAP Lambda 関数 WorkMail を使用した Amazon の例

CAP Lambda 関数 WorkMail を使用して EWS エンドポイントをクエリする Amazon の例については、Amazon リポジトリのサーバーレスアプリケーションにあるこのAWSサンプルアプリケーションを参照してください。 WorkMail GitHub

Microsoft Exchange の可用性設定を設定する

有効なユーザーのカレンダーの空き時間情報リクエストをすべて Amazon にリダイレクトするには WorkMail、Microsoft Exchange で可用性アドレス空間を設定します。

次の PowerShell コマンドを使用してアドレス空間を作成します。

```
$credentials = Get-Credential
```

プロンプトで、Amazon WorkMail サービスアカウントの認証情報を入力します。ユーザーネームは **domain\username** (例: ***orgname*.awsapps.com\workmail_service_account_*username***) と入力します。ここで、 は Amazon WorkMail 組織の名前***orgname***を表します。詳細については、「Microsoft Exchange と Amazon でサービスアカウントを作成する WorkMail」を参照してください。

```
Add-AvailabilityAddressSpace -ForestName orgname.awsapps.com -AccessMethod OrgWideFB -
Credentials $credentials
```

詳細については、「Microsoft Docs で を追加するAvailabilityAddressSpace」を参照してください。

Microsoft Exchange と Amazon WorkMail ユーザー間の E メールルーティングを有効にする

Microsoft Exchange Server と Amazon 間の E メールルーティングを使用すると WorkMail、ユーザーは Amazon に移行した後も既存の E メールアドレスを保持できます WorkMail。メールルー

ティングを使用すると、Microsoft Exchange Server を組織の受信メール用のSimple Mail Transfer Protocol (SMTP) サーバーとして維持できます。

E メールルーティングを使用する前に、以下の前提条件を満たしている必要があります。

- 組織の相互運用性モードが有効である。詳細については、「相互運用性を有効にする」を参照してください。
- Amazon WorkMail コンソールにドメインが表示されていることを確認します。
- Microsoft Exchange Server がインターネットに電子メールを送信できることを確認してください。送信コネクタの設定が必要になる場合があります。送信コネクタの詳細については、Microsoft ドキュメントの「Exchange Server で送信コネクタを作成してメールをインターネットに送信する」を参照してください。

ユーザーの E メールルーティングを有効にする

組織に変更を適用する前に、まずテストユーザーに対して次の手順を実行することをお勧めします。

1. Amazon に移行するユーザーアカウントを有効にします WorkMail。詳細については、既存ユーザーの有効化を参照してください。
2. Amazon WorkMail コンソールで、有効なユーザーに少なくとも 2 つの E メールアドレスが関連付けられていることを確認します。
   - <*workmailuser*@*orgname*.awsapps.com> (これは自動的に追加され、Microsoft Exchange なしでテストに使用できます。)
   - <*workmailuser*@*yourdomain*.com> (これは自動的に追加され、Microsoft Exchange のプライマリアドレスです。)

     詳細については、ユーザーの E メールアドレスの編集を参照してください。
3. すべてのデータは、Microsoft Exchange のメールボックスから Amazon のメールボックスに移行してください WorkMail。詳細については、「Amazon への移行 WorkMail」を参照してください。
4. すべてのデータが移行されたら、Microsoft Exchange 上のユーザーのメールボックスを無効にします。次に、Amazon を指す外部 SMTP アドレスを持つメールユーザー (またはメール対応ユーザー) を作成します WorkMail。これを行うには、Exchange Management Shell で次のコマンドを使用します。

> **Important**
>
> 以下のステップを実行すると、メールボックスの内容は削除されます。E メールルーティングを有効にする WorkMail 前に、データが Amazon に移行されていることを確認してください。一部のメールクライアントは、このコマンドを実行して WorkMail もシームレスに Amazon に切り替えられません。詳細については、「メールクライアントの設定」を参照してください。

```
$old_mailbox = Get-Mailbox exchangeuser
```

```
Disable-Mailbox $old_mailbox
```

```
$new_mailuser = Enable-MailUser $old_mailbox.Identity -
ExternalEmailAddress workmailuser@orgname.awsapps.com -PrimarySmtpAddress
 $old_mailbox.PrimarySmtpAddress
```

```
Set-MailUser $new_mailuser -EmailAddresses $old_mailbox.EmailAddresses -
HiddenFromAddressListsEnabled $old_mailbox.HiddenFromAddressListsEnabled
```

上記のコマンドでは、*orgname* は Amazon WorkMail 組織の名前を表します。詳細については、「メールボックスの無効化」および「Microsoft でのメールユーザーの有効化」を参照してください TechNet。

5. ユーザーにテスト電子メールを送信します (上記の例では、**workmailuser@yourdomain.com**)。E メールルーティングが正しく有効になっている場合、ユーザーは Amazon WorkMail メールボックスにログインして E メールを受信できます。

> **Note**
>
> Microsoft Exchange では、受信メールのプライマリサーバーを好きなだけ維持して、2 つの環境間の相互運用性を確保できます。Microsoft Exchange との相互運用性を確保するために、DNS レコードは後で Amazon を指す WorkMail ように更新しないでください。

セットアップ後の設定

上記のステップでは、ユーザーのメールボックスを Microsoft Exchange Server から Amazon に移動しますが WorkMail、ユーザーは連絡先として Microsoft Exchange に保持されます。移行されたユーザーは外部メール ユーザーになったため、Microsoft Exchange Server によって追加の制約が課されます。移行を完了するには追加の設定要件がある場合もあります。

- デフォルトでは、ユーザーは E メールをグループに送信できない場合があります。この機能を有効にするには、すべてのグループの信頼できる送信者リストにユーザーを追加する必要があります。詳細については、「Microsoft での配信管理」を参照してください TechNet。
- ユーザーはリソースを予約できない可能性があります。この機能を有効にするには、ユーザーがアクセスする必要があるすべてのリソースの `ProcessExternalMeetingMessages` を設定する必要があります。詳細については、Microsoft の「Set-CalendarProcessing」を参照してください TechNet。

メールクライアントの設定

一部のメールクライアントは、シームレスに Amazon に切り替えません WorkMail。これらのクライアントでは、さらにセットアップを行う必要がある場合があります。実行するアクションは、メールクライアントによって異なります。

- Windows 上の Microsoft Outlook – Outlook を再起動する必要があります。起動時に、元のメールボックス、または一時的なメールボックスを使用するかを選択する必要があります。一時メールボックスのオプションを選択します。次に、Microsoft Exchange メールボックスを再設定します。
- MacOS 上の Microsoft Outlook – Outlook を再起動すると、次のメッセージが表示されます: Outlook はサーバー ***orgname***.awsapps.com にリダイレクトされました。このサーバーで設定を構成しますか? 提案を許可します。
- iOS のメール – このメールアプリケーションでは、メールの受信が停止し、[メールを取得できません] エラーが生成されます。Microsoft Exchange メールボックスを再度、作成および設定します。

相互運用モードの無効化とメールサーバーの廃棄

Amazon の Microsoft Exchange メールボックスを設定したら WorkMail、相互運用性モードを無効にできます。ユーザーやレコードを移行していない場合は、相互運用モードを無効にしても、設定には影響ありません。

> **Warning**
>
> 相互運用モードを無効にする前に、必要なステップをすべて完了していることを確認してください。完了していないと、E メールがバウンスするか、意図しない動作が生じる場合があります。移行が完了していない場合に相互運用性を無効にすると、移行が中断する場合があります。このオペレーションは元に戻すことができません。

相互運用モードのサポートを無効にするには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで、[組織] を選択し、相互運用モードを無効にする組織を選択します。
3. 「組織の設定」 で、「相互運用モードを無効化」を選択します。
4. [相互運用モードを無効化] ダイアログ ボックスで、組織の名前を入力し、[相互運用モードを無効化] を選択します。

相互運用性のサポートを無効にすると、Amazon で有効になっていないユーザーとグループはアドレス帳から WorkMail 削除されます。Amazon WorkMail コンソールを使用して、不足しているユーザーまたはグループを有効にすることはできます。これらはアドレス帳に追加されます。Microsoft Exchange のリソースは有効にできないため、以下のステップが完了するまで、アドレス帳に表示されることはできません。

- Amazon でリソース WorkMailを作成する – Amazon でリソースを作成し WorkMail 、これらのリソースの代理人と予約オプションを設定できます。詳細については、リソースの使用を参照してください。
- AutoDiscover DNS レコードを作成する – 組織内のすべてのメールドメインの AutoDiscover DNS レコードを設定します。これにより、ユーザーは Microsoft Outlook とモバイルクライアントから

Amazon WorkMail メールボックスに接続できます。詳細については、「AutoDiscover を使用してエンドポイントを設定する」を参照してください。

- MX DNS レコードを Amazon に切り替える WorkMail – すべての受信 E メールを Amazon に配信するには WorkMail、MX DNS レコードを Amazon に切り替える必要があります WorkMail。DNS レコードへの変更がすべての DNS サーバーに反映されるまでに最大 72 時間かかる場合があります。
- メールサーバーを廃止する – すべての E メールが Amazon に直接ルーティングされていることを確認したら WorkMail、今後使用する予定がない場合は、メールサーバーを廃止できます。

トラブルシューティング

最も一般的に発生する Amazon の WorkMail 相互運用性と移行エラーに対するソリューションを以下に示します。

Exchange Web Services (EWS) URL が無効または接続できない – 適切な EWS URL であることを確認します。詳細については、「Amazon での可用性設定の構成 WorkMail」を参照してください。

EWS 検証時の接続エラー – 一般的なエラーです。以下のような原因が考えられます。

- Microsoft Exchange のインターネット接続がありません。
- ファイアウォールが、インターネットからのアクセスを許可するように設定されていません。ポート 443 (HTTPS リクエストのデフォルトポート) が開いていることを確認します。

インターネット接続とファイアウォール設定を確認してもエラーが解決しない場合は、AWS Support までお問い合わせください。

Microsoft Exchange の相互運用性を設定する際のユーザー名とパスワードが無効 – 一般的なエラーです。以下のような原因が考えられます。

- ユーザー名の形式が正しくありません。次のパターンを使用します。

```
DOMAIN\username
```

- お使いの Microsoft Exchange サーバーは、EWS の基本認証用に設定されていません。詳細については、Microsoft MVP アワードプログラムのブログの仮想ディレクトリ: Exchange 2013 を参照してください。

ユーザーが winmail.dat アタッチメントで E メールを受信する – これは、暗号化された S/MIME E メールが Exchange から Amazon WorkMail に送信され、Outlook 2016 for Mac または IMAP クライアントで受信された場合に発生する可能性があります。Exchange の管理シェルで次のコマンドを実行します。

Set-RemoteDomain -Identity "Default" -TNEFEnabled $false

上記のポイントを確認したが、エラーが解決しない場合は、「AWS サポート」までお問い合わせください。

Amazon WorkMail クォータ

Amazon WorkMail は、エンタープライズのお客様と小規模ビジネスオーナーの両方が使用できます。クォータの設定を変更しなくても、ほとんどのユースケースがサポートされていますが、この製品の不正使用からお客様のユーザーとインターネットを保護するために、そのため、お客様によっては、当社が設定したクォータに達する可能性があります。このセクションでは、これらのクォータとそれらの変更方法について説明します。

クォータ値には、変更できるものと、変更できないハードクォータがあります。クォータ増加の要求の詳細については、Amazon Web Services 全般のリファレンス のAWSService Quotasを参照してください。

Amazon WorkMail の組織とユーザーのクォータ

30 日間の無料トライアルでは、最大 25 人のユーザーを Amazon WorkMail 組織に追加できます。この期間が終了すると、Amazon WorkMail アカウントを削除または閉鎖しない限り、すべてのアクティブなユーザーに対して課金されます。

これらのクォータの評価時、別のユーザーに送信されるすべてのメッセージが考慮されます。これには、E メール、会議出席依頼、会議出席依頼の返信、仕事依頼のほか、ルールの結果として自動的に転送またはリダイレクトされるメッセージも含まれます。

> **Note**
>
> 特定の組織のクォータの増加をリクエストする場合は、リクエストに組織名を含める必要があります。

リソース	デフォルトのクォータ	変更リクエストの上限
AWS アカウントあたりの Amazon WorkMail 組織	100	組織のディレクトリタイプに基づいて増やすことができます。AWS Directory Service クォータと引き上げリクエストは、AWS Directory Service コンソールで表示できます。詳細については、AWS 全般のリファレンス の「ドメインのクォータ」を参照してください。
Amazon WorkMail 組織あたりのユーザー	1,000	組織のディレクトリ タイプに応じて、次のように増やすことができます。 • Amazon WorkMail ディレクトリ: 最大 1,000 万ユーザー • Simple AD または AD Connector (ラージ): 最大 5,000 ユーザー* • Simple AD または AD Connector (スモール): 最大 500 ユーザー* • AWS Directory Service がホストする Microsoft AD: セットアップと設定に応じて最大 1,000 万ユーザー、 * Simple AD または AD Connector を使用している場合、詳細については AWS Directory Service を参照してください。

リソース	デフォルトのクォータ	変更リクエストの上限
無料トライアルユーザー数	最初の 30 日間で最大 25 ユーザー	無料トライアル期間はいずれかの組織の最初の 25 ユーザーにのみ適用されます。その他のユーザーは無料トライアル期間の対象にはなりません。
宛先として指定される 1 日あたりの受取人の数 (AWS アカウントごと)	組織外の 100,000 人の受取人 (組織内の受取人にハードクォータはありません)	上限はありません。ただし、Amazon WorkMail はビジネス E メールサービスであり、一括 E メールサービスとして使用することを意図していません。バルク E メールサービスについては、Amazon SES または Amazon Pinpoint を参照してください。
いずれかのテストドメインを使用して宛先として指定される 1 日あたりの受取人の数 (AWS アカウントごと)	組織内外に関係なく 200 受信者	テストメールドメインは長期間の使用を想定していません。独自のドメインを追加してデフォルトのドメインとして使用することをお勧めします。

グループの基盤となるディレクトリによって設定されます。

WorkMail 組織設定のクォータ

リソース	デフォルトのクォータ
Amazon WorkMail 組織あたりのドメイン数	1,000 これはハードクォータであり、変更できません。

リソース	デフォルトのクォータ
ルールあたりの E メールフロールールの送信者パターンの数	250 これはハードクォータであり、変更できません。
組織あたりの E メールフロールールの送信者パターンの数	1,000 これはハードクォータであり、変更できません。

ユーザーごとのクォータ

これらのクォータの評価時、別のユーザーに送信されるすべてのメッセージが考慮されます。これには、E メール、会議出席依頼、会議出席依頼の返信、仕事依頼のほか、ルールの結果として自動的に転送またはリダイレクトされるメッセージも含まれます。

リソース	デフォルトのクォータ	変更リクエストの上限クォータ
メールボックスの最大サイズ	50 GB これはハードクォータであり、変更できません。	該当しない
ユーザーあたりの最大エイリアス数	100 これはハードクォータであり、変更できません。	該当しない
独自のドメインを使用して宛先として指定される 1 日あたりの受信者の数 (ユーザーごと)	組織外の 10,000 人の受取人 (組織内の受信者にハードクォータはありません)	上限はありません。ただし、Amazon WorkMail はビジネス E メールサービスであり、一括 E メールサービスとして使用することを意図していません。バルク E メールサービスについては、Amazon

リソース	デフォルトのクォータ	変更リクエストの上限クォータ
		SES または Amazon Pinpoint を参照してください。

メッセージのクォータ

これらのクォータの評価時、別のユーザーに送信されるすべてのメッセージが考慮されます。これには、E メール、会議出席依頼、会議出席依頼の返信、仕事依頼のほか、ルールの結果として自動的に転送またはリダイレクトされるメッセージも含まれます。

リソース	デフォルトのクォータ
受信メッセージの最大サイズ	29 MB のエンコードされていないデータ。 メッセージは MIME 形式で受信されます。受信する MIME メッセージの最大サイズは 40 MB です。 これはハードクォータであり、変更できません。
送信メッセージの最大サイズ	29 MB のエンコードされていないデータ。 メッセージは MIME 形式で送信されます。送信 MIME メッセージの最大サイズは 40 MB です。 これはハードクォータであり、変更できません。
メッセージあたりの受取人の最大数	500 これはハードクォータであり、変更できません。
メッセージあたりの添付ファイルの最大数	500

リソース	デフォルトのクォータ
	これはハードクォータであり、変更できません。

組織の使用

Amazon では WorkMail、組織は会社のユーザーを表します。Amazon WorkMail コンソールに、利用可能な組織のリストが表示されます。利用可能な がない場合は、Amazon を使用するために組織を作成する必要があります WorkMail。

トピック

組織の作成

Amazon を使用するには WorkMail、まず組織を作成する必要があります。1 つの AWS アカウントに複数の Amazon WorkMail 組織を含めることができます。組織を作成する際は、組織のドメインも選択し、ユーザーディレクトリと暗号化の設定を行います。

新しいユーザーディレクトリを作成するか、Amazon を既存のディレクトリ WorkMail と統合できます。Amazon は、オンプレミスの Microsoft Active Directory、 AWS Managed Active Directory、または Simple AD WorkMail で使用できます。をオンプレミスディレクトリと統合することで、Amazon の既存のユーザーとグループを使用でき WorkMail 、ユーザーは既存の認証情報を使用してサインインできます。オンプレミスディレクトリを使用している場合は、まず AWS Directory Service で AD Connector をセットアップする必要があります。AD Connector は、ユーザーとグループを Amazon WorkMail アドレス帳と同期させ、ユーザー認証リクエストを実行します。詳細については、AWS Directory Service 管理ガイドのアクティブディレクトリコネクターを参照してください。

また、Amazon AWS KMS keyがメールボックスコンテンツの暗号化 WorkMail に使用する を選択することもできます。Amazon のデフォルトの AWSマネージドマスターキーを選択するか WorkMail、AWS Key Management Service () で既存の KMS キーを使用できますAWS KMS。詳細については、[AWS Key Management Serviceデベロッパーガイド] の[キーの作成] を参照してください。AWS Identity and Access Management (IAM) ユーザーとしてサインインしている場合は、自身を KMS

キーの主要管理者にします。詳細については、「AWS Key Management Service デベロッパーガイド」の「キーの有効化と無効化」を参照してください。

考慮事項

Amazon WorkMail 組織を作成するときは、次の点に注意してください。

- Amazon は現在、複数のアカウントと共有しているマネージド Microsoft Active Directory サービスをサポート WorkMail していません。
- Microsoft Exchange と AD Connector を備えたオンプレミスのアクティブディレクトリを使用している場合は、組織の相互運用性設定を構成することをお勧めします。これにより、メールボックスを Amazon に移行したり WorkMail、会社のメールボックスのサブセット WorkMail に Amazon を使用したりするときに、ユーザーの中断を最小限に抑えることができます。詳細については、「Amazon WorkMail と Microsoft Exchange 間の相互運用性」を参照してください。
- 無料テストドメインオプションを選択すると、提供されたテストドメインで Amazon WorkMail 組織の使用を開始できます。テストドメインの形式は *example*.awsapps.com です。テストメールドメインは、Amazon WorkMail 組織で有効なユーザーを維持している限り、Amazon WorkMail およびその他のサポートされているAWSサービスで使用できます。ただし、テストドメインを他の目的で使用することはできません。Amazon WorkMail 組織が少なくとも 1 人の有効なユーザーを維持していない場合、テストドメインが他のお客様が登録および使用できるようになる可能性があります。
- Amazon WorkMail はマルチリージョンディレクトリをサポートしていません。

トピック

組織の作成

Amazon WorkMail コンソールで新しい組織を作成します。

組織を作成するには

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

必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。

2. ナビゲーションバーで [組織] を選択します。

   [組織] ページが表示され、組織があれば表示されます。

3. [組織を作成]を選択します。
4. [Eメールドメイン]で、組織内の E メールアドレスに使用するドメインを選択します。

   - 既存の Route 53 ドメイン — Amazon Route 53 (Route 53) ホストゾーンで管理する既存のドメインを選択します。
   - 新しい Route 53 ドメイン — Amazon で使用する新しい Route 53 ドメイン名を登録します WorkMail。
   - 外部ドメイン — 外部ドメインネームシステム（ DNS ）プロバイダで管理する既存のドメインを入力します。
   - 無料のテストドメイン — Amazon が提供する無料のテストドメインを使用します WorkMail。テストドメイン WorkMail を使用して Amazon を調べ、後で組織にドメインを追加できます。

5. (オプション) ドメインが Amazon Route 53 を介して管理されている場合は、Route 53 ドメインを選択します。
6. [エイリアス] では、組織の一意のエイリアスを入力します。
7. [詳細設定] を選択し、[ユーザーディレクトリ] で、次のいずれかのオプションを選択します。

   - 新しい Amazon WorkMail ディレクトリを作成する – ユーザーを追加および管理するための新しいディレクトリを作成します。
   - 既存のディレクトリを使用する — 既存のディレクトリを使用して、オンプレミスの Microsoft アクティブディレクトリ、AWS マネージドアクティブディレクトリ、または Simple AD などのユーザーを管理します。

8. [暗号化] で、次のいずれかのオプションを選択します。

   - Amazon WorkMail マネージドキーを使用する – アカウントに新しい暗号化キーを作成します。
   - 既存のKMS キーを使用する — AWS KMSで作成済みの既存の KMS キーを使用します。

9. [組織を作成]を選択します。

外部ドメインを使用する場合は、適切な テキスト（TXT）とメールエクスチェンジャー（MX）レコードを DNS サービスに追加して検証します。TXT レコードでは、DNS サービスに関するメモを入力できます。MX レコードは、受信メールサーバーを指定します。

ドメインを組織のデフォルトとして設定してください。詳細については、ドメインの検証 および デフォルトのドメインの選択を参照してください。

お客様の組織が [アクティブ] の場合に、ユーザーを追加し、E メールクライアントを設定できます。詳細については、ユーザーの追加「」および「Amazon の E メールクライアントの設定 WorkMail」を参照してください。

組織の詳細の表示

各 Amazon WorkMail 組織は、組織の詳細ページを表示できます。このページには、AWS Command Line Interface で使用できる ID など、組織の情報が表示されます。ページ上のメッセージには、未確認のドメインやユーザー不足など、セットアップと組織化の完了に必要な手順も表示されます。このメッセージは、特定の E メールクライアントを設定するための最初のステップも提供します。

組織の詳細を表示するには

1. ナビゲーションバーで、[組織] を選択します。

   [組織] ページが表示され、組織が表示されます。
2. 表示する組織を選択します。

Amazon WorkDocs または WorkSpaces ディレクトリの統合

Amazon WorkDocs または WorkMail で Amazon を使用するには WorkSpaces、次のステップを使用して互換性のあるディレクトリを作成します。

互換性のある Amazon WorkDocs または WorkSpaces ディレクトリを追加するには

1. Amazon WorkDocs または を使用して互換性のあるディレクトリを作成します WorkSpaces。

   a. Amazon WorkDocs の手順については、「Amazon 管理ガイド」の「クイックスタートの開始方法」を参照してください。 WorkDocs

   b. WorkSpaces 手順については、「Amazon 管理ガイド」の「Amazon WorkSpaces Quick Setup の開始方法」を参照してください。 WorkSpaces

2. Amazon WorkMail コンソールで、Amazon WorkMail 組織を作成し、既存のディレクトリの使用を選択します。詳細については、「組織の作成」を参照してください。

組織の状態と説明

組織を作成したら、その組織は以下のいずれかの状態になります。

状態	説明
[アクティブ]	組織は正常で、使用準備ができています。
[作成中]	組織の作成ワークフローを実行中です。
[失敗]	組織を作成できませんでした。
[障害]	組織は正しく機能していないか、問題が検出されました。
無効	組織は非アクティブです。
[リクエスト済み]	組織の作成リクエストがキューに入っており、作成待ちです。
検証しています	組織のすべての設定のヘルスチェックを実行中です。

組織の削除

組織の E メール WorkMail に Amazon が不要になった場合は、Amazon から組織を削除できます WorkMail。

> **Note**
>
> この操作は元に戻すことができません。組織を削除すると、メールボックスデータを回復できなくなります。

組織を削除するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. [組織] 画面の組織のリストで、削除する組織を選択してから、[削除] を選択します。
3. [組織を削除] で、組織名を入力し、既存のユーザーディレクトリを削除するか保持するかを選択したら、組織の名前を入力します。
4. 次に、[組織を削除] を選択します。

> **Note**
>
> Amazon に独自のディレクトリを指定しなかった場合は WorkMail、ディレクトリが自動的に作成されます。組織の削除時にこの既存のディレクトリを保持する場合、Amazon 、Amazon WorkMail、または で使用されていない限り WorkDocs、そのディレクトリに対して課金されます WorkSpaces。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。
> 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 管理ガイド」 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。

組織を削除しようとすると、無効な Amazon Simple Email Service (Amazon SES) ルールセットに関するエラーメッセージが表示されることがあります。このエラーが表示される場合は、Amazon SES コンソールで Amazon SES ルールを編集して、無効なルールセットを削除します。編集するルールには、ルール名に Amazon WorkMail 組織 ID が含まれている必要があります。Amazon SES ルールを編集方法については、Amazon Simple Email Service デベロッパーガイド の 受信ルールの作成 を参照してください。

どのルールセットが無効か判断する必要がある場合は、最初にルールを保存します。無効なルールセットに対してエラーメッセージが表示されます。

E メールアドレスの検索

E メールアドレスが Organization で使用されているかどうかは、ユーザー、リソース、またはグループごとに確認できます。

E メールアドレスを検索するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. 組織 ページで、E メールアドレスの検索 を選択します。
4. [検索] を選択します。

組織の設定の操作

以下のセクションでは、Amazon WorkMail Organizations で利用できる設定を使用する方法について説明します。選択した設定は、組織全体に適用されます。

トピック

- メールボックス移行を有効にする
- ジャーナリングを有効にする
- 相互運用性を有効にする
- SMTP ゲートウェイを有効にする
- E メールフローの管理
- 受信メールへの DMARC ポリシーの適用

メールボックス移行を有効にする

メールボックス移行は、Microsoft Exchange や G Suite Basic などのソースから Amazon にメールボックスを転送するときに有効にします WorkMail。移行は大規模な移行プロセスの一環として有効にします。詳細については、このガイドの「はじめに」セクションにある「Amazon への移行 WorkMail」を参照してください。

ジャーナリングを有効にする

ジャーナリングを有効化して、E メール通信を記録することができます。ジャーナリングを使用するときは、通常、統合されたサードパーティのアーカイブツールと eDiscovery ツールを使用します。これにより、データストレージ、プライバシー保護、情報保護に関する、E メールストレージのコンプライアンス規制を満たすことができます。

詳細については、このガイドの「はじめに」セクションにある「Amazon WorkMail での E メールジャーナリングの使用」を参照してください。

相互運用性を有効にする

相互運用性により、Microsoft Exchange から移行し、会社のメールボックスのサブセット WorkMail として Amazon を使用できます。詳細については、このガイドの「はじめに」セクションにある「Amazon での可用性設定の構成 WorkMail」を参照してください。

SMTP ゲートウェイを有効にする

送信 E メールフロールールで使用するように Simple Mail Transfer Protocol (SMTP) ゲートウェイを有効にします。アウトバウンド E メールフロールールを使用すると、Amazon WorkMail 組織から送信された E メールメッセージを SMTP ゲートウェイ経由でルーティングできます。詳細については、「送信 E メールルールアクション」を参照してください。

> **Note**
>
> 送信 E メールフロールール用に設定された SMTP ゲートウェイは、主要な証明機関の証明書を使用して Transport Layer Security (TLS) v1.2 をサポートしている必要があります。基本認証のみサポートされています。

SMTP ゲートウェイを設定するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。

3. ナビゲーションペインで [組織の設定] を選択します。

   「組織の設定」 ページが開き、一連のタブが表示されます。
4. [SMTP ゲートウェイ] タブを選択し、[ゲートウェイを作成] を選択します。
5. 次のように入力します。

   - [ゲートウェイ名] — 一意の名前を入力します。
   - [ゲートウェイアドレス] — ゲートウェイのホスト名または IP アドレスを入力します。
   - [ポート番号] — ゲートウェイのポート番号を入力します。
   - [ユーザー名] - ユーザー名を入力します。
   - [パスワード] — 強力なパスワードを入力してください。
6. [作成] を選択します。

   SMTP ゲートウェイは、送信 E メールフロールールで使用できます。

送信 E メールフロールールで使用するように SMTP ゲートウェイを設定すると、送信メッセージは SMTP ゲートウェイとルールを一致させようとします。ルールに一致するメッセージは、対応する SMTP ゲートウェイにルーティングされ、その SMTP ゲートウェイが残りのメール配信を処理します。

Amazon WorkMail が SMTP ゲートウェイに到達できない場合、システムは E メールメッセージを送信者にバウンスします。その場合は、前の手順に従ってゲートウェイの設定を修正してください。

E メールフローの管理

メールの管理に役立つように、メールフロールールを設定できます。電子メールフロールールは、アドレスまたはドメインに基づいてE メールメッセージに対して 1 つ以上のアクションを実行できます。送信者と受信者の両方の E メールアドレスまたはドメインに基づいたE メールフロールールを使用できます。

電子メールフロールールを作成するときは、指定したルールパターンが一致した場合にE メールに適用されるルールアクションを指定します。

トピック

- 受信 E メールルールアクション
- 送信 E メールルールアクション
- 送信者および受取人パターン

- E メールフロールールの作成
- E メールフロールールを編集
- Amazon AWS Lambda用 の設定 WorkMail
- Amazon WorkMail Message Flow API へのアクセスの管理
- E メールフロールールのテスト
- E メールフロールールの削除

受信 E メールルールアクション

受信 E メールフロールールは、望ましくない E メールがユーザーのメールボックスに届かないようにするのに役立ちます。インバウンド E メールフロールールは、ルールアクションとも呼ばれ、Amazon WorkMail 組織内のすべてのユーザーに送信されるすべての E メールメッセージに自動的に適用されます。これは、個々のメールボックスの E メールルールとは異なります。

> **Note**
>
> オプションで、ルールを AWS Lambda 関数で使用して、ユーザーのメールボックスに配信される前に受信 E メールを処理できます。Amazon での Lambda の使用の詳細については WorkMail、「」を参照してくださいAmazon AWS Lambda用 の設定 WorkMail。Lambda の詳細については、「AWS Lambda デベロッパーガイドhttps://docs.aws.amazon.com/lambda/latest/dg/welcome.html」を参照してください。

インバウンド E メールフロールールは、ルールアクションとも呼ばれ、Amazon WorkMail 組織内のすべてのユーザーに送信されるすべての E メールメッセージに自動的に適用されます。これは、個々のメールボックスの E メールルールとは異なります。

次のルールアクションは、受信メールの処理方法を定義します。各ルールで、送信者および受信者パターンと共に以下のいずれかのアクションを指定します。

[アクション]	説明
E メールを削除する	E メールメッセージは無視されます。E メールは配信されず、送信者には配信不能が通知されません。

[アクション]	説明
バウンス応答を送信する	E メールメッセージは配信されず、送信者にはバウンスメッセージで配信不能が通知されます。
迷惑メールフォルダに配信	E メールメッセージは、Amazon スパム検出システムによって元々スパムとして識別されていない場合でも、ユーザーの WorkMail スパムフォルダまたは迷惑メールフォルダに配信されます。
デフォルト値	E メールメッセージは、Amazon WorkMail スパム検出システムによってチェックされた後に配信されます。スパム E メールは迷惑メールフォルダーに配信されます。他のすべての E メールメッセージは受信トレイに配信されます。 送信者パターンの特定度が低いその他の E メールフロールールは、無視されます。ドメインベースの E メールフロールールに例外を追加するには、特定度の高い送信者パターンを持つデフォルトアクションを設定します。詳細については、「送信者および受取人パターン」を参照してください。

[アクション]	説明
迷惑メールフォルダーに配信しない	E メールメッセージは、Amazon WorkMail スパム検出システムによってスパムとして識別された場合でも、常にユーザーの受信トレイに配信されます。 **Important** デフォルトのスパム検出システムを使用しないようにすると、指定したアドレスからのリスクの高いコンテンツがユーザーに配信される可能性があります。
AWS Lambda を実行する	ユーザーの受信トレイに配信する前または配信中に、E メールメッセージを Lambda 関数に渡して処理します。

Note

受信 E メールは、まず Amazon SES に配信され、次に Amazon に配信されます WorkMail。Amazon SES が受信 E メールメッセージをブロックしている場合、ルールアクションは適用されません。例えば、既知のウイルスが検出された場合や明示的な IP フィルタリングルールのために、Amazon SES は E メールメッセージをブロックします。[デフォルト]、[迷惑メールフォルダに配信]、[迷惑メールフォルダーに配信しない] などのルールアクションには効果がありません。

送信 E メールルールアクション

送信 E メールフロールールを使用して、SMTP ゲートウェイを介して E メールを直接送信するか、指定した受信者への送信者の E メールメッセージの送信をブロックするために使用できます。SMTP ゲートウェイの詳細については、SMTP ゲートウェイを有効にする を参照してください。

送信 E メールフロールールは、E メールが送信された後に E メールメッセージを AWS Lambda 関数に渡して処理するためにも使用できます。Lambda の詳細については、AWS Lambda デベロッパーガイドを参照してください。

次のルールアクションは、送信メールの処理方法を定義します。各ルールで、送信者および受信者パターンと共に以下のいずれかのアクションを指定します。

[アクション]	説明
デフォルト値	E メールメッセージは、標準フローを介して送信されます。
E メールを削除する	E メールメッセージは削除されます。送信されず、送信者には通知されません。
バウンス応答を送信する	E メールメッセージは送信されず、送信者には管理者が E メールメッセージをブロックしたことを示すメッセージで通知されます。
SMTP ゲートウェイにルーティング	設定された SMTP ゲートウェイ経由で E メールメッセージが送信されます。
Lambda を実行する	E メールメッセージが送信される前または送信中に、E メールメッセージを Lambda 関数に渡して処理します。

送信者および受取人パターン

E メールフロールールは、特定の E メールアドレスに適用したり、特定のドメインまたは一連のドメインのすべての E メールアドレスに適用したりできます。パターンを定義して、ルールが適用される E メールアドレスを決定します。

送信者パターンと受信者パターンのどちらでも、以下のいずれかの形式が使用されます。

- E メールアドレスは、以下のように 1 つの E メールアドレスに一致します。

```
mailbox@example.com
```

- ドメイン名は、以下のようにそのドメインのすべての E メールアドレスに一致します。

```
example.com
```

- ワイルドカードドメインは、そのドメインとそのサブドメインのすべての E メールアドレスに一致します。ワイルドカードは、以下のようにドメインの前にのみ指定できます。

```
*.example.com
```

- スターは、任意のドメインのすべての E メールアドレスに一致します。

```
*
```

> **Note**
>
> この + 記号は、送信者パターンまたは受信者パターンの内部では有効ではありません。

1 つのルールに対して複数のパターンを指定できます。詳細については、受信 E メールルールアクション および 送信 E メールルールアクション を参照してください。

受信 E メールフロールールは、受信メールメッセージの Sender または From のいずれかのヘッダーがパターンに一致する場合に適用されます。Sender アドレスがあれば、まず一致します。Sender ヘッダーがなければ、または Sender ヘッダーがいずれのルールとも一致しなければ、From アドレスが一致します。E メールメッセージの受信者が複数あり、それぞれ異なるルールに一致する場合、一致した受信者に各ルールが適用されます。

送信 E メールフロールールは、受信者と、送信メールメッセージの Sender または Fromのいずれかのヘッダーがパターンに一致する場合に適用されます。E メールメッセージの受信者が複数あり、それぞれ異なるルールに一致する場合、一致した受信者に各ルールが適用されます。

複数のルールが一致する場合、特定度の最も高いルールのアクションが適用されます。たとえば、特定の E メールアドレスに対するルールはドメイン全体に対するルールよりも優先されます。複数のルールの特定度が同じ場合、最も制限の厳しいアクションが適用されます。例えば、ドロップ アクションは バウンス アクションよりも優先されます。アクションの優先順位は、受信 E メールルールアクション と 送信 E メールルールアクション に示されている順序と同じです。

> **Note**
>
> ルールを作成するとき、ドロップアクションやバウンスアクションを使用する送信者パターンが重複している場合は、注意が必要です。予期しないアクションの優先順位になって、多くの受信 E メールメッセージが配信されないことがあります。

E メールフロールールの作成

メールフロールールは、受信メールメッセージと送信メールメッセージにルールアクションを適用します。アクションは、メッセージが指定されたパターンに一致した場合に適用されます。新しい E メールフロールールはすぐに反映されます。

E メールフロールールを作成するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで [組織の設定] を選択します。

   「組織の設定」ページが開き、一連のタブが表示されます。このページから、インバウンドルールまたはアウトバウンドルールを作成できます。以下のステップでは、両方のタイプを作成する方法について説明します。

   インバウンドルールを作成するには

   1. [インバウンドルール] タブを選択してから、[ルールを編集] を選択します。
   2. [ルール名] に、一意の名前を入力します。
   3. 「アクション」で、リストを開いてアクションを選択します。リスト内の各項目には説明があり、「詳細はこちら」リンクがある項目もあります。

> **Note**
>
> Lambdaを実行 アクションを選択すると、追加のコントロールが表示されます。これらのコントロールの使用方法については、次のセクション、Amazon AWS Lambda用の設定 WorkMail を参照してください。

4. [送信者ドメインまたはアドレス] に、ルールを適用する送信者ドメインまたはアドレスを入力します。
5. [送信先ドメインまたはアドレス] に、送信先ドメインとメールアドレスを任意に組み合わせて入力します。
6. [作成] を選択します。

アウトバウンドルールを作成するには

1. [アウトバウンドルール] タブを選択し、[作成] を選択します。
2. [ルール名] に、一意の名前を入力します。
3. 「アクション」で、リストを開いてアクションを選択します。リスト内の各項目には説明があり、「詳細はこちら」リンクがある項目もあります。

> **Note**
>
> Lambdaを実行 アクションを選択すると、追加のコントロールが表示されます。これらのコントロールの使用については、次のセクション「Amazon AWS Lambda用 の設定 WorkMail」を参照してください。

4. [送信者のドメインまたはアドレス] に、有効な送信者ドメインと電子メールアドレスを任意に組み合わせて入力します。
5. [送信先ドメインまたはアドレス] に、有効な送信先ドメインと電子メールアドレスを任意に組み合わせて入力します。
6. [作成] を選択します。

作成した新しい E メールフロールールをテストできます。詳細については、「E メールフロールールのテスト」を参照してください。

E メールフロールールを編集

メールメッセージの 1 つ以上のルールアクションを変更する必要があるときはいつでも、メールフロールールを編集します。このセクションの手順は、電子メールメッセージの受信と送信に適用されます。

E メールフロールールを編集するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで [組織の設定] を選択します。

   組織の設定ページが開き、タブセットが表示されます。
4. [インバウンドルール] または [アウトバウンドルール] タブを選択します。
5. 変更するルールの横にあるラジオボタンを選択して、[編集] を選択します。
6. 必要に応じてルール内の 1 つまたは複数のアクションを変更し、[保存] を選択します。

Amazon AWS Lambda用 の設定 WorkMail

受信および送信メールフロールールの [Lambda を実行] アクションを使用して、ルールに一致する E メールメッセージを AWS Lambda 関数に渡して処理します。

Amazon の Lambda 実行アクションの次の設定から選択します WorkMail。

同期 [Lambda を実行] の設定

フロールールに一致する E メールメッセージは、送信または配信される前に処理のために Lambda 関数に渡されます。この設定を使用してメールの内容を変更します。さまざまなユースケースに合わせて、受信または送信のメールフローを制御することもできます。たとえば、Lambda 関数に渡されるルールは、機密性の高いメールメッセージの配信をブロックしたり、添付ファイルを削除したり、免責事項を追加したりできます。

非同期 [Lambda を実行] の設定

フロールールに一致する E メールメッセージは、送信または配信中の処理のために Lambda 関数に渡されます。この設定は、E メールの配信には影響せず、受信または送信の E メールメッセージのメトリクスの収集などのタスクに使用されます。

同期設定と非同期設定のどちらを選択した場合でも、Lambda 関数に渡されるイベントオブジェクトには、受信または送信の E メールイベントのメタデータが含まれます。メタデータ内のメッセージ ID を使用して、E メールメッセージの完全なコンテンツにアクセスすることもできます。詳細については、「AWS Lambda を使用したメッセージコンテンツの取得」を参照してください。E メールイベントの詳細については、Lambda イベントデータ を参照してください。

受信および送信 E メールフロールールの詳細については、E メールフローの管理 を参照してください。Lambda の詳細については、AWS Lambda デベロッパーガイドを参照してください。

> **Note**
>
> 現在、Lambda E メールフロールールは、設定されている Amazon WorkMail 組織と同じ AWS リージョンおよび 内の Lambda 関数のみを参照AWS アカウントします。

AWS Lambda for Amazon の開始方法 WorkMail

Amazon AWS Lambdaで の使用を開始するには WorkMail、 WorkMail Hello World Lambda 関数AWS Serverless Application Repositoryを からアカウントにデプロイすることをお勧めします。この関数には、お客様に必要なすべてのリソースと権限が設定されています。その他の例については、「」の「 amazon-workmail-lambda-templatesリポジトリ」を参照してください GitHub。

独自の Lambda 関数を作成することを選択した場合、AWS Command Line Interface (AWS CLI) を使用して権限を設定する必要があります。次のコマンドの例を使用するには、次の操作を行います。

- `MY_FUNCTION_NAME` の部分はお客様の Lambda 関数の名前に置き換えます。
- を Amazon WorkMail AWS リージョン`REGION`に置き換えます。利用可能な Amazon WorkMail リージョンには`us-east-1`、 (米国東部 (バージニア北部))`us-west-2`、 (米国西部 (オレゴン))、`eu-west-1` (欧州 (アイルランド)) などがあります。
- `AWS_ACCOUNT_ID` を、ご自身の 12 桁の AWS アカウント ID に置き換えます。
- を Amazon WorkMail 組織 ID `WORKMAIL_ORGANIZATION_ID`に置き換えます。これは、[組織] ページの組織のカードに記載されています。

```
aws --region REGION lambda add-permission --function-name MY_FUNCTION_NAME
--statement-id AllowWorkMail
--action "lambda:InvokeFunction"
--principal workmail.REGION.amazonaws.com
--source-arn
 arn:aws:workmail:REGION:AWS_ACCOUNT_ID:organization/WORKMAIL_ORGANIZATION_ID
```

AWS CLI の使用に関する詳細は、AWS Command Line Interface ユーザーガイドを参照してください。

同期 [Lambda を実行] ルールの設定

同期 [Lambda を実行] ルールを設定するには、[Lambda の実行] アクションを持つ E メールフロールールを作成し、[同期して実行] チェックボックスをオンにます。メールフロールールの作成の詳細については、E メールフロールールの作成 を参照してください。

同期ルールの作成を完了するには、Lambda Amazon リソースネーム (ARN) を追加し、次のオプションを設定します。

フォールバックアクション

Lambda 関数の実行に失敗した場合、Amazon のアクション WorkMail が適用されます。このアクションは、[すべての受信者] が設定されていない場合、Lambda 応答からはずされた受信者にも適用されます。[フォールバックアクション] を別の Lambda アクションにすることはできません。

[ルール] (分)

Amazon が呼び出しに WorkMail 失敗した場合に Lambda 関数が再試行される期間。[フォールバックアクション] は、この期間の終了時に適用されます。

> **Note**
>
> 同期 [Lambda を実行] ルールは、* 宛先指定の条件のみをサポートしています。

Lambda イベントデータ

Lambda 関数は、以下のイベントデータを使用してトリガーされます。データの表示は、Lambda 関数に使用されているデータプログラミング言語に応じて異なります。

```
{
    "summaryVersion": "2018-10-10",
    "envelope": {
        "mailFrom" : {
            "address" : "from@example.com"
        },
        "recipients" : [
           { "address" : "recipient1@example.com" },
           { "address" : "recipient2@example.com" }
        ]
    },
    "sender" : {
        "address" :  "sender@example.com"
    },
    "subject" : "Hello From Amazon WorkMail!",
    "messageId": "00000000-0000-0000-0000-000000000000",
    "invocationId": "00000000000000000000000000000000",
    "flowDirection": "INBOUND",
    "truncated": false
}
```

イベント JSON には、次に示すデータが含まれます。

summaryVersion

LambdaEventData のバージョン番号。LambdaEventData で後方互換性のない変更を加えた場合にのみ更新されます。

envelope

E メールメッセージのエンベロープ。次のフィールドが含まれています。

mailFrom

[送信元] アドレス。通常、E メールメッセージを送信したユーザーの E メールアドレスです。ユーザーが E メールメッセージを別のユーザーとして送信したか別のユーザーの代理で送信した場合、[mailFrom] フィールドは、実際の送信者の E メールアドレスではなく、E メールメッセージの名目上の送信者であるユーザーの E メールアドレスを返します。

受信者

受信者の E メールアドレスのリスト。Amazon WorkMail は To 、CC 、または BCC を区別しません。

> **Note**
>
> 受信 E メールフロールールの場合、このリストには、ルールを作成する Amazon WorkMail 組織内のすべてのドメインの受信者が含まれます。この Lambda 関数は、送信者からの SMTP 会話ごとに個別に呼び出され、受信者フィールドには、その SMTP 会話からの受信者がリストされます。外部ドメインの受信者は含まれません。

送信者

別のユーザーの代理で E メールメッセージを送信したユーザーの E メールアドレス。このフィールドは、E メールメッセージが別のユーザーの代理で送信された場合にのみ設定されます。

subject

E メールの件名。256 文字の制限を超えると切り捨てられます。

messageId

Amazon WorkMail Message Flow SDK の使用時に E メールメッセージの全コンテンツにアクセスするために使用される一意の ID。

invocationId

一意の Lambda 呼び出しの ID。この ID は、同じ に対して Lambda 関数が複数回呼び出された場合も変わりませんLambdaEventData。再試行を検出し、重複を避けるために使用します。

flowDirection

E メールフローの方向を示します。INBOUND または OUTBOUND のどちらかです。

truncated

件名の長さではなく、ペイロードサイズに適用されます。`true` の場合、ペイロードサイズが 128 KB の制限を超えると、受信者のリストが制限を満たすように切り捨てられます。

同期 [Lambda を実行] 応答スキーマ

同期的な Run Lambda アクションを含む E メールフロールールが受信または送信 E メールメッセージと一致する場合、Amazon は設定された Lambda 関数を WorkMail 呼び出し、応答を待ってから E メールメッセージに対してアクションを実行します。この Lambda 関数は、アクション、アクションタイプ、適用可能なパラメータ、およびアクションが適用される受信者をリストする事前定義されたスキーマに従って応答を返します。

次の例は、同期 [Lambda を実行] 応答です。応答は、Lambda 関数に使用されるプログラミング言語によって異なります。

```
{
    "actions": [
      {
        "action" : {
          "type": "string",
          "parameters": { various }
        },
        "recipients": [list of strings],
        "allRecipients": boolean
      }
    ]
}
```

レスポンス JSON には、次のデータが含まれます。

アクション

受信者に対して実行するアクション。

type

アクションタイプ。非同期 [Lambda を実行] アクションの場合、アクションタイプは返されません。

インバウンドルールのアクションタイプには、BOUNCE、DROP、DEFAULT、BYPASS_SPAM_CHECK、MOVE_TO_JUNK があります。詳細については、「受信 E メールルールアクション」を参照してください。

アウトバウンドルールのアクションタイプには、BOUNCE、DROP、DEFAULT があります。詳細については、「送信 E メールルールアクション」を参照してください。

parameters

追加のアクションパラメータ。BOUNCE アクションタイプで、bounceMessage キーおよび string 値を持つ JSON オブジェクトとしてサポートされます。このバウンスメッセージは、バウンス E メールメッセージを作成するために使用されます。

受信者

アクションを実行する必要がある E メールアドレスのリスト。元の受信者リストに含まれていない場合でも、新しい受信者を応答に追加できます。アクションに対して AllRecipients が true の場合、このフィールドは必須ではありません。

> **Note**
>
> 受信メールに対して Lambda アクションが呼び出されると、組織からの新しい受信者のみを追加できます。新しい受信者は、BCC として応答に追加されます。

allRecipients

true の場合、Lambda 応答内の別の特定のアクションの対象とならないすべての受信者にアクションを適用します。

同期 [Lambda を実行] アクション制限

Amazon が同期 Lambda アクションの Lambda 関数を WorkMail 呼び出す場合、次の制限が適用されます。

- Lambda 関数は 15 秒以内に応答します。応答しない場合、失敗した呼び出しとして扱われます。

> **Note**
>
> システムが、指定した [ルールタイムアウト] 間隔で呼び出しを再試行します。

- 最大 256 KB の Lambda 関数応答が許可されます。
- 応答では、最大 10 個の固有のアクションが許可されます。10 を超えるアクションは、設定されたフォールバックアクションの対象となります。
- 送信 Lambda 関数には、最大 500 人の受信者が許可されます。
- [ルールタイムアウト] の最大値は 240 分です。最小値の 0 が設定されている場合、Amazon がフォールバックアクション WorkMail を適用する前の再試行はありません。

同期 [Lambda を実行] アクションのエラー

エラー、無効なレスポンス、または Lambda タイムアウトが原因で Amazon が Lambda 関数を呼び出 WorkMail せない場合、Amazon はエクスポネンシャルバックオフで呼び出しを WorkMail 再試行します。これにより、ルールのタイムアウト期間が完了するまで処理速度が低下します。次に、フォールバックアクションが、E メールメッセージのすべての受信者に適用されます。詳細については、「同期 [Lambda を実行] ルールの設定」を参照してください。

同期 [Lambda を実行] 応答の例

次の例は、一般的な同期 [Lambda を実行] 応答の構造を示します。

Example : 指定した受信者を E メールメッセージから削除します。

次の例は、E メールメッセージから受信者を削除するための同期 [Lambda を実行] 応答の構造を示します。

```
{
    "actions": [
      {
        "action": {
          "type": "DEFAULT"
        },
        "allRecipients": true
      },
      {
        "action": {
          "type": "DROP"
        },
        "recipients": [
          "drop-recipient@example.com"
        ]
      }
    ]
}
```

Example : カスタム E メールメッセージでバウンスする

次の例は、カスタム E メールメッセージでバウンスするため同期 [Lambda を実行] 応答の構造を示します。

```
{
```

```
    "actions" : [
      {
        "action" : {
          "type": 'BOUNCE',
          "parameters": {
            "bounceMessage" : "Email in breach of company policy."
          }
        },
        "allRecipients": true
      }
    ]
}
```

Example : E メールメッセージに受信者を追加する

次の例は、E メールメッセージに受信者を追加するための同期 [Lambda を実行] 応答の構造を示します。これにより、E メールメッセージの [To] または [CC] フィールドは更新されません。

```
{
    "actions": [
      {
        "action": {
          "type": "DEFAULT"
        },
        "recipients": [
          "new-recipient@example.com"
         ]
      },
      {
        "action": {
          "type": "DEFAULT"
        },
        "allRecipients": true
      }
    ]
}
```

Lambda アクションを実行するための Lambda 関数を作成するときに使用するその他のコード例については、「Amazon WorkMail Lambda テンプレート」を参照してください。

Amazon での Lambda の使用に関する詳細情報 WorkMail

Lambda 関数をトリガーする E メールメッセージの完全なコンテンツにアクセスすることもできます。詳細については、「AWS Lambda を使用したメッセージコンテンツの取得」を参照してください。

AWS Lambda を使用したメッセージコンテンツの取得

Amazon の E メールフローを管理するように AWS Lambda関数を設定すると WorkMail、Lambda を使用して処理される E メールメッセージの全コンテンツにアクセスできます。Amazon 用の Lambda の使用開始の詳細については WorkMail、「」を参照してくださいAmazon AWS Lambda用の設定 WorkMail。

E メールメッセージの全コンテンツにアクセスするには、Amazon WorkMail Message Flow API の GetRawMessageContentアクションを使用します。呼び出し時に Lambda 関数に渡される E メールメッセージ ID は、API にリクエストを送信します。これを受けて、API は E メールメッセージの完全な MIME コンテンツで応答します。詳細については、「Amazon API リファレンス」の「Amazon WorkMail Message Flow」を参照してください。 WorkMail

次の例では、Python ランタイム環境を使用する Lambda 関数が、メッセージコンテンツ全体を取得する方法を示します。

> **Tip**
>
> からアカウントに Amazon WorkMail Hello World Lambda 関数AWS Serverless Application Repositoryをデプロイすることから始めると、必要なすべてのリソースとアクセス許可を持つ Lambda 関数がアカウントに作成されます。その後、ユースケースに基づいて Lambda 関数にビジネスロジックを追加できます。

```
import boto3
import email
import os

def email_handler(event, context):
    workmail = boto3.client('workmailmessageflow',
 region_name=os.environ["AWS_REGION"])
    msg_id = event['messageId']
    raw_msg = workmail.get_raw_message_content(messageId=msg_id)

    parsed_msg = email.message_from_bytes(raw_msg['messageContent'].read())
```

```
    print(parsed_msg)
```

転送中のメッセージの内容を分析する方法の詳細な例については、「」のamazon-workmail-lambda-templatesリポジトリを参照してください GitHub。

> **Note**
>
> Amazon WorkMail Message Flow API は、転送中の E メールメッセージへのアクセスにのみ使用します。メッセージは、送受信されてから 24 時間以内にのみアクセス可能です。ユーザーのメールボックス内のメッセージにプログラムでアクセスするには、IMAP や Exchange Web Services (EWS) など WorkMail、Amazon でサポートされている他のプロトコルのいずれかを使用します。

AWS Lambda を使用したメッセージコンテンツの更新

E メールフローを管理する同期AWS Lambda関数を設定したら、Amazon WorkMail Message Flow API の `PutRawMessageContent`アクションを使用して、送信中の E メールメッセージの内容を更新できます。Amazon の Lambda 関数の開始方法の詳細については WorkMail、「」を参照してください同期 [Lambda を実行] ルールの設定。API の詳細については、「 PutRawMessageContent」を参照してください。

> **Note**
>
> PutRawMessageContent API には boto3 1.17.8 が必要です。または、Lambda 関数にレイヤーを追加できます。正しい boto3 バージョンをダウンロードするには、「」の「boto」ページ GitHubを参照してください。レイヤーの追加の詳細については、関数でレイヤーの使用を設定するを参照してください。
> 以下に `"LayerArn":"arn:aws:lambda:${AWS::Region}:489970191081:layer:WorkMailLambdaLayer:2"` のレイヤーの例を示します。この例では、`${AWS::Region}` を us-east-1 など、適切な AWS リージョンで代用します。

> **Tip**
>
> Amazon WorkMail Hello World Lambda 関数を AWS Serverless Application Repository からアカウントにデプロイすることから始めると、必要なリソースとアクセス許可を持つ

Lambda 関数がアカウントに作成されます。その後、ユースケースに基づいて Lambda 関数にビジネスロジックを追加できます。

先へ進む場合、次の点に注意してください。

- GetRawMessageContent API を使用して、元のメッセージコンテンツを取得します。詳細については、AWS Lambda を使用したメッセージコンテンツの取得 を参照してください。
- 元のメッセージが表示されたら、MIME コンテンツを変更します。完了したら、メッセージをアカウントの Amazon Simple Storage Service (Amazon S3) バケットにアップロードします。S3 バケットが Amazon WorkMail オペレーションAWS アカウントと同じ を使用し、API コールと同じ AWS リージョンを使用していることを確認します。
- Amazon WorkMail がリクエストを処理するには、S3 オブジェクトにアクセスするために S3 バケットに正しいポリシーが必要です。詳細については、「Example S3 policy」を参照してください。
- PutRawMessageContent API を使用して、更新されたメッセージコンテンツを Amazon に送り返します WorkMail。

> **Note**
>
> PutRawMessageContent API は、更新されたメッセージの MIME コンテンツが RFC 標準を満たしていること、およびRawMessageContentデータ型に記載されている基準を満たしていることを確認します。Amazon WorkMail 組織への受信メールは、必ずしもこれらの基準を満たしているわけではないため、PutRawMessageContentAPI によって拒否される場合があります。このような場合の問題の修正方法の詳細については、返されたエラーメッセージを参照してください。

Example S3 ポリシーの例

```
{
    "Version": "2008-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {"Service": "workmail.REGION.amazonaws.com"
            },
```

```
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::My-Test-S3-Bucket/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "AWS_ACCOUNT_ID"
                },
                "Bool": {
                    "aws:SecureTransport": "true"
                },
                "ArnLike": {
                    "aws:SourceArn":
 "arn:aws:workmailmessageflow:REGION:AWS_ACCOUNT_ID:message/WORKMAIL_ORGANIZATION_ID/*"
                }
            }
        }
    ]
}
```

次の例は、Lambda 関数が Python ランタイムを使用して、送信中の E メールメッセージの件名を更新する方法を示しています。

```
    import boto3
    import os
    import uuid
    import email

    def email_handler(event, context):
        workmail = boto3.client('workmailmessageflow',
 region_name=os.environ["AWS_REGION"])
        s3 = boto3.client('s3', region_name=os.environ["AWS_REGION"])

        msg_id = event['messageId']
        raw_msg = workmail.get_raw_message_content(messageId=msg_id)
        parsed_msg = email.message_from_bytes(raw_msg['messageContent'].read())

        # Updating subject. For more examples, see https://github.com/aws-samples/
amazon-workmail-lambda-templates.
        parsed_msg.replace_header('Subject', "New Subject Updated From Lambda")
```

```
        # Store updated email in S3
        key = str(uuid.uuid4());
        s3.put_object(Body=parsed_msg.as_bytes(), Bucket="Your-S3-Bucket", Key=key)

        # Update the email in WorkMail
        s3_reference = {
            'bucket': "Your-S3-Bucket",
            'key': key
        }
        content = {
            's3Reference': s3_reference
        }
        workmail.put_raw_message_content(messageId=msg_id, content=content)
```

送信中のメッセージのコンテンツを分析するその他の例については、「」の amazon-workmail-lambda-templatesリポジトリを参照してください GitHub。

Amazon WorkMail Message Flow API へのアクセスの管理

AWS Identity and Access Management (IAM) ポリシーを使用して、Amazon WorkMail Message Flow API へのアクセスを管理します。

Amazon WorkMail Message Flow API は、単一のリソースタイプ、つまり転送中の E メールメッセージで動作します。送信中の各 E メールメッセージには、一意の Amazon リソースネーム (ARN) が関連付けられています。

以下の例は、送信中の E メールメッセージに関連付けられた ARN の構文を示しています。

```
arn:aws:workmailmessageflow:region:account:message/organization/context/messageID
```

前の例の変更可能なフィールドには、以下が含まれます。

- Region – Amazon WorkMail 組織の AWS リージョン。
- アカウント – Amazon WorkMail 組織の AWS アカウント ID。
- 組織 – Amazon WorkMail 組織 ID。
- コンテキスト - メッセージが組織に送信される `incoming`であるのか、それとも組織からの `outgoing`であるのかを示します。
- メッセージ ID – Lambda 関数への入力として渡される一意の E メールメッセージ ID。

以下の例には、送信中の受信 E メールメッセージに関連付けられた ARN の ID の例が含まれています。

```
arn:aws:workmailmessageflow:us-east-1:111122223333:message/m-
n1pq2345678r901st2u3vx45x6789yza/incoming/d1234567-8e90-1f23-456g-hjk7lmnop8q9
```

これらの ARNs IAM ユーザーポリシーの Resourceセクションのリソースとして使用して、転送中の Amazon WorkMail メッセージへのアクセスを管理できます。

Amazon WorkMail メッセージフローアクセスの IAM ポリシーの例

次のポリシー例では、 内のすべての Amazon WorkMail 組織のすべてのインバウンドメッセージとアウトバウンドメッセージへのフル読み取りアクセスを IAM エンティティに付与しますAWS アカウント。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent"
            ],
            "Resource": "arn:aws:workmailmessageflow:region:account:message/*",
            "Effect": "Allow"
        }
    ]
}
```

AWS アカウント に複数の組織がある場合は、1 つ以上の組織へのアクセスを制限することもできます。これは、特定の Lambda 関数を特定の組織でのみ使用する必要がある場合に便利です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent"
            ],
            "Resource":
 "arn:aws:workmailmessageflow:region:account:message/organization/*",
            "Effect": "Allow"
```

```
        }
    ]
}
```

また、組織が受信するメッセージ (incoming) か送信するメッセージ (outgoing) かによって、メッセージへのアクセスを許可するように選択することもできます。これを行うには、ARN で修飾子 incoming または outgoing を使用します。

次のポリシー例では、受信するメッセージへのアクセスのみを組織に許可します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent"
            ],
            "Resource":
 "arn:aws:workmailmessageflow:region:account:message/organization/incoming/*",
            "Effect": "Allow"
        }
    ]
}
```

次のポリシー例では、 内のすべての Amazon WorkMail 組織のすべてのインバウンドメッセージとアウトバウンドメッセージへのフル読み取りおよび更新アクセスを IAM エンティティに付与します AWS アカウント。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent",
                "workmailmessageflow:PutRawMessageContent"
            ],
            "Resource": "arn:aws:workmailmessageflow:region:account:message/*",
            "Effect": "Allow"
        }
    ]
}
```

E メールフロールールのテスト

現在のルール設定を確認するには、特定の E メールアドレスに対して設定がどのように動作するかをテストします。

E メールフロールールをテストするには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで、[組織の設定] 、[インバウンド/アウトバウンドルール] の順に選択します。
4. [構成のテスト] の横に、テストする送信者および受信者のフル E メールアドレスを入力します。
5. [テスト] を選択します。指定した E メールアドレスに対して実行されるアクションが表示されます。

E メールフロールールの削除

E メールフロールールを削除すると、変更がすぐに適用されます。

E メールフロールールを削除するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで、[組織の設定] 、[インバウンド/アウトバウンドルール] の順に選択します。
4. ルールを選択してから、[削除] を選択します。
5. 確認プロンプトで、[削除] を選択します。

受信メールへの DMARC ポリシーの適用

E メールドメインは、セキュリティのためにドメインネームシステム (DNS)レコードを使用します。スプーフィングやフィッシングなどの一般的な攻撃からユーザーを保護します。多くの場合、DNS レコードには、E メールを送信するドメイン所有者によって設定される、ドメインベースのメッセージ認証、レポート、および適合性 (DMARC) レコードが含まれます。DMARC レコードには、E メールが DMARC チェックに失敗したときに実行するアクションを指定するポリシーが含まれます。組織に送信される E メールに DMARC ポリシーを適用するかどうかを選択できます。

新しい Amazon WorkMail 組織では、DMARC の適用がデフォルトで有効になっています。

DMARC 適用を有効にするには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで [組織の設定] を選択します。組織の設定ページが表示され、一連のタブが表示されます。
4. [DMARC] タブを選択し、[編集] を選択します。
5. DMARC 強制スライダーをオンの位置に動かします。
6. DMARC 適用を有効にすると、送信者のドメイン設定に基づいて受信 E メールが削除または隔離される可能性があることを確認するの横にあるチェックボックスをオンにします。
7. [保存] を選択します。

DMARC 適用を無効にするには

- 前のセクションの手順に従い、DMARC 強制スライダーをオフの位置に移動してください。

E メールイベントのログ記録を使用した DMARC 適用の追跡

DMARC 適用を有効にすると、送信者がドメインをどのように構成したかに応じて、受信メールがドロップしたりスパムとしてマークされたりすることがあります。送信者が E メールドメインの設定を誤ると、ユーザーが正当なメールを受信できなくなることがあります。ユーザーに配信されていない E メールをチェックするには、Amazon WorkMail 組織の E メールイベントログ記録を有効に

します。こうすることで、送信者の DMARC ポリシーに基づいて除外された受信メールについて、E メールイベントログにクエリを実行できます。

E メールイベントのログ記録を使用して DMARC の適用を追跡する前に、Amazon WorkMail コンソールで E メールイベントのログ記録を有効にします。ログデータを最大限に活用するには、E メールイベントがログに記録される時間をとります。詳細と手順については、the section called “E メールイベントログ記録をオンにする” を参照してください。

E メールイベントのログ記録を使用して DMARC 適用を追跡するには

1. CloudWatch Insights コンソールの「ログ」で「インサイト」を選択します。
2. ロググループの選択 (複数可) で、Amazon WorkMail 組織のロググループを選択します。例えば、/aws/workmail/events/組織-alias などです。
3. クエリする期間を選択します。
4. 次のクエリを実行します。stats count() by event.dmarcPolicy | filter event.dmarcVerdict == "FAIL"
5. [クエリを実行] を選択します。

また、これらのイベントにカスタムメトリクスを設定することもできます。詳細については、メトリクスフィルターの作成を参照してください。

組織へのタグ付け

Amazon WorkMail 組織リソースにタグを付けると、次のことが可能になります。

- AWS Billing and Cost Management コンソールで組織を区別する。
- AWS Identity and Access Management (IAM) アクセス許可ポリシーステートメントの `Resource`要素に追加することで、Amazon WorkMail 組織のリソースへのアクセスを制御します。

Amazon WorkMail リソースレベルのアクセス許可の詳細については、「」を参照してくださいリソース。タグに基づくアクセス制御の詳細については、Amazon WorkMail タグに基づく認可 を参照してください。

Amazon WorkMail 管理者は、Amazon WorkMail コンソールを使用して組織にタグを付けることができます。

Amazon WorkMail 組織にタグを追加するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. [タグ] を選択します。
4. [組織] で、[新しいタグを追加] を選択します。
5. キー には、タグを識別する名前を入力します。
6. (オプション) [値] にタグの値を入力します。
7. (オプション) 組織にさらにタグを追加するには、ステップ 4 ~ 6 を繰り返します。最大 50 個のタグを追加できます。
8. [保存] を選択して変更を保存します。

Amazon WorkMail コンソールで組織タグを表示できます。

開発者は、AWS SDK または AWS Command Line Interface(AWS CLI) を使用して組織にタグを付けることもできます。詳細については、「Amazon WorkMail API リファレンス」または`UntagResource`「 コマンドリファレンス`TagResource`」の`ListTagsForResource`「、AWS CLI、および コマンド」を参照してください。

Amazon WorkMail コンソールを使用して、組織からタグをいつでも削除できます。

Amazon WorkMail 組織からタグを削除するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. [タグ] を選択します。
4. [組織タグ] で、削除するタグの横にある [削除] を選択します。
5. [送信] を選択して変更を保存します。

アクセスコントロールルールの使用

Amazon のアクセスコントロールルール WorkMail により、管理者は組織のユーザーとなりすましロールに Amazon へのアクセスを許可する方法を制御できます WorkMail。各 Amazon WorkMail 組織には、使用するアクセスプロトコルや IP アドレスに関係なく、組織に追加されたすべてのユーザーとなりすましロールにメールボックスアクセスを許可するデフォルトのアクセスコントロールルールがあります。管理者は、デフォルトのルールを編集または独自のルールへの置き換え、新しいルールの追加、ルールの削除を行うことができます。

> **Warning**
>
> 管理者が組織のすべてのアクセスコントロールルールを削除すると、Amazon は組織のメールボックスへのすべてのアクセスを WorkMail ブロックします。

管理者は、次の条件に基づいてアクセスを許可または拒否するアクセスコントロールルールを適用できます。

- プロトコル — メールボックスへのアクセスに使用されるプロトコル。例としては、Autodiscover 、EWS 、IMAP 、SMTP 、、ActiveSyncOutlook for Windows 、Webmail などがあります。
- IP アドレス - メールボックスにアクセスするために使用される IPv4 CIDR の範囲。
- Amazon WorkMail ユーザー – メールボックスへのアクセスに使用される組織内のユーザー。
- なりすましロール — メールボックスへのアクセスに使用される組織内のなりすましロール。詳細については、「なりすましロールの管理」を参照してください。

管理者は、ユーザーのメールボックスおよびフォルダのアクセス許可に加えて、アクセスコントロールルールを適用します。詳細については、「Amazon WorkMail ユーザーガイド」の「」および「フォルダとフォルダのアクセス許可メールボックスのアクセス許可の使用の共有」を参照してください。 https://docs.aws.amazon.com/workmail/latest/userguide/share-folders.html

> **Note**
>
> - Outlook for Windows へのアクセスを有効にする場合は、自動検出と EWS へのアクセスも有効にすることをお勧めします。
> - アクセスコントロールルールは、Amazon WorkMail コンソールまたは SDK アクセスには適用されません。代わりに AWS Identity and Access Management (IAM) ロールま

たはポリシーを使用してください。詳細については、「Amazon の Identity and Access Management WorkMail」を参照してください。

アクセスコントロールルールの作成

Amazon WorkMail コンソールから新しいアクセスコントロールルールを作成します。

新しいアクセスコントロールルールを作成するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. [管理ルールにアクセス] を選択します。
4. [ルールを作成] を選択します。
5. [説明] に、ルールの説明を入力します。
6. [効果] で、[許可] または [拒否] を選択します。これにより、次のステップで選択した条件に基づいてアクセスが許可または拒否されます。
7. [このルールは以下のリクエストに適用される] で、特定のプロトコル、IP アドレス、またはユーザーを含めるか除外するかなど、ルールに適用する条件を選択します。
8. (オプション) IP アドレス範囲またはユーザー ID を入力する場合は、[追加] を選択してルールに追加します。
9. [ルールの作成] を選択します。

アクセスコントロールルールを編集

Amazon WorkMail コンソールから新規およびデフォルトのアクセスコントロールルールを編集します。

アクセスコントロールルールを編集するには

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

必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。

2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. [管理ルールにアクセス] を選択します。
4. 編集するルールを選択します。
5. [ルールを編集] を選択します。
6. 必要に応じて、説明、効果、および条件を編集します。
7. [変更の保存] をクリックします。

> **Important**
>
> アクセスルールを変更すると、影響を受けるメールボックスが更新されたルールに従うまでに 5 分かかる場合があります。影響を受けるメールボックスにアクセスするクライアントは、その間、一貫性のない動作を示すことがあります。ただし、ルールをテストすると、すぐに正しい動作が表示されます。ルール設定の詳細については、次のセクションのステップを参照してください。

アクセスコントロールルールのテスト

組織のアクセスコントロールルールがどのように適用されるかを確認するには、Amazon WorkMail コンソールからルールをテストします。

組織のアクセスコントロールルールをテストするには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. [管理ルールにアクセス] を選択します。
4. [ルールのテスト] を選択します。
5. [コンテキストをリクエスト] で、テストするプロトコルを選択します。

6. [ソース IP アドレス] に、テストする IP アドレスを入力します。
7. [要求の実行者] では、テスト対象の [ユーザー] または [なりすましロール] を選択します。
8. テストするユーザーまたはなりすましロールを選択します。
9. [テスト] を選択します。

テスト結果が [効果] の下に表示されます。

アクセスコントロールルールの削除

Amazon WorkMail コンソールから不要になったアクセスコントロールルールを削除します。

> **Warning**
> 管理者が組織のすべてのアクセスコントロールルールを削除すると、Amazon は組織のメールボックスへのすべてのアクセスを WorkMail ブロックします。

アクセスコントロールルールを削除するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. [管理ルールにアクセス] を選択します。
4. 削除するルールを選択します。
5. [ルールを削除] を選択します。
6. [削除] を選択します。

メールボックス保持ポリシーの設定

Amazon WorkMail 組織のメールボックス保持ポリシーを設定できます。保持ポリシーは、選択した期間が経過すると、ユーザーのメールボックスから電子メールメッセージを自動的に削除します。どのメールボックスフォルダに保存ポリシーを適用するかを選択できます。また、フォルダごとに異なるアイテム保持ポリシーを設定するかどうかも選択できます。メールボックス保持ポリシーは、組

織内のすべてのユーザーメールボックス内の選択したフォルダに適用されます。ユーザーは保持ポリシーを上書きできません。

メールボックス保持ポリシーを設定するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. [保持ポリシー] を選択します。
4. [フォルダのアクション] で、ポリシーに含める各メールボックスフォルダの横にある [削除] または [完全に削除] を選択します。
5. 削除する前に、各メールボックスフォルダに E メールメッセージを保存する日数を入力します。
6. [保存] を選択します。

組織の保持ポリシーを適用するまでに、48 時間かかることをご了承ください。フォルダの削除アクションを選択すると、ユーザーは Amazon WorkMail ウェブアプリケーションおよびサポートされているクライアントから削除された E メールメッセージを復元できます。フォルダの [完全に削除] アクションを選択した場合、削除した E メールメッセージを復元することはできません。

アイテムを保存する期間は、アイテムが作成、変更、または移動された日時に基づいて決まります。たとえば、保持ポリシーが 1 年後にアイテムを削除した場合、ポリシーは、そのアイテムに対して作成または最後にアクションを実行した日から保持日数をカウントします。リテンションポリシーを実施した日付による影響はありません。

ドメインの操作

カスタムドメインを使用する WorkMail ように Amazon を設定できます。ドメインを組織のデフォルトにして、 AutoDiscover for Microsoft Outlook を有効にすることもできます。

トピック

ドメインの追加

Amazon WorkMail 組織には最大 100 個のドメインを追加できます。新しいドメインを追加すると、Amazon Simple Email Service (Amazon SES) 送信権限付与ポリシーがドメイン ID ポリシーに自動的に追加されます。これにより、Amazon WorkMail はドメインのすべての Amazon SES 送信アクションにアクセスでき、E メールをドメインにリダイレクトできます。メールを外部ドメインにリダイレクトすることもできます。

> **Note**
>
> ベストプラクティスは、<postmaster@> と <abuse@> のエイリアスをすべてのドメインへ追加することです。組織の特定のユーザーがこれらのエイリアスに送信された E メールを受信するようにする場合は、それらのエイリアスの配布グループを作成できます。

Amazon WorkMail 組織をカスタムドメインで設定するときは、ドメインの DNS レコードについて次の点に注意してください。

- MX レコードおよび自動検出 CNAME レコードの場合は、有効期限 (TTL) 値を 3600 にします。MX レコードの更新やメールボックスの移行の後に TTL を短くすることで、メールサーバーによって古い MX レコードや無効な MX レコードが使用されなくなります。
- ユーザーとディストリビューショングループを作成し、メールボックスを正常に移行したら、MX レコードを更新して Amazon への E メールの転送を開始する必要があります WorkMail。DNS レコードの更新処理には、最大で 48 時間かかる場合があります。
- DNS プロバイダによっては、DNS レコードの末尾にドメイン名が自動的に付加される場合があります。既にドメイン名が含まれているレコード (_amazonses.example.com など) を追加すると、ドメイン名が重複したレコード (_amazonses.example.com.example.com など) になる場合があります。レコード名でドメイン名の重複を避けるには、DNS レコードのドメイン名の末尾にピリオドを追加します。これは、DNSプロバイダに対して、レコード名が完全修飾されていることを示すもので、ドメイン名と関係なくなります。また、DNS プロバイダによってドメイン名が追加されないようにします。
- コピーされたレコード名にはドメイン名が含まれています。使用する DNS サービスによって、ドメイン名が既にドメインの DNS レコードに追加されている場合があります。
- DNS レコードを作成したら、Amazon WorkMail コンソールの更新アイコンを選択して、検証ステータスとレコード値を表示します。ドメインの検証の詳細については、ドメインの検証 を参照してください。
- ドメインを `MAIL FROM` ドメインとして設定することをお勧めします。 AutoDiscover for iOS デバイスを有効にするには、ドメインを`MAIL FROM`ドメインとして設定する必要があります。コンソールの [Enhance deliverability] (配信性能の向上) セクションで、`MAIL FROM` ドメインのステータスが確認できます。詳細については、「カスタムの MAIL FROM ドメインの設定」を参照してください。

ドメインを追加するには

1. にサインインAWS Management Consoleし、https://console.aws.amazon.com/workmail/ で Amazon WorkMail コンソールを開きます。
2. 必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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. ナビゲーションペインで、[Organizations] (組織) を選択し、ドメインを追加する組織の名前を選択します。
4. ナビゲーションペインで、[Domains] (ドメイン) を選択し、[Add domain] (ドメインの追加) を選択します。
5. [Add domain] (ドメインの追加) 画面で、追加するドメイン名前を入力します。ドメイン名には、基本ラテン (ASCII) 文字のみを含めることができます。

> **Note**
>
> Amazon Route 53 パブリックホストゾーンで管理されているドメインがある場合、ドメイン名を入力するときに表示されるドロップダウンメニューからそのドメインを選択できます。

6. [Add domain] (ドメインの追加) を選択します。

ページが表示され、新しいドメインの DNS レコードが一覧表示されます。ページでは、レコードを次のセクションにグループ化します。

- ドメインの所有権
- WorkMail 設定
- セキュリティの向上
- E メール配信の向上

これらの各セクションには 1 つ以上の DNS レコードが含まれ、各レコードには [Status] (ステータス) 値が表示されます。次のリストに、レコードとその使用可能なステータス値を示します。

TXT 所有権

検証済み — 解決および検証済みのレコード。

保留中 — まだ検証されていないレコード。

失敗 – 所有権を検証できません。レコードが一致しないか、または接続できません。

MX WorkMail 設定

検証済み — 解決および検証済みのレコード。

見つからない — レコードを解決できません。

不整合 — 予想されるレコードに値が一致しません。

AutoDiscover

検証済み — 解決および検証済みのレコード。

見つからない — レコードを解決できません。

不整合 — 予想されるレコードに値が一致しません。

> **Note**
>
> AutoDiscover 検証プロセスでは、正しい AutoDiscover セットアップもチェックされます。このプロセスでは、各フェーズの設定が検証されます。検証が終了すると、[Status] (ステータス) 列の [Verified] (検証済み) の横に緑色のチェックマークが表示されます。[Verified] (検証済み) にカーソルを合わせると、どのフェーズがプロセスによって検証されたかを確認できます。 AutoDiscover フェーズの詳細については、「」を参照してください AutoDiscover によるエンドポイントの設定の有効化。

DKIM CNAME

検証済み — 解決および検証済みのレコード。

保留中 — まだ検証されていないレコード。

失敗 – 所有権を検証できません。レコードが一致しないか、または接続できません。

詳細については、Amazon Simple Email Service デベロッパーガイドの Amazon SES における DKIM での E メールの認証を参照してください。

SPF TXT

検証済み — 解決および検証済みのレコード。

見つからない — レコードを解決できません。

不整合 — 予想されるレコードに値が一致しません。

SPF 検証の詳細については、「SPF での E メールの認証」を参照してください。

DMARC TXT

検証済み — 解決および検証済みのレコード。

見つからない — レコードを解決できません。

不整合 — 予想されるレコードに値が一致しません

Amazon の DMARC レコードの詳細については WorkMail、Amazon Simple Email Service デベロッパーガイドの「Amazon SES を使用した DMARC への準拠」を参照してください。

ドメインからの TXT メール

検証済み — 解決および検証済みのレコード。

保留中 — まだ検証されていないレコード。

失敗 – 所有権を検証できません。レコードが一致しないか、または接続できません。

ドメインからの MX メール

検証済み — 解決および検証済みのレコード。

見つからない — レコードを解決できません。

不整合 — 予想されるレコードに値が一致しません。

7. 次のステップでは、使用する DNS プロバイダに基づいて適切なアクションを選択します。

   Route 53 ドメインを使用する場合

   - ページの上部で、[Update all in Route 53] (Route 53 のすべてを更新) を選択します。

   別の DNS プロバイダを使用する場合

   - レコードをコピーし、DNS プロバイダに貼り付けます。レコードを一括でコピーすることも、一度に 1 つずつコピーすることもできます。レコードを一括してコピーするには、[Copy all] (すべてコピー) を選択します。これにより、DNS プロバイダにインポートできるファイルゾーンが作成されます。レコードを一度に 1 つずつコピーするには、レコード名の横にある重なり合う四角形を選択し、それぞれを DNS プロバイダに貼り付けます。

8. 各レコードの [Status] (ステータス) を更新するには、更新アイコンを選択します。これにより、Amazon でドメインの所有権と適切な設定が検証されます WorkMail。

ドメインの削除

ドメインは不要になったら削除できます。ただし、まずドメインをメールアドレスとして使用している個人またはグループを削除する必要があります。

ドメインを削除するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 全般のリファレンス」の「 リージョン名とエンドポイント」を参照してください。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ドメインのリストで、ドメイン名の横にあるチェックボックスをオンにし、[Remove] (削除) を選択します。
4. [Remove domain] (ドメインの削除) ダイアログボックスで、削除するドメインの名前を入力し、[Remove] (削除) を選択します。

デフォルトのドメインの選択

組織に関連付けられたドメインを、その組織内のユーザーおよびグループのデフォルトにすることができます。ドメインをデフォルトにしても、既存の E メールアドレスは変更されません。

ドメインをデフォルトにするには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 全般のリファレンス」の「 リージョン名とエンドポイント」を参照してください。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ドメインのリストで、使用するドメイン名の横にあるチェックボックスをオンにし、[Set as default] (デフォルトに設定) を選択します。

ドメインの検証

Amazon WorkMail コンソールでドメインを追加した後、ドメインを検証する必要があります。ドメインを検証すると、ドメインを所有していることが確認され、ドメインの E メールサービス WorkMail として Amazon が使用されます。

TXT レコードと MX レコードを DNS サービスに追加することによりドメインを検証します。TXT レコードを使用すると、DNS サービスにメモを追加できます。MX レコードは、受信メールサーバーを指定します。

Amazon SES コンソールを使用して TXT レコードと MX レコードを作成し、次に Amazon WorkMail コンソールを使用してレコードを DNS サービスに追加します。以下の手順に従ってください。

TXT レコードと MX レコードを作成するには

1. Amazon SES コンソール (https://console.aws.amazon.com/ses/) を開きます。
2. ナビゲーションペインで、[Domains] (ドメイン) を選択し、[Verify a New Domain] (新しいドメインの検証) をクリックします。

   [Verify a New Domain] (新しいドメインを検証) ダイアログボックスが表示されます。
3. [Domain] (ドメイン) ボックスで、ドメインの追加 セクションで作成したドメインの名前を入力します。
4. (オプション) DomainKeys アイデンティファイドメール (DKIM) を使用する場合は、DKIM 設定の生成チェックボックスを選択します。
5. [Verify This Domain] (このドメインを検証) を選択します。

   コンソールに TXT レコードと MX レコードのリストが表示されます。
6. TXT リストの下にある [Download Record Set as CSV] (レコードセットを CSV としてダウンロードする) リンクをクリックします。

   [Save As] (名前を付けて保存) ダイアログボックスが表示されます。ダウンロードする場所を選択し、[Save] (保存) をクリックします。
7. ダウンロードした CSV ファイルを開き、すべての内容をコピーします。

TXT レコードと MX レコードを作成したら、それらを DNS プロバイダに追加します。次のステップでは、Route 53 を使用します。別の DNS プロバイダを使用していて、レコードの追加方法がわからない場合は、プロバイダのドキュメントを参照してください。

1. AWS Management Console にサインインし、Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
2. ナビゲーションペインで [Hosted Zones] を選択します。次に、検証するドメインの横にあるラジオボタンを選択します。
3. ドメインの DNS レコードのリストから、[Import zone file] (ゾーンファイルのインポート) を選択します。
4. [Zone file] (ゾーンファイル) で、コピーしたレコードをテキストボックスに貼り付けます。テキストボックスの下にファイルのリストが表示されます。
5. リストの末尾までスクロールし、[Import] (インポート) をクリックします。

> **Note**
>
> 検証プロセスが完了するまで最大 72 時間かかることをご了承ください。

DNS サービスでの TXT レコードと MX レコードの検証

ドメインを所有していることを検証する TXT レコードが、DNS サービスに正常に追加されたことを確認します。この手順では、Windows および Linux で使用できる nslookup ツールを使用します。Linux では、dig を使用することもできます。

nslookup ツールを使用するには、最初にドメインにサービスを提供する DNS サーバーを見つける必要があります。その後、これらのサーバーに対して、TXT レコードを表示するためのクエリを実行します。DNS サーバーにはドメイン up-to-date の情報が最も多く含まれているため、ドメインの DNS サーバーをクエリできます。この情報が他の DNS サーバーに伝達されるまでに時間がかかることがあります。

nslookup を使用して DNS サービスに TXT レコードが追加されていることを確認する

1. ドメインのネームサーバーを検索します。
   a. コマンドプロント (Windows) またはターミナル (Linux) を開きます。

b. 次のコマンドを実行して、ドメインにサービスを提供しているすべてのネームサーバーを一覧表示します。*example.com*をドメインに置き換えます。

```
nslookup -type=NS example.com
```

次のステップで、これらのサーバーのいずれかをクエリします。

2. Amazon WorkMail TXT レコードが正しく追加されていることを確認します。

a. 次のコマンドを実行し、自分のドメインを *example.com* に置き換え、*ns1.name-server.net* をステップ 1。のネームサーバーに置き換えます。

```
nslookup -type=TXT _amazonses.example.com ns1.name-server.net
```

b. nslookup からの出力に表示される "text =" 文字列を確認します。この文字列が Amazon WorkMail コンソールの検証済み送信者リストのドメインの TXT 値と一致することを確認します。

次の例では、_amazonses.example.com で値が fmxqxT/icOYx4aA/bEUrDPMeax9/s3frblS+niixmqk= の TXT レコードを見つけます。レコードが正しく更新されている場合、コマンドの出力は以下のようになります。

```
_amazonses.example.com text = "fmxqxT/icOYx4aA/bEUrDPMeax9/s3frblS+niixmqk="
```

dig を使用して DNS サービスに TXT レコードが追加されていることを確認する

1. ターミナルセッションを開きます。
2. 次のコマンドを実行して、ドメインの TXT レコードを一覧表示します。*example.com*をドメインに置き換えます。

```
dig +short example.com txt
```

3. コマンドの出力TXTに続く文字列が、Amazon WorkMail コンソールの検証済み送信者リストでドメインを選択したときに表示される TXT 値と一致することを確認します。

nslookup を使用して DNS サービスに MX レコードが追加されていることを確認するには

1. ドメインのネームサーバーを見つけます。

a. コマンドプロントを開きます。

b. 次のコマンドを実行して、ドメインのすべてのネームサーバーを一覧表示します。

```
nslookup -type=NS example.com
```

次のステップで、これらのサーバーのいずれかをクエリします。

2. MX レコードが正しく追加されていることを確認します。

a. 次のコマンドを実行し、自分のドメインを *example.com* に置き換え、*ns1.name-server.net* を前のステップで特定したいずれかのネームサーバーに置き換えます。

```
nslookup -type=MX example.com ns1.name-server.net
```

b. コマンドの出力で、`mail exchange =` に続く文字列が以下のいずれかの値と一致することを確認します。

米国東部 (バージニア北部) リージョン – `10 inbound-smtp.us-east-1.amazonaws.com`

米国西部 (オレゴン) リージョン – `10 inbound-smtp.us-west-2.amazonaws.com`

欧州 (アイルランド) リージョン – `10 inbound-smtp.eu-west-1.amazonaws.com`

> **Note**
>
> `10` は MX preference 番号または優先順位を表します。

dig を使用して DNS サービスに MX レコードが追加されていることを確認する

1. ターミナルセッションを開きます。
2. 次のコマンドを実行してドメインの MX レコードを一覧表示します。

```
dig +short example.com mx
```

3. `MX` に続く文字列が、以下のいずれかの値と一致することを確認します。

米国東部 (バージニア北部) リージョン – `10 inbound-smtp.us-east-1.amazonaws.com`

米国西部 (オレゴン) リージョン – `10 inbound-smtp.us-west-2.amazonaws.com`

欧州 (アイルランド) リージョン – `10 inbound-smtp.eu-west-1.amazonaws.com`

> **Note**
>
> 10 は MX preference 番号または優先順位を表します。

ドメイン検証のトラブルシューティング

ドメインの検証に関する一般的な問題のトラブルシューティングについては、次の提案を参照してください。

TXT レコード名でのアンダースコアの使用が DNS サービスによって許可されていない

`_amazonses` を TXT レコード名から削除します。

同じドメインを複数回検証しようするが、同じ名前の TXT レコードを複数持つことができない

DNS サービスにより同じ名前を持つ複数の TXT レコードを持つことが許可されない場合は、以下のいずれかの対処法を使用します。

- (推奨) TXT レコードに複数の値を割り当てます (DNS サービスによって許可される場合)。例えば、DNS が Amazon Route 53 によって管理されている場合、次のように、同じ TXT レコードに対して複数の値を設定できます。
  1. Route 53 コンソールで、最初のリージョンのドメインを検証したときに追加した `_amazonses` TXT レコードを選択します。
  2. [Value] (値) で、最初の値の後にカーソルを置き、[Enter] キーを押します。
  3. 追加のリージョンの値を追加し、レコードセットを保存します。
- ドメインを 2 回だけ検証する必要がある場合は、その名前の `_amazonses` で TXT レコードを作成することで、ドメインを 1 回検証できます。その後、そのレコード名の `_amazonses` を使用せずに別のレコードを作成します。

Amazon WorkMail コンソールは、ドメインの検証が失敗したことを報告する

Amazon WorkMail は DNS サービスに必要な TXT レコードを見つけることができません。DNS サービスでの TXT レコードと MX レコードの検証 の手順に従って必要な TXT レコードが適切に DNS サービスに追加されていることを確認します。

DNS プロバイダが TXT レコードの末尾にドメイン名を追加した

既にドメイン名が含まれている TXT レコード (_amazonses.example.com など) を追加すると、ドメイン名が重複したレコード (_amazonses.example.com.example.com など) になる場合があります。ドメイン名の重複を避けるには、TXT レコードのドメイン名の末尾にピリオドを追加します。これにより、レコード名が完全修飾され、このドメイン名は TXT レコードに含まれていることが DNS プロバイダに示されます。

Amazon が MX レコードが不整合であると WorkMail 報告する

既存のメールサーバーから移行するときに、MX レコードが不整合 のステータスを返す可能性があります。以前のメールサーバーを指す WorkMail のではなく、Amazon を指すように MX レコードを更新します。サードパーティーの E メールプロキシが Amazon とともに使用されると、MX レコードも不整合として返されます WorkMail。この場合、不整合警告を無視しても安全です。

AutoDiscover によるエンドポイントの設定の有効化

AutoDiscover では、E メールアドレスとパスワードのみを使用して Microsoft Outlook とモバイルクライアントを設定できます。このサービスは Amazon への接続を維持し WorkMail 、エンドポイントまたは設定を変更するたびにローカル設定を更新します。さらに、 AutoDiscover を使用すると、クライアントはオフラインアドレスブック、不在アシスタント、カレンダーで空き時間を表示する機能などの追加の Amazon WorkMail 機能を使用できます。

クライアントは次の AutoDiscover フェーズを実行して、サーバーエンドポイント URLs。

- フェーズ 1 – クライアントはローカルアクティブディレクトリに対してセキュアコピープロトコル (SCP) ルックアップを実行します。クライアントがドメインに参加していない場合は、このステップ AutoDiscover をスキップします。
- フェーズ 2 – クライアントは以下の URL にリクエストを送信し、結果を検証します。これらのエンドポイントは HTTPS でのみ使用できます。
  - https://*company.tld*/autodiscover/autodiscover.xml
  - https://autodiscover.*company.tld*/autodiscover/autodiscover.xml
- フェーズ 3 – クライアントは autodiscover.company.tld に対して DNS ルックアップを実行し、得られたエンドポイントに対する非認証 GET リクエストをユーザーの E メールアドレスから送信します。サーバーが 302 リダイレクトを返した場合、クライアントは返された HTTPS エンドポイントに対して AutoDiscover リクエストを再送信します。

これらのフェーズがすべて失敗した場合、クライアントは自動的に設定されません。モバイルデバイスの手動設定については、デバイスを手動で接続するを参照してください。

Amazon にドメインを追加すると、プロバイダーに AutoDiscover DNS レコードを追加するように求められます WorkMail。これにより、クライアントは AutoDiscover プロセスのフェーズ 3 を実行できます。ただし、これらのステップは、Android の E メールアプリケーションなど、一部のモバイルデバイスでは機能しません。そのため、 AutoDiscover フェーズ 2 を手動で設定する必要がある場合があります。

次の方法を使用して、ドメインの AutoDiscover フェーズ 2 を設定できます。

(推奨) Route 53 と Amazon を使用する CloudFront

> **Note**
>
> 以下のステップでは、https://autodiscover.*company.tld*/autodiscover/autodiscover.xml のプロキシを作成する方法を示しています。https://*company.tld*/autodiscover/autodiscover.xml のプロキシを作成するには、`autodiscover.` プレフィックスを以下の手順でドメインから削除します。
> CloudFront と Route 53 を使用すると、料金が発生する可能性があります。適用可能な料金の詳細については、「Amazon CloudFront の料金」および「Amazon Route 53 の料金」を参照してください。

Route 53 と で AutoDiscover フェーズ 2 を有効にするには CloudFront

1. autodiscover.*company.tld* の SSL 証明書を取得し、AWS Identity and Access Management (IAM) または AWS Certificate Manager にアップロードします。詳細については、IAM ユーザーガイドのサーバー証明書の使用または AWS Certificate Manager ユーザーガイドの使用開始を参照してください 。
2. 新しい CloudFront ディストリビューションを作成します。
    1. で CloudFront コンソールを開きますhttps://console.aws.amazon.com/cloudfront/v4/home。
    2. ナビゲーションペインで、[Distribution] (ディストリビューション) を選択します。
    3. [Create Distribution] (ディストリビューションを作成) を選択します。
    4. [Web] (ウェブ) で [Get Started] (使用を開始) を選択します。
    5. [Origin Settings] (元の設定) で、以下の値を入力します。
        - [Origin Domain Name] (元のドメイン名) – リージョンの適切なドメイン名

- 米国東部 (バージニア北部) - **autodiscover-service.mail.us-east-1.awsapps.com**
- 米国西部 (オレゴン) - **autodiscover-service.mail.us-west-2.awsapps.com**
- 欧州 (アイルランド) – **autodiscover-service.mail.eu-west-1.awsapps.com**

- 元のプロトコルポリシー — 目的のポリシー: **Match Viewer**

> **Note**
>
> オリジンのパス は空白にしてください。[Origin ID] (オリジン ID) の自動入力値を変更しないでください。

6. [Default Cache Behavior Settings] (デフォルトのキャッシュ動作設定) で、リスト化されている設定の以下の値を選択します。
   - ビューワープロトコルポリシー: HTTPS Only (HTTPS のみ)
   - 許可される HTTP メソッド: GET、HEAD、OPTIONS、PUT、POST、PATCH、DELETE
   - 選択されたリクエストヘッダーに基づいたキャッシュ: All (すべて)
   - Cookie の転送: All (すべて)
   - クエリ文字列の転送とキャッシュ: None (Improves Caching) (なし (キャッシングが向上))
   - スムーズストリーミング: No (なし)
   - 閲覧者のアクセスを制限: No (なし)
7. [Distribution Settings] (ディストリビューション設定) で、以下の値を選択します。
   - 料金クラス: Use only US, Canada, and Europe (米国、カナダ、ヨーロッパのみを使用)
   - [Alternate Domain Names (CNAMEs)] (代替ドメイン名 (CNAME)) で、*company.tld* がドメイン名の場合は、**autodiscover.*company.tld*** または ***company.tld*** を入力してください。
   - SSL 証明書: 独自 SSL 証明書 (IAM に保存)
   - カスタム SSL クライアントのサポート: [All Clients] (すべてのクライアント) または [Only Clients that Support Server Name Indication (SNI)] (Support Server Name Indication (SNI) をサポートするクライアントのみ) を選択します。古いバージョンの Android は、後者のオプションでは動作しない可能性があります。

> **Note**
>
> [All Clients] (すべてのクライアント) を選択する場合は、[Default Root Object] (デフォルトのルートオブジェクト) を空欄のままにします。

- [Logging] (ログ記録): [On] (オン) または [Off] (オフ) を選択します。[On] (オン) にするとログ記録が有効になります。
- [Comment] (コメント) に、**`AutoDiscover type2 for autodiscover.`*`company.tld`*** と入力します。
- [Distribution State] (ディストリビューションの状態) で、[Enabled] (有効) を選択します。

8. [Create Distribution] (ディストリビューションを作成) を選択します。

3. Route 53 コンソールで、ドメイン名のインターネットトラフィックを CloudFront ディストリビューションにルーティングするレコードを作成します。

> **Note**
>
> これらのステップは、example.com の DNS レコードが Route 53 でホストされていることを前提としています。Route 53 を使用しない場合は、DNS プロバイダのマネジメントコンソールの手順に従ってください。

1. コンソールのナビゲーションペインで、[Hosted Zones] (ホストゾーン) を選択し、ドメインを選択します。
2. ドメインのリストで、使用するドメイン名を選択します。
3. [Records] (レコード) で、[Create record] (レコードの作成) を選択します。
4. [Quick create record] (レコードのクイック作成) で、以下のパラメータを設定します。
   - [Record Name] (レコード名) で、レコードの名前を入力します。
   - [Routing policy] (ルーティングポリシー) で、[Simple routing] (シンプルルーティング) を選択します。
   - [Alias] (エイリアス) スライダーを選択して、オンにします。オン状態にすると、スライダーが青に変わります。
   - [Record type] (レコードタイプ) リストで、[A - Routes traffic to an IPv4 address and some AWS resources] (A – IPv4 アドレスと一部の AWS リソースにトラフィックをルーティングします) を選択します。

- 一覧表示するトラフィックのルーティングで、 をディストリビューションする CloudFront エイリアスを選択します。
- 検索ボックスが [Route traffic to] (トラフィックのルーティング先) リストの下に表示されます。テキストボックスに CloudFrontディストリビューションの名前を入力します。検索ボックスを選択すると表示されるリストからディストリビューションを選択することもできます。

5. [Create record] (レコードを作成) を選択します。

Apache ウェブサーバーの使用

以下のステップでは、Apache ウェブサーバーを使用して https://autodiscover.*company.tld*/autodiscover/autodiscover.xml のプロキシを作成する方法を示しています。https://*company.tld*/autodiscover/autodiscover.xml のプロキシを作成するには、「autodiscover」 プレフィックスを次のステップでドメインから削除します。

Apache ウェブサーバーで AutoDiscover フェーズ 2 を有効にするには

1. SSL 対応の Apache サーバーで以下のディレクティブを実行します。

```
SSLProxyEngine on ProxyPass /autodiscover/autodiscover.xml https://autodiscover-service.mail.REGION.awsapps.com/autodiscover/autodiscover.xml
```

2. 必要に応じて、次の Apache モジュールを有効にします。方法がわからない場合は、Apache ヘルプを参照してください。

- `proxy`
- `proxy_http`
- `socache_shmcb`
- `ssl`

のテストとトラブルシューティングについては、次のセクションを参照してください AutoDiscover。

AutoDiscover フェーズ 2 のトラブルシューティング

の DNS プロバイダーを設定したら AutoDiscover、 AutoDiscover エンドポイント設定をテストできます。エンドポイントが正しく設定されている場合、エンドポイントは未承認のリクエストメッセージで応答します。

基本的な未承認リクエストを作成するには

1. ターミナルから、 AutoDiscover エンドポイントへの認証されていない POST リクエストを作成します。

   ```
   $ curl -X POST -v https://autodiscover.''company.tld''/autodiscover/
   autodiscover.xml
   ```

   エンドポイントが正しく設定されている場合は、次の例に示すように、`401 unauthorized` メッセージを返します。

   ```
   $ curl -X POST -v https://autodiscover.''company.tld''/autodiscover/
   autodiscover.xml
   ...
   HTTP/1.1 401 Unauthorized
   ```

2. 次に、実際の AutoDiscover リクエストをテストします。以下の XML コンテンツを含む `request.xml` ファイルを作成します。

   ```
   <?xml version="1.0" encoding="utf-8"?>

   <Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/mobilesync/
   requestschema/2006">
       <Request>
           <EMailAddress>testuser@company.tld</EMailAddress>
           <AcceptableResponseSchema>
               http://schemas.microsoft.com/exchange/autodiscover/mobilesync/
   responseschema/2006
           </AcceptableResponseSchema>
       </Request>
   </Autodiscover>
   ```

3. 作成した `request.xml` ファイルを使用して、エンドポイント AutoDiscover に対して認証リクエストを行います。忘れずに *`testuser@company.tld`* を有効な E メールアドレスに置き換えてください。

```
$ curl -d @request.xml -u testuser@company.tld -v https://autodiscover.company.tld/
autodiscover/autodiscover.xml
```

エンドポイントが正しく設定されている場合、レスポンスは次の例のようになります。

```
$ curl -d @request.xml -u testuser@company.tld -v https://autodiscover.company.tld/
autodiscover/autodiscover.xml

Enter host password for user 'testuser@company.tld':
<?xml version="1.0" encoding="UTF-8"?>
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/
responseschema/2006" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Response xmlns="http://schemas.microsoft.com/exchange/autodiscover/mobilesync/
responseschema/2006">
    <Culture>en:us</Culture>
    <User>
        <DisplayName>User1</DisplayName>
        <EMailAddress>testuser@company.tld</EMailAddress>
    </User>
    <Action>
        <Settings>
            <Server>
                <Type>MobileSync</Type>
                <Url>https://mobile.mail.us-east-1.awsapps.com/Microsoft-Server-
ActiveSync</Url>
                <Name>https://mobile.mail.us-east-1.awsapps.com/Microsoft-Server-
ActiveSync</Name>
            </Server>
        </Settings>
    </Action>
</Response>
```

ドメイン ID ポリシーの編集

ドメイン識別ポリシーでは、E メールアクション (E メールのリダイレクトなど) に対するアクセス許可を指定します。例えば、Amazon WorkMail 組織内の任意の E メールアドレスに E メールをリダイレクトできます。

> **Note**
>
> 2022 年 4 月 1 日以降、Amazon はAWSアカウントプリンシパルの代わりにサービスプリンシパルを使用して承認 WorkMail を開始しました。2022 年 4 月 1 日より前にドメインを追加した場合は、認証に AWS アカウントプリンシパルを使用する古いポリシーが存在する可能性があります。その場合、最新のポリシーに更新することをお勧めします。このセクションでは、方法について説明します。組織は、更新中も通常どおりメールを送信し続けます。

カスタムの Amazon SES ポリシーを使用しない場合にのみ、以下の手順に従います。カスタムの Amazon SES ポリシーを使用する場合は、自分で更新する必要があります。詳細については、このトピックで後述する「カスタムの Amazon SES サービスプリンシパルポリシー」を参照してください。

> **Important**
>
> 既存のドメインを削除しないでください。そうすると、メールサービスが中断されます。既存のドメインを再入力するだけで済みます。

ドメイン ID ポリシーを更新するには

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

   必要に応じて AWS リージョンを変更します。これを行うには、検索ボックスの右側にある [Select a region] (リージョンの選択) リストを開き、目的のリージョンを選択します。リージョンの詳細については、Amazon Web Services 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。
2. ナビゲーションペインで [Organizations] (組織) を選択し、組織の名前を選択します。
3. ナビゲーションペインで、[Domains] (ドメイン) を選択します。
4. 再入力するドメインの名前を強調表示してコピーし、Add Domain (ドメインを追加) を選択します。

   [Add source] (ソースの追加) ダイアログボックスが表示されます。
5. コピーした名前を [Domain name] (ドメイン名) ボックスに貼り付け、[Add domain] (ドメインの追加) を選択します。
6. 組織内の残りのドメインについて、手順 3～5 を繰り返します。

カスタムの Amazon SES サービスプリンシパルポリシー

カスタムの Amazon SES ポリシーを使用する場合は、この例をドメインで使用するように変更します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AuthorizeWorkMail",
      "Effect": "Allow",
      "Principal": {
        "Service": "workmail.REGION.amazonaws.com"
      },
      "Action": [
        "ses:*"
      ],
      "Resource": "arn:aws:ses:REGION:AWS_ACCOUNT_ID:identity/WORKMAIL-DOMAIN-NAME",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn":
 "arn:aws:workmail:REGION:AWS_ACCOUNT_ID:organization/WORKMAIL_ORGANIZATION_ID"
        }
      }
    }
  ]
}
```

SPF での E メールの認証

Sender Policy Framework (SPF) は、E メールのなりすましに対抗するために設計された E メールの検証標準です。なりすまし は、悪意のあるアクターから送信されたメールを、正当なユーザーが送信したメールのように見えるようにする行為です。Amazon WorkMail対応ドメインの SPF の設定については、「Amazon SES での SPF による E メールの認証」を参照してください。

カスタムの MAIL FROM ドメインの設定

デフォルトでは、Amazon は送信 E メールのドメインとして amazonses.com のサブMAIL FROMドメイン WorkMail を使用します。ドメインの DMARC ポリシーが SPF に対してのみ設定されている場合、配信が失敗する可能性があります。これを解決するには、独自のドメインを MAIL FROM

ドメインとして設定します。自分のドメインを MAIL FROM ドメインを設定する方法を知るには、Amazon Simple Email Service デベロッパーガイドのカスタム MAIL FROM ドメインの設定を参照してください。

> **Important**
>
> iOS デバイスで を有効にする場合は、カスタム MAIL FROM AutoDiscover ドメインが必要です。

カスタム MAIL FROM ドメインの詳細については、「Amazon SES でカスタム MAIL FROM ドメインをサポートするようになりました」を参照してください。

ユーザーの使用

Amazon からユーザーを作成および削除できます WorkMail。さらに、ユーザーの E メールパスワードのリセット、メールボックスクォータとデバイスアクセスの管理、メールボックス権限の制御を行うことができます。

トピック

ユーザーのリストの表示

ユーザーのリストを表示するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで、Organizations を選択し、組織の名前を選択します。
3. ナビゲーションペインで [Users (ユーザー)] を選択します。
4. さらに、ユーザー名 、表示名 、またはプライマリ E メールアドレス でユーザーをフィルタリングできます。

> **Note**
>
> 検索では大文字と小文字が区別されます。

ユーザーの追加

ユーザーを追加すると、Amazon WorkMail は自動的にユーザー用のメールボックスを作成します。ユーザーは、Amazon WorkMail ウェブアプリケーション、モバイルデバイス、または macOS や PC の Microsoft Outlook を使用して、ログインしてメールにアクセスできます。

ユーザーを追加するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで、[組織] を選択し、ユーザーを追加する組織の名前を選択します。
3. ナビゲーションペインで、ユーザー を選択し、ユーザー を追加 を選択します。

   ユーザーの追加画面が表示されます。
4. [ユーザーの詳細] の [ユーザー名] フィールドに、ユーザーの名前を入力します。名前は [メールアドレス] ボックスにも表示されます。ユーザーにユーザー名とは異なるメールアドレスを割り当てたい場合は、「メールアドレス」フィールドを編集できます。
5. (オプション) [名] ボックスと [姓] ボックスにユーザーの名と姓を入力します。
6. 「表示名」ボックスに、ユーザーの表示名を入力します。
7. E メールアドレスボックスに、E メールエイリアスを受け入れるか、別のエイリアスを入力します。
8. デフォルトでは、ユーザーはグローバルアドレスリストに表示されます。グローバルアドレスリストからユーザーを非表示にするには、グローバルアドレスリストに表示チェックボックスをオフにします。
9. リモートユーザーを選択して、リモートユーザーとしてユーザーを組織に追加します。
10. パスワード設定 で、パスワード ボックスにユーザーのパスワードを入力し、パスワードを繰り返します。

11. [ユーザーを追加] を選択します。

ユーザーの有効化

Amazon を企業の Active Directory WorkMail と統合する場合、または Simple AD ディレクトリにユーザーが既にある場合は、Amazon でそれらのユーザーを有効にできます WorkMail。また、次の手順に従って、アカウントが無効になったユーザーを再度有効にします。

ユーザーを有効にするには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで、[組織] を選択し、ドメインを追加する組織の名前を選択します。
3. ナビゲーションペインで [Users (ユーザー)] を選択します。

   ユーザーのリストが表示されます。有効、無効、システムユーザーステータスのユーザーアカウントがリストに表示されます。
4. アカウントが無効になっているユーザーのリストから、有効にするユーザーのチェックボックスを選択し、 を有効にするを選択します。

   [ユーザーを有効化] ダイアログボックスが表示されます。
5. 必要に応じて、各ユーザーのプライマリメールアドレスを確認して変更し、[有効化] を選択します。

ユーザーエイリアスの管理

ユーザーに E メールエイリアスを追加または削除できます。

E メールエイリアスをユーザーに追加するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。

2. ナビゲーションペインで、Organizations を選択し、ユーザーを追加する組織の名前を選択します。
3. ナビゲーションペインで、ユーザー を選択し、エイリアスを追加するユーザーの名前を選択します。
4. ユーザーの詳細 セクションで、エイリアス タブを選択します。
5. エイリアス タブで、エイリアスの追加 を選択します。
6. エイリアス ボックスにエイリアスを入力します。
7. エイリアスのドメインを選択します。
8. [追加] を選択します。

ユーザーから E メールエイリアスを削除するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで、Organizations を選択し、ユーザーを削除する組織の名前を選択します。
3. ナビゲーションペインで、ユーザー を選択し、エイリアスを削除するユーザーの名前を選択します。
4. ユーザーの詳細 セクションで、エイリアス タブを選択します。
5. エイリアス タブで、削除するエイリアスに対してチェックボックスをオンにします。
6. 削除するエイリアスを確認します。
7. エイリアスの削除ウィンドウで、 の削除を選択します。

ユーザーの無効化

組織内のユーザーはいつでも無効にできます。ユーザーを無効にすると、すぐにアクセスできなくなります。30 日以上無効になっているユーザーは、Amazon から受信トレイが削除されます WorkMail。

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

必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。

2. ナビゲーションペインで、[組織] を選択し、無効化するユーザーを含む組織の名前を選択します。
3. ナビゲーションペインで [Users (ユーザー)] を選択します。

   すべてのユーザーのリストが表示され、有効、無効、およびシステムユーザー状態にあるアカウントが表示されます。
4. 有効なユーザーのリストから、無効にするアカウントのチェックボックスを選択し、 の無効化を選択します。

   [ルールを無効化] ダイアログボックスが表示されます。
5. [無効化] を選択します。

ユーザー詳細の編集

ユーザーの詳細を編集するときに、以下を変更できます。

- 個人データ – 名前、E メールアドレス、電話番号、その他の個人情報。
- メールボックスのクォータ (サイズ) — クォータの範囲は 1 MB から 51,200 MB (50 GB) です。Amazon は、クォータの 90% に達したことをユーザーに WorkMail 通知します。また、ユーザーのメールボックスクォータを変更しても、料金には影響しません。料金の詳細については、「Amazon WorkMail 料金表」を参照してください。
- モバイルデバイスへのアクセス — デバイスの削除やデータ消去、デバイスの詳細の表示ができます。
- メールボックスのアクセス権 — ユーザーにメールボックスを使用する権限を付与し、メールボックスへのさまざまなレベルのアクセス権をユーザーに付与します。

> **Note**
>
> Amazon を AD Connector ディレクトリ WorkMail と統合する場合、 からこれらの詳細を編集することはできませんAWS Management Console。代わりに、アクティブディレクトリ管理ツールを使用して編集する必要があります。組織の相互運用性モードが有効な場合は、

制限が適用されます。詳細については、「相互運用性モードの制約事項」を参照してください。

ユーザーの詳細を編集するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで、[組織] を選択して、使用する組織を選択します。
3. ナビゲーションペインで [ユーザー] を選択してから、編集するユーザーの名前を選択します。

個人データを編集するには

1. [ユーザーの詳細] セクションで [編集] を選択します。
2. [ユーザーの詳細] で、必要に応じてユーザーの個人情報を入力または変更します。
3. 完了したら、[変更を保存] を選択します。

メールボックスクォータを編集するには

1. [ユーザーの詳細] で [クォータ] タブを選択し、[編集] を選択します。
2. 「メールボックスクォータの更新」ボックスに、メールボックスのサイズを入力します。**1** から **51200** までの値を入力できます。
3. [変更の保存] をクリックします。

モバイルデバイスのデータを管理するには

> **Note**
>
> モバイルデバイスを管理するには、ユーザーはまずデバイスを Amazon のインスタンスに接続する必要があります WorkMail。モバイルデバイスの接続については、「Amazon 用のモバイルデバイスクライアントのセットアップ WorkMail」を参照してください。

1. [ユーザー詳細] で [モバイルデバイス] タブを選択します。
2. 現在のデバイスリストを表示するには、[更新] を選択します。
3. デバイスの詳細を表示するには、デバイス ID 列からデバイス名を選択します。
4. デバイスを削除またはワイプするには、デバイス名の横にあるラジオボタンを選択し、必要に応じて [削除] または [ワイプ] を選択します。
5. 表示されたダイアログボックスで、削除または消去操作を確認します。ユーザーは、デバイスを Amazon と WorkMail 再度同期すると再び表示されることに注意してください。

メールボックスのアクセス許可を編集するには

1. [アクセス許可] タブを選択します。
2. 次のいずれかを実行します。

    1. 権限を追加するには、[権限を追加] を選択します。[新しい権限の追加] リストを開いてユーザーまたはグループを選択し、ユーザーまたはグループの権限設定を選択して、[保存] を選択します。
    2. ユーザー権限を編集するには、ユーザー名の横にあるボタンを選択します。[編集] を選択し、4 つのオプションをすべて選択して、次に [保存] を選択します。

    権限オプションの詳細については、「メールボックスのアクセス許可の使用」を参照してください。
3. すべての権限を削除するには、[削除] を選択し、削除を確定します。

ユーザーパスワードのリセット

ユーザーがパスワードを忘れた場合や、Amazon へのサインインに問題がある場合は WorkMail、パスワードをリセットできます。

> **Note**
>
> Amazon を AD Connector ディレクトリ WorkMail と統合している場合は、Active Directory でユーザーパスワードをリセットする必要があります。

ユーザーのパスワードをリセットするには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで [Users (ユーザー)] を選択します。
4. ユーザーのリストで、ユーザーの名前の横にあるチェックボックスを選択し、パスワードをリセット を選択します。
5. [パスワードをリセット] ダイアログボックスで、新しいパスワードを入力し、[リセット] を選択します。

Amazon WorkMail パスワードポリシーのトラブルシューティング

パスワードのリセットが成功しない場合は、新しいパスワードがパスワードポリシーの要件を満たしていることを確認します。

パスワードポリシーの要件は、Amazon WorkMail 組織が使用するディレクトリタイプによって異なります。

Amazon WorkMail ディレクトリと Simple AD ディレクトリのパスワードポリシー

デフォルトでは、Amazon WorkMail ディレクトリまたは Simple AD ディレクトリのパスワードは次の条件を満たす必要があります。

- 空ではない。
- 8 文字以上である。
- 64 文字未満である。
- 基本ラテン文字または Latin-1 supplement 文字で構成される。

パスワードは、以下の 5 種類のグループのうち 3 種類の文字を含んでいる必要があります。

- 英大文字

- 英小文字
- 数字 (0 ~ 9)
- 特殊文字 (<、~、または ! など)
- Latin-1 supplement 文字 (é、ü、または ñ など)

Amazon WorkMail ディレクトリのパスワードポリシーは変更できません。

Simple AD パスワードポリシーを変更するには、Simple AD ディレクトリの Amazon Elastic Compute Cloud (Amazon EC2) Windows インスタンスにある AD 管理ツールを使用します。詳細については、AWS Directory Service 管理ガイドのアクティブディレクトリ管理ツールのインストールを参照してください。

AWS Managed Microsoft AD ディレクトリのパスワードポリシー

AWS Managed Microsoft AD ディレクトリのデフォルトのパスワードポリシーに関する詳細は、AWS Directory Service 管理ガイドの AWS Managed Microsoft AD のパスワードポリシーを管理するを参照してください。

AD Connector パスワードポリシー

AD Connector は接続するアクティブディレクトリドメインのパスワードポリシーを使用します。パスワードポリシー設定の詳細については、Active Directory ドメインのマニュアルを参照してください。

通知の使用

Amazon WorkMail Push Notifications API を使用すると、新しい E メールやカレンダーの更新など、メールボックスの変更に関するプッシュ通知を受け取ることができます。通知を受け取るには、URL (またはプッシュ通知のレスポンダ) を登録する必要があります。この機能を使用すると、アプリケーションに WorkMail ユーザーのメールボックスからの変更がすぐに通知されるため、デベロッパーは Amazon ユーザー用のレスポンシブアプリケーションを作成できます。

詳細については、Exchange の通知サブスクリプション、メールボックスイベント、および EWS を参照してください。

メールボックスの変更イベント (NewMail、作成済み、変更済みを含む) について、受信トレイやカレンダーなど特定のフォルダ、またはすべてのフォルダをサブスクライブできます。

EWS Java API やマネージド EWS C# API などのクライアントライブラリを使用して、この機能にアクセスできます。AWS Lambda と API Gateway (AWS Serverless フレームワークを使用) を使用して開発されたプッシュレスポンダーの完全なサンプルアプリケーションは、AWS GitHub ページにあります。これには EWS Java API が使用されています。

プッシュサブスクリプションのリクエストの例を次に示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:t="http://
schemas.microsoft.com/exchange/services/2006/types">
   <soap:Body>
      <m:Subscribe xmlns:m="http://schemas.microsoft.com/exchange/services/2006/
messages">
         <m:PushSubscriptionRequest>
            <t:FolderIds>
               <t:DistinguishedFolderId Id="inbox" />
            </t:FolderIds>
            <t:EventTypes>
               <t:EventType>NewMailEvent</t:EventType>
               <t:EventType>CopiedEvent</t:EventType>
               <t:EventType>CreatedEvent</t:EventType>
               <t:EventType>DeletedEvent</t:EventType>
               <t:EventType>ModifiedEvent</t:EventType>
               <t:EventType>MovedEvent</t:EventType>
            </t:EventTypes>
            <t:StatusFrequency>1</t:StatusFrequency>
            <t:URL>https://YOUR_PUSH_RESPONDER_URL</t:URL>
         </m:PushSubscriptionRequest>
      </m:Subscribe>
   </soap:Body>
</soap:Envelope>
```

サブスクリプションのリクエスト結果の成功例を次に示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance">
   <Header xmlns="http://schemas.xmlsoap.org/soap/envelope/">
      <ServerVersionInfo xmlns="http://schemas.microsoft.com/exchange/
services/2006/types" MajorVersion="14" MinorVersion="2" MajorBuildNumber="390"
 Version="Exchange2010_SP2" MinorBuildNumber="3" />
```

```
   </Header>
   <soap:Body>
      <m:SubscribeResponse xmlns:m="http://schemas.microsoft.com/exchange/
services/2006/messages" xmlns:t="http://schemas.microsoft.com/exchange/services/2006/
types">
         <m:ResponseMessages>
            <m:SubscribeResponseMessage ResponseClass="Success">
               <m:ResponseCode>NoError</m:ResponseCode>
               <m:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</m:SubscriptionId>
               <m:Watermark>AAAAAAA=</m:Watermark>
            </m:SubscribeResponseMessage>
         </m:ResponseMessages>
      </m:SubscribeResponse>
   </soap:Body>
</soap:Envelope>
```

その後、通知はサブスクリプションリクエストで指定された URL に送信されます。通知の例を次に示します。

```
<soap:Envelope
    xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Header>
        <t:RequestServerVersion
            xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types"
            xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages"
 Version="Exchange2010_SP2">
        </t:RequestServerVersion>
    </soap:Header>
    <soap:Body>
        <m:SendNotification
            xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types"
            xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
            <m:ResponseMessages>
                <m:SendNotificationResponseMessage ResponseClass="Success">
                    <m:ResponseCode>NoError</m:ResponseCode>
                    <m:Notification>
                        <t:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</
t:SubscriptionId>
                        <t:PreviousWatermark>ygwAAAAAAAA=</t:PreviousWatermark>
                        <t:MoreEvents>false</t:MoreEvents>
                        <t:ModifiedEvent>
                            <t:Watermark>ywwAAAAAAAA=</t:Watermark>
                            <t:TimeStamp>2018-02-02T15:15:14Z</t:TimeStamp>
```

```
                            <t:FolderId Id="AAB2L089bS1kNDgxOGYwOGE5OTQ0="></
t:FolderId>
                            <t:ParentFolderId Id="AAB2L089bS1kNDgxOGYwOGE="></
t:ParentFolderId>
                        </t:ModifiedEvent>
                    </m:Notification>
                </m:SendNotificationResponseMessage>
            </m:ResponseMessages>
        </m:SendNotification>
    </soap:Body>
</soap:Envelope>
```

プッシュ通知レスポンダが通知を受信したことを認識するには、以下のように応答する必要があります。

```
<?xml version="1.0"?>
  <s:Envelope xmlns:s= "http://schemas.xmlsoap.org/soap/envelope/">
    <s:Body>
      <SendNotificationResult xmlns="http://schemas.microsoft.com/exchange/
services/2006/messages">
        <SubscriptionStatus>OK</SubscriptionStatus>
      </SendNotificationResult>
    </s:Body>
  </s:Envelope>
```

プッシュ通知の受信をサブスクリプション解除するには、クライアントは SubscriptionStatus フィールドでサブスクリプション解除レスポンスを送信する必要があります。その例を次に示します。

```
<?xml version="1.0"?>
  <s:Envelope xmlns:s= "http://schemas.xmlsoap.org/soap/envelope/">
    <s:Body>
      <SendNotificationResult xmlns="http://schemas.microsoft.com/exchange/
services/2006/messages">
        <SubscriptionStatus>Unsubscribe</SubscriptionStatus>
      </SendNotificationResult>
    </s:Body>
  </s:Envelope>
```

プッシュ通知レスポンダーの正常性を検証するために、Amazon は「ハートビート」(とも呼ばれます) WorkMail を送信しますStatusEvent。送信される頻度は、初期サブスクリプショ

ンリクエストで指定されている StatusFrequency パラメータによって決まります。例えば、StatusFrequency が **1** に等しい場合、1 分ごとに StatusEvent が送信されます。この値は 1 ~ 1440 分の範囲で指定できます。この StatusEvent は次のようになります。

```
<?xml version="1.0 (http://www.w3.org/TR/REC-xml/)" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Header>
    <t:RequestServerVersion xmlns:t="http://schemas.microsoft.com/exchange/
services/2006/types" xmlns:m="http://schemas.microsoft.com/exchange/services/2006/
messages" Version="Exchange2010_SP2"/>
</soap:Header>
<soap:Body>
    <m:SendNotification xmlns:t="http://schemas.microsoft.com/exchange/services/2006/
types" xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
    <m:ResponseMessages>
        <m:SendNotificationResponseMessage ResponseClass="Success">
            <m:ResponseCode>NoError</m:ResponseCode>
            <m:Notification>
                <t:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</t:SubscriptionId>
                <t:PreviousWatermark>AAAAAAAAAAA=</t:PreviousWatermark>
                <t:MoreEvents>false</t:MoreEvents>
                <t:StatusEvent>
                    <t:Watermark>AAAAAAAAAAA=</t:Watermark>
                </t:StatusEvent>
            </m:Notification>
        </m:SendNotificationResponseMessage>
    </m:ResponseMessages>
</m:SendNotification>
</soap:Body>
</soap:Envelope>
```

クライアントのプッシュ通知レスポンダが応答しない場合 (前と同じ OK ステータス)、最大 StatusFrequency 数分にわたって通知が再試行されます。例えば、StatusFrequency が 5 に等しく、最初の通知が失敗した場合、最大 5 分にわたり通知が再試行され、再試行の間に工クスポネンシャルパックオフが行われます。再試行時間の有効期限が切れた後でも通知が配信されない場合、サブスクリプションは無効になり、新しい通知は配信されません。メールボックスイベントについての通知を引き続き受信するには、新しいサブスクリプションを作成する必要があります。現時点では、メールボックスあたり最大 3 つのサブスクリプションにサブスクライブできます。

署名または暗号化された E メールの有効化

S/MIME を使用すると、組織内外の署名または暗号化された E メールをユーザーが送信できるようになります。

> **Note**
>
> グローバルアドレス一覧 (GAL) のユーザー証明書は、接続されているアクティブディレクトリセットアップでのみサポートされています。

暗号化または署名された E メールをユーザーが送信できるようにするには

1. アクティブディレクトリ (AD) Connector をセットアップします。オンプレミスディレクトリに AD Connector をセットアップすると、ユーザーは既存の社内認証情報を引き続き使用できます。
2. ユーザー証明書を自動的に発行してアクティブディレクトリに保存するように、Certificate Autoenrollment を設定します。Amazon WorkMail は Active Directory からユーザー証明書を受け取り、GAL に発行します。詳細については、証明書の自動登録を設定するを参照してください。
3. 生成された証明書を、Microsoft Exchange を実行しているサーバーからエクスポートしてメールで送信することで、ユーザーに配布します。
4. 各ユーザーは E メールプログラム (Windows Outlook など) とモバイルデバイスに証明書をインストールします。

グループの使用

グループを Amazon のディストリビューションリストとして使用 WorkMail して、<sales@example.com> や <support@example.com> などの一般的な E メールアドレスの E メールを受信できます。グループに複数の E メールのエイリアスを作成できます。

また、グループをセキュリティグループとして使用し、メールボックスやカレンダーを特定のチームと共有することもできます。

グループには独自のメールボックスがないため、グループに付与できるメールボックスの権限に影響します。メールボックスアクセス権限の設定については、メールボックスへのグループのアクセス許可の管理 を参照してください。

> **Note**
>
> 新しく追加されたグループが Microsoft Outlook のオフラインアドレス帳に表示されるまで、最大 2 時間かかることがあります。

トピック

グループのリストの表示

グループのリストを表示するには

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

必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。

2. ナビゲーションペインで、Organizations を選択し、組織の名前を選択します。
3. ナビゲーションペインで、[グループ] を選択します。
4. さらに、グループ名またはプライマリ E メールアドレス でグループをフィルタリングできます。

> **Note**
>
> 検索では大文字と小文字が区別されます。

グループの追加

Amazon WorkMail コンソールからグループを追加できます。

グループを追加するには

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

   コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで、グループ を選択し、グループ を追加 を選択します。

   グループの追加ページが表示されます。
4. [グループ名]で、グループ名を入力します。
5. [メールアドレス] に、グループのプライマリメールアドレスを入力します。
6. グループの E メールアドレスを確認し、必要に応じて更新します。
7. デフォルトでは、グループはグローバルアドレスリストに表示されます。グローバルアドレスリストからグループを非表示にするには、グローバルアドレスリストに表示チェックボックスをオフにします。
8. [Add Group (グループの追加)] を選択します。

グループの有効化

Amazon を企業の Active Directory WorkMail と統合する場合、またはシンプルな Active Directory で使用可能なグループがすでにある場合は、それらのグループを Amazon のセキュリティグループまたはディストリビューションリストとして使用できます WorkMail。

既存のディレクトリグループを有効にするには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで、[グループ] を選択します。
4. 有効にするグループの横にあるチェックボックスを選択し、 を有効にするを選択します。

   グループを有効化 ダイアログボックスが表示され、操作の確認を求められます。
5. 必要に応じて、各グループのプライマリ E メールアドレスを確認して変更し、 を有効にするを選択します。

グループへのメンバーの追加

Amazon WorkMail グループを作成して有効にしたら、Amazon WorkMail コンソールを使用してそのグループにメンバーを追加します。

> **Note**
>
> Amazon WorkMail が接続された Active Directory サービスまたは Microsoft Active Directory と統合されている場合は、Active Directory を使用してグループメンバーを管理できます。ただし、変更が Amazon に反映されるまでに時間がかかる場合があります WorkMail。

グループにメンバーを追加するには

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

必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。

2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで、[グループ] を選択します。
4. グループの名前を選択します。
5. グループの詳細ページで、メンバータブを選択します。
6. グループまたはユーザー で追加するグループまたはユーザーを選択します。
7. ドロップダウンからユーザーまたはグループを選択します。
8. [保存] を選択します。

変更が反映されるまで数分かかる場合があります。

グループの詳細の編集

グループの詳細を編集できます。

グループの詳細を編集するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで、グループ を選択し、編集するグループを選択します。
4. グループの詳細ページで、必要に応じて E メールアドレスを更新します。
5. デフォルトでは、グループはグローバルアドレスリストに表示されます。グローバルアドレスリストからグループを非表示にするには、グローバルアドレスリストに表示チェックボックスをオフにします。
6. [変更の保存] をクリックします。

グループからメンバーを削除する

Amazon WorkMail コンソールを使用して、グループからメンバーを削除します。

> **Note**
>
> Amazon WorkMail が接続された Active Directory または Microsoft Active Directory と統合されている場合は、Active Directory を使用してグループメンバーを管理できます。ただし、そうすることで、変更を Amazon に伝達するのに必要な時間を作成できます WorkMail。

グループからメンバーを削除するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで、[グループ] を選択してから、グループ名を選択します。
4. グループの詳細ページで、メンバータブを選択します。
5. グループから削除するメンバーを選択します。
6. [削除] を選択します。

変更が反映されるまで数分かかる場合があります。

グループエイリアスの管理

グループに E メールエイリアスを追加または削除できます。

E メールエイリアスをグループに追加するには。

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。

2. ナビゲーションペインで Organizations を選択し、エイリアスを追加する組織の名前を選択します。
3. ナビゲーションペインで、グループ を選択し、エイリアスを追加するグループの名前を選択します。
4. グループの詳細 セクションで、エイリアス を選択します。
5. エイリアス で、エイリアスの追加 を選択します。
6. エイリアス ボックスにエイリアスを入力します。
7. エイリアスのドメインを選択します。
8. [追加] を選択します。

グループから E メールエイリアスを削除するには。

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで Organizations を選択し、エイリアスを削除する組織の名前を選択します。
3. ナビゲーションペインでグループ を選択し、エイリアスを削除するグループの名前を選択します。
4. グループの詳細 セクションで、エイリアス を選択します。
5. エイリアス で、削除するエイリアスに対してチェックボックスをオンにします。
6. [削除] を選択します。
7. 削除するエイリアスを確認します。
8. エイリアスの削除ウィンドウで、 の削除を選択します。

グループの無効化

不要になったグループは無効にすることができます。

グループを無効にするには

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

必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。

2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで、[グループ] を選択します。
4. グループ名 で、無効にするグループを選択し、次に の無効化 を選択します。
5. [Disable group(s)] (グループを無効化) ダイアログボックスで、[Disable] (無効) を選択します。

グループの削除

グループを削除する前に、グループを無効にする必要があります。グループ の無効化の詳細については、「グループの無効化」を参照してください。

グループを削除するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで、[グループ] を選択します。
4. 削除する無効化されたグループの横にあるチェックボックスを選択し、削除を選択します。

   削除ダイアログボックスが表示されます。
5. グループ名を入力して削除を確定ボックスに、グループ名を入力し、削除を選択します。

> **Note**
>
> グループを完全に削除するには、Amazon の `DeleteGroup` API アクションを使用します WorkMail。詳細については、「Amazon WorkMail API リファレンスDeleteGroup」の「」を参照してください。

リソースの使用

Amazon WorkMail は、ユーザーがリソースを予約するのに役立ちます。たとえば、ユーザーは会議室や、プロジェクター、電話、車などの機器を予約できます。リソースを予約するには、ユーザーがそのリソースを会議出席依頼に追加します。

トピック

リソースのリストの表示

リソースのリストを表示するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで、Organizations を選択し、組織の名前を選択します。
3. ナビゲーションペインで、[リソース] を選択します。
4. さらに、リソース名またはプライマリ E メールアドレス でリソースをフィルタリングできます。

> **Note**
>
> 検索では大文字と小文字が区別されます。

リソースの追加

新しいリソースを組織に追加し、ユーザーがそれを予約できるようにすることができます。

リソースを追加するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで、リソース を選択し、リソース を追加します。

   「リソースを追加」ページが表示されます。
4. [リソース名] ボックスに、リソースの名前を入力します。
5. [リソースの説明] ボックスに、リソースの説明を入力します。
6. 「リソースタイプ」でオプションを選択します。
7. リソースの E メールアドレスを確認し、必要に応じて更新します。
8. デフォルトでは、リソースはグローバルアドレスリストに表示されます。グローバルアドレスリストからリソースを非表示にするには、グローバルアドレスリストで表示チェックボックスをオフにします。
9. [Add resource] (リソースを追加) を選択します。

リソースの詳細を編集する

名前、説明、タイプ、E メールアドレス、予約オプション、代理人など、リソースの一般的な詳細を編集できます。

リソースの一般的な詳細を編集するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。

2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで [リソース] を選択してから、編集するリソースを選択します。
4. リソースの詳細ページで、必要に応じてリソース名 、説明 、リソースタイプ 、または E メールアドレスを更新します。
5. デフォルトでは、リソースはグローバルアドレスリストに表示されます。グローバルアドレスリストからリソースを非表示にするには、グローバルアドレスリストで表示チェックボックスをオフにします。
6. [変更の保存] をクリックします。

予約リクエストを自動的に承諾または拒否するようにリソースを設定できます。

リソースの予約オプションを編集できます。

リソースの予約オプションを変更するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで [リソース] を選択してから、編集するリソースを選択します。ページが表示され、リソースの詳細が表示されます。
4. 下向きのオプションで、編集を選択します。
5. 必要に応じて、オプションの横にあるチェックボックスを選択またはオフにして、オプションを有効または無効にします。

> **Note**
>
> 自動予約オプションのいずれかを無効にした場合は、予約リクエストを処理する代理人を作成する必要があります。次のステップでは、デリゲートの作成方法を説明します。

代理人を追加して、自動予約オプションが設定されていないリソースの予約リクエストを管理できます。リソース代理人は、すべての予約リクエストのコピーを自動的に受信し、リソースカレンダーへ

のフルアクセスが許可されます。また、リソースのすべての予約リクエストを承諾する必要があります。

リソース代理人を追加するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで、[リソース] を選択し、デリゲートを追加するリソースの名前を選択します。
4. (オプション) オプション タブで、編集 を選択し、すべてのリソースリクエストを自動的に受け入れる チェックボックスをオフにしてから、保存 を選択します。
5. 「委任」タブを選択し、「代理人を追加」を選択します。

   [ソースを追加] ダイアログボックスが表示されます。
6. 「代理人を検索」リストを開いて代理人を選択し、「保存」を選択します。

リソースの代理人を削除するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで、Organizations を選択し、代理人を削除する組織の名前を選択します。
3. ナビゲーションペインで、リソース を選択し、代理人を削除するリソースの名前を選択します。
4. 委任 を選択し、削除する代理人を選択します。
5. の削除を選択します。

リソースエイリアスの管理

リソースに E メールエイリアスを追加または削除できます。

リソースにメールエイリアスを追加するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで Organizations を選択し、エイリアスを追加する組織の名前を選択します。
3. ナビゲーションペインで、リソース を選択し、エイリアスを追加するリソースの名前を選択します。
4. リソースの詳細 セクションで、エイリアス を選択します。
5. エイリアス で、エイリアスの追加 を選択します。
6. エイリアス ボックスにエイリアスを入力します。
7. エイリアスのドメインを選択します。
8. [追加] を選択します。

リソースから E メールエイリアスを削除するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで Organizations を選択し、エイリアスを削除する組織の名前を選択します。
3. ナビゲーションペインで、リソース を選択し、エイリアスを削除するリソースの名前を選択します。
4. リソースの詳細 セクションで、エイリアス を選択します。
5. エイリアス で、削除するエイリアスに対してチェックボックスをオンにします。
6. [削除] を選択します。

7. 削除するエイリアスを確認します。
8. エイリアスの削除ウィンドウで、 の削除を選択します。

リソースを有効にする。

デフォルトでは、Amazon WorkMail はリソースを作成します。ユーザーまたは他の誰かがリソースを無効にした場合、30 日以内にリソースを再度有効にできます。

リソースを有効にするには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。リージョンの詳細については、Amazon Web Services 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。
2. ナビゲーションペインで、[組織] を選択し、有効化するリソースを含む組織の名前を選択します。
3. ナビゲーションペインで、[リソース] を選択します。
4. リソースの一覧から、有効にするリソースの横にあるボタンを選択し、[有効化] をクリックします。

   [リソースを有効化] ダイアログボックスが表示されます。
5. [Enable (有効化)] を選択します。

リソースを無効にする。

リソースを無効にすると、そのリソースは予約できなくなります。たとえば、改装中は会議室を無効にし、使用可能になったら会議室を有効にすることができます。

リソースを無効にするには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。リージョンの詳細について

は、Amazon Web Services 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。

2. ナビゲーションペインで、[組織] を選択し、無効化するリソースを含む組織の名前を選択します。
3. ナビゲーションペインで、[リソース] を選択します。
4. リソースの一覧から、無効にするリソースの横にあるボタンを選択し、[無効化] をクリックします。

   [ルールの無効化] ダイアログボックスが表示されます。
5. [無効化] を選択します。

リソースの削除

不要になったリソースは削除できます。ただし、最初にリソースを無効にする必要があります。リソースを無効化する方法については、前のセクションのステップを参照してください。

リソースを削除するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。リージョンの詳細については、Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、希望する組織を選択します。
3. ナビゲーションペインで、[リソース] を選択します。
4. リソースの一覧から、無効にするリソースの横にあるボタンを選択し、[削除] をクリックします。

   [ルールを削除] ダイアログボックスが表示されます。
5. 「削除を確認するリソース名を入力してください」ボックスに、削除するリソースの名前を入力し、「リソースを削除」を選択します。

モバイルデバイスの使用

このセクションのトピックでは、Amazon に接続されたモバイルデバイスを管理する方法について説明します WorkMail。

トピック

組織のモバイルデバイスポリシーの編集

組織のモバイルデバイスポリシーを編集して、モバイルデバイスがAmazonとやり取りする方法を変更できます WorkMail。

組織のモバイルデバイスポリシーを編集するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 全般のリファレンス」の「 リージョン名とエンドポイント」を参照してください。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで、[モバイルポリシー] を選択します。続いて、[モバイルポリシー 画面で、[編集] を選択します。
4. 必要に応じて以下のいずれかを更新します。

   a. [デバイスで暗号化が必要]: モバイルデバイス上の E メールデータの暗号化を必須にします。

   b. [ストレージカードで暗号化が必要]: モバイルデバイスのリムーバブルストレージ上の E メールデータの暗号化を必須にします。

   c. [パスワードが必要]: モバイルデバイスをロックするためのパスワードを必須にします。

d. [簡単なパスワードを許可]: デバイスの PIN をパスワードとして使用します。

e. [最小パスワード長]: 有効なパスワードに必要な文字の最小数を設定します。

f. [英数字パスワードが必要]: パスワードが文字と数字で構成されていることを必須にします。

g. 許可される失敗回数:デバイスのロック解除に失敗した回数を指定します。この回数を超えると、ユーザーのデバイスが消去されます。デバイスを消去すると、個人ファイルを含むすべてのデータが削除されます。

h. [パスワードの有効期限]: パスワードが有効期限切れになり変更が必要になるまでの日数を指定します。

i. [画面のロックの有効化]: ユーザーの入力がなくなってからユーザーの画面をロックするまでの秒数を指定します。

j. [Enforce password history] (パスワード履歴を記録する): 同じパスワードの継続使用とみなされるまでのそのパスワードの入力回数を指定します。

5. [保存] を選択します。

モバイルデバイスの管理

このセクションのトピックでは、モバイルデバイスのリモートワイプ方法について説明します。組織からデバイスを削除し、デバイスの詳細を表示します。組織のモバイルデバイスポリシーを編集する方法については、組織のモバイルデバイスポリシーの編集 を参照してください。

トピック

- モバイルデバイスのリモートワイプ
- デバイスのリストからのユーザーのモバイルデバイスの削除
- モバイルデバイス詳細の表示

モバイルデバイスのリモートワイプ

このセクションのステップでは、モバイルデバイスのリモートワイプ方法について説明します。次の点に注意してください。

- デバイスはオンラインで、Amazon に接続されている必要があります WorkMail。誰かがデバイスを切断すると、ユーザーがデバイスを再接続したときにワイプ操作が再開されます。
- ワイプ操作の反映には 5 分かかることがあります。

> **Important**
>
> ほとんどのモバイルデバイスはリモートワイプにより出荷時設定にリセットされます。この手順を実行すると、個人用ファイルを含むすべてのデータを削除できます。

ユーザーのモバイルデバイスをリモートワイプするには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 全般のリファレンス」の「 リージョン名とエンドポイント」を参照してください。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで [ユーザー] を選択してから、編集するユーザーの名前をユーザーのリストで選択します。
4. [モバイルデバイス] タブを選択します。
5. デバイスのリストで、デバイスの横にあるボタンを選択し、[ワイプ] を選択します。
6. ワイプがリクエストされているかどうかを概要で確認します。
7. デバイスがワイプされたら、デバイスリストから削除します。次のセクションのステップでは、方法について説明します。

   > **Important**
   >
   > ワイプしたデバイスをユーザーのデバイスリストに戻すには、まずデバイスリストからそのデバイスを削除してください。削除しないと、システムはデバイスを再度ワイプします。

デバイスのリストからのユーザーのモバイルデバイスの削除

誰かが特定のモバイルデバイスの使用をやめた場合、またはデバイスをリモートでワイプした場合は、そのデバイスをデバイスリストから削除できます。ユーザーがデバイスをもう一度設定すると、そのデバイスはリストに表示されます。

デバイスのリストからユーザーのモバイルデバイスを削除するには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで [ユーザー] を選択してから、編集するユーザーの名前を選択します。
4. 「モバイルデバイス」タブを選択します。
5. デバイスのリストで、削除するデバイスを選択してから、[デバイスを削除]を選択します。

モバイルデバイス詳細の表示

ユーザーのモバイルデバイスの詳細を表示できます。

> **Note**
>
> デバイスによっては、すべての詳細情報がサーバーに送信されないことがあります。利用可能なデバイスの詳細がすべて表示されない場合があります。

デバイスの詳細を表示するには

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

   必要に応じて、リージョンを変更します。ナビゲーションバーから、ニーズに合ったリージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインで [ユーザー] を選択し、[モバイルデバイス] タブを選択します。
4. デバイスのリストで、詳細を表示するデバイスの ID を選択します。

   以下の表は、デバイスのステータスコードを示しています。

[ステータス]	説明
PROVISIONING_REQUIRED	ユーザーまたは管理者が、デバイスを Amazon WorkMail で使用できるようにプロビジョニングするようリクエストしました。デバイスの現在のポリシーが Amazon WorkMail コンソールで変更された場合も、デバイスはこのステータスに設定されます。
PROVISIONING_SUCCEEDED	デバイスが正常にプロビジョンされました。指定されたポリシーがデバイスに適用されました。
WIPE_REQUIRED	管理者が Amazon WorkMail コンソールでワイプをリクエストしました。
WIPE_SUCCEEDED	デバイスが正常にワイプされました。

モバイルデバイスアクセスルールの管理

Amazon WorkMail のモバイルデバイスアクセスルールを使用すると、管理者は特定の種類のモバイルデバイスのメールボックスアクセスを制御できます。デフォルトでは、各 Amazon WorkMail 組織は、タイプ、モデル、オペレーティングシステム、ユーザーエージェントに関係なく、すべてのデバイスへのメールボックスアクセスを許可するルールを使用します。そのデフォルトルールを編集したり、独自のルールに置き換えたりできます。ルールは追加、変更、削除できます。

> **Warning**
>
> 組織のすべてのモバイルデバイスアクセスルールを削除すると、Amazon WorkMail はすべてのモバイルデバイスアクセスをブロックします。

次のデバイスプロパティに基づいて、アクセスを許可または拒否するルールを作成できます。

- デバイスタイプ — 「iPhone」、「iPad」、または「Android」
- デバイスモデル -「iPhone10c1」、「iPad5c1」、または「HTCOneX」

- デバイスオペレーティングシステム -「iOS 12.3.1 16F203」、または「Android 8.1.0」
- デバイスユーザーエージェント -「iOS/14.2 (18B92) exchangesyncd/1.0」、または「Android-Mail/7.7.16.163886392.release」

AWS管理コンソールでデバイスのプロパティを表示するには、「モバイルデバイスの詳細の表示」を参照してください。

> **Note**
>
> 一部のデバイスおよびクライアントでは、すべてのフィールドのプロパティがレポートされない場合があります。これらのケースを回避する方法については、Dealing with empty fields を参照してください。

> **Important**
>
> Amazon WorkMail モバイルデバイスアクセスルールは、Microsoft Exchange ActiveSync プロトコルを使用するデバイスにのみ適用されます。IMAP などの別のプロトコルを使用するモバイルクライアントは、ここにリストされているデバイスのプロパティを報告しないため、これらのルールは適用されません。
>
> 他のプロトコルを使用するデバイスのアクセスを制限する必要がある場合は、アクセスコントロールルールを作成します。これらの詳細については、アクセスコントロールルールの使用を参照してください。例えば、他のプロトコルやウェブメールへのアクセスを社内 IP アドレスの範囲に制限しても、他の場所からの Microsoft ActiveSync を許可し、モバイルデバイスアクセスルールを使用して、許可されるクライアントの種類とバージョンをさらに制限できます。

トピック

- モバイルデバイスアクセスルールの仕組み
- モバイルデバイスアクセスルールの使用

モバイルデバイスアクセスルールの仕組み

モバイルデバイスアクセスルールは、Microsoft Exchange ActiveSync プロトコルを使用するデバイスにのみ適用されます。各ルールには、ルールが適用されるタイミングを指定する一連の条件と、デ

バイスの ALLOW または DENY のアクセス効果があります。ルールは、ルールのすべての条件がユーザーのモバイルデバイスのプロパティと一致する場合のみ、アクセスリクエストに適用されます。条件のないルールは、すべてのリクエストに適用されます。各条件は、デバイスのレポートされたプロパティに対して、大文字と小文字を区別しないプレフィクスの一致を使用します。

Amazon WorkMail は、ルールを次のように評価します。

- DENY ルールがデバイスプロパティと一致すれば、ポリシーによってデバイスがブロックされます。DENY ルールは優先されます ALLOW ルールよりも優先されます。
- ALLOW ルールが少なくとも 1 つ一致し、DENY ルールは一致するものがなければ、ポリシーはデバイスを許可します。
- ルールが適用されない場合、デバイスはブロックされます。

> **Important**
>
> モバイルデバイスは、ルールがオペレーションに使用するプロパティを報告します。Microsoft ActiveSync デバイスのプロビジョニングプロセス中に、デバイスのプロパティがレポートされます。Amazon WorkMail は、モバイルクライアントが正しい情報や最新情報を報告していることを個別に検証することはできません。

モバイルデバイスアクセスルールの使用

API または AWS コマンドラインインターフェイス (CLI) を使用して、モバイルデバイスアクセスルールを作成および管理できます。AWS CLI の詳細については、AWS コマンドラインインターフェイスユーザーガイドを参照してください。

> **Important**
>
> Amazon WorkMail 組織のアクセスルールを変更すると、影響を受けるデバイスが更新されたルールに従うまでに 5 分かかることがあり、その間にデバイスが一貫性のない動作を示すことがあります。ただし、ルールをテストすると、すぐに正しい動作が表示されます。詳細については、「Testing mobile device access rules」を参照してください。

モバイルデバイスアクセスルールの一覧表示

次の例は、モバイルデバイスアクセスルールを一覧表示する方法を示しています。

```
aws workmail list-mobile-device-access-rules --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56
```

モバイルデバイスアクセスルールの作成

次の例では、すべての Android デバイスがメールボックスへのアクセスをブロックするルールを作成します。

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name BlockAllAndroid --effect DENY --device-types
 "android"
```

次の例では、特定のバージョンの iOS のみを許可するルールを作成します。デフォルト ALLOW-all ルールは必ず削除してください。

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name AllowLatestiOS --effect ALLOW --device-
operating-systems "iOS 14.3"
```

モバイルデバイスアクセスルールの更新

次の例では、識別子を追加してデバイスルールを更新します。

```
aws workmail update-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --mobile-device-access-rule-id 1a2b3c4d --
name AllowLatestiOS --effect ALLOW --device-operating-systems "iOS 14.4"
```

モバイルデバイスアクセスルールの削除

次の例では、指定された ID を持つモバイルデバイスアクセスルールを削除します。

```
aws workmail delete-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --mobile-device-access-rule-id 1a2b3c4d
```

モバイルデバイスアクセスルールのテスト

アクセスルールをテストするには、GetMobileDeviceAccessEffect API、または AWS CLI の [get-mobile-device-access-effect] コマンドを使用します。AWS CLI の詳細については、AWSAWS コマンドラインインターフェイスユーザーガイドを参照してください。

テストする際、シミュレートされたモバイルデバイスのプロパティを渡すと、API または CLI がアクセス効果 (ALLOW または DENY) を返します。アクセス効果はプロパティを持つ実際のモバイルデバイスが受け取ることになります。例えば、このコマンドは、iOS 14.2 を実行している iPhone とデフォルトのメールアプリケーションが、メールボックスにアクセスできるかどうかをテストします。

```
aws workmail get-mobile-device-access-effect --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --device-type "iPhone" --device-model "iPhone10C1"
 --device-operating-system "iOS 14.2.1 16F203" --device-user-agent "iOS/14.2 (18B92)
 exchangesyncd/1.0"
```

空のフィールドの取り扱い

一部のモバイルデバイスまたはクライアントでは、1 つ以上のフィールドの情報をレポートしないため、値が空のままになることがあります。ルールは、条件で特別な値を $NONE を使用して、これらのデバイスと一致させることができます。例えば、 DeviceTypes=["iphone", "ipad", "$NONE"] を持つルールは、「"iphone"」または「"ipad"」のデバイスタイプを報告するデバイスと一致するか、デバイスタイプをまったく報告しないデバイスと一致します。

NotDeviceTypes または NotDeviceUserAgents のような負の条件は、これらの空の値と一致しません。例えば、NotDeviceTypes=["android"] を持つルールは、「"android"」以外のデバイスタイプを報告するデバイスと一致します。ただし、ルールは、デバイスタイプをまったく報告しないデバイスには一致しません。

モバイルデバイスのアクセスオーバーライドの管理

モバイル デバイス アクセス オーバーライドを使用して、モバイル デバイス アクセス ルールの結果をオーバーライドします。オーバーライドは特定のユーザーとデバイスに適用され、デフォルトのアクセスルールが逆になります。オーバーライドを使用して、アクセスルールに 1 回限りの例外を設定したり、特定のユーザーとデバイスのペアを許可または拒否したりすることもできます。さらに、DefaultDenyAll モバイルデバイスのアクセスルールでオーバーライドを使用できます。これにより、アクセス決定はサードパーティーのモバイルデバイス管理 (MDM) ソリューションに委ねられます。詳細については、「オーバーライドの管理」および「モバイルデバイス管理ソリューションとの統合」を参照してください。

トピック

- モバイルデバイスのアクセスオーバーライドの仕組み
- オーバーライドの管理

モバイルデバイスのアクセスオーバーライドの仕組み

特定のユーザーとデバイスの組み合わせに対してモバイルデバイスのアクセスオーバーライドを作成します。オーバーライドにより、特定のユーザーおよびデバイスのモバイル デバイス アクセス ルールを評価するときに、デフォルトのアクセス結果が逆転します。例えば、アクセスルールが通常アクセスを拒否する場合、アクセスオーバーライドはそのユーザーとデバイスの E メールの同期を許可できます。逆に、アクセスルールで通常アクセスを許可する場合は、ユーザーとデバイスが E メールを同期できないようにするオーバーライドを作成できます。モバイルデバイスのアクセスオーバーライドを削除すると、 WorkMail Amazonは再び現在のモバイルデバイスアクセスルールの結果を尊重して、そのユーザーとデバイスにアクセス権を付与するかどうかを決定します。

> **Important**
>
> Amazon WorkMail 組織のモバイルデバイスのアクセスオーバーライドを変更すると、影響を受けるデバイスが更新されたオーバーライドに従うまでに 5 分かかることがあります。

オーバーライドの管理

モバイルデバイスのアクセスオーバーライドは、API または AWS Command Line Interfaceを使用して作成、更新、削除できます。詳細については AWS CLI、『AWS コマンドラインインターフェイスユーザーガイド』を参照してください。

デバイス ID を検索するには、 AWS Management Consoleを使用します。詳細については、モバイルデバイス詳細の表示を参照してください。

モバイルデバイスのアクセスオーバーライドの一覧表示

この例は、指定した Amazon WorkMail 組織のすべてのモバイルデバイスアクセスオーバーライドを一覧表示する方法を示しています。

```
aws workmail list-mobile-device-access-overrides --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56
```

モバイルデバイスのアクセスオーバーライドの作成と更新

これにより、モバイルデバイスのアクセスオーバーライドが作成され、指定した Amazon WorkMail 組織、ユーザー、デバイス ID へのアクセスが拒否されます。

```
aws workmail put-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0 --effect DENY
```

既存のモバイルデバイスのアクセスオーバーライドは、異なる効果を持つように変更できます。これにより、以前に作成したモバイルデバイスのアクセスオーバーライドが更新され、アクセスを拒否するのではなく許可します。

```
aws workmail put-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0 --effect ALLOW
```

モバイルデバイスのアクセスオーバーライドを削除する

これにより、指定した Amazon WorkMail 組織、ユーザー、デバイス ID のモバイルデバイスアクセスオーバーライドが削除されます。

```
aws workmail delete-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0
```

モバイルデバイス管理ソリューションとの統合

WorkMail Amazonは、モバイルデバイスポリシーとモバイルデバイスアクセスルールを通じて、いくつかの基本的なモバイルデバイス管理機能をサポートしています。ただし、これらの機能はMicrosoft Exchange ActiveSync (EAS) プロトコルを介してのみモバイルデバイスと通信できるため、デバイスのセキュリティ対策を詳しく調べて実施する機能は限られています。デバイスのセキュリティとコンプライアンスをより詳細に制御する必要がある管理者は、サードパーティーのモバイルデバイス管理 (MDM) ソリューションを使用できます。

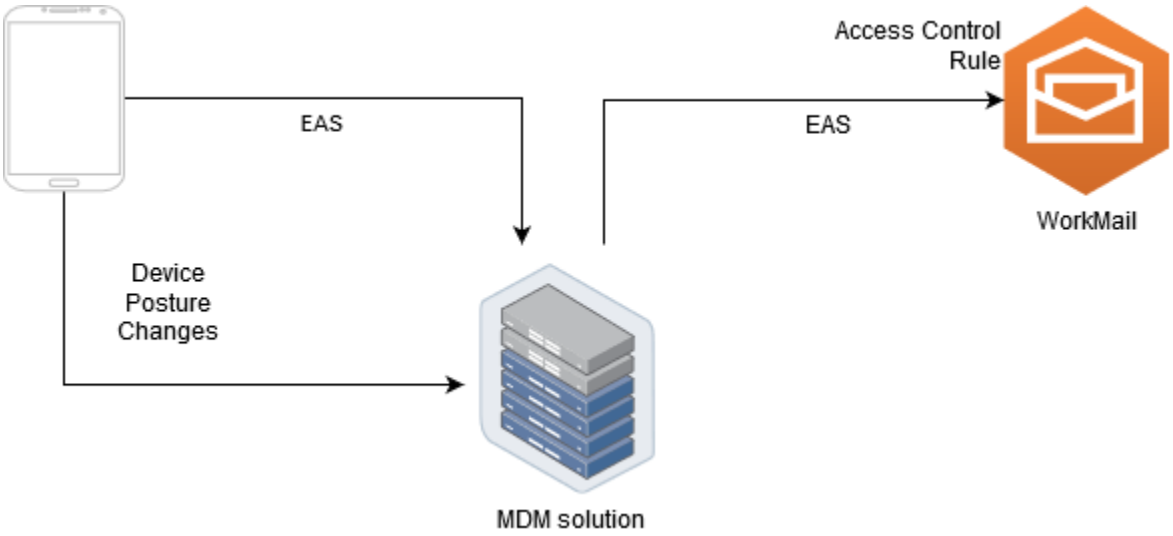
モバイルデバイス管理ソリューションの概要

MDM ソリューションは、代理または直接の 2 つのモードで構成できます。ソリューションがサポートするモードについては、MDM のドキュメントを参照してください。

プロキシモードでは、モバイルデバイスは MDM ソリューション経由で Exchange Active Sync (EAS) プロトコルを使用して Amazon にアクセスします。 WorkMailMDM ソリューションはデバイスポスチャを使用して Amazon データへのアクセスを許可または拒否します。 WorkMailAmazon WorkMail 側では、MDM ソリューションの 1 つまたは複数の IP アドレスからのみ EAS アクセスを

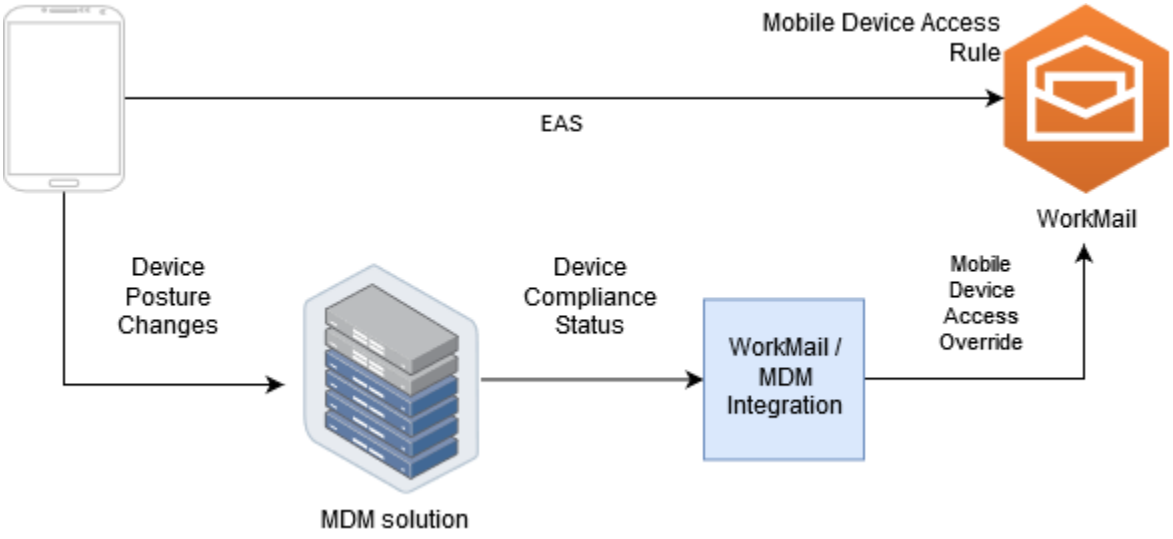
許可するアクセスコントロールルールを使用します。詳細については、[アクセスコントロールルールの使用]を参照してください。

次の図は、一般的なプロキシモードの設定を示しています。



ダイレクトモードでは、 WorkMail モバイルデバイスはEASを使用してAmazonに直接アクセスします。MDM ソリューションはデバイスのポスチャの変更を受け取り、各デバイスがこれらの要件を満たしているかどうかを継続的に評価します。MDM ソリューションは、デバイスのコンプライアンス違反などの体制の変更を検出すると、いくつかのアクションを実行し、通常は通知またはイベントを発行します。 WorkMail Amazonの管理者は、これらのコンプライアンスステータスイベントを監視し、モバイルデバイスのアクセスオーバーライドを自動的に作成して、デバイスがMDMデバイス要件に準拠したり違反したりしたときに、デバイスへのアクセスを許可または拒否するシステムを設定できます。

次の図は、一般的なダイレクトモードの設定を示しています。



サードパーティの MDM WorkMail ソリューションとダイレクトモードで統合するように組織を設定する

ダイレクトモードでサードパーティーのモバイルデバイス管理 (MDM) ソリューションと統合するには、次の要件を満たす必要があります。

- ActiveSyncユーザーデバイスへのアクセスをプロトコルのみに制限するアクセス制御ルールを作成します。
- デフォルトの「deny-to-all」モバイルデバイスのアクセスルールを作成して、未知または管理対象外のモバイルデバイスがすべてデフォルトで拒否されるようにします。
- デバイスがセキュリティ体制を変更したとき、つまりコンプライアンス違反になったときにカスタム通知またはイベントを発行するモバイルデバイス管理ソリューションを採用します。
- これらの通知を聞くためのカスタムソフトウェアコンポーネントを作成し、Amazon WorkMail SDK を呼び出してモバイルデバイスのアクセスオーバーライドを作成します。

これらのコンポーネントにより、 WorkMail すべてのユーザーデバイスがAmazonメールボックスへのアクセスを許可される前に、MDMコンプライアンス要件を満たしていることが保証されます。

アクセスコントロールルールを使用して、モバイルデバイスからのアクセスを制限します。ActiveSync

ActiveSync すべてのデバイスがプロトコルのみを使用するようにする必要があります。また、アクセスコントロールルールを使用してそのようにすることもできます。たとえば、社内の IP アドレス範囲からのみ他のメールプロトコルへのアクセスを許可し、 ActiveSync 企業ファイアウォールの外部からメールにアクセスする場合にのみ許可することができます。デバイス ID ActiveSync を使用してデバイスを識別することしかできないため、これを行う必要があります。インターネットメッセージアクセスプロトコル (IMAP) や Exchange Web サービスなどのプロトコルは使用できません。詳細については、「アクセスコントロールルールの使用」を参照してください。

デフォルトで「すべて拒否」アクセスルールを作成する

すべてのモバイルデバイスのアクセス決定をサードパーティーのモバイルデバイス管理ソリューションに任せるには、ユーザー単位またはデバイス単位で上書きされない限り、すべてのデバイスを自動的に拒否するアクセスルールを作成します。詳細については、「モバイルデバイスアクセスルールの管理」を参照してください。

この例では、「すべて拒否」ルールを示します。

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name DefaultDenyAll --effect DENY
```

デバイス体制の変更に対応し、モバイルデバイスのアクセスオーバーライドを作成する

デバイス体制の変更に関する通知を送信するように MDM ソリューションを設定する必要があります。これらの通知は、Amazon WorkMail SDK を使用してモバイルデバイスのアクセスオーバーライドを作成または更新できるコンポーネントが使用する必要があります。デフォルトでは、このトピックで前述したデフォルトの「 WorkMail すべて拒否」のモバイルデバイスアクセスルールにより、Amazonは管理対象外のデバイスまたは新しくプロビジョニングされたデバイスへのアクセスを拒否します。MDM ソリューションがデバイスがすべての要件を満たしていると判断し、デバイスが準拠していることを示す通知を発行すると、このコンポーネントは指定されたユーザーとデバイスに対して ALLOW の効果を持つモバイルデバイスアクセスオーバーライドを作成して、この通知に応答できます。デバイスが後でコンプライアンス違反になった場合、モバイルデバイス管理ソリューションは別の通知を発行し、アクセスオーバーライドを削除または変更して、そのデバイスへのアクセスを拒否できます。詳細については、「モバイルデバイスのアクセスオーバーライドの管理」を参照してください。

MDM WorkMail と統合された Amazon の例については、AWS このサンプルアプリケーションを参照してください。

メールボックスのアクセス許可の使用

Amazon WorkMail でメールボックスのアクセス許可を使用し、ユーザーやグループに対して他のユーザーのメールボックスを操作する権限を付与できます。メールボックスの権限はメールボックス全体に適用されます。これにより、複数のユーザーがメールボックスの認証情報を共有しなくても同じメールボックスにアクセスできます。メールボックスのアクセス許可を持つユーザーは、メールボックスのデータの読み取りや変更、共有メールボックスからの E メールの送信ができます。

> **Note**
>
> グローバルアドレス一覧で非表示になっているユーザーのメールボックスに対する権限を持つユーザーは、非表示になっているユーザーのメールボックスには引き続きアクセスできます。

付与できるアクセス許可は以下のとおりです。

- [フルアクセス]: メールボックスに対する読み取りと書き込みのフルアクセスを許可します。フォルダレベルのアクセス許可を変更する権限も含まれます。

  > **Note**
  >
  > このオプションは ユーザーのみ使用できます。グループに完全なアクセス権を与えることはできません。

- [代理で送信]: 別のユーザーに代わって E メールを送信することをユーザーやグループに許可します。メールボックスの所有者は [送信元:] ヘッダーに表示され、差出人は [差出人:] ヘッダーに表示されます。
- [所有者として送信] - メールボックスの所有者として E メールを送信することをユーザーやグループに許可します。メッセージの実際の差出人は表示されません。[送信元:] ヘッダーと [差出人:] ヘッダーの両方にメールボックスの所有者が表示されます。
- なし — ユーザーまたはグループがメールを送信できないようにします。

> **Note**
>
> メールボックスのアクセス許可をグループに付与すると、そのグループのすべてのメンバー (ネストされたグループのメンバーも含む) に、これらのアクセス許可が適用されます。

メールボックスのアクセス許可を付与すると、Amazon WorkMail の AutoDiscover サービスにより、追加したユーザーやグループのメールボックスに対するアクセスが自動的に更新されます。

Windows の Microsoft Outlook クライアントの場合、フルアクセス許可を持つユーザーは、共有メールボックスに自動的にアクセスできます。変更が反映されるまで最大 60 分待ってから、Microsoft Outlook を再起動します。

Amazon WorkMail ウェブアプリケーションおよびその他の E メールクライアントの場合、フルアクセス許可を持つユーザーは、共有メールボックスを手動で開くことができます。開いたメールボックスは、ユーザーが閉じない限り、セッション間でも開いたままになります。

トピック

- メールボックスとフォルダのアクセス許可について
- ユーザーのメールボックスへのアクセス許可の管理
- メールボックスへのグループのアクセス許可の管理

メールボックスとフォルダのアクセス許可について

メールボックスのアクセス許可は、メールボックス内のすべてのフォルダに適用されます。これらのアクセス許可を有効化できるのは、AWS アカウント所有者または Amazon WorkMail 管理 API を呼び出すことを承認された IAM ユーザーのみです。メールボックスまたはグループ全体のアクセス許可を設定および変更するには、AWS Management Console または Amazon WorkMail API を使用します。コンソールから最大 100 のメールボックスとグループのアクセス許可を管理できます。より多くのユーザーとグループのアクセス許可を管理するには、Amazon WorkMail API を使用します。

フォルダのアクセス許可は、単一のフォルダにのみ適用されます。エンドユーザーは、電子メールクライアントまたは Amazon WorkMail ウェブアプリケーションを使用してフォルダーのアクセス許可を設定できます。Amazon WorkMail ウェブアプリケーションを使用してフォルダを共有する方法の詳細については、Amazon WorkMail ユーザーガイドの「フォルダとフォルダ権限の共有」を参照してください。

ユーザーのメールボックスへのアクセス許可の管理

Amazon WorkMail コンソールを使用して、ユーザーだけでなくグループのメールボックス権限も管理できます。次のセクションでは、ユーザーのアクセス許可を管理する方法について説明します。グループのアクセス許可を管理する方法については、「メールボックスへのグループのアクセス許可の管理」を参照してください。

トピック

- アクセス許可を追加
- メールボックスへのユーザーのアクセス許可を編集する

アクセス許可を追加

権限を追加すると、あるユーザーに別のユーザーのメールボックスで 1 つ以上のタスクを実行する権限が付与されます。たとえば、従業員 A が上司の従業員 B に代わってメッセージを送信する必要があるとします。その権限を付与するには、従業員 B のメールボックス設定に移動し、従業員 A に要求されたタスクを実行する権限を付与します。

メールボックスのアクセス許可を追加するには

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

   必要に応じて、リージョンを変更します。ナビゲーションバーから、必要に応じてリージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで、[組織] を選択し、ドメインを追加する組織の名前を選択します。
3. ナビゲーションペインで、[ユーザー] を選択し、アクセス許可を管理するユーザーの名前を選択します。
4. [アクセス許可] タブを選択してから、[アクセス許可を追加] を選択します。

   [アクセス許可を追加] ダイアログボックスが表示されます。
5. [新しい権限を追加] リストを開き、メールボックスにアクセスする必要があるユーザーまたはグループを選択します。
6. [メールボックスの権限] と [送信権限] で、必要なオプションを選択します。
7. [追加] を選択します。

新しいアクセス許可が反映されるまでに最大 5 分かかります。

メールボックスへのユーザーのアクセス許可を編集する

ユーザーのメールボックス権限を編集すると、そのユーザーのメールボックスに対する他のユーザーのアクセス権が変更されます。メールボックスの権限を編集しても、メールボックスの元のユーザーのアクセス権は変わりません。

メールボックスのアクセス許可を編集するには

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

   必要に応じて、リージョンを変更します。ナビゲーションバーから、必要に応じてリージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで、[組織] を選択し、アクセス許可を管理する組織の名前を選択します。
3. ナビゲーションペインで [ユーザー] を選択して、編集するアクセス許可を持つユーザーの名前を選択し、[アクセス許可] タブを選択します。
4. [アクセス許可] タブを選択します。

   メールボックスにアクセスできるユーザーとグループのリストが表示されます。
5. 変更するユーザーまたはグループの横にあるラジオボタンを選択してから、次のいずれかを実行します。

   ユーザーのアクセス許可を削除するには

   1. [削除] を選択します。

      [アクセス許可を管理する] ダイアログボックスが表示されます。
   2. [アカウントを削除] ダイアログボックスで、[削除] を選択します。

   ユーザーの権限を編集するには

   1. [編集] を選択します。

      [アクセス許可を編集する] ダイアログボックスが表示されます。
   2. 必要に応じて権限を設定し、[保存] を選択します。

別のユーザーにメールボックスへのアクセス許可を付与するには

1. [アクセス許可を追加] を選択します。

   [アクセス許可を追加] ダイアログボックスが表示されます。
2. [新しいアクセス許可を追加] リストを開き、追加するユーザーを選択します。
3. 必要に応じてアクセス許可を設定し、[追加] を選択します。

変更したアクセス許可が反映されるまでに最大 5 分かかります。

メールボックスへのグループのアクセス許可の管理

Amazon WorkMail のグループアクセス許可を追加または削除できます。

> **Note**
>
> グループにはアクセスするメールボックスがないため、フルアクセス権限をグループに適用することはできません。

グループのアクセス許可を管理するには

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

   コンソールウィンドウの上部にあるバーで、[リージョンを選択]リストを開き、AWS リージョンを変更します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで、[組織] を選択し、アクセス許可を管理する組織の名前を選択します。
3. ナビゲーションペインで、[グループ] を選択し、アクセス許可を設定するグループの名前を選択します。
4. [アクセス許可] タブを選択してから、[アクセス許可を追加] を選択します。

   [アクセス許可を追加] ダイアログボックスが表示されます。
5. [新しいアクセス許可を追加] リストを開き、メールボックスの権限を付与するユーザーまたはグループを選択します。
6. [メールボックスのアクセス許可] と [アクセス許可を送信] で、必要なオプションを選択します。

7. [追加] を選択します。

変更したアクセス許可が反映されるまでに最大 5 分かかります。

メールボックスへのプログラムによるアクセス

Amazon WorkMail メールボックスにプログラムからアクセスするには、Exchange ウェブサービス (EWS) プロトコルを使用します。EWS では、メールボックス内のすべての種類のアイテムにアクセスできます。Amazon WorkMail で使用できる EWS ライブラリは次のとおりです。

- Java — EWS Java API
- .Net – EWS Managed API
- Python – Exchangelib

Amazon WorkMail では IMAP プロトコルと SMTP プロトコルもサポートされており、E メールを送受信するために使用できます。Amazon WorkMail プロトコルでサポートされている URL は、Amazon WorkMail エンドポイントとクォータで確認できます。

EWS プロトコルを使用する場合、Amazon WorkMail では次の認証方法がサポートされています。

- 基本認証 — 基本認証では、E メールアドレスとパスワードを入力します。
- なりすましロール— なりすましロールを使用すると、ユーザーの認証情報を入力せずにユーザーのメールボックスにアクセスできます。

トピック

なりすましロールの管理

なりすましロールを使用すると、管理者はユーザーの認証情報を入力せずにユーザーのメールボックスにプログラム的にアクセスするように構成できます。サービスとツールはなりすましロールを引き受け、ユーザーのメールボックスでアクションを実行できます。なりすましは EWS プロトコルでのみサポートされます。

なりすましロールの概要

なりすましを許可するには、管理者は次のプロパティでなりすましロールを作成する必要があります。

- ロールタイプ — [フルアクセス] または [読み取り専用] を選択します。ロールタイプによって、ロールが実行できる操作の種類が制限されます。
- ルール — なりすましロールになりすますことのできるユーザーを定義するルールのリスト。

Amazon WorkMail は、以下の条件に基づいてルールを評価します。

- いずれかの 拒否 ルールが一致すると、ポリシーはなりすましを拒否します。拒否ルールは許可ルールよりも優先されます。
- 少なくとも 1 つの 許可ルールが一致し、拒否ルールが一致しない場合、ポリシーはなりすましを許可します。
- ルールが適用されない場合、なりすましは拒否されます。

> **Note**
>
> Amazon WorkMail 組織内のすべてのユーザーのなりすましを許可するには、許可効果のある、条件なしのルールを作成します。

> **Warning**
>
> なりすましロールがユーザーになりすますことを許可するルールを作成する必要があります。ルールを指定しない場合、なりすましロールがユーザーのアクセス権を引き継ぐことはできません。

なりすましロールを作成すると、そのロールを使用してユーザーのメールボックスにアクセスできるようになります。詳細については、「なりすましロールを使用する」を参照してください。

セキュリティに関する考慮事項

なりすましロールを使用すると、Amazon WorkMail 組織とAWS アカウントの中でセキュリティ上の問題が発生する可能性があります。なりすましロールを作成する際に考慮すべき潜在的な問題をいくつか紹介します。

- 推移的権限 — ユーザー A がユーザー B のメールボックスにアクセスでき、ユーザー A になりすますことができるなりすましロールが許可されている場合、このなりすましロールはユーザー A のアクセス権限を装い、ユーザー B のメールボックスにアクセスする可能性があります。

- アクセスコントロール — アクセスコントロールルールを使用して、なりすましロールのアクセスを制限できます。詳細については、「アクセスコントロールルールの使用」を参照してください。
- IAM ポリシー — `workmail:ImpersonationRoleId`条件を使用して、特定の Amazon WorkMail 組織となりすましロールに`AssumeImpersonationRole`アクションを割り当てることができます。IAM ポリシーの例を表示するには、Amazon と IAM WorkMail の連携方法 を参照してください。

なりすましロールを作成

Amazon WorkMail コンソールからなりすましロールを作成できます。

なりすましロールを作成するには

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

   必要に応じて、リージョンを変更します。ナビゲーションバーから、必要に応じてリージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. [なりすましロール] を選択し、[ロールを作成] を選択します。
4. 「なりすましロールを作成」ダイアログボックスが表示されます。[認証情報] で以下の情報を入力します。

   - 名前 — なりすましロールの一意の名前を入力します。
   - (オプション) [説明] - なりすましロールの説明を入力します。
   - ロールタイプ — [読み取り専用] または [フルアクセス] を選択します。
5. [ルール] で [ルールを追加] を選択します。
6. [ソースを追加] ダイアログボックスが表示されます。次の情報を入力します。

   - 名前 - ルールの一意の名前を入力します。
   - (オプション)[説明] - ルールの説明を入力します。
   - [効果] で、[許可] または [拒否] を選択します。これにより、次のステップで選択した条件に基づいてアクセスが許可または拒否されます。
   - (オプション)「このルール:」で、「選択したユーザーになりすましたリクエストに一致」を選択して、特定のユーザーが含まれるようにします。[選択したユーザー以外のユーザーになりすましたリクエストに一致] を選択して、選択したユーザー以外のユーザーを追加します。

7. [ルールを追加] を選択します。

> **Note**
>
> ルールは、対応するロールを保存したときにのみ保存されます。

8. [ロールを作成] を選択します。

なりすましロールの編集

Amazon WorkMail コンソールから、なりすましロールを編集できます。

なりすましロールを編集するには

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

   必要に応じて、リージョンを変更します。ナビゲーションバーから、必要に応じてリージョンを選択します。詳細については、「Amazon Web Services 全般のリファレンス」の「 のリージョンとエンドポイント」を参照してください。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. 「なりすましロール」を選択します。
4. 編集するなりすましロールの名前を選択し、[編集] を選択します。
5. 「なりすましロールを編集」ダイアログボックスが表示されます。[ロール] で以下の情報を入力します。

   - 名前 — なりすましロールの一意の名前を入力します。
   - (オプション) [説明] - なりすましロールの説明を入力します。
   - ロールタイプ — なりすましロールにユーザーのメールボックスへの読み取り専用アクセス権を付与するには、[読み取り専用] を選択します。なりすましロールにユーザーのメールボックス内のアイテムの読み取りと変更を行う権限を与えるには、「フルアクセス」を選択します。
6. [ルール] で、編集するルールを選択し、[編集] を選択します。
7. [ルールを編集] ダイアログボックスが表示されます。次の情報を入力します。

   - 名前 — ルールの名前を編集します。
   - (オプション) [説明] ルールの説明を更新または入力します。

- 「効果」で「許可」を選択すると、ルールに設定された条件が満たされた場合にアクセスが許可されます。アクセスを拒否するには、「拒否」を選択します。
- (オプション)「このルール:」で、「選択したユーザーになりすましたリクエストに一致」を選択して、特定のユーザーが含まれるようにします。[選択したユーザー以外のユーザーになりすますリクエストに一致]を選択して、選択したユーザー以外のユーザーを追加します。

8. [保存] を選択します。
9. [変更を保存] をクリックします。

> **Important**
>
> なりすましルールを変更すると、影響を受けるメールボックスの更新までに最大 5 分かかります。ルールの更新プロセス中に、メールボックスの動作に一貫性がなくなることがあります。ただし、ロールをテストすると、Amazon WorkMail は更新されたルールに基づいて期待どおりに応答します。詳細については、「なりすましロールのテスト」を参照してください。

なりすましロールのテスト

Amazon WorkMail コンソールからなりすましロールをテストできます。

なりすましロールをテストするには

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

   必要に応じて、リージョンを変更します。ナビゲーションバーから、必要に応じてリージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. 「なりすましロール」を選択します。
4. テストするなりすましロールを選択します。
5. [テストルール] を選択します。
6. 「なりすましロールをテスト」ダイアログボックスが表示されます。「対象ユーザー」で、なりすましアクセスをテストするユーザーを選択します。

7. [テスト] を選択します。

なりすましロールの削除

Amazon WorkMail コンソールから、なりすましロールを削除できます。

なりすましロールを削除するには

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

   必要に応じて、リージョンを変更します。ナビゲーションバーから、必要に応じてリージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. 「なりすましロール」を選択します。
4. 削除したいなりすましロールの名前を選択します。
5. [削除] をクリックします。
6. [ロールを削除] ダイアログボックスが表示されます。削除を確認するには、ロールの名前をダイアログボックスに入力し、[削除] を選択します。

なりすましロールを使用する

メールボックスのデータにアクセスするには、Amazon WorkMail API アクション`AssumeImpersonationRole`を使用します。Amazon WorkMail API の詳細については、「API リファレンス」を参照してください。

`AssumeImpersonationRole` は `Token` を返します。この `Token` は、HTTP ヘッダー `Authorization` を介して 15 分以内に EWS プロトコルに渡す必要があります。

次の例では、EWS プロトコルでなりすましロールを使用する方法を示します。例で使用されている定数は、組織とアカウントに固有の次の詳細を指定します。

- *`WORKMAIL_ORGANIZATION_ID`* - Amazon WorkMail 組織 ID
- *`IMPERSONATION_ROLE_ID`*— なりすましロール ID
- *`WORKMAIL_EWS_URL`* — Amazon WorkMail エンドポイントとクォータで利用可能な EWS エンドポイント

- *EMAIL_ADDRESS*— ユーザーメールボックスのメールアドレス

Example Java — EWS Java API

```
import software.amazon.awssdk.services.workmail.WorkMailClient;
import software.amazon.awssdk.services.workmail.model.AssumeImpersonationRoleRequest;
import software.amazon.awssdk.services.workmail.model.AssumeImpersonationRoleResponse;

import microsoft.exchange.webservices.data.core.ExchangeService;
import microsoft.exchange.webservices.data.core.enumeration.misc.ExchangeVersion;
import microsoft.exchange.webservices.data.misc.ImpersonatedUserId;
import microsoft.exchange.webservices.data.core.enumeration.misc.ConnectingIdType;

// ...

AssumeImpersonationRoleResponse response = workMailClient.assumeImpersonationRole(
    AssumeImpersonationRoleRequest.builder()
        .organizationId(WORKMAIL_ORGANIZATION_ID)
        .impersonationRoleId(IMPERSONATION_ROLE_ID)
        .build());

ExchangeService exchangeService = new
 ExchangeService(ExchangeVersion.Exchange2010_SP2);
exchangeService.setUrl(URI.create(WORKMAIL_EWS_URL));
exchangeService.getHttpHeaders().put("Authorization", "Bearer " + response.token());
exchangeService.setImpersonatedUserId(new
 ImpersonatedUserId(ConnectingIdType.SmtpAddress, EMAIL_ADDRESS));
```

Example .Net – EWS Managed API

```
using Amazon.WorkMail;
using Amazon.WorkMail.Model;

using Microsoft.Exchange.WebServices.Data;

// ...

AssumeImpersonationRoleRequest request = new AssumeImpersonationRoleRequest();
request.OrganizationId = WORKMAIL_ORGANIZATION_ID;
request.ImpersonationRoleId = IMPERSONATION_ROLE_ID;
AssumeImpersonationRoleResponse response =
 workMailClient.AssumeImpersonationRole(request);
```

```
ExchangeService service = new ExchangeService(ExchangeVersion.Exchange2010_SP2);
service.Url = new Uri(WORKMAIL_EWS_URL);
service.HttpHeaders.Add("Authorization", "Bearer " + response.Token);
service.ImpersonatedUserId = new
 ImpersonatedUserId(ConnectingIdType.SmtpAddress, EMAIL_ADDRESS);
```

Example Python – Exchangelib

```
import boto3

from requests.auth import AuthBase
from exchangelib.transport import AUTH_TYPE_MAP
from exchangelib import Configuration, Account, Version, IMPERSONATION
from exchangelib.version import EXCHANGE_2010_SP2


work_mail_client = boto3.client("workmail")

class ImpersonationRoleAuth(AuthBase):
    def __init__(self):
         self.token = work_mail_client.assume_impersonation_role(
             OrganizationId=WORKMAIL_ORGANIZATION_ID,
             ImpersonationRoleId=IMPERSONATION_ROLE_ID
        )["Token"]

     def __call__(self, r):
         r.headers["Authorization"] = "Bearer " + self.token
         return r

AUTH_TYPE_MAP["ImpersonationRoleAuth"] = ImpersonationRoleAuth

ews_config = Configuration(
     service_endpoint=WORKMAIL_EWS_URL,
     version=Version(build=EXCHANGE_2010_SP2),
     auth_type="ImpersonationRoleAuth"
)
ews_account = Account(
     config=ews_config,
     primary_smtp_address=EMAIL_ADDRESS,
     access_type=IMPERSONATION
)
```

メールボックスコンテンツのエクスポート

Amazon WorkMail API リファレンスで StartMailboxExportJob API アクションを使用して Amazon WorkMail メールボックスのコンテンツを Amazon Simple Storage Service (Amazon S3) バケットにエクスポートします 。このアクションは、指定したメールボックスから Amazon S3 バケットの `.zip` ファイルへ、MIME 形式で、すべての E メールメッセージとカレンダーアイテムをエクスポートします。連絡先やタスクなどのその他のアイテムはエクスポートされません。

メールボックスのエクスポートジョブの終了にかかる時間は、メールボックス内のアイテムのサイズと数によって異なります。メールボックスのエクスポートジョブは一定期間にわたって行われるため、単一の時点でのメールボックスコンテンツのスナップショットを表すものではありません。エクスポートジョブのステータスを確認するには、Amazon WorkMail API リファレンスの DescribeMailboxExportJob または ListMailboxExportJobs API アクションを使用してください。

メールボックスエクスポートジョブが完了すると、Amazon S3 バケット内の `.zip` ファイルは、お客様が提供する対称 AWS Key Management Service (AWS KMS) カスタマーマスターキー (CMK) を使用して暗号化されます。なぜなら AWS KMS 暗号化は Amazon S3 と統合され、復号されたデータは、ユーザーが AWS KMS CMK へのアクセス権を持っている限り、ダウンロードしたユーザーに表示されます。

前提条件

メールボックスコンテンツをエクスポートするための前提条件は次のとおりです。

- プログラムする機能。
- Amazon WorkMail 管理者アカウント。
- Amazon S3 バケットでパブリックアクセスが許可されていないことを確認します。詳細については、Amazon Simple Storage Service ユーザーガイドの Amazon S3 ブロックパブリックアクセスの使用および Amazon Simple Storage Service ユーザーガイドを参照してください。
- 対称 AWS KMS CMK 詳細については、AWS Key Management Service デベロッパーガイドの使用開始を参照してください。
- Amazon S3 バケットへの書き込みアクセス許可を付与し、送信されたファイルを AWS KMS CMK で暗号化するポリシーを持つ AWS Identity and Access Management (IAM) ロール。詳細については、「Amazon と IAM WorkMail の連携方法」を参照してください。

IAM ポリシーの例とロールの作成

次の例は、Amazon S3 バケットへの書き込みアクセス許可を付与し、送信されたファイルをAWS KMS CMKで暗号化する IAM ポリシーの例を示しています この例のポリシーを以下の 例: メールボックスコンテンツのエクスポート 手順で使用するには、ポリシーをJSON ファイルとして mailbox-export-policy.json のファイル名で保存します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:GetBucketPolicyStatus"
            ],
            "Resource": [
                "arn:aws:s3:::AWSDOC-EXAMPLE-BUCKET",
                "arn:aws:s3:::AWSDOC-EXAMPLE-BUCKET/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:111122223333:key/KEY-ID"
            ],
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "s3.us-east-1.amazonaws.com"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::AWSDOC-EXAMPLE-
BUCKET/S3-PREFIX*"
                }
            }
        }
    ]
```

```
}
```

次の例は、作成した IAM ロールにアタッチされている IAM 信頼ポリシーです。この例のポリシーを以下の 例: メールボックスコンテンツのエクスポート 手順で使用するには、ポリシーをJSON ファイルとして mailbox-export-trust-policy.json のファイル名で保存します。

aws:SourceArn および aws:SourceAccount の条件を同時に使用する必要はありません。例えば、同じ AWS アカウントで、同じロールを使用して異なる Amazon WorkMail 組織からメッセージをエクスポートする必要がある場合、ポリシーから aws:SourceArn を削除できます。条件キーの詳細については、AWS Identity and Access Management 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。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "export.workmail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:workmail:us-east-1:111122223333:organization/m-
a123b4c5de678fg9h0ij1k2lm234no56"
        }
      }
    }
  ]
}
```

AWS CLI を使用して、以下のコマンドを実行することにより、アカウントに IAM ロールを作成します。

```
aws iam create-role --role-name WorkmailMailboxExportRole --assume-role-policy-
document file://mailbox-export-trust-policy.json --region us-east-1
```

```
aws iam put-role-policy --role-name WorkmailMailboxExportRole --policy-
name MailboxExport --policy-document file://mailbox-export-policy.json
```

AWS CLI の詳細については、AWS Command Line Interface ユーザーガイドを参照してください。

例: メールボックスコンテンツのエクスポート

前のセクションで IAM ロールとポリシーを作成したら、次のステップを実行してメールボックスのコンテンツをエクスポートします。Amazon WorkMail 組織 ID とユーザー ID (エンティティ ID) が必要です。これは、Amazon WorkMail コンソールまたは Amazon WorkMail API を使用してアクセスできます。

例: メールボックスコンテンツをエクスポートするには

1. AWS CLI を使用して、メールボックスエクスポートジョブを開始します。

   ```
   aws workmail start-mailbox-export-job --organization-id m-
   a123b4c5de678fg9h0ij1k2lm234no56 --entity-
   id S-1-1-11-1111111111-2222222222-3333333333-3333 --kms-key-
   arn arn:aws:kms:us-east-1:111122223333:key/KEY-ID --role-arn
    arn:aws:iam::111122223333:role/WorkmailMailboxExportRole --s3-bucket-name AWSDOC-
   EXAMPLE-BUCKET --s3-prefix S3-PREFIX
   ```

2. AWS CLI を使用して、Amazon WorkMail 組織のメールボックスエクスポートジョブの状態をモニタリングします。

   ```
   aws workmail list-mailbox-export-jobs --organization-id m-
   a123b4c5de678fg9h0ij1k2lm234no56
   ```

   または、**start-mailbox-export-job** コマンドによって生成されたジョブ ID を使用して、そのメールボックスエクスポートジョブの状態のみをモニタリングします。

   ```
   aws workmail describe-mailbox-export-job --organization-id m-
   a123b4c5de678fg9h0ij1k2lm234no56 --job-id JOB-ID
   ```

メールボックスのエクスポートジョブの状態が完了済みの場合、エクスポートされたメールボックスアイテムは指定した Amazon S3 バケットの `.zip` ファイルにあります。

以下は、エクスポートされたメールボックスの出力ログの例です。

```
{
  "totalNonExportableItems" : "13",
  "totalMessages" : "76",
  "sha384Hash" : "4de93a***96a1dd",
  "totalBytes" : "161892",
  "totalFolders" : "15",
  "startTime" : "168***380",
  "endTime" : "168***384"
}
```

> **Note**
>
> TotalNonExportableItems は、メモや連絡先などのサポートされていないアイテムです。

考慮事項

Amazon WorkMail のメールボックスジョブをエクスポートする場合は、以下の考慮事項が適用されます。

- 特定の Amazon WorkMail 組織に対して、最大 10 個のメールボックスエクスポートジョブを同時に実行できます。
- 1 つのメールボックスのメールボックスエクスポートジョブは、24 時間に 1 回だけ実行できます。
- 以下のリソースはすべて同じ AWS リージョンにある必要があります。
  - Amazon WorkMail 組織ごとのユーザー組織
  - AWS KMS CMK
  - Amazon S3 バケット

トラブルシューティング

このセクションのトピックでは、Amazon の問題のトラブルシューティング方法について説明しますWorkMail。

トピック

- E メールヘッダーの表示
- メールルーティング

E メールヘッダーの表示

メールヘッダーの情報は、一般ユーザーの E メールの問題のトラブルシューティングに役立ちます。Amazon WorkMail では、任意のメッセージのヘッダー情報を表示できます。

Amazon で E メールヘッダーを表示するには WorkMail

1. Amazon WorkMail ウェブアプリケーションで、E メールメッセージをダブルクリックして開きます。
2. メッセージの右上隅の [送信日] の横にある [メッセージオプション] (歯車と封筒のアイコン) を選択します。

E メールヘッダーは、[インターネットヘッダー] の下に表示されます。

メールルーティング

ユーザーが E メールの受信を停止すると、Amazon WorkMail 組織でメールルーティングの問題が発生している可能性があります。このセクションのステップでは、配信とルーティングの問題を解決する一般的な方法について説明します。

受信メールに関する問題:

- Amazon WorkMail 組織に関連付けられているドメインの MX レコードを確認します。`WorkMail`は唯一のエントリで、 の優先度が最も低い必要があります。MX レコードが複数あると、間違ったサービスがメッセージを受信する可能性があります。MX レコードの詳細については、「ドメインの検証」を参照してください。

- Amazon WorkMail コンソールで、組織のドメインベースのメッセージ認証、レポート、および適合性 (DMARC) 設定を確認します。DMARC レコードは、ユーザーのアカウント認証情報を危険にさらす可能性のある、なりすましやフィッシングなどの一般的な攻撃から保護するために使用されます。DMARC の詳細については、「受信メールへの DMARC ポリシーの適用」を参照してください。
- Simple Email Service のインバウンドルールを確認してください。ルールに Amazon 以外のアクションが含まれている場合 WorkMail、これらのアクションは失敗し、Amazon WorkMail によるメールの受信が停止する可能性があります。Amazon SES ルールの詳細については、Amazon Simple Email Service デベロッパーガイドの「Amazon WorkMail アクションとの統合」を参照してください。
- Amazon でメッセージ追跡を有効にし WorkMail、配信の問題がないかログを確認します。メッセージを追跡する方法の詳細については、「E メールイベントロギングを有効にする」を参照してください。

アウトバウンドメールの問題

- SPF レコードに Amazon SES が含まれていることを確認してください。Amazon WorkMail コンソールのドメインページを確認して確認します。SPF の詳細については、「SPF での E メールの認証」を参照してください。
- Amazon にドメインを使用するアクセス許可 WorkMail があることを確認します。ない場合は、ドメインを再度追加してください。 このガイドのドメインの追加では、その方法について説明しています。

Amazon WorkMail での E メールジャーナリングの使用

ジャーナリングを設定して E メールの通信を記録するには、アーカイブ機能と eDiscovery 機能が統合されたサードパーティーのツールを使用します。これにより、プライバシー保護、データストレージ、情報保護に関する、E メールストレージのコンプライアンス規制を満たすことができます。

ジャーナリングの使用

Amazon WorkMail では、指定の組織のユーザー宛に送信される E メールメッセージや、その組織のユーザーより送信される E メールメッセージをすべてジャーナリングすることができます。E メールメッセージはすべて、システム管理者が指定したメールアドレス宛に `journal record` という形式でコピーが送信されます。この形式は、Microsoft メールプログラムと互換性があります。E メールジャーナリングの使用には追加料金はかかりません。

E メールジャーナリングでは、2 種類のメールアドレス (ジャーナリング用メールアドレスと報告用メールアドレス) を使用します。ジャーナリング用メールアドレスは、専用のメールボックス、またはアカウントに統合されているサードパーティーデバイスのメールアドレスです。ジャーナルレポートはこのメールアドレス宛に送信されます。レポート用メールアドレスは、システム管理者のメールアドレスです。ジャーナルレポートのエラー通知はこのメールアドレス宛に送信されます。

ジャーナルレコードは、ドメインに自動的に追加されているメールアドレスから送信されます。次のようになります。

```
amazonjournaling@yourorganization.awsapps.com
```

このメールアドレスに関連付けられているメールボックスは存在しないため、この名前またはメールアドレスを使用して作成することはできません。

> **Note**
>
> 次のドメインレコードをAmazon Simple Email Service (Amazon SES) コンソールから削除しないでください。E メールジャーナリングの動作が停止します。
>
> ```
> yourorganization.awsapps.com
> ```

受信メールメッセージまたは送信メールメッセージごとに 1 つのジャーナルレコードが生成されます。受取人やユーザーグループの数は関係ありません。ジャーナルレコードを生成できない場合は、エラーを通知する E メールが生成され、報告用メールアドレスに送信されます。

E メールジャーナリングを有効にするには

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

   必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。詳細については、「Amazon Web Services 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。
2. ナビゲーションペインで [組織] を選択し、組織の名前を選択します。
3. ナビゲーションペインの [組織の設定] で、[ジャーナリング] タブを選択し、[編集] を選択します。
4. ジャーナリングステータススライダーをオンの位置に移動します。
5. [ジャーナリングの E メールアドレス] に、E メールジャーナリングプロバイダーによって生成された E メールアドレスを入力します。

   > **Note**
   >
   > 専用ジャーナルプロバイダーを使用することをお勧めします。

6. [レポート用 E メールアドレス] に、E メール管理者のメールアドレスを入力します。
7. [保存] を選択します。変更はすぐに適用されます。

ドキュメント履歴

次の表は、『Amazon WorkMail 管理者ガイド』の各リリースにおける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を受け取るには、RSS フィードにサブスクライブできます。

変更	説明	日付
監査ログのサポート	監査ログは、メールボックスへのユーザーのアクセスの監視、不審なアクティビティの監査、アクセス制御と可用性プロバイダーの構成のデバッグに使用できます。詳細については、『Amazon WorkMail 管理者ガイド』の「監査ログの有効化」と「Amazon WorkMail での口ギングとモニタリング」を参照してください。	2024 年 3 月 20 日
トランスポート層セキュリティ (TLS) サポート	Amazon はトランスポート層セキュリティ (TLS) 1.0 と 1.1 WorkMail のサポートを終了しました。TLS 1.0 または 1.1 を使用している場合は、TLS バージョンを 1.2 にアップグレードする必要があります。	2023 年 11 月 2 日
リモートユーザー	リモートユーザーは、Amazon WorkMail 組織外でホストされている、または異なる E メールドメインでホストされている Amazon WorkMail ユーザーです。詳細については、『Amazon WorkMail 管理者ガ	2023 年 9 月 18 日

	イド』の「ユーザー」を参照してください。	
メールボックスへのプログラムによるアクセス	Amazon WorkMail では現在、メールボックスへのプログラムによるアクセスを許可する偽装ロールを提供しています。詳細については、『Amazon WorkMail 管理者ガイド』の「メールボックスへのプログラムによるアクセス」を参照してください。	2022 年 10 月 4 日
Amazon でのカスタム可用性プロバイダーの設定 WorkMail	Amazon はカスタム・アベイラビリティ・プロバイダー (CAP) WorkMail の使用をサポートしています。詳細については、『Amazon WorkMail 管理者ガイド』の「カスタム可用性プロバイダの設定」を参照してください。	2022 年 6 月 30 日
組織を作成するためのコンソールの変更	組織を作成するための Amazon WorkMail コンソールのエクスペリエンスが更新されました。詳細については、『Amazon WorkMail 管理者ガイド』の「組織の作成」を参照してください。	2020 年 10 月 23 日

メールボックスコンテンツのエクスポート	StartMailboxExportJob API アクションを使用して、Amazon WorkMail メールボックスのコンテンツを Amazon Simple Storage Service (Amazon S3) バケットにエクスポートします。詳細については、『Amazon WorkMail 管理者ガイド』の「メールボックスのコンテンツのエクスポート」を参照してください。	2020 年 9 月 22 日
メールボックス保持ポリシー	Amazon WorkMail 組織のメールボックス保存ポリシーを設定して、選択した期間が過ぎるとメールメッセージを自動的に削除するようにします。詳細については、『Amazon WorkMail 管理者ガイド』の「メールボックスの保存ポリシーの設定」を参照してください。	2020 年 5 月 28 日
同期および非同期Lambda の実行アクション	Amazon E メールフロールールの Run Lambda アクションの同期設定または非同期設定を選択します。 WorkMail 詳細については、『Amazon WorkMail 管理者ガイド』WorkMailの「Amazon AWS Lambda 用の設定」を参照してください。	2020 年 5 月 11 日

アクセスコントロールルールの使用	アクセス制御ルールにより、Amazon WorkMail 管理者は組織のメールボックスへのアクセス方法を制御できます。詳細については、『Amazon WorkMail 管理者ガイド』の「アクセスコントロールルールの使用」を参照してください。	2020 年 2 月 12 日
組織へのタグ付け	Amazon WorkMail 組織にタグを付けると、 AWS Billing and Cost Management コンソールで組織を区別したり、組織リソースへのアクセスを制御したりできます。詳細については、『Amazon WorkMail 管理者ガイド』の「組織にタグを付ける」を参照してください。	2020 年 1 月 23 日
受信メールに DMARC ポリシーを適用する	詳細については、 WorkMail Amazon管理者ガイドの「受信メールへのDMARCポリシーの適用」を参照してください。	2019 年 10 月 17 日
Lambda を使用したメッセージコンテンツの取得	Amazon WorkMail メッセージフロー API を使用して AWS Lambda 、メッセージコンテンツを取得します。詳細については、『Amazon WorkMail 管理者ガイド』の「Lambda によるメッセージコンテンツの取得」を参照してください。	2019 年 9 月 12 日

Amazon WorkMail メールイベントのロギング	Amazon WorkMail コンソールで E メールイベントロギングを有効にして、組織の E メールメッセージを追跡します。詳細については、『Amazon WorkMail 管理者ガイド』の「メッセージの追跡」を参照してください。	2019 年 5 月 13 日
Route 53 DNS レコードの挿入	Route 53 パブリックホストゾーンで管理されるドメインを設定すると、Amazon WorkMail は自動的に DNS レコードを挿入します。詳細については、『Amazon WorkMail 管理者ガイド』の「ドメインの追加」を参照してください。	2019 年 2 月 13 日
受信 E メールのルールアクションに関する Lambda の設定	Amazon WorkMail では、インバウンド E メールのフロールールで使用する Lambda 関数の設定をサポートしています。詳細については、Amazon WorkMail 管理者ガイドの「E メールフローの管理」を参照してください。	2019 年 1 月 24 日
Amazon 向けLambda 設定 WorkMail	Amazon WorkMail では、アウトバウンド E メールのフロールールで使用する Lambda 関数の設定をサポートしています。詳細については、『WorkMail アマゾン管理者ガイド』の「Amazon WorkMail 用 Lambda の設定」を参照してください。	2018 年 11 月 19 日

SMTP ルーティング	Amazon WorkMail では、送信メールフロールールで使用する SMTP ゲートウェイの設定をサポートしています。詳細については、『Amazon WorkMail 管理者ガイド』の「SMTP ゲートウェイの設定」を参照してください。	2018 年 11 月 1 日
カスタムドメインのデバッグツール	Amazon WorkMail はカスタムドメイン用のデバッグツールを追加しました。詳細については、『Amazon WorkMail 管理者ガイド』の「ドメインの追加」を参照してください。	2018 年 10 月 15 日
Outlook 2019 のサポート	Amazon WorkMail は Windows と macOS 用の Outlook 2019 をサポートしています。詳細については、『Amazon WorkMail 管理者ガイド』の「Amazon WorkMail システム要件」を参照してください。	2018 年 10 月 1 日
さまざまな更新	トピックレイアウトと組織へのさまざまな更新。	2018 年 7 月 12 日
メールボックスのアクセス許可	Amazon WorkMail のメールボックス権限を使用して、他のユーザーのメールボックスで作業する権限をユーザーまたはグループに付与できます。詳細については、『Amazon WorkMail 管理者ガイド』の「メールボックスの権限の使用」を参照してください。	2018 年 4 月 9 日

のSupport AWS CloudTrail	Amazon WorkMail と統合されています AWS CloudTrail。詳細については、『Amazon WorkMail 管理者ガイド』の「Amazon WorkMail API AWS CloudTrail呼び出しのロギング」を参照してください。	2017 年 12 月 12 日
E メールフローに対応	送信者の E メールアドレスまたはドメインに基づき、受信メールを処理する E メールフロールールを設定できます。詳細については、Amazon WorkMail 管理者ガイドの「E メールフローの管理」を参照してください。	2017 年 7 月 5 日
高速セットアップの更新	クイックセットアップで Amazon WorkMail ディレクトリが作成されるようになりました。詳細については、『Amazon WorkMail WorkMail 管理者ガイド』の「クイックセットアップによる Amazon のセットアップ」を参照してください。	2017 年 5 月 10 日
E メールクライアントのサポート範囲の拡大	Mac および IMAP メールクライアント用の Microsoft Outlook 2016 WorkMail で Amazon を使用できるようになりました。詳細については、『Amazon WorkMail 管理者ガイド』の「Amazon WorkMail のシステム要件」を参照してください。	2017 年 1 月 9 日

SMTP ジャーナリングに対応	ジャーナリングを設定して、E メール通信を記録することができます。詳細については、『Amazon WorkMail 管理者ガイド』の「Amazon WorkMail での E メールジャーナリングの使用」を参照してください。	2016 年 11 月 25 日
外部の E メールアドレスへの E メールのリダイレクトに対応	E メールのリダイレクトルールを設定するには、Amazon SES 識別ポリシーをドメイン向けに更新します。詳細については、『Amazon WorkMail 管理者ガイド』の「ドメイン ID ポリシーの編集」を参照してください。	2016 年 10 月 26 日
相互運用性をサポート	Amazon WorkMail とMicrosoft エクスチェンジ間の相互運用性を有効にすることができます。詳細については、『WorkMail アマゾン管理者ガイド』の「Amazon WorkMail と Microsoft Exchange の相互運用性」を参照してください。	2016 年 10 月 25 日
一般提供	Amazon WorkMail の一般提供リリースです。	2016 年 1 月 4 日
リソースの予約に対応	会議室や機器などのリソースの予約に対応しました。詳細については、『Amazon WorkMail 管理者ガイド』の「リソースの使用」を参照してください。	2015 年 10 月 19 日

E メールの移行ツールに対応	E メールの移行ツールに対応。詳細については、『Amazon WorkMail 管理者ガイド』 WorkMailの「Amazon への移行」を参照してください。	2015 年 8 月 16 日
Amazon のプレビューリリース WorkMail	Amazon WorkMail ンのプレビューリリースです。	2015 年 1 月 28 日

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。