リファレンスガイド

AWS アカウント管理

AWS アカウント管理: リファレンスガイド

Table of Contents

とは AWS アカウント 1
の機能 AWS アカウント 3
初めての AWS ユーザーですか? 3
関連 AWS サービス 4
ルートユーザーの使用 4
サポートとフィードバック 5
その他の AWS リソース 5
アカウントの使用の開始 7
ステップ 1: アカウントを作成する 7
ステップ 2: (推奨) をインストールする AWS CLI 10
ステップ 3: (推奨) AWS MCP サーバーを設定する 10
アカウントへのアクセス 10
ガバナンス構造の計画 12
複数の を使用する利点 AWS アカウント 12
複数の の管理 AWS アカウント 13
を使用するタイミング AWS Organizations 14
信頼されたアクセスを有効にする 15
委任管理者アカウントの有効化 16
SCP を使用したアクセスの制限 18
を使用するタイミング AWS Control Tower 19
API 操作モードについて 20
アカウント属性を更新するアクセス許可の付与 21
アカウントの設定 24
アカウントエイリアスの作成または更新 24
アカウント AWS リージョン で を有効または無効にする 24
リージョンの可用性リファレンス 27
リージョンを有効化または無効化する前の考慮事項 30
処理時間とリクエスト制限 31
スタンドアロンアカウントのリージョンの有効化または無効化 31
組織内のリージョンの有効化または無効化 33
の請求を更新する AWS アカウント 36
ルートユーザーの E メールと の更新 36
スタンドアロンアカウント AWS アカウント または管理アカウントのルートユーザー E メール メールを更新する 37

組織 AWS アカウント 内の任意の のルートユーザー E メールを更新する 38
ルートユーザーのパスワードの更新 41
AWS アカウント 名前を更新する 42
スタンドアロンのアカウント名を更新する AWS アカウント 43
組織 AWS アカウント 内の のアカウント名を更新する 45
の代替連絡先を更新する AWS アカウント 46
電話番号と E メールアドレスの要件 47
スタンドアロンの代替連絡先を更新する AWS アカウント 47
組織 AWS アカウント 内の任意の の代替連絡先を更新する 51
account:AlternateContactTypes コンテキストキー 54
のプライマリ連絡先を更新する AWS アカウント 55
電話番号と E メールアドレスの要件 55
スタンドアロンアカウント AWS アカウント または管理アカウントのプライマリ連絡先を更新する 56
組織内の AWS メンバーアカウントのプライマリ連絡先を更新する 58
アカウント ID の表示 61
AWS アカウント ID を検索する 61
の正規ユーザー ID を検索する AWS アカウント 64
アカウントの保護 67
データ保護 68
AWS PrivateLink 69
エンドポイントを作成する 69
Amazon VPC エンドポイントポリシー 70
エンドポイントポリシー 70
Identity and Access Management 71
オーディエンス 71
アイデンティティを使用した認証 71
ポリシーを使用したアクセスの管理 73
AWS アカウント管理と IAM 75
アイデンティティベースのポリシーの例 83
アイデンティティベースのポリシーを使用する 86
トラブルシューティング 89
AWS マネージドポリシー 91
AWSAccountManagementReadOnlyAccess 92
AWSAccountManagementFullAccess 93
ポリシーの更新 94

コンプライアンス検証 94
耐障害性 95
インフラストラクチャセキュリティ 95
アカウントのモニタリング 97
CloudTrail ログ 97
CloudTrail でのアカウント管理情報 98
アカウント管理のログエントリについて 99
EventBridge によるアカウント管理イベントのモニタリング 102
アカウント管理イベント 102
アカウントのトラブルシューティング 105
アカウント作成の問題 105
アカウント閉鎖の問題 106
アカウントを削除またはキャンセルする方法がわからない 106
[アカウント] ページに [アカウントを閉鎖する] ボタンが表示されない 106
アカウントを閉鎖したが、まだ確認 E メールを受け取っていない 107
アカウントを閉鎖しようとすると、「ConstraintViolationException」エラーが表示される . 107
メンバーアカウントを閉鎖しようとすると「CLOSE_ACCOUNT_QUOTA_EXCEEDED」エラーが表示される 107
管理アカウントを閉鎖する前に AWS 組織を削除する必要がありますか? 108
その他の問題 108
のクレジットカードを変更する必要があります AWS アカウント 108
不正行為を報告する必要がある AWS アカウント 108
を閉じる必要があります AWS アカウント 108
アカウントの閉鎖 109
アカウントを閉鎖する前の確認事項 109
アカウントの閉鎖方法 111
アカウントの閉鎖後に予想されること 114
閉鎖後期間 114
を再開する AWS アカウント 115
API リファレンス 116
アクション 118
AcceptPrimaryEmailUpdate 119
DeleteAlternateContact 124
DisableRegion 129
EnableRegion 133
GetAccountInformation 137

GetAlternateContact ... 143
GetContactInformation ... 149
GetGovCloudAccountInformation ... 153
GetPrimaryEmail ... 159
GetRegionOptStatus ... 163
ListRegions ... 167
PutAccountName ... 172
PutAlternateContact ... 177
PutContactInformation ... 183
StartPrimaryEmailUpdate ... 187
関連アクション ... 191
CreateAccount ... 191
CreateGovCloudAccount ... 191
DescribeAccount ... 191
データ型 ... 191
AlternateContact ... 193
ContactInformation ... 195
Region ... 199
ValidationExceptionField ... 200
共通パラメータ ... 200
一般的なエラータイプ ... 202
HTTP クエリリクエストの作成 ... 205
エンドポイント ... 206
HTTPS の必要性 ... 206
AWS アカウント管理 API リクエストの署名 ... 206
クォータ ... 208
インドでのアカウントの管理 ... 210
India AWS アカウント で を作成する AWS ... 210
顧客検証情報の管理 ... 213
顧客検証ステータスの確認 ... 213
顧客検証情報の作成 ... 213
顧客検証情報の編集 ... 214
顧客確認用にインドで受け入れられるドキュメント ... 215
AWS India アカウントを管理する ... 216
ドキュメント履歴 ... 217
... ccxx

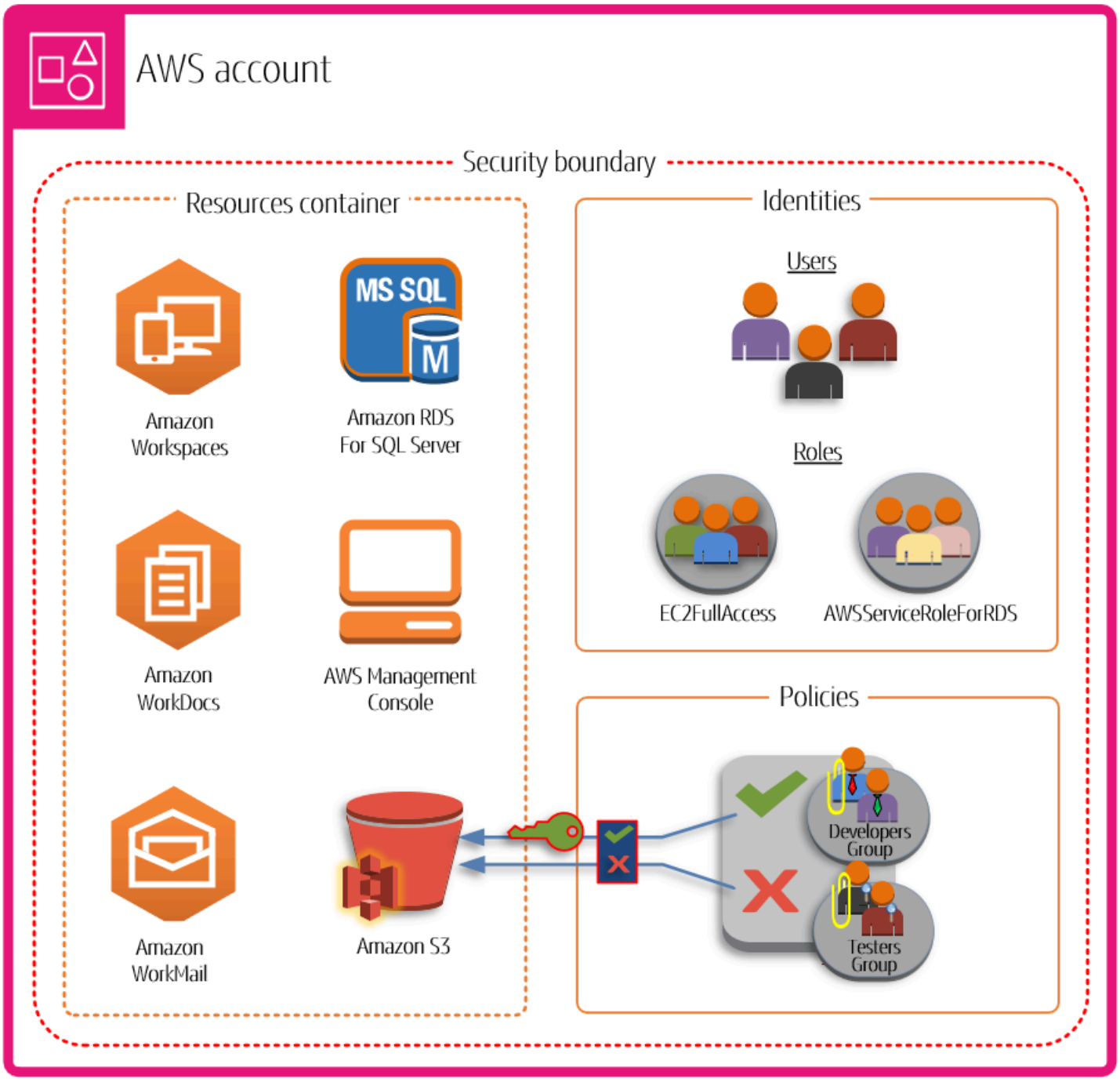
とは AWS アカウント

は、お客様が確立した正式なビジネス関係 AWS アカウント を表します AWS。で AWS リソースを作成および管理し AWS アカウント、アカウントはアクセスと請求のための ID 管理機能を提供します。それぞれに一意の ID AWS アカウント があり、他の ID と区別されます AWS アカウント。

クラウドリソースとデータは、 AWS アカウントに格納されています。アカウントは Identity and access management の分離境界として機能します。2 つのアカウント間でリソースとデータを共有する必要がある場合は、このアクセスを明示的に許可する必要があります。デフォルトでは、アカウント間のアクセスは許可されていません。例えば、本番環境および非本番環境のリソースとデータを格納するために異なるアカウントを指定する場合、デフォルトではこれらの環境間でのアクセスは許可されません。

AWS アカウント は、 AWS サービスへのアクセスの基本的な部分でもあります。次の図に示すように、 AWS アカウント には 2 つの主要な関数があります。

- リソースコンテナ – AWS アカウント は、 AWS 顧客として作成するすべての AWS リソースの基本的なコンテナです。例えば、Amazon Simple Storage Service (Amazon S3) バケット、Amazon Relational Database Service (Amazon RDS) データベース、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスはすべてリソースです。すべてのリソースは、リソースを含む、または所有しているアカウントのアカウント ID を含む Amazon リソースネーム (ARN) によって一意に識別されます。
- セキュリティ境界 – AWS アカウント は、 AWS リソースの基本的なセキュリティ境界でもあります。アカウントで作成したリソースは、そのアカウントに対する認証情報を持つユーザーが使用できます。アカウントで作成できる主要なリソースの 1 つに、ユーザーやロールなどの ID があります。ID には、 AWSへのサインイン (認証) に使用できる認証情報があります。また、ID には、ユーザーがアカウント内のリソースで何を実行できるか (認可) を指定するアクセス許可ポリシーもあります。



複数の を使用すること AWS アカウント は、環境をスケーリングするためのベストプラクティスです。これは、コストの自然な請求境界を提供し、セキュリティのためにリソースを分離し、新しいビジネスプロセスに適応できるだけでなく、個人やチームに柔軟性を与えるためです。詳細については、「複数の を使用する利点 AWS アカウント」を参照してください。

の機能 AWS アカウント

AWS アカウント には、次の主要機能が含まれています。

- コストのモニタリングと制御 – アカウントは、 AWS コストを割り当てるデフォルトの手段です。このため、異なるビジネスユニットやワークロードのグループごとに異なるアカウントを使用することで、クラウド支出をより簡単に追跡、制御、予測、予算編成、報告できるようになります。アカウントレベルでのコストレポートに加えて、 には、 AWS Organizations ある時点で を使用することを選択した場合に、アカウント全体のコストを統合してレポートするためのサポート AWS も組み込まれています。また、 AWS Service Quotas を使用して、 AWS コストに劇的な影響を与える可能性のある AWS リソースの予期しない過剰なプロビジョニングや悪意のあるアクションから保護することもできます。
- 分離単位 – AWS アカウント は、 AWS リソースの自律性と分離を実現するのに役立つリソースのセキュリティ、アクセス、請求の境界を提供します。設計上、アカウント内でプロビジョニングされたすべてのリソースは、独自の AWS 環境内であっても、他のアカウントでプロビジョニングされたリソースから論理的に分離されます。この分離境界により、アプリケーション関連の問題、設定ミス、または悪意のあるアクションのリスクを制限する方法が提供されます。1 つのアカウント内で問題が発生した場合に、他のアカウントに含まれるワークロードへの影響を軽減または排除することができます。
- ビジネスワークロードのミラーリング – 複数のアカウントを使用して、共通のビジネス目的を持つワークロードを個別のアカウントにグループ化します。その結果、所有権と意思決定がそれらのアカウントに沿ったものになり、他のアカウントのワークロードをセキュリティ保護および管理する方法との依存関係や競合を回避できます。全体的なビジネスモデルに応じて、異なるアカウントで個別のビジネスユニットや子会社を分離することを選択できます。このアプローチにより、時間の経過に伴ってそれらのユニットを売却することも容易になる可能性があります。

初めての AWS ユーザーですか?

を初めて使用する場合 AWS、最初のステップは にサインアップすることです AWS アカウント。サインアップすると、 は指定した詳細でアカウント AWS を作成し、アカウントを割り当てます。を作成したら AWS アカウント、ルートユーザーとしてサインインし、ルートユーザーの多要素認証 (MFA) を有効にして、ユーザーに管理アクセスを割り当てます。

新しいアカウントを設定するステップバイステップの手順については、「の開始方法 AWS アカウント」を参照してください。

関連 AWS サービス

AWS アカウント は、次のサービスとシームレスに連携します。

- IAM

  AWS アカウント は AWS Identity and Access Management (IAM) と緊密に統合されています。アカウントで IAM を使用することで、そのアカウントで作業する他のユーザーに対して、そのユーザーが自分の業務を遂行するために必要なアクセスのみを付与できるようになります。また、IAM を使用して、アカウント固有の情報だけでなく、すべての AWS リソースへのアクセスを制御します。 AWS アカウントの構造の設定を大きく進める前に、IAM の主要な概念とベストプラクティスを十分に理解しておくことが重要です。詳細については、「IAM ユーザーガイド」の「IAM でのセキュリティベストプラクティス」を参照してください。

- AWS Organizations

  会社が大きい場合、または成長する可能性がある場合は、会社の特定の構造を反映する複数の AWS アカウントをセットアップすることをお勧めします。 は、マルチアカウント環境を構築および管理するための基盤となるインフラストラクチャと機能 AWS Organizations を提供します。既存のアカウントを組織に結合して、アカウントを一元管理することができます。自動的に組織の一部であるアカウントを作成し、他のアカウントを組織に招待することができます。アカウントの一部または全部に影響するポリシーをアタッチすることもできます。詳細については、「を使用するタイミング AWS Organizations」を参照してください。

- AWS Control Tower

  AWS Control Tower は、安全なマルチアカウント AWS 環境をセットアップして管理するための簡単な方法を提供します。 は、 を使用してマルチアカウント環境の作成 AWS Control Tower を自動化し、初期アカウントのセットをインスタンス化し AWS Organizations、環境のいくつかのデフォルトのガードレールと設定を使用します。 AWS Control Tower を使用して、アカウントが組織のポリシーに準拠していることを確認すると同時に、いくつかのステップ AWS アカウントで新しい をプロビジョニングできます。詳細については、「を使用するタイミング AWS Control Tower」を参照してください。

の使用 AWS アカウントのルートユーザー

を作成するときは AWS アカウント、まず、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 AWS アカウント root ユーザーと呼ばれる 1 つのサインインアイデンティティから始めます。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

ユーザー認証情報を必要とするタスクについては、「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。

日常業務にルートユーザーを使用することを回避するために、AWS IAM アイデンティティセンターで管理ユーザーを設定する方法について説明します。ルートユーザーのセキュリティに関するその他の推奨事項については、「AWS アカウントのルートユーザーのベストプラクティス」を参照してください。

> **Important**
>
> のルートユーザー認証情報を持つユーザーは、請求情報を含むアカウント内のすべてのリソースに AWS アカウント 無制限にアクセスできます。

ルートユーザーのパスワードを変更またはリセットしたり、ルートユーザーのアクセスキー (アクセスキー ID とシークレットアクセスキー) を作成または削除したりできます。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、「サインインユーザーガイド」の「ルートユーザー AWS マネジメントコンソール として にサインインする」を参照してください。 AWS

AWS アカウント管理のサポート

AWS アカウント管理サポートフォーラムを使用して、フィードバックや質問を投稿できます。AWS フォーラムの一般的な情報については、「」を参照してくださいAWS re:Post。

探している回答が見つからない場合は AWS re:Post、 を使用してアカウントまたは請求関連のサポートケースを作成できます AWS マネジメントコンソール。詳細については、「Example: Create a support case for account and billing」を参照してください。

その他の AWS リソース

- AWS トレーニングとコース – AWS スキルを磨き、実践的な経験を積むのに役立つ、ロールベースのコースや専門コース、セルフペースラボへのリンク。
- AWS デベロッパーツール – 革新的なアプリケーションの構築に役立つドキュメント、コード例、リリースノート、その他の情報を提供するデベロッパーツールとリソースへのリンク AWS。
- AWS サポート センター – AWS サポートケースを作成および管理するためのハブ。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 などの便利なリソースへのリンクも含まれています。

- AWS サポート – AWS 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 の高速応答サポートチャネルである サポートに関する情報のプライマリウェブページ。
- お問い合わせ — AWS 請求、アカウント、イベント、不正使用、その他の問題に関するお問い合わせの中心的な連絡先です。
- AWS サイト規約 – 当社の著作権と商標、お客様のアカウント、ライセンス、サイトアクセス、およびその他のトピックに関する詳細情報。

の開始方法 AWS アカウント

を初めて使用する場合は AWS、 にサインアップする必要があります AWS アカウント。これを行うと、 AWS は提供された詳細情報を使用してアカウントを作成してお客様に割り当てます。

にサインアップするには AWS アカウント、次の情報を提供する必要があります。

- ルートユーザーの E メールアドレスと – この E メールアドレスは、ルートユーザーのサインイン名として使用され、アカウントの回復に必要です。このアドレスに送信される電子メールを受信できる必要があります。特定のタスクを実行する前に、このアドレスに送信された電子メールへのアクセス権があることを確認する必要があります。
- AWS アカウント名 – アカウントの名前は、請求書、請求情報とコスト管理ダッシュボード、コンソールなどの AWS Organizations コンソールなど、複数の場所に表示されます。アカウントに名前を付ける際に標準的な方法を使用することで、アカウント名を認識しやすいものにすることをお勧めします。会社のアカウントの場合は、組織-目的-環境 (例えば、AnyCompany-audit-prod) のような命名基準を使用することを検討してください。個人アカウントの場合は、名-姓-目的 (例えば、paulo-santos-testaccount) のような命名基準を使用することを検討してください。
- 住所 – 連絡先と請求先住所がインドにある場合、アカウントのユーザー契約は、インドの現地 AWS 販売者である Amazon Web Services India Private Limited (AWS インド) と締結されます。検証プロセスの一部として CVV を指定する必要があります。銀行によっては、ワンタイムパスワードを入力する必要がある場合もあります。 AWS India は、検証プロセスの一環として支払い方法 2 INR を請求します。 AWS India は、検証が完了した後に 2 INR を返金します。
- 電話番号 – この番号は、本人確認とアカウントの所有権の確認に使用されます。この電話番号で通話と SMS メッセージを受信できる必要があります。

> **Important**
>
> このアカウントがビジネス用である場合は、従業員が転職したり退職したり AWS アカウント しても、会社が へのアクセスを保持できるように、会社の電話番号を使用してください。

ステップ 1: アカウントを作成する

これらの手順は、インド AWS アカウント 以外で を作成するためのものです。インドでのアカウントの作成については、「India AWS アカウント で を作成する AWS」を参照してください。が管理

する組織の一部であるアカウントを作成するには AWS Organizations、AWS Organizations 「 ユーザーガイド」の「組織内のメンバーアカウントの作成」を参照してください。

AWS マネジメントコンソール

を作成するには AWS アカウント

1. AWSのサインアップページを開きます。
2. ルートユーザーの E メールアドレスと AWS アカウント 名前を入力し、E メールアドレスの検証を選択します。これにより、検証コードが E メールアドレスに送信されます。

> **Important**
>
> このアカウントがビジネス用である場合は、安全な企業ディストリビューションリスト (などit.admins@example.com) を使用して、従業員が転職したり退職したり AWS アカウント しても、会社が へのアクセスを保持できるようにします。この E メールアドレスはアカウントのルートユーザー認証情報のリセットに使用できるため、この配信リストやアドレスへのアクセスを保護してください。

3. 検証コードを入力し、[検証] を選択します。
4. ルートユーザーの強力なパスワードを入力し、確認してから、続行を選択します。パスワードが次の条件を満たす AWS 必要があります。
   - 8 ~ 128 文字で構成されていること。
   - 英字の大文字、英字の小文字、数字、記号 (! @ # $ % ^ & * () <> [] {} | _+-=) のうち、少なくとも 3 つの文字タイプを使用する必要があります。
   - AWS アカウント 名前や E メールアドレスと同じにすることはできません。
5. アカウントプランを選択します。詳細については、「 無料利用枠プラン」を参照してください。
6. 連絡先情報を入力し、 AWS カスタマーアグリーメントを読んで同意します。承諾する前に、必ず用語を理解してください。

> **Important**
>
> このアカウントがビジネス用である場合は、個人の電話番号ではなく会社の電話番号を入力するのがベストプラクティスです。個人の E メールアドレスや個人の電話番

号でアカウントのルートユーザーを設定すると、アカウントが安全でなくなる可能性があります。

7. 請求情報を入力します。請求情報に別の AWS 請求先住所を使用する場合は、新しい住所を使用するを選択します。

   有効な支払い方法を追加するまでは、サインアッププロセスを続行できません。

8. ID の確認が必要になる場合があります。

   a. 国またはリージョンコードには、数分以内に連絡できる電話番号を入力します。

   b. 電話番号には、数分以内に到達できる電話番号を入力します。

   c. SMS の送信 を選択します。

   d. 自動システムから連絡があったら、受け取ったコードを入力し、続行を選択します。

9. 利用可能な AWS サポート プランのいずれかを選択します。利用可能な Support プランとその利点の説明については、「サポート プランの比較」を参照してください。

10. [登録を完了] を選択します。アカウントがアクティブ化されていることを示す確認ページが表示されます。

11. アカウントが有効化されたことを確認する E メールメッセージが届いているか、E メールフォルダとスパムフォルダを確認します。有効化は、通常は数分で完了しますが、場合によっては最大 24 時間かかることがあります。

12. アクティベーションメッセージを受信したら、 にサインインAWS マネジメントコンソールして使用を開始できます AWS のサービス。アカウント設定の管理方法に関する一般情報については、「を設定する AWS アカウント」を参照してください。

複数の AWS アカウント マネージドスルーの場合は AWS Organizations、IAM Identity Center の管理ユーザーに管理アクセスを割り当てます。手順については、「IAM Identity Center ユーザーガイド」の「IAM Identity Center 管理ユーザーの AWS アカウント アクセスを設定する」を参照してください。

AWS CLI & SDKs

組織内の管理アカウントにサインインした状態で CreateAccount 操作を実行すると、 AWS Organizations が管理する組織にメンバーアカウントを作成できます。

AWS Command Line Interface (AWS CLI) または AWS API オペレーションを使用して、組織の AWS アカウント 外部でスタンドアロンを作成することはできません。

ステップ 2: (推奨) をインストールする AWS CLI

「 のインストール」の AWS CLI 手順に従って、 をインストールします。 AWS CLIバージョン 2.32.0 以降が必要です。

を使用して AWS CLI 、エージェントにユーザーに代わって AWS リソースを管理させることができます。

をインストールしたら AWS CLI、次のコマンドを使用してプログラムでサインインします。

```
aws login
```

これにより、認証情報が 15 分ごとに自動的にローテーションされ、手動操作なしでセッションが最大 12 時間有効になります。

次のコマンドを使用して、認証情報が機能していることを確認します。

```
aws sts get-caller-identity
```

へのアクセスの詳細については AWS アカウント、「」を参照してくださいへのアクセス AWS アカウント。

ステップ 3: (推奨) AWS MCP サーバーを設定する

AWS MCP サーバーは、モデルコンテキストプロトコル (MCP) AWS を通じて へのアクセスをエージェントに許可するマネージドサーバーです。エージェントは、認証なしで AWS ドキュメントを検索し、サービス情報を取得できます。 AWS API コールを実行する、サンドボックス環境で Python スクリプトを実行する、または厳選されたスキルに従うには、エージェントは既存の IAM 認証情報を使用して認証します。詳細については、「 エージェントツールキットとは AWS 」を参照してください。

へのアクセス AWS アカウント

には、次のいずれか AWS アカウント の方法でアクセスできます。

AWS マネジメントコンソール

> AWS マネジメントコンソール は、 AWS アカウント 設定と AWS リソースの管理に使用できるブラウザベースのインターフェイスです。

AWS コマンドラインツール

AWS コマンドラインツールを使用すると、システムのコマンドラインでコマンドを発行して、AWS アカウント および AWS タスクを実行できます。コマンドラインを使用すると、コンソールよりも高速かつ便利になります。コマンドラインツールは、 AWS タスクを実行するスクリプトを構築する場合にも便利です。 は、次の 2 セットのコマンドラインツール AWS を提供します。

- AWS Command Line Interface (AWS CLI)。 のインストールと使用の詳細については AWS CLI、 AWS Command Line Interface ユーザーガイドを参照してください。
- AWS Tools for Windows PowerShell。Tools for Windows PowerShell のインストールおよび使用の方法については、AWS Tools for PowerShell ユーザーガイドを参照してください。

AWS SDK

AWS SDKs は、さまざまなプログラミング言語とプラットフォーム (Java、Python、Ruby、.NET、iOS、Android など) 用のライブラリとサンプルコードで構成されています。SDK は、暗号署名によるリクエスト、エラーの管理、リクエストの自動再試行などのタスクを処理します。 AWS SDKs「Amazon Web Services のツール」を参照してください。

AWS アカウント管理 HTTPS クエリ API

AWS アカウント管理 HTTPS クエリ API を使用すると、 AWS アカウント および へのプログラムによるアクセスが可能になります AWS。HTTPS クエリ API を使用すると、HTTPS リクエストを直接サービスに発行できます。HTTPS API を使用する場合は、認証情報を使用してリクエストにデジタル署名するコードを含める必要があります。詳細については、「HTTP クエリリクエストを作成して API を呼び出す」を参照してください。

AWS アカウント ガバナンス構造を計画する

1 つのアカウントで AWS ジャーニーを開始したかもしれませんが、 では、ワークロードのサイズと複雑さが大きくなるにつれて、複数のアカウントを設定する AWS ことをお勧めします。中規模企業であっても大企業であっても、データとワークロードのニーズを確実に満たすガバナンス構造の計画を作成する必要があります。

このセクションでは、マルチアカウントガバナンス構造を実現するために AWS で使用できる利点とガバナンスサービスについて説明します。

トピック

- 複数の を使用する利点 AWS アカウント
- を使用するタイミング AWS Organizations
- を使用するタイミング AWS Control Tower
- API 操作モードについて

複数の を使用する利点 AWS アカウント

AWS アカウント で基本的なセキュリティ境界を形成します AWS クラウド。これらはリソースのコンテナとして機能し、安全で適切に管理された環境を作成するために不可欠な重要な分離レイヤーを提供します。詳細については、「とは AWS アカウント」を参照してください。

リソースを分離 AWS アカウント することで、クラウド環境で次の原則をサポートできます。

- セキュリティコントロール - アプリケーションごとに異なるセキュリティプロファイルがあり、それらの周りに異なるコントロールポリシーとメカニズムが必要になる場合があります。例えば、監査人と話す方がはるかに簡単で、Payment Card Industry (PCI) セキュリティ標準の対象となるワークロードのすべての要素を AWS アカウント ホストする単一の を指すことができます。
- 分離 – AWS アカウント はセキュリティ保護の単位です。潜在的なリスクとセキュリティ上の脅威は、他の に影響を与え AWS アカウント ずに に含める必要があります。チームやセキュリティプロファイルが異なるため、セキュリティニーズが異なる場合があります。
- 多数のチーム - チームごとに異なる責任とリソースニーズがあります。チームを別々の場所に移動することで、チームが互いに干渉するのを防ぐことができます AWS アカウント。
- データの分離 — チームの分離に加えて、データストアをアカウントに分離することが重要です。これにより、そのデータストアにアクセスして管理できるユーザーの数を制限できます。これに

は、高度にプライベートなデータへの暴露が含まれており、一般データ保護規則 (GDPR) への適合に役立ちます。

- 業務プロセス - 事業単位や製品によって目的やプロセスが異なる場合があります。複数の を使用すると AWS アカウント、ビジネスユニットの特定のニーズをサポートできます。
- 請求 — アカウントは、請求レベルで項目を分ける唯一の真の方法です。複数のアカウントは、ビジネスユニット、機能チーム、または個々のユーザー間で課金レベルでアイテムを分離するのに役立ちます。明細項目を区切りながら、すべての請求書を 1 つの支払者 (AWS Organizations と一括請求を使用) に統合できます AWS アカウント。
- クォータ割り当て – AWS サービスクォータは、それぞれ個別に適用されます AWS アカウント。ワークロードを異なる AWS アカウント に分けることで、互いのクォータを消費し合うのを防止できます。

このドキュメントで説明しているすべての推奨事項と手順は、AWS Well-Architected フレームワークに適合するものです。このフレームワークは、柔軟性、耐障害性、スケーラブルなクラウドインフラストラクチャの設計を支援することを目的としています。小規模から始める場合でも、フレームワークにおけるこのガイダンスを守りながら進めることをお勧めします。そうすることで、成長に伴う継続的な運用に影響を与えることなく、環境を安全に拡張できます。

複数の の管理 AWS アカウント

複数のアカウントを追加する前に、アカウントの管理計画を策してください。そのためには、組織内のすべての を管理する無料の AWS サービスAWS Organizationsである AWS アカウント を使用することをお勧めします。

AWS は も提供します。これにより AWS Control Tower、Organizations に AWS マネージドオートメーションのレイヤーが追加され AWS CloudTrail AWS Config、Amazon CloudWatch AWS Service Catalogなどの他の AWS サービスと自動的に統合されます。これらのサービスには追加料金が発生する可能性があります。詳細については、「AWS Control Tower 料金表」を参照してください。

関連情報

- を使用するタイミング AWS Organizations
- を使用するタイミング AWS Control Tower

を使用するタイミング AWS Organizations

AWS Organizations は、 をグループ AWS アカウント として管理するために使用できる AWS サービスです。このサービスには、アカウントのすべての請求書をグループ化し、単一の支払者によって処理可能にする一括請求 (コンソリデーティッドビリング) などの機能が備わっています。ポリシーベースのコントロールを使用して、組織のセキュリティを一元的に管理することもできます。詳細については AWS Organizations、AWS Organizations 「 ユーザーガイド」を参照してください。

信頼されたアクセス

AWS Organizations を使用してアカウントをグループとして管理する場合、組織のほとんどの管理タスクは組織の管理アカウントでのみ実行できます。デフォルトでは、組織自体の管理に関連する操作のみが含まれます。Organizations とその AWS サービス間の信頼されたアクセスを有効にすることで、この追加機能を他の サービスに拡張できます。信頼されたアクセスは、組織とそれに含まれるアカウントに関する情報にアクセスするためのアクセス許可を指定された AWS サービスに付与します。アカウント管理の信頼されたアクセスを有効にすると、アカウント管理サービスは、組織のすべてのメンバーアカウントのメタデータ (主要連絡先情報や代替連絡先情報など) にアクセスするためのアクセス許可を組織およびその管理アカウントに付与します。

詳細については、「AWS アカウント管理の信頼されたアクセスを有効にする」を参照してください。

委任管理者

信頼されたアクセスを有効にしたら、いずれかのメンバーアカウントを AWS アカウント管理の委任管理者アカウントとして指定することもできます。これにより、委任管理者アカウントは、これまで管理アカウントのみが行えた、組織内のメンバーアカウントに対するアカウント管理のメタデータ管理タスクを実行できるようになります。委任管理者アカウントは、アカウント管理サービスの管理タスクにのみアクセスできます。委任管理者アカウントは、管理者アカウントが持つ組織に対するすべての管理者アクセス権を持っているわけではありません。

詳細については、「アカウント管理の委任管理者 AWS アカウントを有効にする」を参照してください。

サービスコントロールポリシー

AWS アカウント が によって管理されている組織の一部である場合 AWS Organizations、組織の管理者は、メンバーアカウントのプリンシパルが実行できる操作を制限できるサービスコントロールポリシー (SCPs) を適用できます。SCP はアクセス許可を付与するものではなく、メンバーアカウントが使用できるアクセス許可を制限するフィルターです。メンバーアカウントのユーザーまたは

ロール (プリンシパル) は、そのアカウントに適用される SCP とプリンシパルにアタッチされた IAM アクセス許可ポリシーの両方によって許可される操作のみを実行できます。例えば、SCP を使用して、アカウントのプリンシパルが自分のアカウントの代替連絡先を変更できないように設定することもできます。

が適用される SCPs「」を参照してくださいAWS Organizations サービスコントロールポリシーを使用してアクセスを制限する。 AWS アカウント

AWS アカウント管理の信頼されたアクセスを有効にする

AWS アカウント管理の信頼されたアクセスを有効にすると、管理アカウントの管理者は、 の各メンバーアカウントに固有の情報とメタデータ (プライマリまたは代替の連絡先の詳細など) を変更できます AWS Organizations。詳細については、「AWS Organizations ユーザーガイド」の「AWS Account Management and AWS Organizations」を参照してください。信頼されたアクセスの仕組みに関する一般的な情報については、「他の AWS サービス AWS Organizations での の使用」を参照してください。

信頼されたアクセスが有効化されたら、`accountID` パラメータをサポートするアカウント管理 API オペレーションで、このパラメータを使用できるようになります。このパラメータを正常に使用できるのは、管理アカウントの認証情報、または組織の委任管理者アカウントの認証情報 (委任管理者アカウントを有効にしている場合) を使用してオペレーションを呼び出した場合のみです。詳細については、「アカウント管理の委任管理者 AWS アカウントを有効にする」を参照してください。

組織内のアカウント管理用の信頼されたアクセスを有効にするには、次の手順を使用します。

> 最小アクセス許可
>
> これらのタスクを実行するには、以下の要件を満たす必要があります。
>
> - これは、組織の管理アカウントからのみ実行できます。
> - 組織で、すべての機能が有効になっている 必要があります。

AWS マネジメントコンソール

AWS アカウント管理の信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサインインします。組織の管理アカウントで、IAM ユーザーとしてサイン・インするか、IAM ロールを引き受けるか、ルートユーザーとしてサイン・インする (推奨されません) 必要があります。

2. ナビゲーションペインで、[Services] (サービス) を選択します。
3. サービスのリストで [AWS Account Management] (アカウント管理) を選択します。
4. [Enable trusted access (信頼されたアクセスを有効にする)] を選択します。
5. AWS 「アカウント管理の信頼されたアクセスを有効にする」ダイアログボックスで、「有効化して確認します」と入力し、「信頼されたアクセスを有効にする」を選択します。

AWS CLI & SDKs

AWS アカウント管理の信頼されたアクセスを有効にするには

次のコマンドの実行後に、組織の管理アカウントの認証情報を使用して、`--accountId` パラメータを使用するアカウント管理 API オペレーションを呼び出し、組織内のメンバーアカウントを参照するすることができます。

- AWS CLI: enable-aws-service-access

  次の の例では、呼び出し元の AWS アカウントの組織でアカウント管理の信頼されたアクセスを有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal account.amazonaws.com
  ```

  このコマンドは成功時に出力を生成しません。

アカウント管理の委任管理者 AWS アカウントを有効にする

委任管理者アカウントを有効にして、 の他のメンバーアカウントの AWS アカウント管理 API オペレーションを呼び出すことができます AWS Organizations。組織の委任管理者アカウントを登録すると、そのアカウントのユーザーとロールは、オプションの `AccountId`パラメータをサポートすることで Organizations モードで機能できる `account`名前空間で AWS CLI および AWS SDK オペレーションを呼び出すことができます。

組織内のメンバーアカウントを委任管理者アカウントとして登録するには、以下の手順を使用します。

AWS CLI & SDKs

アカウント管理サービス用の委任管理者アカウントを登録するには

次のコマンドを使用して、アカウント管理サービス用の委任管理者を有効にすることができます。

> **最小アクセス許可**
>
> これらのタスクを実行するには、以下の要件を満たす必要があります。
>
> - これは、組織の管理アカウントからのみ実行できます。
> - 組織で、すべての機能が有効になっている必要があります。
> - 組織内のアカウント管理で信頼されたアクセスが有効にになっている必要があります。

次のサービスプリンシパルを指定する必要があります。

```
account.amazonaws.com
```

- AWS CLI: register-delegated-administrator

  次の例では、組織のメンバーアカウントをアカウント管理サービスの委任管理者として登録します。

  ```
  $ aws organizations register-delegated-administrator \
      --account-id 123456789012 \
      --service-principal account.amazonaws.com
  ```

  このコマンドは成功時に出力を生成しません。

  このコマンドを実行したら、アカウント 123456789012 の認証情報を使用して、 `--account-id`パラメータを使用して組織内のメンバーアカウントを参照するアカウント管理 AWS CLI および SDK API オペレーションを呼び出すことができます。

AWS マネジメントコンソール

このタスクは、 AWS アカウント管理コンソールではサポートされていません。このタスクは、AWS CLI またはいずれかの AWS SDKs からの API オペレーションを使用してのみ実行できます。

AWS Organizations サービスコントロールポリシーを使用してアクセスを制限する

このトピックでは、 AWS Organizations のサービスコントロールポリシー (SCP) を使用して組織のアカウントのユーザーやロールが実行できる操作を制限する方法を、例を示して説明します。サービスコントロールポリシーの詳細については、 AWS Organizations ユーザーガイドの以下のトピックを参照してください。

- SCP の作成
- OU およびアカウントに SCP をアタッチする
- SCP についての戦略
- SCP ポリシー構文

Example例 1: アカウントが自分の代替連絡先を変更できないようにする

次の例は、スタンドアロンアカウントモードで `PutAlternateContact` と `DeleteAlternateContact` の操作がどのメンバーアカウントからも呼び出されないようにするものです。これにより、影響を受けるアカウントのプリンシパルが自分の代替連絡先を変更できなくなります。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact"
            ],
            "Resource": [ "arn:aws:account::*:account" ]
        }
    ]
}
```

Example例 2: 組織内の他のメンバーアカウントの代替連絡先をメンバーアカウントに変更できないようにする

次の例では、Resource 要素を「*」として一般化しており、これは要素がスタンドアロンモードと組織モードのリクエストの両方に適用されることを意味します。つまり、アカウント管理についてと委任管理者アカウントでも、SCP が適用されると組織内の任意のアカウントの代替連絡先を変更できなくなります。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact"
            ],
            "Resource": [ "*" ]
        }
    ]
}
```

Example例 3: OU のメンバーアカウントが独自の代替連絡先を変更できないようにする

次の SCP の例には、アカウントの組織パスと 2 つの OU のリストを比較する条件が含まれています。これにより、指定された OU 内の任意のアカウントのプリンシパルが独自の代替連絡先を変更できないようにブロックされます。

を使用するタイミング AWS Control Tower

AWS Organizations は、 AWS 環境全体を一元的に管理および保護できる基本的なサービスです。この AWS Organizations中心的なアプローチの重要な要素は です AWS Control Tower。 は Organizations 内のマネジメントコンソール AWS Control Tower として機能し、規範的なベストプラクティスを適用して、安全でマルチアカウント AWS 環境をセットアップおよび管理するための効率的な方法を提供します。

が提供するこのセキュリティのベストプラクティスアプローチは、 のコア機能 AWS Control Tower を拡張します AWS Organizations。 は、組織とアカウントが推奨されるセキュリティおよびコンプライアンス標準に確実に準拠できるように、一連の予防ガードレールと検出ガードレール AWS Control Tower を適用します。

を使用して適切に設計された AWS Organizations 構造を確立することで AWS Control Tower、スケーラブルで安全で準拠した AWS 環境を迅速にデプロイできます。クラウド管理とガバナンスに対するこの一元化されたアプローチは、最高レベルのセキュリティとコンプライアンス AWS クラウドを維持しながら、 の能力を最大限に活用したい企業にとって不可欠です。

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

API 操作モードについて

AWS アカウントの属性を操作する API オペレーションは、常に 2 つのオペレーションモードのいずれかで機能します。

- スタンドアロンコンテキスト — このモードは、アカウント内のユーザーまたはロールが同じアカウント内のアカウント属性にアクセスする、またはそのアカウント属性を変更する場合に使用されます。スタンドアロンコンテキストモードは、アカウント管理 AWS CLI または AWS SDK オペレーションのいずれかを呼び出すときに `AccountId`パラメータを含めない場合に自動的に使用されます。
- 組織コンテキスト — このモードは、組織内の 1 つのアカウントのユーザーまたはロールが、同じ組織内の別のメンバーアカウントのアカウント属性にアクセスする、またはそのアカウント属性を変更する場合に使用されます。アカウント管理 AWS CLI または AWS SDK オペレーションのいずれかを呼び出すときに `AccountId`パラメータを含めると、組織コンテキストモードが自動的に使用されます。このモードでは、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのみから操作を呼び出すことができます。

AWS CLI および AWS SDK オペレーションは、スタンドアロンまたは組織のコンテキストで機能します。

- `AccountId` パラメータを含めない場合、操作はスタンドアロンコンテキストで実行され、リクエスト作成に使用したアカウントにリクエストが自動的に適用されます。これは、アカウントが組織のメンバーであるかどうかにはかかわりません。

- AccountId パラメータを含めた場合は、操作は組織コンテキストで実行され、指定した組織アカウントで動作します。
  - 操作を呼び出すアカウントが、アカウント管理サービスの管理アカウントまたは委任管理者アカウントである場合、AccountId パラメータにその組織の任意のメンバーアカウントを指定して、指定したアカウントを更新することができます。
  - 代替連絡先に関する操作のいずれかを呼び出して、AccountId パラメータに自身のアカウント番号を指定できる組織内のアカウントは、アカウント管理サービス用の委任管理者アカウントとして指定されたアカウントのみです。管理アカウントを含むその他のアカウントは、AccessDenied 例外を受信します。
- スタンドアロンモードで操作を実行する場合、すべてのリソースを許可する "*"、またはスタンドアロンアカウント用の構文を使う ARN のどちらかの Resource 要素を含む IAM ポリシーで、操作の実行が許可されている必要があります。
- 組織モードで操作を実行する場合、すべてのリソースを許可する Resource のいずれかの "*" 要素を含む IAM ポリシー、または組織内のメンバーアカウント用の構文に従った ARN で、操作の実行が許可されている必要があります。

アカウント属性を更新するアクセス許可の付与

ほとんどの AWS オペレーションと同様に、IAM アクセス許可ポリシー AWS アカウント を使用して、 のアカウント属性を追加、更新、または削除するためのアクセス許可を付与します。 https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.htmlIAM アクセス許可ポリシーを IAM プリンシパル (ユーザーまたはロール) にアタッチすると、そのプリンシパルがどのリソースに対して、どのような条件で、どのアクションを実行できるかを指定することができます。

以下は、アクセス許可ポリシーを作成する際のアカウント管理特有の考慮事項です。

の Amazon リソースネーム形式 AWS アカウント

- ポリシーステートメントの resource要素に含める AWS アカウント ことができる の Amazon リソースネーム (ARN) は、参照するアカウントがスタンドアロンアカウントであるか、組織内のアカウントであるかに基づいて構築されます。「API 操作モードについて」に関する前のセクションを参照してください。
  - スタンドアロンアカウントのアカウント ARN:

```
arn:aws:account::{AccountId}:account
```

AccountID パラメータを含めないことによってスタンドアロンモードでアカウント属性のオペレーションを実行する場合は、この形式を使用する必要があります。

- 組織内のメンバーアカウントのアカウント ARN:

  ```
  arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
  ```

  AccountID パラメータを含めることによって組織モードでアカウント属性のオペレーションを実行する場合は、この形式を使用する必要があります。

IAM ポリシーのコンテキストキー

アカウント管理サービスには、付与するアクセス許可をきめ細かく制御するための[アカウント管理サービス固有の条件キー]もいくつか用意されています。

account:AccountResourceOrgPaths

コンテキストキー account:AccountResourceOrgPaths を使用すると、組織の階層から特定の組織単位 (OU) へのパスを指定できます。その OU に含まれるメンバーアカウントのみが条件に一致します。次の例のスニペットは、指定された 2 つの OU のいずれかに所属するアカウントにのみポリシーを適用するように制限しています。

account:AccountResourceOrgPaths は複数値を持つ文字列型のため、[ForAnyValue または ForAllValues 複数値文字列演算子]を使用する必要があります。また、組織内の OUs へのパスを参照している場合でもaccount、条件キーのプレフィックスは であることに注意してください。

```
"Condition": {
    "ForAnyValue:StringLike": {
        "account:AccountResourceOrgPaths": [
            "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*",
            "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/*"
        ]
    }
}
```

account:AccountResourceOrgTags

コンテキストキー account:AccountResourceOrgTags を使用すると、組織内のアカウントにアタッチできるタグを参照できます。タグはキーと値の文字列のペアで、アカウント内のリソースを

分類し、ラベル付けするために使用できます。詳細については、AWS Resource Groups ユーザーガイドの「タグエディタの使用」を参照してください。属性ベースのアクセス制御戦略の一環としてタグを使用する方法については、「IAM ユーザーガイド」の「AWSの ABAC とは」を参照してください。次の例のスニペットは、project キー、および blue または red のいずれかの値を含むタグを持つ組織内のアカウントにのみポリシーを適用するように制限しています

account:AccountResourceOrgTags は複数値を持つ文字列型のため、ForAnyValue または ForAllValues 複数値文字列演算子を使用する必要があります。また、組織のメンバーアカウントのタグを参照している場合でもaccount、条件キーのプレフィックスは であることに注意してください。

```
"Condition": {
    "ForAnyValue:StringLike": {
        "account:AccountResourceOrgTags/project": [
            "blue",
            "red"
        ]
    }
}
```

> **Note**
>
> タグは、組織内のアカウントにのみアタッチすることができます。スタンドアロンにタグをアタッチすることはできません AWS アカウント。

を設定する AWS アカウント

このセクションでは、 の管理方法について説明します AWS アカウント。

> **Note**
>
> AWS アカウント が Amazon Web Services India Private Limited (AWS インド) を使用してインドで作成された場合は、追加の考慮事項があります。詳細については、「インドでのアカウントの管理」を参照してください。

トピック

- AWS アカウント エイリアスを作成する
- アカウント AWS リージョン で を有効または無効にする
- の請求を更新する AWS アカウント
- ルートユーザーの E メールアドレスと の更新
- ルートユーザーのパスワードの更新
- AWS アカウント 名前を更新する
- の代替連絡先を更新する AWS アカウント
- のプライマリ連絡先を更新する AWS アカウント
- AWS アカウント 識別子を表示する

AWS アカウント エイリアスを作成する

IAM ユーザーの URL に AWS アカウント ID の代わりに会社名 (またはeasy-to-remember識別子) を含める場合は、アカウントエイリアスを作成できます。

アカウントエイリアスを作成または更新する方法については、IAM ユーザーガイドのAWS アカウント「ID のエイリアスの使用」を参照してください。

アカウント AWS リージョン で を有効または無効にする

AWS リージョン は、 に複数のアベイラビリティーゾーン AWS がある世界の物理的な場所です。アベイラビリティーゾーンは 1 つ以上の個別の AWS データセンターで構成され、それぞれが冗長な

電源、ネットワーク、および接続を備え、別々の施設に収容されています。つまり、それぞれ AWS リージョン が物理的に分離され、他のリージョンから独立しています。リージョンでは耐障害性や安定性が提供され、レイテンシーを低減することもできます。エンドユーザー AWS リージョン に近い でワークロードを実行すると、パフォーマンスが向上し、レイテンシーが短縮されます。利用可能なリージョンと今後予定されているリージョンのマップについては、リージョンとアベイラビリティーゾーンを参照してください。ワークロードの AWS リージョン と回復性アーキテクチャの詳細については、AWS マルチリージョンの基本を参照してください。

AWS リージョン は、アカウントの可用性の 2 つのカテゴリに分類されます。

- デフォルトリージョン – 2019 年 3 月 20 日より前に設立されたリージョンは、デフォルトで有効になっています。アカウントがアクティブ化された直後に、これらのデフォルトリージョンでリソースを作成および管理できます。デフォルトのリージョンを有効または無効にすることはできません。
- オプトインリージョン – 2019 年 3 月 20 日以降に設立されたリージョンはデフォルトで無効になっており、オプトインリージョンと呼ばれます。無効なオプトインリージョンはコンソールのナビゲーションバーに表示されず、有効にするまでこれらのリージョンを使用してワークロードを作成することはできません。これらのオプトインリージョンを使用するには、まず で有効にする必要があります AWS アカウント。オプトインリージョンを有効にすると、ナビゲーションバーでそのリージョンを選択し、そこでリソースを作成および管理できます。スタンドアロンアカウントのオプトインリージョンを有効にするには、スタンドアロンアカウントのリージョンの有効化または無効化「」を参照してください。メンバーアカウントのオプトインリージョンを有効にするには、「」を参照してください組織内のリージョンの有効化または無効化。

にサインアップすると AWS アカウント、 は連絡先住所の国に基づいてオプトインリージョン AWS を推奨します。 AWS オプトインリージョンがある国の顧客には、その国のオプトインリージョンを有効にするための推奨事項が連絡先情報ページに表示されます。インド、オーストラリア、カナダなど、オプトインリージョンとデフォルトリージョンの両方を持つ国のお客様には、オプトインリージョンがデフォルトリージョンよりも近い場合、オプトインリージョンを選択することをお勧めします。アカウントがアクティブ化されたら、アカウントの他のオ AWS プトインリージョンを有効にするか、サインアップ中に有効にしたオプトインリージョンを無効にするかを選択できます。

を作成すると AWS アカウント、IAM データおよび認証情報がすべてのデフォルトリージョンで動作するように自動的に設定されます。これにより、ルートユーザーおよび IAM ID は、既存の認証情報を使用してこれらのリージョン AWS のサービスにアクセスするための適切なアクセス許可を持つことができます。 AWS オプトインリージョンはデフォルトで無効になり、IAM データおよび認証情報はこれらのリージョンで最初に使用できなくなり、そのリージョン AWS のサービスへのアクセスが

できなくなります。オプトインリージョンを有効にすると、 AWS は IAM データおよび認証情報をそのリージョンに伝播します。伝播が完了し、オプトインリージョンが有効になると、ルートユーザーと IAM ID は、デフォルトリージョンで使用するのと同じ IAM 認証情報を使用して AWS 、新しく有効になったオプトインリージョンのサービスにアクセスできます。

オプトインリージョンを無効にすると、IAM 認証情報が非アクティブ化され、そのオプトインリージョンのリソースへの IAM アクセスが失われます。オプトインリージョンを無効にしても、そのリージョンのリソースは削除されず、無効にしたオプトインリージョンのリソース (ある場合) の料金は引き続き標準レートで発生します。

> **Important**
>
> リージョンを無効にすると、リージョン内のリソースへの IAM アクセスが無効になります。これにより、問題のリソースは削除されず、引き続き料金が発生します。リージョンを無効にする前に、残りのリソースをすべて削除します。

AWS はリージョンをパーティションにグループ化します。各リージョンは 1 つのパーティションに厳密に属し、各パーティションには 1 つ以上のリージョンがあります。パーティションには AWS Identity and Access Management (IAM) の独立したインスタンスがあり、異なるパーティションのリージョン間のハード境界を提供します。 AWS 商用リージョンはawsパーティションにあり、中国のリージョンはaws-cnパーティションにあり、 AWS GovCloud (US) リージョンはaws-us-govパーティションにあります。を作成したパーティションに応じて AWS アカウント、そのパーティション AWS リージョン 内で を使用できます。

- aws パーティションのアカウントを使用すると、商用パーティション内の複数のリージョンにアクセスできるため、要件を満たす場所で AWS リソースを起動できます。例えば、ヨーロッパの顧客に近づけるため、または法的要件を満たすために、ヨーロッパで Amazon EC2 インスタンスを起動したい場合があります。
- aws-us-gov パーティションのアカウントでは、 AWS GovCloud (米国西部) リージョンと AWS GovCloud (米国東部) リージョンにアクセスできます。詳細については、「AWS GovCloud (US)」を参照してください。
- aws-cn パーティションを使用すると、北京および寧夏リージョンにのみアクセスできます。詳細については「Amazon Web Services in China」(中国でのAmazon ウェブ サービス) を参照してください。

トピック

- リージョンの可用性リファレンス
- リージョンを有効化または無効化する前の考慮事項
- 処理時間とリクエスト制限
- スタンドアロンアカウントのリージョンの有効化または無効化
- 組織内のリージョンの有効化または無効化

リージョンの可用性リファレンス

次の表は、可用性タイプ AWS リージョン 別にリストされています。デフォルトのリージョンは自動的に有効になり、無効にすることはできませんが、オプトインリージョンを使用するには手動で有効にする必要があります。

Opt-in Regions

次のリージョンはオプトインリージョンであり、使用する前に有効にする必要があります。

名前	コード	ステータス
アフリカ (ケープタウン)	af-south-1	GA
アジアパシフィック (香港)	ap-east-1	GA
アジアパシフィック (台北)	ap-east-2	GA
アジアパシフィック (ハイデラバード)	ap-south-2	GA
アジアパシフィック (ジャカルタ)	ap-southeast-3	GA
アジアパシフィック (メルボルン)	ap-southeast-4	GA
アジアパシフィック (マレーシア)	ap-southeast-5	GA
アジアパシフィック (ニュージーランド)	ap-southeast-6	GA
アジアパシフィック (タイ)	ap-southeast-7	GA
カナダ西部 (カルガリー)	ca-west-1	GA
欧州 (チューリッヒ)	eu-central-2	GA

名前	コード	ステータス
欧州 (ミラノ)	eu-south-1	GA
欧州 (スペイン)	eu-south-2	GA
イスラエル (テルアビブ)	il-central-1	GA
中東 (アラブ首長国連邦)	me-central-1	GA
中東 (バーレーン)	me-south-1	GA
メキシコ (中部)	mx-central-1	GA

Default Regions

次のリージョンは、デフォルトで有効になっていて、無効にすることはできません。

名前	コード
アジアパシフィック (東京)	ap-northeast-1
アジアパシフィック (ソウル)	ap-northeast-2
アジアパシフィック (大阪)	ap-northeast-3
アジアパシフィック (ムンバイ)	ap-south-1
アジアパシフィック (シンガポール)	ap-southeast-1
アジアパシフィック (シドニー)	ap-southeast-2
カナダ (中部)	ca-central-1
欧州 (フランクフルト)	eu-central-1
欧州 (ストックホルム)	eu-north-1
欧州 (アイルランド)	eu-west-1

名前	コード
欧州 (ロンドン)	eu-west-2
欧州 (パリ)	eu-west-3
南米 (サンパウロ)	sa-east-1
米国東部 (バージニア北部)	us-east-1
米国東部 (オハイオ)	us-east-2
米国西部 (北カリフォルニア)	us-west-1
米国西部 (オレゴン)	us-west-2

リージョン名と対応するコードのリストについては、「AWS 全般のリファレンスガイド」の「リージョンエンドポイント」を参照してください。各リージョン (エンドポイントなし) でサポートされている AWS サービスのリストについては、AWS 「リージョンサービスリスト」を参照してください。

Important

AWS では、レイテンシーを減らすために、グローバルエンドポイントの代わりに Regional AWS Security Token Service (AWS STS) エンドポイントを使用することをお勧めします。リージョン AWS STS エンドポイントからのセッショントークンは、すべての AWS リージョンで有効です。リージョン AWS STS エンドポイントを使用する場合、変更を加える必要はありません。ただし、グローバル AWS STS エンドポイント (https://sts.amazonaws.com) からのセッショントークンは、 AWS リージョン 有効にした またはデフォルトで有効になっている でのみ有効です。アカウントの新しいリージョンを有効にする場合は、リージョン AWS STS エンドポイントからセッショントークンを使用するか、グローバル AWS STS エンドポイントをアクティブ化して、すべての で有効なセッショントークンを発行できます AWS リージョン。すべてのリージョンで有効なセッショントークンは大きくなります。セッショントークンを保存すると、これらの大きなトークンがシステムに影響する可能性があります。 AWS STS エンドポイントが AWS リージョンと連携する方法の詳細については、AWS 「 リージョン AWS STS での の管理」を参照してください。

リージョンを有効化または無効化する前の考慮事項

リージョンを有効化または無効化する前に、以下の点について考慮することが重要です。

- リージョンのオプトステータスに関係なく、クロスリージョン推論ジオグラフィですべての送信先リージョンを使用できます。Amazon Bedrock (「クロスリージョン推論によるスループットの向上」を参照) や Amazon Q Developer (「Amazon Q Developer でのクロスリージョン処理」を参照) などの特定の AWS 生成 AI サービスは、クロスリージョン推論を使用します。これらのサービスを使用すると、選択した地域内で、リソースと IAM データに対して有効にしていないリージョンを含む最適な AWS リージョンが自動的に選択されます。これにより、利用可能なコンピューティングとモデルの可用性を最大化することで、カスタマーエクスペリエンスが向上します。
- IAM アクセス許可を使用してリージョンへのアクセスを制御 – AWS Identity and Access Management (IAM) には、リージョンを有効化、無効化、取得、一覧表示できるユーザーを制御できる 4 つのアクセス許可が含まれています。詳細については、「IAM ユーザーガイド」の「AWS: AWS リージョンの有効化と無効化を許可する」を参照してください。`aws:RequestedRegion` 条件キーを使用して、 AWS のサービス での へのアクセスを制御することもできます AWS リージョン。
- リージョンの有効化/無効化は無料 – リージョンを有効または無効にしても料金はかかりません。新しいリージョンで作成したリソースに対してのみ課金されます。
- Amazon EventBridge 統合 – EventBridge でリージョンオプトステータス更新通知をサブスクライブできます。ステータスが変更されるたびに EventBridge 通知が作成され、お客様はワークフローを自動化できます。
- 詳細なリージョンオプトステータス – オプトインリージョンの有効化/無効化は非同期的に行われるため、リージョンオプトリクエストには次の 4 つのステータスがあります。
  - `ENABLING`
  - `DISABLING`
  - `ENABLED`
  - `DISABLED`

  オプトインまたはオプトアウトは、そのステータスが `ENABLING` または `DISABLING` である場合はキャンセルできません。それ以外の場合は、`ConflictException` がスローされます。完了した (有効/無効) リージョンオプトリクエストは、基盤となる主要な AWS サービスのプロビジョニングによって異なります。ステータスが であっても、すぐには使用できない AWS サービスもありますENABLED。

処理時間とリクエスト制限

リージョンを有効または無効にする場合は、次のタイミングとリクエストの制限に注意してください。

- リージョンの有効化は、場合によっては数分から数時間かかる – リージョンを有効にすると、AWS はリージョンへの IAM リソースの配信など、そのリージョンでアカウントを準備するためのアクションを実行します。このプロセスは、ほとんどのアカウントでは数分で完了しますが、場合によっては数時間かかることもあります。このプロセスが完了するまでそのリージョンを使用することはできません。
- リージョンの無効化は必ずしも即時に表示されるわけではない - リージョンを無効にした後もサービスやコンソールが一時的に表示される場合があります。リージョンを無効にすると、有効になるまでに数分から数時間かかる場合があります。
- 1 つのアカウントが同時に持つことができる進行中のリージョンオプトリクエストは最大 6 件 - 1 つのリクエストは、1 つのアカウントに対する特定の 1 つのリージョンの有効化または無効化のいずれかに相当します。
- 組織は、 AWS 組織全体で一度に 50 件のリージョンオプトリクエストを開くことができます。管理アカウントは、組織の完了保留中のオープンリクエストをいつでも 50 件持つことができます。1 つのリクエストは、1 つのアカウントに対する特定の 1 つのリージョンの有効化または無効化のいずれかに相当します。

スタンドアロンアカウントのリージョンの有効化または無効化

AWS アカウント がアクセスできるリージョンを更新するには、次の手順を実行します。 AWS マネジメントコンソール 以下の手順は、常にスタンドアロンコンテキストでのみ機能します。を使用して AWS マネジメントコンソール 、 オペレーションの呼び出しに使用したアカウントで使用可能なリージョンのみを表示または更新できます。

AWS マネジメントコンソール

スタンドアロンのリージョンを有効または無効にするには AWS アカウント

> **最小アクセス許可**
>
> 以下の手順の手順を実行するには、IAM ユーザーまたはロールに次のアクセス許可が必要です。

- account:ListRegions (のリスト AWS リージョン と、現在有効か無効かを表示する必要があります) 。
- account:EnableRegion
- account:DisableRegion

1. に、AWS マネジメントコンソール AWS アカウントのルートユーザー 最小限のアクセス許可を持つ IAM ユーザーまたはロールとしてサインインします。
2. ウィンドウの右上にあるアカウント名を選択し、[アカウント] を選択します。
3. [アカウント] ページで、[AWS リージョン] セクションまでスクロールダウンします。
4. 有効または無効にするリージョンを選択し、目的のアクションの [有効化] または [無効化] を選択します。確認のプロンプトが表示されます。
5. [有効化] オプションを選択した場合は、表示されたテキストを確認してから、[リージョンを有効にする] を選択します。

   [無効化] オプションを選択した場合は、表示されたテキストを確認し、確認のために **disable** と入力して、[リージョンを無効にする] を選択します。

   オプトインリージョンを有効にすると、リージョンナビゲーションバーからそのリージョンを選択できます。リージョンを選択する手順については、「AWS マネジメントコンソールのナビゲーションバーからリージョンを選択する」を参照してください。アカウントのリージョン固有のコンソール設定については、「AWS マネジメントコンソールのデフォルトのリージョンの設定」を参照してください。

AWS CLI & SDKs

リージョンのオプトステータスを有効化、無効化、読み取り、一覧表示するには、次の AWS CLI コマンドまたは AWS SDK と同等のオペレーションを使用します。

- EnableRegion
- DisableRegion
- GetRegionOptStatus
- ListRegions

最小アクセス許可

次の手順を実行するには、そのオペレーションにマッピングするためのアクセス許可が必要です。

- account:EnableRegion
- account:DisableRegion
- account:GetRegionOptStatus
- account:ListRegions

これらの個別のアクセス許可を使用すると、一部のユーザーにリージョンオプト情報の読み取りのみを許可し、他のユーザーには読み取りと書き込みを許可するということもできます。

次の例では、組織内の指定されたメンバーアカウントのリージョンを有効にします。使用される認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかから取得する必要があります。

同じコマンド (enable-region は disable-region に置き換える) を使用してリージョンを無効にすることもできます。

```
aws account enable-region --region-name af-south-1
```

このコマンドは成功時に出力を生成しません。

このオペレーションは非同期です。次のコマンドを使用すると、リクエストの最新ステータスを確認できます。

```
aws account get-region-opt-status --region-name af-south-1
  {
    "RegionName": "af-south-1",
    "RegionOptStatus": "ENABLING"
  }
```

組織内のリージョンの有効化または無効化

のメンバーアカウントの有効なリージョンを更新するには AWS Organizations、次の手順を実行します。

> **Note**
>
> AWS Organizations 管理ポリシー `AWSOrganizationsReadOnlyAccess`または `AWSOrganizationsFullAccess`が更新され、 AWS Organizations コンソールからアカウントデータにアクセスできるように、 AWS アカウント管理 APIsへのアクセス許可が付与されます。更新された管理ポリシーを表示するには、「Organizations AWS 管理ポリシーの更新」を参照してください。

> **Note**
>
> 組織の管理アカウントまたは委任管理者アカウントからメンバーアカウントに対してこれらの操作を実行する前に、以下を行う必要があります。
>
> - メンバーアカウントの設定を管理するために、組織内のすべての機能を有効にします。これにより、管理者がメンバーアカウントを制御できるようになります。これは、組織を作成すると、デフォルトで設定されます。組織が一括決済のみに設定されていて、すべての機能を有効にする場合は、「組織内のすべての機能の有効化」を参照してください。
> - AWS アカウント管理サービスの信頼されたアクセスを有効にします。これを設定するには、「AWS アカウント管理の信頼されたアクセスを有効にする」を参照してください。

AWS マネジメントコンソール

組織内のリージョンを有効または無効にする手順

1. 組織の管理アカウントの認証情報を使用して AWS Organizations コンソールにサインインします。
2. [AWS アカウント] ページで、更新するアカウントを選択します。
3. [アカウント設定] タブを選択します。
4. [リージョン] で、有効または無効にするリージョンを選択します。
5. [アクション] を選択し、[有効化] または [無効化] オプションのいずれかを選択します。
6. [有効化] オプションを選択した場合は、表示されたテキストを確認してから、[リージョンを有効にする] を選択します。
7. [無効化] オプションを選択した場合は、表示されたテキストを確認し、確認のために disable と入力して、[リージョンを無効にする] を選択します。

AWS CLI & SDKs

組織メンバーアカウントのリージョンオプトステータスを有効化、無効化、読み取り、一覧表示するには、次の AWS CLI コマンドまたは AWS SDK と同等のオペレーションを使用します。

- `EnableRegion`
- `DisableRegion`
- `GetRegionOptStatus`
- `ListRegions`

> **最小アクセス許可**
>
> 次の手順を実行するには、そのオペレーションにマッピングするためのアクセス許可が必要です。
>
> - `account:EnableRegion`
> - `account:DisableRegion`
> - `account:GetRegionOptStatus`
> - `account:ListRegions`

これらの個別のアクセス許可を使用すると、一部のユーザーにリージョンオプト情報の読み取りのみを許可し、他のユーザーには読み取りと書き込みを許可するということもできます。

次の例では、組織内の指定されたメンバーアカウントのリージョンを有効にします。使用される認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかから取得する必要があります。

同じコマンド (`enable-region` は `disable-region` に置き換える) を使用してリージョンを無効にすることもできます。

```
aws account enable-region --account-id 123456789012 --region-name af-south-1
```

このコマンドは成功時に出力を生成しません。

> **Note**
>
> 組織が同時に持つことができるリージョンリクエストは、最大 20 個のみです。これを超えると、TooManyRequestsException が発生します。

このオペレーションは非同期です。次のコマンドを使用すると、リクエストの最新ステータスを確認できます。

```
aws account get-region-opt-status --account-id 123456789012 --region-name af-south-1
  {
    "RegionName": "af-south-1",
    "RegionOptStatus": "ENABLING"
  }
```

の請求を更新する AWS アカウント

AWS Billing および コスト管理コンソールを使用して、すべての AWS アカウント 請求設定を更新できます。アカウントの請求関連の設定を更新する方法については、「AWS Billing and Cost Management ユーザーガイド」を参照してください。

ルートユーザーの E メールアドレスと の更新

AWS アカウントのルートユーザーの E メールアドレスと を更新する必要があるビジネス上の理由はさまざまです。例えば、セキュリティと管理のレジリエンスなどです。このトピックでは、スタンドアロンアカウントとメンバーアカウントの両方のルートユーザーの E メールアドレスと を更新するプロセスについて説明します。

> **Note**
>
> への変更は、どこでも伝播されるまでに最大 4 時間かかる AWS アカウント ことがあります。

ルートユーザーの E メールと は、アカウントがスタンドアロンであるか、組織の一部であるかに応じて、異なる方法で更新できます。

- スタンドアロン AWS アカウント – 組織に関連付けられ AWS アカウント ていない場合は、 AWS マネジメントコンソールを使用してルートユーザーの E メールを更新できます。これを行う方法については、「スタンドアロンのルートユーザーの E メールと を更新する AWS アカウント」を参照してください。
- AWS アカウント 組織内 – AWS 組織の一部であるメンバーアカウントの場合、管理アカウントまたは委任管理者アカウントのユーザーは、 AWS Organizations コンソールから、または CLI と SDKs を介してプログラムで、メンバーアカウントの Amazon AWS メールを一元的に更新できます。これを行う方法については、「組織 AWS アカウント 内の任意の のルートユーザー E メール メールを更新する」を参照してください。

トピック

- スタンドアロンアカウント AWS アカウント または管理アカウントのルートユーザー E メール メールを更新する
- 組織 AWS アカウント 内の任意の のルートユーザー E メールを更新する

スタンドアロンアカウント AWS アカウント または管理アカウントのルートユーザー E メール メールを更新する

スタンドアロンのルートユーザーの E メールアドレス AWS アカウント、次の手順を実行します。

AWS マネジメントコンソール

> **Note**
>
> としてサインインする必要があります。そのため AWS アカウントのルートユーザー、追加の IAM アクセス許可は必要ありません。IAM ユーザーまたはロールとしてこれらの手順を実行することはできません。

1. AWS アカウントの E メールアドレスとパスワードを使用して、AWS マネジメントコンソールとして にサインインします AWS アカウントのルートユーザー。
2. コンソールの右上隅のアカウント名またはアカウント番号を選択してから [Account] (アカウント) を選択します。
3. [アカウント] ページで、[アカウントの詳細] の横にある [アクション] を選択し、[E メールアドレスとパスワードの更新] を選択します。

4. [アカウントの詳細] ページで、[E メールアドレス] の横にある [編集] を選択します。
5. [E メールアドレスの編集] ページで、[新しい E メールアドレス] と [新しい E メールアドレスの確認] のフィールドに入力し、現在の [パスワード] を確認します。次に [保存し続行] を選択します。no-reply@verify.signin.aws から新しい E メールアドレスに検証コード送信されます。
6. [アカウント E メールの編集] ページの [検証コード] で、E メールから受け取ったコードを入力し、[更新の確認] を選択します。

> **Note**
>
> 検証コードが到着するまでに最大 5 分かかる場合があります。受信箱で E メールが見つからない場合は、スパムフォルダや迷惑メールフォルダを確認してください。

AWS CLI & SDKs

このタスクは、 AWS CLI またはいずれかの AWS SDKs からの API オペレーションではサポートされていません。このタスクは、 を使用してのみ実行できます AWS マネジメントコンソール。

組織 AWS アカウント 内の任意の のルートユーザー E メールを更新する

AWS Organizations コンソールを使用して組織内のメンバーアカウントのルートユーザーの E メールアドレス、次の手順を実行します。

> **Note**
>
> メンバーアカウントのルートユーザーの E メールアドレスと を更新する前に、このオペレーションの影響を理解しておくことをお勧めします。詳細については、「AWS Organizations ユーザーガイド」の「AWS Organizationsでメンバーアカウントのルートユーザーの E メールアドレスと の更新」を参照してください。

ルートユーザーとしてサインインした後、 のアカウントページから直接、メンバーアカウントのルートユーザーの E メールアドレスを更新することもできます。 AWS マネジメントコンソール ステップバイステップの手順については、「スタンドアロンアカウント AWS アカウント または管理アカウントのルートユーザー E メール メールを更新する」の手順に従います。

AWS Management Console

> **注意事項**
>
> - 組織内の管理アカウントまたは委任管理者アカウントからメンバーアカウントに対してこの手順を実行するには、アカウント管理サービス用の信頼されたアクセスを有効にする必要があります。
> - この手順を使用して、オペレーションの呼び出しに使用している組織とは異なる組織のアカウントにアクセスすることはできません。

AWS Organizations コンソールを使用してメンバーアカウントのルートユーザーの E メールアドレスを更新するには

1. AWS Organizations コンソール にサインインします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. [AWS アカウント] ページで、ルートユーザーの E メールアドレスと を更新するメンバーアカウントを選択します。
3. [アカウントの詳細] セクションで、[アクション] ボタンを選択し、[E メールアドレスの更新] を選択します。
4. [E メール] で、ルートユーザーの新しい E メールアドレスを入力し、[保存] を選択します。これにより、新しい E メールアドレスにワンタイムパスワード (OTP) が送信されます。

   > **Note**
   >
   > コードを待っている間に Organizations コンソールでこのページを閉じる必要がある場合は、コードの送信から 24 時間以内に OTP プロセスを返して終了できます。これを行うには、[アカウントの詳細] ページで [アクション] ボタンを選択し、[E メール更新の完了] を選択します。

5. [検証コード] で、前のステップで新しい E メールアドレスに送信されたコードを入力し、[確認] を選択します。これにより、アカウントのルートユーザーに更新がコミットされます。

AWS CLI & SDKs

ルートユーザーの E メールアドレス (プライマリ E メールアドレスとも呼ばれます) を取得または更新するには、次の AWS CLI コマンドまたは AWS SDK と同等のオペレーションを使用します。

- GetPrimaryEmail
- StartPrimaryEmailUpdate
- AcceptPrimaryEmailUpdate

> **注意事項**
>
> - 組織内の管理アカウントまたは委任管理者アカウントからメンバーアカウントに対してこれらの操作を実行するには、アカウント管理サービス用の信頼されたアクセスを有効にする必要があります。
> - オペレーションの呼び出しに使用している組織とは異なる組織のアカウントにアクセスすることはできません。

> **最小アクセス許可**
>
> 各操作については、その操作に対応するアクセス許可が必要です。
>
> - `account:GetPrimaryEmail`
> - `account:StartPrimaryEmailUpdate`
> - `account:AcceptPrimaryEmailUpdate`
>
> これらのアクセス許可を個別に使用すると、一部のユーザーにルートユーザーの E メールアドレスと の情報の読み取りのみを許可し、他のユーザーには読み取りと書き込みの両方の許可を付与するといったことができるようになります。

ルートユーザーの E メールアドレスと の更新プロセスを完了するには、以下の例に示す順序でプライマリ E メール API を一緒に使用する必要があります。

Example **GetPrimaryEmail**

次の例では、組織内の指定されたメンバーアカウントからルートユーザーの E メールアドレスとを取得します。使用される認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかから取得する必要があります。

```
$ aws account get-primary-email --account-id 123456789012
```

Example **StartPrimaryEmailUpdate**

次の例では、ルートユーザーの E メールアドレスと の更新プロセスを開始し、新しい E メールアドレスを識別し、組織内の指定されたメンバーアカウントの新しい E メールアドレスにワンタイムパスワード (OTP) を送信します。使用される認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかから取得する必要があります。

```
$ aws account start-primary-email-update --account-id 123456789012 --primary-email
 john@examplecorp.com
```

Example **AcceptPrimaryEmailUpdate**

次の例では、OTP コードを受け入れ、新しい E メールアドレスを組織内の指定されたメンバーアカウントに設定します。使用される認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかから取得する必要があります。

```
$ aws account accept-primary-email-update --account-id 123456789012 --otp 12345678
 --primary-email john@examplecorp.com
```

ルートユーザーのパスワードの更新

AWS アカウントルートユーザーのパスワードを編集するには、以下の手順を実行します。

AWS マネジメントコンソール

ルートユーザーパスワードを編成するには

> **Note**
>
> としてサインインする必要があります。そのため AWS アカウントのルートユーザー、追加の IAM アクセス許可は必要ありません。IAM ユーザーまたはロールとしてこれらの手順を実行することはできません。

1. AWS アカウントの E メールアドレスとパスワードを使用して、 AWS マネジメントコンソールとして にサインインします AWS アカウントのルートユーザー。
2. コンソールの右上隅のアカウント名またはアカウント番号を選択してから [Account] (アカウント) を選択します。
3. [アカウント] ページで、[アカウントの詳細] の横にある [アクション] を選択し、[E メールアドレスとパスワードの更新] を選択します。
4. [アカウントの詳細] ページで、[パスワード] の横にある [編集] を選択します。
5. [パスワードの編集] ページで、[現在のパスワード]、[新しいパスワード]、[新しいパスワードの確認] の各フィールドに入力します。その後、[パスワードの更新] を選択します。ルートユーザーのパスワードの設定に関するベストプラクティスを含む追加のガイダンスについては、「IAM ユーザーガイド」の「AWS アカウントのルートユーザーのパスワードを変更する」を参照してください。

AWS CLI & SDKs

このタスクは、 AWS CLI またはいずれかの AWS SDKs からの API オペレーションではサポートされていません。このタスクは、 を使用してのみ実行できます AWS マネジメントコンソール。

AWS アカウント 名前を更新する

複数の を管理する場合は AWS アカウント、ビジネスユニットやアプリケーションに合わせた明確な命名規則を使用して、識別と整理を行います。再編成、合併、買収、命名規則の更新中に、一貫した識別および管理基準を維持するためにアカウント名を変更する必要がある場合があります。

アカウントの名前は、請求書や請求情報、コスト管理ダッシュボード、コンソールなどの AWS Organizations コンソールなど、複数の場所に表示されます。アカウント名を付ける際に標準的な方

法を使用することで、アカウント名を認識しやすいものにすることをお勧めします。会社のアカウントの場合は、organization-purpose-environment (例えば、sales-catalog-prod) のような命名基準を使用することを検討してください。プライバシーとセキュリティ上の理由から、個人を特定できる情報 (PII) を反映するアカウント名は使用しないでください。

- スタンドアロン AWS アカウント – 組織に関連付けられ AWS アカウント ていない場合は、 AWS マネジメントコンソール、、 AWS CLI および SDKs を使用してアカウント名を更新できます。これを行う方法については、「スタンドアロンのアカウント名を更新する AWS アカウント」を参照してください。
- AWS アカウント 組織内 – の一部であるメンバーアカウントの場合 AWS Organizations、管理アカウントまたは委任管理者アカウントのユーザーは、 AWS Organizations コンソールから、またはプログラムで AWS CLI および SDKs を介して、組織内の任意のメンバーアカウントのアカウント名を一元的に更新できます。これを行う方法については、「組織 AWS アカウント 内の のアカウント名を更新する」を参照してください。

> **Note**
>
> への変更は、どこでも伝播されるまでに最大 4 時間かかる AWS アカウント 場合があります。

トピック

- スタンドアロンのアカウント名を更新する AWS アカウント
- 組織 AWS アカウント 内の のアカウント名を更新する

スタンドアロンのアカウント名を更新する AWS アカウント

スタンドアロンのアカウント名を変更するには AWS アカウント、次の手順を実行します。

AWS マネジメントコンソール

> **最小アクセス許可**
>
> ルートユーザー、IAM ユーザー、または IAM ロールを使用して、アカウント名を更新できます。ルートユーザーを使用している場合、アカウント名を更新するために追加の IAM アクセス許可は必要ありません。IAM ユーザーまたは IAM ロールを使用する場合は、少なくとも次の IAM アクセス許可が必要です。

- account:GetAccountInformation
- account:PutAccountName

スタンドアロンアカウントのアカウント名を更新するには

1. AWS アカウントの E メールアドレスとパスワードを使用して、AWS マネジメントコンソールとして にサインインします AWS アカウントのルートユーザー。
2. コンソールの右上隅のアカウント名またはアカウント番号を選択してから [Account] (アカウント) を選択します。
3. [アカウント] ページで、[アカウントの詳細] の横にある [アクション] を選択し、[アカウント名の更新] を選択します。
4. [名前] で、更新する新しいアカウント名を入力し、[保存] を選択します。

AWS CLI & SDKs

最小アクセス許可

ルートユーザー、IAM ユーザー、または IAM ロールを使用して、アカウント名を更新できます。次の手順を実行するには、IAM ユーザーまたは IAM ロールに少なくとも以下の IAM アクセス許可が必要です。

- account:GetAccountInformation
- account:PutAccountName

スタンドアロンアカウントのアカウント名を更新するには

以下のいずれかのオペレーションを使用することもできます。

- AWS CLI: put-account-name

```
$ C:\> aws account put-account-name \
        --account-name "New-Account-Name"
```

- AWS SDKs: PutAccountName

組織 AWS アカウント 内の のアカウント名を更新する

では、すべての機能モード AWS Organizations を使用して、管理アカウントと委任管理者アカウントの両方で、承認された IAM ユーザーまたは IAM ロールがアカウント名を一元管理できます。

組織内のメンバーアカウントのアカウント名を変更するには、次の手順を実行します。

要件

AWS Organizations コンソールでアカウント名を更新するには、いくつかの事前設定を行う必要があります。

- メンバーアカウントで設定を管理するには、所属する組織によってすべての機能が有効にされる必要があります。これにより、管理者がメンバーアカウントを制御できるようになります。これは、組織を作成すると、デフォルトで設定されます。組織が一括決済のみに設定されていて、すべての機能を有効にする場合は、「組織内のすべての機能の有効化」を参照してください。
- AWS アカウント管理サービスの信頼されたアクセスを有効にする必要があります。これを設定するには、「AWS アカウント管理の信頼されたアクセスを有効にする」を参照してください。

AWS マネジメントコンソール

> **最小アクセス許可**
>
> メンバーアカウントのアカウント名を更新するには、IAM ユーザーまたは IAM ロールに次のアクセス許可が必要です。
>
> - `organizations:DescribeOrganization` (コンソールのみ)
> - `account:PutAccountName`

メンバーアカウントのアカウント名を更新するには

1. Organizations コンソール (https://console.aws.amazon.com/organizations/) を開きます。
2. 左側のナビゲーションペインで、[AWS アカウント] を選択します。
3. [AWS アカウント] ページで、更新するメンバーアカウントを選択し、[アクション] ドロップダウンメニューを選択し、[アカウント名の更新] を選択します。
4. [名前] で更新された名前を入力し、[保存] を選択します。

AWS CLI & SDKs

> **最小アクセス許可**
>
> メンバーアカウントのアカウント名を更新するには、IAM ユーザーまたは IAM ロールに次のアクセス許可が必要です。
>
> - `organizations:DescribeOrganization` (コンソールのみ)
> - `account:PutAccountName`

メンバーアカウントのアカウント名を更新するには

以下のいずれかのオペレーションを使用することもできます。

- AWS CLI: put-account-name

```
$ C:\> aws account put-account-name \
        --account-id 111111111111 \
        --account-name "New-Account-Name"
```

- AWS SDKs: PutAccountName

の代替連絡先を更新する AWS アカウント

代替連絡先を使用すると AWS 、アカウントに関連付けられた最大 3 つの代替連絡先に連絡できます。代替連絡先は、特定の人物である必要はありません。請求、運用、およびセキュリティ関連の問題を管理するチームがある場合は、代わりに E メール配布リストを追加できます。これらは、アカウントのルートユーザーに関連付けられている E メールアドレスに加えて指定されます。主要アカウント連絡先は、ルートアカウントの E メールアドレスに送信されたすべての E メール通信を引き続き受信します。

アカウントに関連付けられている次の各連絡先タイプのいずれか 1 つのみを指定できます。

- 請求に関するお問い合わせ先
- 操作問い合わせ先
- セキュリティ問い合わせ先

アカウントがスタンドアロンであるか、組織の一部であるかに応じて、代替連絡先を異なる方法で追加または編集できます。

- スタンドアロン AWS アカウント – 組織に関連付けられ AWS アカウント ていない場合は、 AWS マネジメントコンソールまたは CLI & SDKs AWS を使用して、独自の代替連絡先を更新できます。この方法については、「スタンドアロンの AWS アカウントの代替連絡先を更新する」を参照してください。
- AWS アカウント 組織内 – AWS 組織の一部であるメンバーアカウントの場合、管理アカウントまたは委任管理者アカウントのユーザーは、 AWS Organizations コンソールから、または CLI と SDKs AWS を介してプログラムで、組織内の任意のメンバーアカウントを一元的に更新できます。これを行う方法については、「組織 AWS アカウント 内の任意の の代替連絡先を更新する」を参照してください。

トピック

- 電話番号と E メールアドレスの要件
- スタンドアロンの代替連絡先を更新する AWS アカウント
- 組織 AWS アカウント 内の任意の の代替連絡先を更新する
- account:AlternateContactTypes コンテキストキー

電話番号と E メールアドレスの要件

アカウントの代替連絡先情報の更新を進める前に、まず、電話番号と E メールアドレスを入力する際の以下の要件を確認することをお勧めします。

- 電話番号には、数字、空白、および文字「+-()」のみを含めることができます。
- E メールアドレスは最大 254 文字で指定することができ、標準の英数字に加えて、E メールアドレスのローカル部分に特殊文字「+=.#|!&-_」を含めることができます。

スタンドアロンの代替連絡先を更新する AWS アカウント

スタンドアロンの代替連絡先を追加または編集するには AWS アカウント、次の手順を実行します。AWS マネジメントコンソール 以下の手順は、常にスタンドアロンコンテキストでのみ機能します。を使用して AWS マネジメントコンソール 、 オペレーションの呼び出しに使用したアカウントの代替連絡先にのみアクセスまたは変更できます。

AWS マネジメントコンソール

スタンドアロンの代替連絡先を追加または編集するには AWS アカウント

> **最小アクセス許可**
>
> 次の手順を実行するには、少なくとも以下のIAM アクセス許可が必要です。
>
> - `account:GetAlternateContact` (代替連絡先の詳細を表示する場合)
> - `account:PutAlternateContact` (代替連絡先を設定または更新する場合)
> - `account:DeleteAlternateContact` (代替連絡先を削除する場合)

1. AWS マネジメントコンソール に最小アクセス許可を持つ、IAM ユーザーまたはロールとしてサインインします。
2. ウィンドウの右上にあるアカウント名を選択し、[アカウント] を選択します。
3. [アカウント] ページで、[代替連絡先] までスクロールダウンして、タイトルの右側で [編集] を選択します。

   > **Note**
   >
   > [編集] オプションが表示されない場合は、アカウントのルートユーザーまたは上記の最小アクセス許可を持つユーザーとしてログインしていない可能性があります。

4. 使用可能なフィールドの値を変更します。

   > **Important**
   >
   > ビジネスでは AWS アカウント、個人に属する電話番号と E メールアドレスではなく、会社の電話番号と E メールアドレスを入力するのがベストプラクティスです。

5. すべての変更を加え終わったら、[Update] (更新) を選択します。

AWS CLI & SDKs

次の AWS CLI コマンドまたは AWS SDK と同等のオペレーションを使用して、代替連絡先情報を取得、更新、または削除できます。

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **注意事項**
>
> - 組織内の管理アカウントまたは委任管理者アカウントからメンバーアカウントに対してこれらの操作を実行するには、アカウントサービス用の信頼されたアクセスを有効にする必要があります。

> **最小アクセス許可**
>
> 各操作については、その操作に対応するアクセス許可が必要です。
>
> - `GetAlternateContact` (代替連絡先の詳細を表示する場合)
> - `PutAlternateContact` (代替連絡先を設定または更新する場合)
> - `DeleteAlternateContact` (代替連絡先を削除する場合)
>
> これらの個別のアクセス許可を使用すると、一部のユーザーに連絡先情報の読み取りのみを許可し、他のユーザーには読み取りと書き込みを許可するということもできます。

Example

次の例では、発信者のアカウントに現在設定されている、請求に関する通知の代替連絡先を取得します。

```
$ aws account get-alternate-contact \
    --alternate-contact-type=BILLING
```

```
{
    "AlternateContact": {
        "AlternateContactType": "BILLING",
        "EmailAddress": "saanvi.sarkar@amazon.com",
        "Name": "Saanvi Sarkar",
        "PhoneNumber": "+1(206)555-0123",
        "Title": "CFO"
    }
}
```

Example

次の例では、操作に関する通知の代替連絡先を発信者のアカウントに新規に設定します。

```
$ aws account put-alternate-contact \
    --alternate-contact-type=OPERATIONS \
    --email-address=mateo_jackson@amazon.com \
    --name="Mateo Jackson" \
    --phone-number="+1(206)555-1234" \
    --title="Operations Manager"
```

このコマンドは成功時に出力を生成しません。

Example

> **Note**
>
> 同じコンタクトタイプ AWS アカウント と同じコンタクトタイプに対して複数のPutAlternateContactオペレーションを実行する場合、 は最初に新しいコンタクトを追加し、同じ AWS アカウント とコンタクトタイプへの連続する呼び出しはすべて既存のコンタクトを更新します。

Example

次の例では、発信者のアカウントに設定されている、セキュリティに関する通知の代替連絡先を削除します。

```
$ aws account delete-alternate-contact \
    --alternate-contact-type=SECURITY
```

このコマンドは成功時に出力を生成しません。

> **Note**
>
> 同じ連絡先を何回も削除しようとすると、メッセージは表示されずに 1 回目で成功します。それ以降の試行はすべて ResourceNotFound 例外を生成します。

組織 AWS アカウント 内の任意の の代替連絡先を更新する

組織 AWS アカウント 内の の代替連絡先の詳細を追加または編集するには、次の手順を実行します。

要件

AWS Organizations コンソールで代替連絡先を更新するには、いくつかの事前設定を行う必要があります。

- メンバーアカウントで設定を管理するには、所属する組織によってすべての機能が有効にされる必要があります。これにより、管理者がメンバーアカウントを制御できるようになります。これは、組織を作成すると、デフォルトで設定されます。組織が一括決済のみに設定されていて、すべての機能を有効にする場合は、「組織内のすべての機能の有効化」を参照してください。
- AWS アカウント管理サービスの信頼されたアクセスを有効にする必要があります。これを設定するには、「AWS アカウント管理の信頼されたアクセスを有効にする」を参照してください。

> **Note**
>
> AWS Organizations 管理ポリシーAWSOrganizationsReadOnlyAccessまたはAWSOrganizationsFullAccessが更新され、 コンソールからアカウントデータにアクセスできるように AWS 、アカウント管理 APIsへのアクセス許可が付与されます AWS Organizations 。更新された管理ポリシーを表示するには、「Organizations AWS 管理ポリシーの更新」を参照してください。

AWS マネジメントコンソール

組織 AWS アカウント 内の の代替連絡先を追加または編集するには

1. 組織の管理アカウントの認証情報を使用して、AWS Organizations コンソールにサインインします。

2. AWS アカウントから、更新するアカウントを選択します。
3. [Contact info] (連絡先情報) を選択して、[Alternate contacts] (代替連絡先) で、連絡先のタイプ ([Billing contact] (請求連絡先)、[Security contact] (セキュリティ問い合わせ先)、または [Operations contact] (操作問い合わせ先)) を指定します。
4. 新しい連絡先を追加するには、[Add] (追加) を選択します。既存の連絡先を更新するには、[Edit] (編集) を選択します。
5. 使用可能なフィールドの値を変更します。

> **Important**
>
> ビジネスでは AWS アカウント、個人に属する電話番号と E メールアドレスではなく、会社の電話番号と E メールアドレスを入力するのがベストプラクティスです。

6. すべての変更を加え終わったら、[Update] (更新) を選択します。

AWS CLI & SDKs

次の AWS CLI コマンドまたは AWS SDK と同等のオペレーションを使用して、代替連絡先情報を取得、更新、または削除できます。

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **注意事項**
>
> - 組織内の管理アカウントまたは委任管理者アカウントからメンバーアカウントに対してこれらの操作を実行するには、アカウントサービス用の信頼されたアクセスを有効にする必要があります。
> - オペレーションの呼び出しに使用している組織とは異なる組織のアカウントにアクセスすることはできません。

> **最小アクセス許可**
>
> 各操作については、その操作に対応するアクセス許可が必要です。

- GetAlternateContact (代替連絡先の詳細を表示する場合)
- PutAlternateContact (代替連絡先を設定または更新する場合)
- DeleteAlternateContact (代替連絡先を削除する場合)

これらの個別のアクセス許可を使用すると、一部のユーザーに連絡先情報の読み取りのみを許可し、他のユーザーには読み取りと書き込みを許可するということもできます。

Example

次の例では、組織内の発信者のアカウントに現在設定されている、請求に関する通知の代替連絡先を取得します。使用される認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかから取得する必要があります。

```
$ aws account get-alternate-contact \
    --alternate-contact-type=BILLING \
    --account-id 123456789012
{
    "AlternateContact": {
        "AlternateContactType": "BILLING",
        "EmailAddress": "saanvi.sarkar@amazon.com",
        "Name": "Saanvi Sarkar",
        "PhoneNumber": "+1(206)555-0123",
        "Title": "CFO"
    }
}
```

Example

次の例では、組織内の指定されたメンバーアカウントの操作に関する代替連絡先を設定します。使用する認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかである必要があります。

```
$ aws account put-alternate-contact \
    --account-id 123456789012 \
    --alternate-contact-type=OPERATIONS \
```

```
    --email-address=mateo_jackson@amazon.com \
    --name="Mateo Jackson" \
    --phone-number="+1(206)555-1234" \
    --title="Operations Manager"
```

このコマンドは成功時に出力を生成しません。

> **Note**
>
> 同じコンタクトタイプ AWS アカウント と同じコンタクトタイプに対して複数のPutAlternateContactオペレーションを実行する場合、 は最初に新しいコンタクトを追加し、同じ AWS アカウント とコンタクトタイプへの連続する呼び出しはすべて既存のコンタクトを更新します。

Example

次の例では、組織内の指定されたメンバーアカウントのセキュリティに関する代替連絡先を削除します。使用する認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかである必要があります。

```
$ aws account delete-alternate-contact \
    --account-id 123456789012 \
    --alternate-contact-type=SECURITY
```

このコマンドは成功時に出力を生成しません。

Example

> **Note**
>
> 同じ連絡先を何回も削除しようとすると、メッセージは表示されずに 1 回目で成功します。それ以降の試行はすべて ResourceNotFound 例外を生成します。

account:AlternateContactTypes コンテキストキー

コンテキストキーを使用してaccount:AlternateContactTypes、IAM ポリシーによって許可 (または拒否) される 3 つの問い合わせタイプを指定できます。例えば、次の例の IAM アクセス許可

ポリシーでは、この条件キーを使用して、組織内の特定のアカウントの BILLING 代替連絡先のみを取得し、変更は行わないことを、アタッチされたプリンシパルに許可しています。

account:AlternateContactTypes は複数値を持つ文字列型のため、ForAnyValue または ForAllValues 複数値文字列演算子を使用する必要があります。

のプライマリ連絡先を更新する AWS アカウント

アカウントに関連付けられている主要連絡先情報を更新できます。これには、連絡先の氏名、会社名、郵送先住所、電話番号、ウェブサイトアドレスなどが含まれます。

アカウントがスタンドアロンであるか、組織の一部であるかに応じて、主要アカウント連絡先の編集方法は異なります。

- スタンドアロン AWS アカウント – 組織に関連付けられ AWS アカウント ていない場合は、 AWS マネジメントコンソールまたは CLI & SDKs AWS を使用して、独自のプライマリアカウントの連絡先を更新できます。これを行う方法については、「スタンドアロン AWS アカウント の主要連絡先の更新」を参照してください。
- AWS アカウント 組織内 – AWS 組織の一部であるメンバーアカウントの場合、管理アカウントまたは委任管理者アカウントのユーザーは、 AWS Organizations コンソールから、または CLI と SDKs AWS を介してプログラムで、組織内の任意のメンバーアカウントを一元的に更新できます。これを行う方法については、「Update AWS アカウント primary contact in your organization」を参照してください。

トピック

- 電話番号と E メールアドレスの要件
- スタンドアロンアカウント AWS アカウント または管理アカウントのプライマリ連絡先を更新する
- 組織内の AWS メンバーアカウントのプライマリ連絡先を更新する

電話番号と E メールアドレスの要件

アカウントの主要連絡先情報の更新を進める前に、まず、電話番号と E メールアドレスを入力する際の以下の要件を確認することをお勧めします。

- 電話番号には数字のみを含める必要があります。

- 電話番号は + と国コードで始まる必要があり、国コードの後に先行ゼロや追加のスペースがあってはなりません。例えば、+1 (米国/カナダ) や +44 (英国) です。
- 電話番号には、市外局番、交換所コード、ローカルコードの間に空白を含めることはできません。例えば、+12025550179 などです。
- セキュリティ上の理由から、電話番号は AWSからの SMS を受信できる必要があります。ほとんどの通話料無料番号は SMS をサポートしていないため、受け付けられません。
- ビジネスでは AWS アカウント、個人に属する電話番号と E メールアドレスではなく、会社の電話番号と E メールアドレスを入力するのがベストプラクティスです。アカウントのルートユーザーを個人の E メールアドレスまたは電話番号で設定すると、その個人が退職した場合にアカウントの復旧が困難になる可能性があります。

スタンドアロンアカウント AWS アカウント または管理アカウントのプライマリ連絡先を更新する

スタンドアロンの主な連絡先の詳細を編集するには AWS アカウント、次の手順を実行します。AWS マネジメントコンソール 以下の手順は、常にスタンドアロンコンテキストでのみ機能します。を使用して AWS マネジメントコンソール 、 オペレーションの呼び出しに使用したアカウントの主要連絡先情報にのみアクセスまたは変更できます。

AWS マネジメントコンソール

スタンドアロンのプライマリ連絡先を編集するには AWS アカウント

> **最小アクセス許可**
>
> 次の手順を実行するには、少なくとも以下のIAM アクセス許可が必要です。
>
> - `account:GetContactInformation` (主要連絡先の詳細を表示する場合)
> - `account:PutContactInformation` (主要連絡先の詳細を更新する場合)

1. AWS マネジメントコンソール に最小アクセス許可を持つ、IAM ユーザーまたはロールとしてサインインします。
2. ウィンドウの右上にあるアカウント名を選択し、[アカウント] を選択します。

3. [Contact information] (連絡先情報) セクションまで下にスクロールし、その隣にある [Edit] (編集) を選択します。
4. 使用可能なフィールドの値を変更します。
5. すべての変更を加え終わったら、[Update] (更新) を選択します。

AWS CLI & SDKs

次の AWS CLI コマンドまたは AWS SDK と同等のオペレーションを使用して、主要な連絡先情報を取得、更新、または削除できます。

- GetContactInformation
- PutContactInformation

> **注意事項**
>
> - 組織内の管理アカウントまたは委任管理者アカウントからメンバーアカウントに対してこれらの操作を実行するには、アカウントサービス用の信頼されたアクセスを有効にする必要があります。

> **最小アクセス許可**
>
> 各操作については、その操作に対応するアクセス許可が必要です。
>
> - `account:GetContactInformation`
> - `account:PutContactInformation`
>
> これらの個別のアクセス許可を使用すると、一部のユーザーに連絡先情報の読み取りのみを許可し、他のユーザーには読み取りと書き込みを許可するということもできます。

Example

次の例では、発信者のアカウントの現在の主要連絡先情報を取得します。

```
$ aws account get-contact-information
{
```

```
    "ContactInformation": {
        "AddressLine1": "123 Any Street",
        "City": "Seattle",
        "CompanyName": "Example Corp, Inc.",
        "CountryCode": "US",
        "DistrictOrCounty": "King",
        "FullName": "Saanvi Sarkar",
        "PhoneNumber": "+15555550100",
        "PostalCode": "98101",
        "StateOrRegion": "WA",
        "WebsiteUrl": "https://www.examplecorp.com"
    }
}
```

Example

次の例では、発信者のアカウントに新しい主要連絡先情報を設定します。

```
$ aws account put-contact-information --contact-information \
'{"AddressLine1": "123 Any Street", "City": "Seattle", "CompanyName": "Example Corp,
 Inc.", "CountryCode": "US", "DistrictOrCounty": "King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
 "StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

このコマンドは成功時に出力を生成しません。

組織内の AWS メンバーアカウントのプライマリ連絡先を更新する

組織内の AWS メンバーアカウントの主要連絡先の詳細を編集するには、次の手順を実行します。

その他の要件

AWS Organizations コンソールでプライマリ連絡先を更新するには、いくつかの事前設定を行う必要があります。

- メンバーアカウントで設定を管理するには、所属する組織によってすべての機能が有効にされる必要があります。これにより、管理者がメンバーアカウントを制御できるようになります。これは、組織を作成すると、デフォルトで設定されます。組織が一括決済のみに設定されていて、すべての機能を有効にする場合は、「組織内のすべての機能の有効化」を参照してください。
- AWS アカウント管理サービスの信頼されたアクセスを有効にする必要があります。これを設定するには、「AWS アカウント管理の信頼されたアクセスを有効にする」を参照してください。

AWS マネジメントコンソール

組織 AWS アカウント 内の の の主要連絡先を編集するには

1. 組織の管理アカウントの認証情報を使用して、AWS Organizations コンソールにサインインします。
2. AWS アカウントから、更新するアカウントを選択します。
3. [連絡先情報] を選択し、[主要連絡先] を見つけます。
4. [Edit] (編集) を選択します。
5. 使用可能なフィールドの値を変更します。
6. すべての変更を加え終わったら、[Update] (更新) を選択します。

AWS CLI & SDKs

次の AWS CLI コマンドまたは AWS SDK と同等のオペレーションを使用して、主要な連絡先情報を取得、更新、または削除できます。

- GetContactInformation
- PutContactInformation

> **注意事項**
>
> - 組織内の管理アカウントまたは委任管理者アカウントからメンバーアカウントに対してこれらの操作を実行するには、アカウントサービス用の信頼されたアクセスを有効にする必要があります。
> - オペレーションの呼び出しに使用している組織とは異なる組織のアカウントにアクセスすることはできません。

> **最小アクセス許可**
>
> 各操作については、その操作に対応するアクセス許可が必要です。
>
> - `account:GetContactInformation`
> - `account:PutContactInformation`

これらの個別のアクセス許可を使用すると、一部のユーザーに連絡先情報の読み取りのみを許可し、他のユーザーには読み取りと書き込みを許可するということもできます。

Example

次の例では、組織内の指定されたメンバーアカウントの現在の主要連絡先情報を取得します。使用される認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかから取得する必要があります。

```
$ aws account get-contact-information --account-id 123456789012
{
    "ContactInformation": {
        "AddressLine1": "123 Any Street",
        "City": "Seattle",
        "CompanyName": "Example Corp, Inc.",
        "CountryCode": "US",
        "DistrictOrCounty": "King",
        "FullName": "Saanvi Sarkar",
        "PhoneNumber": "+15555550100",
        "PostalCode": "98101",
        "StateOrRegion": "WA",
        "WebsiteUrl": "https://www.examplecorp.com"
    }
}
```

Example

次の例では、組織内の指定されたメンバーアカウントの主要連絡先情報を設定します。使用する認証情報は、組織の管理アカウント、またはアカウント管理の委任管理者アカウントのいずれかである必要があります。

```
$ aws account put-contact-information --account-id 123456789012 \
--contact-information '{"AddressLine1": "123 Any Street", "City": "Seattle",
 "CompanyName": "Example Corp, Inc.", "CountryCode": "US", "DistrictOrCounty":
 "King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
 "StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

このコマンドは成功時に出力を生成しません。

AWS アカウント 識別子を表示する

AWS は、それぞれに次の一意の識別子を割り当てます AWS アカウント。

AWS アカウント ID

AWS アカウントを一意に識別する 12 桁の数値 (012345678901 など)。多くの AWS リソースには、Amazon リソースネーム (ARNs) のアカウント ID が含まれます。アカウント ID 部分では、あるアカウントのリソースと、別のアカウントのリソースを区別します。 AWS Identity and Access Management (IAM) ユーザーの場合は、アカウント ID またはアカウントエイリアス AWS マネジメントコンソール を使用して にサインインできます。アカウント ID は、他の識別情報と同様に、慎重に使用および共有する必要がありますが、秘密情報、センシティブ情報、または機密情報とは見なされません。

正規ユーザー ID

ID の難読化された形式79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2beであるなどの英数字識別子 AWS アカウント 。この ID を使用して、Amazon Simple Storage Service (Amazon S3) を使用してバケットとオブジェクトへのクロスアカウントアクセスを許可する AWS アカウント ときに、 を識別できます。Amazon S3 AWS アカウント の正規ユーザー ID は、ルートユーザーまたは IAM ユーザーとして取得できます。

これらの識別子を表示するには AWS 、 で認証されている必要があります。

> **Warning**
>
> AWS リソースを共有するために AWS アカウント 識別子を必要とする第三者に AWS 認証情報 (パスワードやアクセスキーを含む) を提供しないでください。これにより、ユーザーが持ってい AWS アカウント るのと同じアクセス権が付与されます。

AWS アカウント ID を検索する

AWS アカウント ID は、 AWS マネジメントコンソール または AWS Command Line Interface () を使用して確認できますAWS CLI。コンソールでは、アカウント ID の場所は、ルートユーザーとしてサインインしているか、IAM ユーザーとしてサインインしているかによって異なります。アカウント ID は、ルートユーザーとしてサインインしているか、IAM ユーザーとしてサインインしているかにかかわらず同じです。

ルートユーザーとしてアカウント ID を検索するには

AWS マネジメントコンソール

ルートユーザーとしてサインインしたときに AWS アカウント ID を検索するには

> **最小アクセス許可**
>
> 次の手順を実行するには、少なくとも以下の IAM アクセス許可が必要です。
>
> - ルートユーザーとしてサインインすると、IAM アクセス許可は必要ありません。

1. 右上のナビゲーションバーでアカウント名またはアカウント番号を選択し、[セキュリティ認証情報] を選択します。

   > **Tip**
   >
   > [セキュリティ認証情報] オプションが表示されない場合、IAM ユーザーではなく IAM ロールを持つフェデレーションユーザーとしてサインインしている可能性があります。その場合は、[アカウント] エントリとその横にあるアカウント ID 番号を探してください。

2. [アカウントの詳細] セクションの [AWS アカウント ID] の横にアカウント番号が表示されます。

AWS CLI & SDKs

を使用して AWS アカウント ID を検索するには AWS CLI

> **最小アクセス許可**
>
> 次の手順を実行するには、少なくとも以下の IAM アクセス許可が必要です。
>
> - ルートユーザーとしてコマンドを実行する場合、IAM アクセス許可は必要ありません。

get-caller-identity コマンドを次のように使用します。

```
$ aws sts get-caller-identity \
    --query Account \
    --output text
123456789012
```

IAM ユーザーとしてアカウント ID を検索する

AWS マネジメントコンソール

IAM ユーザーとしてサインインしたときに AWS アカウント ID を検索するには

> **最小アクセス許可**
>
> 次の手順を実行するには、少なくとも以下のIAM アクセス許可が必要です。
>
> - `account:GetAccountInformation`

1. 右上のナビゲーションバーでユーザー名を選択し、続いて [認証情報] を選択します。

   > **Tip**
   >
   > [セキュリティ認証情報] オプションが表示されない場合、IAM ユーザーではなく IAM ロールを持つフェデレーションユーザーとしてサインインしている可能性があります。その場合は、[アカウント] エントリとその横にあるアカウント ID 番号を探してください。

2. ページ上部の [アカウントの詳細] で、[AWS アカウント ID] の横にアカウント番号が表示されます。

AWS CLI & SDKs

を使用して AWS アカウント ID を検索するには AWS CLI

> **最小アクセス許可**
>
> 次の手順を実行するには、少なくとも以下の IAM アクセス許可が必要です。
>
> - IAM ユーザーまたはロールとしてコマンドを実行する場合は、次のものが必要です。

- sts:GetCallerIdentity

get-caller-identity コマンドを次のように使用します。

```
$ aws sts get-caller-identity \
    --query Account \
    --output text
123456789012
```

の正規ユーザー ID を検索する AWS アカウント

AWS マネジメントコンソール または AWS アカウント を使用して、 の正規ユーザー ID を確認できます AWS CLI。の正規ユーザー ID AWS アカウント は、そのアカウントに固有です。の正規ユーザー ID は、ルートユーザー、フェデレーティッドユーザー、または IAM ユーザー AWS アカウントとして取得できます。

ルートユーザーまたは IAM ユーザーとして正規ユーザー ID を検索する

AWS マネジメントコンソール

ルートユーザーまたは IAM ユーザーとしてコンソールにサインインしたときに、アカウントの正規ユーザー ID を検索するには

> **最小アクセス許可**
>
> 次の手順を実行するには、少なくとも以下の IAM アクセス許可が必要です。
>
> - ルートユーザーとしてコマンドを実行する場合、IAM アクセス許可は必要ありません。
> - IAM ユーザーとしてサインインすると、次のことが必要です。
>   - account:GetAccountInformation

1. ルートユーザーまたは IAM ユーザー AWS マネジメントコンソール として にサインインします。
2. 右上のナビゲーションバーでアカウント名またはアカウント番号を選択し、[セキュリティ認証情報] を選択します。

> **Tip**
>
> [セキュリティ認証情報] オプションが表示されない場合、IAM ユーザーではなく IAM ロールを持つフェデレーションユーザーとしてサインインしている可能性があります。その場合は、[アカウント] エントリとその横にあるアカウント ID 番号を探してください。

3. [アカウントの詳細] セクションで、[正規ユーザー ID] の横に、正規ユーザー ID が表示されます。正規ユーザー ID を使用して、Amazon S3 アクセスコントロールリスト (ACL) を設定できます。

AWS CLI & SDKs

を使用して正規ユーザー ID を検索するには AWS CLI

同じ AWS CLI および API コマンドは AWS アカウントのルートユーザー、、IAM ユーザー、または IAM ロールで機能します。

list-buckets コマンドを次のように使用します。

```
$ aws s3api list-buckets \
    --max-items 10 \
    --page-size 10 \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

IAM ロールを持つフェデレーションユーザーとして正規 ID を検索する

AWS マネジメントコンソール

IAM ロールを持つフェデレーションユーザーとしてコンソールにサインインしている場合に、アカウントの正規ユーザー ID を検索する手順

> **最小アクセス許可**
>
> - Amazon S3 バケットを一覧表示して表示するには、アクセス許可が必要です。

1. IAM ロールを持つフェデレーティッドユーザー AWS マネジメントコンソール として にサインインします。
2. バケットの詳細を表示するには、Amazon S3 コンソールでバケット名を選択します。
3. [アクセス許可] タブを選択します。
4. [アクセスコントロールリスト] セクションの [バケット所有者] の下に、 AWS アカウント の正規 ID が表示されます。

AWS CLI & SDKs

を使用して正規ユーザー ID を検索するには AWS CLI

同じ AWS CLI および API コマンドは AWS アカウントのルートユーザー、、IAM ユーザー、または IAM ロールで機能します。

list-buckets コマンドを次のように使用します。

```
$ aws s3api list-buckets \
    --max-items 10 \
    --page-size 10 \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

AWS アカウント管理のセキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、最もセキュリティの影響を受けやすい組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを活用できます。

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

- クラウドのセキュリティ – AWS は、 で AWS サービスを実行するインフラストラクチャを保護する責任があります AWS クラウド。 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。サードパーティーの監査者は、AWS コンプライアンスプログラムコンプライアンスプログラムの一環として、当社のセキュリティの有効性を定期的にテストおよび検証。アカウント管理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、AWS のサービス「コンプライアンスプログラムによる対象範囲内」を参照してください。
- クラウド内のセキュリティ – 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、ユーザーは、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、 AWS アカウント管理を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。セキュリティおよびコンプライアンス上の目的に合わせてアカウント管理を設定する方法について説明します。また、アカウント管理リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- AWS アカウント管理でのデータ保護
- AWS PrivateLink AWS アカウント管理用
- AWS アカウント管理の Identity and Access Management
- AWS AWS アカウント管理の 管理ポリシー
- AWS アカウント管理のコンプライアンス検証
- AWS アカウント管理の耐障害性
- のインフラストラクチャセキュリティ AWS アカウント管理

AWS アカウント管理でのデータ保護

責任 AWS 共有モデル、 AWS アカウント管理のデータ保護に適用されます。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。ユーザーは、このインフラストラクチャでホストされ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、「Data Privacy FAQChina」を参照してください。 欧州におけるデータ保護に関する情報については、General Data Protection Regulation (GDPR) Center 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 アイデンティティセンターまたは 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 は必須ですが、TLS 1.3 を推奨します。
- 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。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- 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 などの高度な管理された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 140-3 検証済み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) 140-3」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を、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含めないことを強くお勧めします。これは、コンソール、API、AWS CLIまたは SDK を使用してアカウント管理または他の AWS のサービス を使用する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

AWS PrivateLink AWS アカウント管理用

Amazon Virtual Private Cloud (Amazon VPC) を使用して AWS リソースをホストする場合、パブリックインターネットを経由することなく、VPC 内から AWS アカウント管理サービスにアクセスできます。

Amazon VPC では、カスタム仮想ネットワークで AWS リソースを起動できます。VPC を使用して、IP アドレス範囲、サブネット、ルートテーブル、ネットワークゲートウェイなどのネットワーク設定を制御できます。VPC の詳細については、Amazon VPC ユーザーガイドを参照してください。

Amazon VPC をアカウント管理に接続するには、まずインターフェイス VPC エンドポイントを定義する必要があり、そうすることで VPC を他の AWS サービスに接続できます。このエンドポイントを使用すると、インターネットゲートウェイやネットワークアドレス変換 (NAT) インスタンス、または VPN 接続などを必要とせずに、信頼性の高いスケーラブルな方法で接続できるようになります。詳細については、「Amazon VPC ユーザーガイド」の「インターフェイス VPC エンドポイント (AWS PrivateLink)」を参照してください。

エンドポイントを作成する

VPC で AWS アカウント管理エンドポイントを作成するには AWS マネジメントコンソール、 AWS Command Line Interface 、 (AWS CLI)、 AWS SDK、 AWS アカウント管理 API、または を使用します CloudFormation。

Amazon VPC コンソールまたは を使用してエンドポイントを作成および設定する方法については AWS CLI、「Amazon VPC ユーザーガイド」の「インターフェイスエンドポイントの作成」を参照してください。

> **Note**
>
> エンドポイントを作成する際に、VPC の接続先になるサービスとして、以下の形式でアカウント管理を指定します。
>
> ```
> com.amazonaws.us-east-1.account
> ```
>
> `us-east-1` リージョンを指定する文字列を表示されているとおり正確に使用する必要があります。グローバルサービスとして、アカウント管理は 1 つの AWS リージョンでのみホストされます。

を使用してエンドポイントを作成および設定する方法については CloudFormation、「CloudFormation ユーザーガイド」のAWS::EC2::VPCEndpoint リソース」を参照してください。

Amazon VPC エンドポイントポリシー

Amazon VPC エンドポイントの作成時にエンドポイントポリシーをアタッチすることで、このサービスエンドポイントで実行できるアクションを制御できます。複数のエンドポイントポリシーをアタッチすることで、複雑な IAM ルールを作成できます。詳細については、「」を参照してください。

- アカウント管理用の Amazon Virtual Private Cloud エンドポイントポリシー
- AWS PrivateLink ガイドの「VPC エンドポイントによるサービスへのアクセスのコントロール」

アカウント管理用の Amazon Virtual Private Cloud エンドポイントポリシー

Amazon SNS の Amazon VPC エンドポイントに対するポリシーを作成して、以下を指定することができます。

- アクションを実行できるプリンシパル。
- プリンシパルが実行できるアクション。
- このアクションを実行できるリソース。

次の例は、アカウント 123456789012 の Alice という名前の 1 人の IAM ユーザーが任意の の代替連絡先情報を取得および変更することを許可する Amazon VPC エンドポイントポリシーを示していますが AWS アカウント、任意のアカウントの代替連絡先情報を削除するすべての IAM ユーザーのアクセス許可を拒否します。

Organization の一部であるアカウントへのアクセス権を AWS 組織のメンバーアカウントの 1 つにあるプリンシパルに付与する場合、 `Resource`要素は次の形式を使用する必要があります。

```
arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
```

エンドポイントポリシーの作成方法の詳細については、AWS PrivateLink ガイドの「VPC エンドポイントによるサービスへのアクセスのコントロール」を参照してください。

AWS アカウント管理の Identity and Access Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 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、誰に請求情報とコスト管理リソースの使用を認可する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで使用できる AWS のサービス です。

トピック

- オーディエンス
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- AWS アカウント管理と IAM の連携方法
- AWS アカウント管理のアイデンティティベースのポリシーの例
- AWS アカウント管理にアイデンティティベースのポリシー (IAM ポリシー) を使用する
- AWS アカウント管理の ID とアクセスのトラブルシューティング

オーディエンス

AWS Identity and Access Management (IAM) の使用方法は、ロールによって異なります。

- サービスユーザー - 機能にアクセスできない場合は、管理者にアクセス許可をリクエストします (「AWS アカウント管理の ID とアクセスのトラブルシューティング」を参照)。
- サービス管理者 - ユーザーアクセスを決定し、アクセス許可リクエストを送信します (「AWS アカウント管理と IAM の連携方法」を参照)
- IAM 管理者 - アクセスを管理するためのポリシーを作成します (「AWS アカウント管理のアイデンティティベースのポリシーの例」を参照)

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。、IAM ユーザー AWS アカウントのルートユーザー、または IAM ロールを引き受けることで認証される必要があります。

(AWS IAM アイデンティティセンター IAM Identity Center)、シングルサインオン認証、Google/Facebook 認証情報などの ID ソースからの認証情報を使用して、フェデレーティッド ID としてサイ

ンインできます。サインインの詳細については、「AWS サインイン ユーザーガイド」の「AWS アカウントにサインインする方法」を参照してください。

プログラムによるアクセスの場合、 は SDK と CLI AWS を提供してリクエストを暗号化して署名します。詳細については、「IAM ユーザーガイド」の「API リクエストに対するAWS 署名バージョン 4」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、まず、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 AWS アカウント root ユーザーと呼ばれる 1 つのサインインアイデンティティから始めます。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。ルートユーザー認証情報を必要とするタスクについては、「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。

フェデレーテッドアイデンティティ

ベストプラクティスとして、人間のユーザーが一時的な認証情報 AWS のサービス を使用して にアクセスするには、ID プロバイダーとのフェデレーションを使用する必要があります。

フェデレーティッド ID は、エンタープライズディレクトリ、ウェブ ID プロバイダー、または ID Directory Service ソースの認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーテッドアイデンティティは、一時的な認証情報を提供するロールを引き受けます。

アクセスを一元管理する場合は、 AWS IAM アイデンティティセンターをお勧めします。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「IAM アイデンティティセンターとは」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、特定の個人やアプリケーションに対する特定のアクセス許可を持つアイデンティティです。長期認証情報を持つ IAM ユーザーの代わりに一時的な認証情報を使用することをお勧めします。詳細については、IAM ユーザーガイドの「ID プロバイダーとのフェデレーションを使用して にアクセスする必要がある AWS」を参照してください。

IAM グループは、IAM ユーザーの集合を指定し、大量のユーザーに対するアクセス許可の管理を容易にします。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可を持つアイデンティであり、一時的な認証情報を提供します。ユーザーから IAM ロール (コンソール) に切り替えるか、 または API オペレーションを呼び出すことで、ロールを引き受けることができます。 AWS CLI AWS 詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールは、フェデレーションユーザーアクセス、一時的な IAM ユーザーのアクセス許可、クロスアカウントアクセス、クロスサービスアクセス、および Amazon EC2 で実行するアプリケーションに役立ちます。詳細については、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。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは、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場合のアクセス許可を定義します。 は、プリンシパル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。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、ポリシーを使用して、どのプリンシパルがどのリソースに対して、どのような条件でアクションを実行できるかを定義することで、誰が何にアクセスできるかを指定します。

デフォルトでは、ユーザーやロールにアクセス許可はありません。IAM 管理者は IAM ポリシーを作成してロールに追加し、このロールをユーザーが引き受けられるようにします。IAM ポリシーは、オペレーションの実行方法を問わず、アクセス許可を定義します。

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のポリシーは、アイデンティティ (ユーザー、グループ、またはロール) にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、アイデンティティがどのリソースに対してどのような条件下でどのようなアクションを実行できるかを制御します。アイデンティティベースポリシーの作成方法については、IAM ユーザーガイド の カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する を参照してください。

アイデンティティベースのポリシーは、インラインポリシー (単一の ID に直接埋め込む) または管理ポリシー (複数の ID にアタッチされたスタンドアロンポリシー) にすることができます。管理ポリシーとインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。例としては、IAM ロール信頼ポリシーや Amazon S3 バケットポリシーなどがあります。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。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。

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。

その他のポリシータイプ

AWS は、より一般的なポリシータイプによって付与されるアクセス許可の上限を設定できる追加のポリシータイプをサポートしています。

- アクセス許可の境界 – アイデンティティベースのポリシーで IAM エンティティに付与することのできるアクセス許可の数の上限を設定します。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境界」を参照してください。
- サービスコントロールポリシー (SCP) - AWS Organizations内の組織または組織単位の最大のアクセス許可を指定します。詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」を参照してください。
- リソースコントロールポリシー (RCP) – は、アカウント内のリソースで利用できる最大数のアクセス許可を定義します。詳細については、「AWS Organizations ユーザーガイド」の「リソースコントロールポリシー (RCP)」を参照してください。
- セッションポリシー – ロールまたはフェデレーションユーザーの一時セッションを作成する際にパラメータとして渡される高度なポリシーです。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

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

AWS アカウント管理と IAM の連携方法

IAM を使用してアカウント管理へのアクセスを管理する前に、アカウント管理で利用できる IAM の機能について学習します。

AWS アカウント管理で使用できる IAM 機能

IAM 機能	アカウント管理のサポート
ID ベースのポリシー	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	あり
ポリシー条件キー	あり
ACL	なし
ABAC (ポリシー内のタグ)	いいえ
一時的な認証情報	あり
プリンシパルアクセス権限	あり
サービスロール	いいえ
サービスリンクロール	いいえ

アカウント管理およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要については、IAM ユーザーガイドのAWS 「IAM と連携する のサービス」を参照してください。

アカウント管理の ID ベースのポリシー

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザー

とロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

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、およびアクションを許可または拒否する条件を指定できます。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

アカウント管理 ID ベースのポリシーの例

アカウント管理 ID ベースのポリシーの例は、「AWS アカウント管理のアイデンティティベースのポリシーの例」でご確認ください。

アカウント管理内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

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コントロールできます。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、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。

クロスアカウントアクセスを有効にするには、全体のアカウント、または別のアカウントの IAM エンティティを、リソースベースのポリシーのプリンシパルとして指定します。詳細については、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。

アカウント管理用のポリシーアクション

ポリシーアクションのサポート: あり

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

JSON ポリシーの Action 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

アカウント管理アクションのリストを確認するには、「サービス認可リファレンス」のAWS 「アカウント管理で定義されるアクション」を参照してください。

ネットワーク管理 のポリシーアクションは、アクションの前に、プレフィックス を使用します。

```
account
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "account:action1",
      "account:action2"
         ]
```

ワイルドカード (*) を使用すると、複数のアクションを指定することができます。たとえば、 AWS アカウントの代替連絡先と連携す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": "account:*AlternateContact"
```

アカウント管理 ID ベースのポリシーの例は、「AWS アカウント管理のアイデンティティベースのポリシーの例」でご確認ください。

アカウント管理のポリシーリソース

ポリシーリソースのサポート: あり

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

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。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。リソースレベ

ルのアクセス許可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": "*"
```

アカウント管理サービスは、IAM ポリシーの Resource要素で次の特定のリソースタイプをサポートし、ポリシーをフィルタリングしてこれらのタイプを区別するのに役立ちます AWS アカウント。

- account

  この resource タイプは、 AWS Organizations サービスによって管理される組織内のメンバーアカウントではないスタンドアロン AWS アカウント のみに一致します。

- accountInOrganization

  このresourceタイプは、 AWS Organizations サービスによって管理 AWS アカウント される組織のメンバーアカウントである のみに一致します。

アカウント管理リソースタイプとその ARNsAWS 「アカウント管理で定義されるリソース」を参照してください。 各リソースの ARN を指定できるアクションについては、AWS 「アカウント管理で定義されるアクション」を参照してください。

アカウント管理 ID ベースのポリシーの例は、「AWS アカウント管理のアイデンティティベースのポリシーの例」でご確認ください。

アカウント管理用のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

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

Condition 要素は、定義された基準に基づいてステートメントが実行される時期を指定します。イコールや未満などの条件演算子を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「グローバル条件コンテキストキー」を参照してください。

アカウント管理サービスは、IAM ポリシーのきめ細かなフィルタリングを提供するために使用できる以下の条件キーをサポートしています。

- account:TargetRegion

  この条件キーは、次のリストで構成される引数を取ります。AWS リージョンコード。これにより、指定したリージョンに適用されるアクションのみに影響を与えるように、ポリシーをフィルタリングできます。

- account:AlternateContactTypes

  この条件キーは、代替連絡先タイプのリストを取ります。

  - 請求
  - 操作
  - SECURITY

  このキーを使用すると、指定された代替連絡先タイプをターゲットとするアクションのみにリクエストをフィルタリングできます。

- account:AccountResourceOrgPaths

  この条件キーは、組織の階層から特定の組織単位 (OU) へのパスのリストで構成される引数を取ります。これにより、一致する OU 内のターゲットアカウントのみに影響を与えるように、ポリシーをフィルタリングできます。

  ```
  o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*
  ```

- account:AccountResourceOrgTags

  この条件キーは、タグキーと値のリストで構成される引数を取ります。これにより、組織のメンバーであり、指定されたタグのキーと値でタグ付けされたアカウントのみに影響を与えるように、ポリシーをフィルタリングできます。

- account:EmailTargetDomain

  この条件キーは、E メールドメインで構成される引数を取ります。これにより、指定した E メールドメインに一致するアクションのみに影響を与えるように、ポリシーをフィルタリングできます。この条件キーでは、大文字と小文字が区別されます。ターゲット E メールアドレスドメインに基づいてアクションを制御するには、ポリシーの条件ブロックで `StringEquals` の代わりに `StringEqualsIgnoreCase` を使用する必要があります。E メールドメインに `example.com`、`company.org`、または `EXAMPLE.COM` などの大文字と小文字の任意の組み合わせが含まれている場合に `account:StartPrimaryEmailUpdate` アクションを完了できるようにするポリシーの例を次に示します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowConditionKey",
            "Effect": "Allow",
            "Action": [
                "account:StartPrimaryEmailUpdate"
            ],
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "account:EmailTargetDomain": [
                        "example.com",
                        "company.org"
                    ]
                }
            }
        }
    ]
}
```

アカウント管理条件キーのリストを確認するには、「サービス認可リファレンス」の AWS 「アカウント管理の条件キー」を参照してください。条件キーを使用できるアクションとリソースについては、AWS 「アカウント管理で定義されるアクション」を参照してください。

アカウント管理 ID ベースのポリシーの例は、「AWS アカウント管理のアイデンティティベースのポリシーの例」でご確認ください。

Account Management のアクセス制御リスト

ACL のサポート: なし

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アクセス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。

アカウント管理を使用した属性ベースのアクセスコントロール

ABAC (ポリシー内のタグ) のサポート: なし

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。では AWS、これらの属性はタグと呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

AWS アカウント管理では、タグベースのアクセスコントロールは `account:AccountResourceOrgTags/key-name`条件キーを介してのみサポートされます。標準の `aws:ResourceTag/key-name` 条件キーは、アカウント名前空間の API ではサポートされていません。

サポートされている条件キーを使用した JSON ポリシーの例

次のポリシー例では、組織内のキー「CostCenter」と「12345」または「67890」の値でタグ付けされたアカウントの連絡先情報を表示するアクセスを許可します。

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "account:GetContactInformation",
            "account:GetAlternateContact"
         ],
         "Resource":"*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "account:AccountResourceOrgTags/CostCenter":[
                  "12345",
                  "67890"
               ]
            }
         }
      }
   ]
}
```

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」および「IAM チュートリアル: タグに基づいて AWS リソースにアクセスするアクセス許可を定義する」を参照してください。

アカウント管理での一時的な認証情報の使用

一時的な認証情報のサポート: あり

一時的な認証情報は、 AWS リソースへの短期アクセスを提供し、フェデレーションまたは切り替えロールを使用する場合に自動的に作成されます。 AWS では、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成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「IAM の一時的な認証情報」および「AWS のサービス と IAM との連携」を参照してください。

アカウント管理のクロスサービスプリンシパル許可

転送アクセスセッション (FAS) のサポート: あり

転送アクセスセッション (FAS) は、 を呼び出すプリンシパルのアクセス許可と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする を使用します。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。

アカウント管理のサービスロール

サービスロールのサポート: なし

サービスロールとは、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 のサービスに許可を委任するロールを作成するを参照してください。

アカウント管理用のサービスリンクロール

サービスにリンクされたロールのサポート: なし

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、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

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、「IAM と提携するAWS のサービス」を参照してください。表の「サービスリンクロール」列に Yes と記載されたサービスを見つけます。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、[はい] リンクを選択します。

AWS アカウント管理の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、ユーザーおよびロールにはアカウント管理リソースを作成または変更するアクセス許可がありません。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。

これらのサンプルの JSON ポリシードキュメントを使用して IAM 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 ポリシーを作成する (コンソール)」を参照してください。

各リソースタイプの ARNsAWS 「アカウント管理のアクション、リソース、および条件キー」を参照してください。

トピック

- ポリシーに関するベストプラクティス
- のアカウントページの使用 AWS マネジメントコンソール
- のアカウントページへの読み取り専用アクセスを提供する AWS マネジメントコンソール
- のアカウントページへのフルアクセスの提供 AWS マネジメントコンソール

ポリシーに関するベストプラクティス

ID ベースのポリシーは、アカウント内のアカウント管理リソースを誰かが作成、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では、 AWS アカウントに費用が発生する場合があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、IAM ユーザーガイド の AWS マネージドポリシー または ジョブ機能のAWS マネージドポリシー を参照してください。

- 最小特権を適用する – IAM ポリシーでアクセス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。たとえば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用されている場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます CloudFormation。詳細については、IAM ユーザーガイド の IAM JSON ポリシー要素:条件 を参照してください。
- IAM アクセスアナライザー 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 アクセスアナライザー は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイド の IAM Access Analyzer でポリシーを検証する を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、MFA をオンにしてセキュリティを強化します。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイド の MFA を使用した安全な API アクセス を参照してください。

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

のアカウントページの使用 AWS マネジメントコンソール

のアカウントページにアクセスするには AWS マネジメントコンソール、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、 の詳細を一覧表示および表示できます AWS アカウント。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。

ユーザーとロールがアカウント管理コンソールを使用できるようにするには、`AWSAccountManagementReadOnlyAccess` または `AWSAccountManagementFullAccess` AWS 管理ポリシーをエンティティにアタッチすることを選択できます。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。

CLI または AWS API AWS 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、多くの場合、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を許可できます。

のアカウントページへの読み取り専用アクセスを提供する AWS マネジメントコンソール

次の例では、 AWS アカウント の IAM ユーザーに、 AWS マネジメントコンソールの [アカウント] ページへの読み取り専用アクセス権を付与します。このポリシーがアタッチされたユーザーは、変更を加えることはできません。

`account:GetAccountInformation` アクションは、[アカウント] ページのほとんどの設定を表示するためのアクセス権を付与します。ただし、現在有効になっている AWS リージョンを表示するには、`account:ListRegions`アクションも含めなければなりません。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "GrantReadOnlyAccessToAccountSettings",
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "account:ListRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

のアカウントページへのフルアクセスの提供 AWS マネジメントコンソール

次の例では、 AWS アカウント の IAM ユーザーに AWS マネジメントコンソールの [アカウント] ページへのフルアクセス権を付与します。このポリシーがアタッチされたユーザーは、アカウントの設定を変更できます。

このポリシーの例は、前述のポリシーの例に、使用可能な書き込みアクセス許可 (CloseAccount を除く) をそれぞれ追加することで作成されており、`account:EnableRegion` および

account:DisableRegion アクセス許可を含むほとんどのアカウント設定をユーザーが変更できるようにします。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "GrantFullAccessToAccountSettings",
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "account:ListRegions",
                "account:PutContactInformation",
                "account:PutAlternateContact",
                "account:DeleteAlternateContact",
                "account:EnableRegion",
                "account:DisableRegion"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS アカウント管理にアイデンティティベースのポリシー (IAM ポリシー) を使用する

AWS アカウント および IAM ユーザーの詳細については、「IAM とは」を参照してください。「IAM ユーザーガイド」の「」を参照してください。

カスタマー管理ポリシーを更新する方法については、「IAM ユーザーガイド」の「IAM ポリシーの編集」を参照してください。

AWS アカウント管理アクションポリシー

この表は、アカウント設定へのアクセス権を付与するアクセス許可の要約を示しています。これらのアクセス許可を使用するポリシーの例については、AWS アカウント管理のアイデンティティベースのポリシーの例 を参照してください。

> **Note**
>
> のアカウントページで特定のアカウント設定への書き込みアクセスを IAM ユーザー に許可するには AWS マネジメントコンソール、その設定の変更に使用するアクセスGetAccountInformation許可 (またはアクセス許可) に加えて、 アクセス許可を付与する必要があります。

アクセス許可名	アクセスレベル	説明
account:ListRegions	[List] (リスト)	使用可能なリージョンをリストするためのアクセス許可を付与します。
account:GetAccount Information	読み取り	アカウントのアカウント情報を取得するためのアクセス許可を付与します。
account:GetAlterna teContact	読み取り	アカウントの代替連絡先を取得するためのアクセス許可を付与します。
account:GetContact Information	読み取り	アカウントの主要連絡先情報を取得するためのアクセス許可を付与します。
account:GetPrimary Email	読み取り	アカウントのプライマリ E メールアドレスを取得するためのアクセス許可を付与します。
account:GetRegionO ptStatus	読み取り	リージョンのオプトインステータスを取得するためのアクセス許可を付与します。
account:AcceptPrim aryEmailUpdate	書き込み	AWS 組織内のメンバーアカウントのプライマリ E メールア

アクセス許可名	アクセスレベル	説明
		ドレスの更新を受け入れるアクセス許可を付与します。
account:CloseAccount	書き込み	アカウントを閉鎖するためのアクセス許可を付与します。 **Note** これはコンソール専用のアクセス許可です。このアクセス許可に対しては、API によりアクセスすることはできません。
account:DeleteAlternateContact	書き込み	アカウントの代替連絡先を削除するためのアクセス許可を付与します。
account:DisableRegion	書き込み	リージョンの使用を無効にするためのアクセス許可を付与します。
account:EnableRegion	書き込み	リージョンの使用を有効にするためのアクセス許可を付与します。
account:PutAccountName	書き込み	アカウントの名を更新するためのアクセス許可を付与します。
account:PutAlternateContact	書き込み	アカウントの代替連絡先を変更するためのアクセス許可を付与します。

アクセス許可名	アクセスレベル	説明
account:PutContactInformation	書き込み	アカウントの主要連絡先情報を更新するためのアクセス許可を付与します。
account:StartPrimaryEmailUpdate	書き込み	AWS 組織内のメンバーアカウントのプライマリ E メールアドレスの更新を開始するアクセス許可を付与します。

AWS アカウント管理の ID とアクセスのトラブルシューティング

以下の情報は、アカウント管理と IAM を併用した場合に発生しうる一般的な問題の診断と解決に役立ちます。

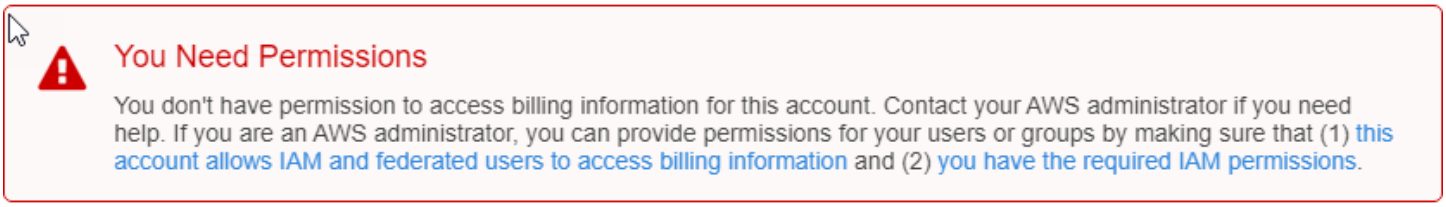
トピック

- [アカウント] ページでのアクションの実行を認可されていない
- iam:PassRole を実行する権限がない
- 自分の 以外のユーザーに自分のアカウントの詳細 AWS アカウント へのアクセスを許可したい

[アカウント] ページでのアクションの実行を認可されていない

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

次の例のエラーは、IAM mateojackson ユーザーがコンソールを使用して の AWS アカウント アカウントページで の詳細を表示しようとしている AWS マネジメントコンソール が、 アクセスaccount:GetAccountInformation許可がない場合に発生します。



この場合、Mateo は、account:*GetWidget* アクションを使用して *my-example-widget* 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:PassRole を実行する権限がない

iam:PassRole アクションの実行を認可されていないことを示すエラーが表示された場合は、アカウント管理にロールを渡すことができるように、ポリシーを更新する必要があります。

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

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用してアカウント管理でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与されたアクセス許可が必要です。Mary には、ロールをサービスに渡すアクセス許可がありません。

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

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

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

自分の 以外のユーザーに自分のアカウントの詳細 AWS アカウント 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:

- これらの機能をアカウント管理でサポートされるかどうかを確認するには、AWS アカウント管理と IAM の連携方法 を参照してください。

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

AWS AWS アカウント管理の 管理ポリシー

AWS アカウント管理では現在、次の 2 つの AWS 管理ポリシーを使用できます。

- AWS マネージドポリシー: AWSAccountManagementReadOnlyAccess
- AWS マネージドポリシー: AWSAccountManagementFullAccess
- AWS 管理ポリシーに対するアカウント管理の更新

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できるように、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ように設計されています。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS マネージドポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) に影響します。 AWS は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、 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。

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」を参照してください。

AWS マネージドポリシー: AWSAccountManagementReadOnlyAccess

AWSAccountManagementReadOnlyAccess ポリシーを IAM アイデンティティにアタッチできます。

以下のポリシーは、読み取り専用の機能へのアクセス許可を提供します。

- に関するメタデータ AWS アカウント
- に対して有効または無効 AWS リージョン になっている AWS アカウント（アカウント内のリージョンのステータスは、 AWS コンソールを使用してのみ表示できます）

これは、Get* または List* オペレーションのいずれかを実行するアクセス許可を付与することによって実現されます。アカウントのメタデータを変更したり、アカウントの AWS リージョン を有効または無効にしたりすることはできません。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- account – プリンシパルがメタデータ情報を取得できるようにします AWS アカウント。また、AWS リージョン 内のアカウントで有効になっている AWS マネジメントコンソールを一覧表示できます。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "account:Get*",
                "account:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS マネージドポリシー: AWSAccountManagementFullAccess

AWSAccountManagementFullAccess ポリシーを IAM アイデンティティにアタッチできます。

このポリシーは、次の項目を表示または変更するための完全な管理者アクセス権を提供します。

- に関するメタデータ AWS アカウント
- に対して有効または無効 AWS リージョン になっている (AWS コンソールを使用してのみ、アカウントのリージョンのステータスを表示または有効または無効に AWS アカウント できます)

これは、あらゆる account オペレーションを実行するアクセス許可を付与することで実現されます。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- account – プリンシパルがメタデータ情報を表示または変更できるようにします AWS アカウント。また、プリンシパルは、アカウントで有効になっている AWS リージョン を一覧表示し、AWS マネジメントコンソール内でそれらの有効と無効を切り替えることができます。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "account:*",
            "Resource": "*"
        }
    ]
}
```

AWS 管理ポリシーに対するアカウント管理の更新

このサービスがこれらの変更の追跡を開始してからのアカウント管理の AWS 管理ポリシーの更新に関する詳細を表示します。このページの変更に関する自動通知については、アカウント管理ドキュメント履歴ページの RSS フィードをサブスクライブしてください。

変更	説明	日付
AWS アカウント管理が新しい AWS 管理ポリシーで起動され、変更の追跡を開始	アカウント管理は、次の AWS 管理ポリシーで最初に起動されます。 • AWSAccountManagementReadOnlyAccess • AWSAccountManagementFullAccess	2021 年 9 月 30 日

AWS アカウント管理のコンプライアンス検証

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 AWS アカウント の一環としてで実行できる AWS サービスのセキュリティと AWS コンプライアンスを評価します。これらのプログラムには、SOC、PCI、FedRAMP、HIPAA などがあります。

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、AWS のサービス「コンプライアンスプログラムによる対象範囲内」を参照してください。一般的な情報については、AWS 「 Compliance ProgramsAssurance」を参照してください。

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

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

- セキュリティ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 AWS を にデプロイする手順について説明します。

- アマゾン ウェブ サービスでの HIPAA セキュリティとコンプライアンスのためのアーキテクチャ – このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

> **Note**
>
> すべての AWS のサービス が HIPAA の対象となるわけではありません。詳細については、HIPAA 対応サービスのリファレンスを参照してください。

- AWS コンプライアンスリソース – 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。
- 「 デベロッパーガイド」の「ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が内部プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub CSPM – これにより AWS のサービス 、 内のセキュリティ状態を包括的に把握 AWS できるため、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できます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

AWS アカウント管理の耐障害性

AWS グローバルインフラストラクチャは、 AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。リージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立および隔離されたアベイラビリティーゾーンがあります。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、フォールトトレランス、および拡張性が優れています。

AWS リージョン および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。

のインフラストラクチャセキュリティ AWS アカウント管理

マネージドサービスとして、 で実行されている AWS サービスは AWS グローバルネットワークセキュリティによって保護 AWS アカウント されます。 AWS セキュリティサービスと がインフラス

トラクチャを保護する方法については AWS 、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。

AWS 公開された API コールを使用して、ネットワーク経由でアカウント設定にアクセスします。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 が必須で、TLS 1.3 をお勧めします。
- 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。

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

をモニタリングする AWS アカウント

モニタリングは、 AWS アカウント管理およびその他の AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。 には、アカウント管理を監視し、問題が発生したときに報告し、必要に応じて自動アクションを実行するための以下のモニタリングツール AWS が用意されています。

- AWS CloudTrail は、 によって、または に代わって行われた API コールおよび関連イベントをキャプチャ (ログ) AWS アカウント し、指定した Amazon Simple Storage Service (Amazon S3) バケットにログファイルを書き込みます。 AWSを呼び出したユーザーとアカウント、呼び出し元の IP アドレス、および呼び出しの発生日時を特定できます。詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。
- Amazon EventBridge は、アプリケーションの可用性の問題やリソースの変更などのシステムイベントに自動的に応答することで、 AWS サービスに自動化を追加します。 AWS サービスからのイベントは、ほぼリアルタイムで EventBridge に配信されます。簡単なルールを記述して、注目するイベントと、イベントがルールに一致した場合に自動的に実行するアクションを指定できます。詳細については、Amazon EventBridge ユーザーガイドを参照してください。

を使用した AWS アカウント管理 API コールのログ記録 AWS CloudTrail

AWS アカウント管理 APIs は、ユーザー AWS CloudTrail、ロール、またはアカウント管理オペレーションを呼び出す サービスによって実行されたアクションを記録する AWS サービスである と統合されています。CloudTrail は、すべてのアカウント管理 API コールをイベントとしてキャプチャします。キャプチャされたコールには、アカウント管理操作へのすべての呼び出しが含まれます。追跡を作成する場合、アカウント管理のイベントを含む Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。追跡を設定しない場合でも、CloudTrail コンソールの [Event history] (イベント履歴) で最新のイベントを表示できます。CloudTrail で収集された情報を使用して、請求情報とコスト管理に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

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

CloudTrail でのアカウント管理情報

アカウントを作成する AWS アカウント と、 で CloudTrail がオンになります。アカウント管理オペレーションでアクティビティが発生すると、CloudTrail はそのアクティビティを CloudTrail イベントとイベント履歴の他の AWS サービスイベントに記録します。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 イベント履歴でのイベントの表示を参照してください。

アカウント管理オペレーションのイベントなど AWS アカウント、 のイベントの継続的な記録については、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、 で証跡を作成すると AWS マネジメントコンソール、その証跡はすべての に適用されます AWS リージョン。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。CloudTrail ログで収集されたイベントデータをさらに分析して処理するように、他の AWS サービスを設定できます。詳細については、次を参照してください:

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

AWS CloudTrail は、このガイドの API リファレンスセクションにあるすべてのアカウント管理 API オペレーションを記録します。たとえば `CreateAccount`、`DeleteAlternateContact`、および `PutAlternateContact` の各オペレーションへのコールは、CloudTrail ログファイル内にエントリを生成します。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストがルートユーザーまたは AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか
- リクエストが、IAM ロールまたはフェデレーティッドユーザーの一時的なセキュリティ認証情報によって行われたか
- リクエストが別の AWS サービスによって行われたかどうか

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

アカウント管理のログエントリについて

「トレイル」は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルには、単一または複数のログエントリがあります。各イベントは任意の送信元からの単一のリクエストを表し、リクエストされたオペレーション、オペレーションの日時、リクエストパラメータなどに関する情報を含みます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

例 1: 次の例は、アカウントの現在の OPERATIONS 代替連絡先を取得する GetAlternateContact 操作の呼び出しを記録する CloudTrail ログエントリを示しています。操作によって返される値は、ログに記録される情報に含まれません。

Example例 1

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn":"arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T19:25:53Z"
      }
    }
  },
  "eventTime": "2021-04-30T19:26:15Z",
  "eventSource": "account.amazonaws.com",
```

```
  "eventName": "GetAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "SECURITY"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-111111111111",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-222222222222",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```


例 2: 次の例は、アカウントに新しい PutAlternateContact 代替連絡先を追加する BILLING 操作の呼び出しを記録する CloudTrail ログエントリを示しています。


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
```

```
  "eventTime": "2021-04-30T18:33:08Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "PutAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "name": "*Alejandro Rosalez*",
    "emailAddress": "alrosalez@example.com",
    "title": "CFO",
    "alternateContactType": "BILLING"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-333333333333",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-444444444444",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```


例 3: 次の例は、アカウントの現在の DeleteAlternateContact 代替連絡先を削除する OPERATIONS 操作の呼び出しを記録する CloudTrail ログエントリを示しています。


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn":"arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
```

```
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
  "eventTime": "2021-04-30T18:33:16Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "DeleteAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "OPERATIONS"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-555555555555",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-666666666666",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```


EventBridge によるアカウント管理イベントのモニタリング

以前は CloudWatch Events と呼ばれていた Amazon EventBridge は、アカウント管理に固有のイベントをモニタリングし、他の を使用するターゲットアクションを開始するのに役立ちます AWS のサービス。からのイベント AWS のサービス は、ほぼリアルタイムで EventBridge に配信されます。

EventBridge を使用すると、受信イベントを照合し、処理のためにターゲットにルーティングするルールを作成できます。

詳細については、「Amazon EventBridge ユーザーガイド」の「Getting started with Amazon EventBridge」を参照してください。

アカウント管理イベント

次の例は、アカウント管理のイベントを示しています。イベントは、ベストエフォートベースで生成されます。

現在、アカウント管理で使用できるのは、リージョンの有効化および無効化と、CloudTrail を介した API 呼び出しに固有のイベントのみです。

イベントタイプ

- リージョンの有効化および無効化に関するイベント

リージョンの有効化および無効化に関するイベント

コンソールまたは API からアカウントでリージョンを有効または無効にすると、非同期タスクが開始されます。最初のリクエストは、ターゲットアカウントで CloudTrail イベントとして記録されます。さらに、有効化または無効化プロセスが開始されたとき、およびそのプロセスが完了したときに、呼び出し元アカウントに EventBridge イベントが送信されます。

次のイベント例は、2020-09-30 にアカウント 123456789012 の ap-east-1 リージョンが ENABLED にされたことを示すリクエストがどのように送信されるかを示しています。

```
{
   "version":"0",
   "id":"11112222-3333-4444-5555-666677778888",
   "detail-type":"Region Opt-In Status Change",
   "source":"aws.account",
   "account":"123456789012",
   "time":"2020-09-30T06:51:08Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:account::123456789012:account"
   ],
   "detail":{
      "accountId":"123456789012",
      "regionName":"ap-east-1",
      "status":"ENABLED"
   }
}
```

GetRegionOptStatus および ListRegions API が返すステータスは、以下の 4 つのステータスのいずれかと一致します。

- ENABLED – 指定された accountId に対してリージョンの有効化が正常に完了しました
- ENABLING – 指定された accountId に対してリージョンの有効化プロセスが進行中です。
- DISABLED – 指定された accountId に対してリージョンの無効化が正常に完了しました

- DISABLING – 指定された accountId に対してリージョンの無効化プロセスが進行中です。

次のイベントパターンの例は、すべてのリージョンイベントをキャプチャするルールを作成します。

```
{
   "source":[
      "aws.account"
   ],
   "detail-type":[
      "Region Opt-In Status Change"
   ]
}
```

次のイベントパターンの例は、 ENABLEDおよび DISABLED リージョンイベントのみをキャプチャするルールを作成します。

```
{
   "source":[
      "aws.account"
   ],
   "detail-type":[
      "Region Opt-In Status Change"
   ],
   "detail":{
      "status":[
         "DISABLED",
         "ENABLED"
      ]
   }
}
```

のトラブルシューティング AWS アカウント

以下のトピックの情報は、 AWS アカウントに関する問題の診断と解決に役立ちます。ルートユーザーに関するヘルプについては、「IAM ユーザーガイド」の「ルートユーザーに関する問題をトラブルシューティングする」を参照してください。サインインプロセスに関するヘルプについては、「AWS サインインユーザーガイド」の「Troubleshooting AWS アカウント sign-in issues」を参照してください。

トラブルシューティングのトピック

- AWS アカウント 作成に関する問題のトラブルシューティング
- AWS アカウント 閉鎖に関する問題のトラブルシューティング
- に関するその他の問題のトラブルシューティング AWS アカウント

AWS アカウント 作成に関する問題のトラブルシューティング

次の表のリファレンスリンクを使用して、新しい の作成に関する問題の診断と修正に役立ててください AWS アカウント。

問題	参照リンク	ソース
アカウントのサインアップまたは作成方法がわからない	の開始方法 AWS アカウント	本ガイド
新しいアカウント AWS を確認するために から電話を受け取らなかった場合、または入力した PIN が機能しない場合はどうすればよいですか?	https://repost.aws/knowledge-center/phone-verify-no-call	AWS re:Post
電話 AWS アカウント による検証を試みたときの「最大試行回数」エラーを解決するにはどうすればよいですか?	https://repost.aws/knowledge-center/maximum-failed-attempts	AWS re:Post

問題	参照リンク	ソース
24 時間以上経過しましたが、アカウントが有効になっていません	https://repost.aws/knowledge-center/create-and-activate-aws-account	AWS re:Post
新しいアカウントの作成後にサインインできない	https://docs.aws.amazon.com/signin/latest/userguide/troubleshooting-sign-in-issues.html	AWS サインインユーザーガイド

さらにヘルプが必要な場合は、AWS re:Post で特定の問題に関連するコンテンツを検索することをお勧めします。さらにサポートが必要な場合は、AWS サポートにお問い合わせください。

AWS アカウント 閉鎖に関する問題のトラブルシューティング

以下の情報を使用すると、アカウント閉鎖プロセス中に発生する一般的な問題を診断して修正するのに役立ちます。アカウント閉鎖プロセスに関する一般的な情報については、「を閉じる AWS アカウント」を参照してください。

トピック

- アカウントを削除またはキャンセルする方法がわからない
- [アカウント] ページに [アカウントを閉鎖する] ボタンが表示されない
- アカウントを閉鎖したが、まだ確認 E メールを受け取っていない
- アカウントを閉鎖しようとすると、「ConstraintViolationException」エラーが表示される
- メンバーアカウントを閉鎖しようとすると「CLOSE_ACCOUNT_QUOTA_EXCEEDED」エラーが表示される
- 管理アカウントを閉鎖する前に AWS 組織を削除する必要がありますか?

アカウントを削除またはキャンセルする方法がわからない

アカウントを閉鎖するには、「を閉じる AWS アカウント」の手順に従います。

[アカウント] ページに [アカウントを閉鎖する] ボタンが表示されない

ルートユーザーとしてサインインしていない場合、[アカウント] ページに [アカウントを閉鎖する] ボタンは表示されません。アカウントを閉鎖するには、ルートユーザー AWS マネジメントコンソール

として にサインインする必要があります。サインインできない場合は、「ルートユーザーに関する問題をトラブルシューティングする」を参照してください。

アカウントを閉鎖したが、まだ確認 E メールを受け取っていない

この確認 E メールは、 AWS アカウントのルートユーザーの E メールアドレスと にのみ送信されます。この E メールが数時間以内に届かない場合は、ルートユーザー AWS マネジメントコンソール として にサインインして、アカウントが閉鎖されたことを確認できます。アカウントが正常に閉鎖されていれば、アカウントが閉鎖されたことを示すメッセージが表示されます。閉鎖したアカウントがメンバーアカウントである場合は、閉鎖したアカウントが AWS Organizations コンソールCLOSEDで とラベル付けされているかどうかを確認することで、正常に閉鎖されたことを確認できます。詳細については、「AWS Organizations ユーザーガイド」の「組織のメンバーアカウントを閉鎖する」を参照してください。

管理アカウントを閉鎖しようとしており、アカウント閉鎖に関する確認 E メールが届かない場合、最も可能性が高いのは、組織にアクティブなメンバーアカウントが含まれていることです。管理アカウントを閉鎖できるのは、組織にアクティブなメンバーアカウントが含まれていない場合のみです。組織にアクティブなメンバーアカウントが残っていないことを確認するには、 AWS Organizations コンソールに移動し、すべてのメンバーアカウントがアカウント名のClosed横に表示されていることを確認します。その後、管理アカウントを閉鎖できます。

アカウントを閉鎖しようとすると、「ConstraintViolationException」エラーが表示される

AWS Organizations コンソールを使用して管理アカウントを閉鎖しようとしていますが、これはできません。管理アカウントを閉鎖するには、管理アカウントのルートユーザー AWS マネジメントコンソール として にサインインし、アカウントページから閉鎖する必要があります。詳細については、「AWS Organizations ユーザーガイド」の「組織の管理カウントの閉鎖」を参照してください。

メンバーアカウントを閉鎖しようとすると「CLOSE_ACCOUNT_QUOTA_EXCEEDED」エラーが表示される

30 日間で閉鎖できるメンバーアカウントは 10% のみです。このクォータは暦月に縛られず、アカウントを閉鎖した時点で開始されます。最初のアカウント閉鎖から 30 日以内に、制限である 10% を超えるアカウントを閉鎖することはできません。アカウントの 10% が 1000 を超える場合でも、閉鎖できるアカウントの最小数は 10 で、最大数は 1000 です。Organizations のクォータの詳細については、「AWS Organizations ユーザーガイド」の「AWS Organizationsのクォータ」を参照してください。

管理アカウントを閉鎖する前に AWS 組織を削除する必要がありますか?

いいえ。管理アカウントを閉鎖する前に AWS 組織を削除する必要はありません。ただし、管理アカウントを閉鎖できるのは、組織にアクティブなメンバーアカウントが含まれていない場合のみです。組織にアクティブなメンバーアカウントが残っていないことを確認するには、 AWS Organizations コンソールに移動し、すべてのメンバーアカウントがアカウント名のClosed横に表示されていることを確認します。その後、管理アカウントを閉鎖できます。

に関するその他の問題のトラブルシューティング AWS アカウント

ここに記載する情報は、 AWS アカウントに関係する問題のトラブルシューティングに役立ちます。

問題

- のクレジットカードを変更する必要があります AWS アカウント
- 不正行為を報告する必要がある AWS アカウント
- を閉じる必要があります AWS アカウント

のクレジットカードを変更する必要があります AWS アカウント

のクレジットカードを変更するには AWS アカウント、サインインできる必要があります。 AWS には、アカウント所有者であることを証明する必要がある保護があります。手順については、AWS Billing ユーザーガイドの「クレジットカード支払い方法の管理」を参照してください。

不正行為を報告する必要がある AWS アカウント

を使用した不正行為の疑い AWS アカウント があり、報告を行う場合は、「 AWS リソースの不正使用を報告する方法」を参照してください。

Amazon.com での購入に問題がある場合は、「Amazon カスタマーサービス」を参照してください。

を閉じる必要があります AWS アカウント

の閉鎖に関する問題のトラブルシューティングについては AWS アカウント、「」を参照してくださいを閉じる AWS アカウント。

を閉じる AWS アカウント

が不要になった場合は AWS アカウント、このセクションの手順に従っていつでも閉じることができます。アカウントを閉鎖した後は 90 日以内であれば、アカウントを再開できます。アカウントを閉鎖した日から AWS がアカウントを完全に閉鎖するまでの期間は、閉鎖後期間と呼ばれます。

アカウントを閉鎖する前の確認事項

を閉じる前に AWS アカウント、次の点を考慮する必要があります。

- アカウントの閉鎖は、そのアカウントに関する AWS 顧客契約終了の通知として扱われます。
- 閉じる AWS アカウント 前に でリソースを削除する必要はありません。ただし、保持する必要があるリソースやデータをバックアップすることをお勧めします。特定のリソースをバックアップする方法については、そのサービスに該当する AWS ドキュメントを参照してください。
- 閉鎖後期間中であれば、アカウントを再開できます。アカウントを再開すると、アカウント内に残っているサービスに対する課金も再開されます。また、未払いの請求書や未処理のリザーブドインスタンスおよび Savings Plans についても引き続き責任を負います。
- アカウント閉鎖前に消費されたサービスに対するすべての未処理の料金および請求額については、引き続き責任を負います。アカウントを閉鎖した翌月に AWS 請求書が届きます。例えば、1 月 15 日にアカウントを閉鎖した場合、1 月 1 日から 1 月 15 日までに発生した使用量に対する請求書が 2 月初旬に届きます。リザーブドインスタンスと Savings Plans の請求書は、アカウントを閉鎖した後も引き続き有効期限が切れるまで届きます。
- アカウントで以前に利用可能だった AWS サービスにアクセスできなくなります。ただし、解約 AWS アカウント 後期間中にサインインして閉鎖された にアクセスできるのは、過去の請求情報を表示したり、アカウント設定にアクセスしたり、 に連絡したりするためのみですAWS サポート。 ???
- AWS アカウント の閉鎖時にそのアカウントに登録されていたのと同じ E メールアドレスを、別の AWS アカウントの主要 E メールアドレスとして使用することはできません。同じ E メールアドレスを別の AWS アカウントで使用したい場合は、閉鎖前に更新することをお勧めします。詳細については、「ルートユーザーの E メールアドレスと の更新」を参照してください。
- AWS アカウント のルートユーザーで多要素認証 (MFA) を有効にしている場合、または IAM ユーザーに MFA デバイスを設定している場合は、アカウントを閉鎖しても MFA は自動的に削除されません。90 日間の閉鎖後期間中に MFA をオンのままにする場合は、その期間中にアカウントにアクセスする必要がある場合に備えて、閉鎖後期間が終了するまで MFA デバイスをアクティブに

しておいてください。ハードウェア TOTP トークンデバイスは、アカウントが完全に閉鎖された後に別のユーザーに関連付けることはできないので注意してください。ハードウェア TOTP トークンを後で別のユーザーで使用する場合は、アカウントを閉鎖する前にハードウェア MFA デバイスを無効にするオプションがあります。IAM ユーザー のMFA デバイスは、アカウント管理者が削除する必要があります。

メンバーアカウントに関するその他の考慮事項

- メンバーアカウントを閉鎖しても、そのアカウントは、閉鎖後期間が終了するまでは組織から削除されません。閉鎖後期間中、閉鎖したメンバーアカウントは、引き続き組織内のアカウントのクォータに対してカウントされます。アカウントがクォータにカウントされないようにするには、そのアカウントを閉鎖する前に「組織からのメンバーアカウントの削除」を参照してください。
- 30 日間のローリング期間のうち、20% または 250 個のメンバーアカウントを最大 1,000 個までしか閉鎖できません。このクォータは暦月に縛られず、アカウントを閉鎖した時点で開始されます。Organizations のクォータの詳細については、「AWS Organizationsのクォータ」を参照してください。
- AWS Control Tower を使用する場合は、アカウントを閉鎖する前にメンバーアカウントの管理を解除する必要があります。「 AWS Control Tower ユーザーガイド」の「メンバーアカウントの管理を解除する」を参照してください。

サービス固有の考慮事項

- AWS Marketplace サブスクリプションは、アカウント閉鎖時に自動的にキャンセルされません。何らかのサブスクリプションがある場合は、まずサブスクリプション内のソフトウェアのすべてのインスタンスを終了します。次に、 AWS Marketplace コンソールのサブスクリプションの管理ページに移動し、サブスクリプションをキャンセルします。
- アカウントが閉鎖されると、 AWS はドメインを停止するまで最大 5 日間毎日 E メールを送信します。ドメインが停止されたら、ドメインのレジストラに応じて、30 日以内にドメインを削除するか、そのレジストラにドメインを解放します。詳細については、「My AWS アカウント is closed or permanently closed」および「My domain is registered with Route 53」を参照してください。
- AWS CloudTrail は基本的なセキュリティサービスです。つまり、ユーザーが作成した証跡は、ユーザーが閉じる AWS アカウント 前に の証跡を明示的に削除しない限り、 AWS アカウント が閉じられた後も引き続き存在し、イベントを配信できます。 AWS アカウント が閉じられた後に証跡の削除をリクエストする方法の詳細については、CloudTrail ユーザーガイド」のAWS アカウント 「クロージャと証跡」を参照してください。

アカウントの閉鎖方法

次の手順 AWS アカウント を使用して を閉じることができます。閉鎖するアカウント [スタンドアロン、メンバー、管理、 AWS GovCloud (US)] のタイプに応じて、各タブに異なるガイダンスが提供されることに注意してください。

アカウントの閉鎖プロセス中に問題が発生した場合は、「AWS アカウント 閉鎖に関する問題のトラブルシューティング」を参照してください。

Standalone account

スタンドアロンアカウントは、 の一部ではない個別に管理されるアカウントです AWS Organizations。

[アカウント] ページからスタンドアロンアカウントを閉鎖する手順

1. 閉じる のルートユーザー AWS マネジメントコンソール として にサインイン AWS アカウント します。IAM ユーザーまたはロールとしてサインインしている間は、アカウントを閉鎖できません。
2. 右上隅のナビゲーションバーでアカウント名または番号を選択し、[アカウント] を選択します。
3. [アカウント] ページで、[アカウントを閉鎖] ボタンを選択します。
4. アカウント ID (閉鎖ダイアログボックスの上部に表示される) を入力して、アカウント閉鎖プロセスを読んで理解したことを確認します。
5. [アカウントを閉鎖] ボタンを選択して、アカウント閉鎖プロセスを開始します。
6. 数分以内に、アカウントが閉鎖されたことを確認する E メールが届きます。

> **Note**
>
> このタスクは、 AWS CLI またはいずれかの AWS SDKs からの API オペレーションではサポートされていません。このタスクは、 を使用してのみ実行できます AWS マネジメントコンソール。

Member account

メンバーアカウントは、 の一部 AWS アカウント である です AWS Organizations。

AWS Organizations コンソールからメンバーアカウントを閉じるには

1. AWS Organizations コンソール にサインインします。
2. [AWS アカウント] ページで、閉鎖するメンバーアカウント名を探し、選択します。OU の階層を移動するか、OU 構造のないアカウントのフラットリストを表示できます。
3. ページの上部のアカウント名の横にある [Close] (閉じる) をクリックします。このオプションは、 AWS 組織がすべての機能モードの場合にのみ使用できます。

> **Note**
>
> 組織が一括請求モードを使用している場合、コンソールに [閉じる] ボタンは表示されません。一括請求モードでアカウントを閉鎖するには、ルートユーザーとして閉鎖するアカウントにサインインします。[アカウント] ページで、[アカウントの閉鎖] ボタンを選択し、アカウント ID を入力し、[アカウントの閉鎖]ボタンを選択します。

4. アカウント閉鎖ガイダンスを読んで、理解していることを確認します。
5. メンバーアカウント ID を入力し、[アカウントを閉鎖] を選択してアカウント閉鎖プロセスを開始します。

> **Note**
>
> 閉鎖したメンバーアカウントは、最初の閉鎖日から最大 90 日間、 AWS Organizations コンソールでアカウント名の横に CLOSED というラベルが表示されます。90 日後、そのメンバーアカウントは AWS Organizations コンソールに表示されなくなります。

アカウントページからメンバーアカウントを閉じるには

必要に応じて、 のアカウントページから直接 AWS メンバーアカウントを閉鎖できます AWS マネジメントコンソール。 ステップバイステップのガイダンスについては、[スタンドアロンアカウント] タブの手順に従ってください。

AWS CLI および SDKs

AWS CLI および SDKs「組織内のメンバーアカウントの閉鎖」を参照してください。 AWS Organizations

Management account

管理アカウントは AWS アカウント 、親アカウントまたはルートアカウントとして機能する です AWS Organizations。

> **Note**
>
> AWS Organizations コンソールから直接管理アカウントを閉鎖することはできません。

[アカウント] ページから管理アカウントを閉鎖する手順

1. 閉鎖する管理アカウントのルートユーザー AWS マネジメントコンソール として にサインインします。IAM ユーザーまたはロールとしてサインインしている間は、アカウントを閉鎖できません。
2. 組織内にアクティブなメンバーアカウントが残っていないことを確認します。これを行うには、AWS Organizations コンソールに移動し、すべてのメンバーアカウントのアカウント名の横に `Closed` が表示されていることを確認します。まだアクティブなメンバーアカウントがある場合は、[メンバーアカウント] タブに示されるアカウント閉鎖ガイダンスを実行してから、次のステップに進んでください。
3. 右上隅のナビゲーションバーでアカウント名または番号を選択し、[アカウント] を選択します。
4. [アカウント] ページで、[アカウントを閉鎖] ボタンを選択します。
5. アカウント ID (閉鎖ダイアログボックスの上部に表示される) を入力して、アカウント閉鎖プロセスを読んで理解したことを確認します。
6. [アカウントを閉鎖] ボタンを選択して、アカウント閉鎖プロセスを開始します。
7. 数分以内に、アカウントが閉鎖されたことを確認する E メールが届きます。

> **Note**
>
> このタスクは、 AWS CLI またはいずれかの AWS SDKs からの API オペレーションではサポートされていません。このタスクは、 を使用してのみ実行できます AWS マネジメントコンソール。

AWS GovCloud (US) account

AWS GovCloud (US) アカウントは、請求と支払い AWS アカウント の目的で常に 1 つの標準にリンクされます。

AWS GovCloud (US) アカウントを閉鎖するには

AWS GovCloud (US) アカウントにリンク AWS アカウント された がある場合は、アカウントを閉じる前に標準アカウントを閉じる AWS GovCloud (US) 必要があります。データのバックアップ方法や意図しない AWS GovCloud (US) 請求を回避する方法などの詳細については、「 AWS GovCloud (US) ユーザーガイド」のAWS GovCloud (US) 「アカウントの閉鎖」を参照してください。

アカウントの閉鎖後に予想されること

アカウントを閉鎖するとすぐに、次のことが発生します。

- アカウントの閉鎖を確認する E メールが、ルートユーザーの E メールアドレスに届きます。この E メールが数時間以内に届かない場合は、「AWS アカウント 閉鎖に関する問題のトラブルシューティング」を参照してください。
- 閉鎖したメンバーアカウントは、元の閉鎖日から最大 90 日間、そのアカウント名の横にCLOSEDラベルを AWS Organizations コンソールに表示します。90 日後、メンバーアカウントは AWS Organizations コンソールに表示されなくなります。
- の のサービスにアクセスするためのアクセス許可 AWS アカウント を他の アカウントに付与している場合、それらのアカウントから行われたアクセスリクエストは、アカウント閉鎖後に失敗します。を再度開くと AWS アカウント、必要なアクセス許可を付与すると、他の AWS アカウント はアカウントの AWS サービスとリソースに再びアクセスできます。

アカウント閉鎖は、すべてのリージョンとサービスですぐに発生するわけではなく、完了までに数時間かかる場合があります。

閉鎖後期間

閉鎖後期間は、アカウントを閉鎖した日から AWS が完全に閉鎖されるまでの期間を指します AWS アカウント。閉鎖後期間は 90 日間です。閉鎖後期間中は、アカウントを再開することによってのみ、コンテンツや AWS サービスにアクセスできます。閉鎖後期間が過ぎると、 AWS は を完全に閉じ AWS アカウント、再度開くことはできなくなります。 AWS はアカウント内のコンテンツとリ

ソースも削除します (CloudTrail 証跡を除く) 。アカウントが完全に閉鎖されると、その AWS アカウント ID は再使用できなくなります。

を再開する AWS アカウント

アカウントは 90 日後に完全に閉鎖され、その後はアカウントを再度開くことができなくなり、アカウントに残っているコンテンツ AWS が削除されます。アカウントが完全に閉鎖される前にアカウントを再開するには、(1) AWS サポートできるだけ早く に連絡する必要があります。また、(2) アカウントの閉鎖日から 30 日以内に、請求書に指定されている必要な情報の提供を含め、未払い残高の全額を受け取る必要があります。

> **Note**
>
> アカウントを再開すると、アカウント内に残っているサービスに対する課金も再開されます。

API リファレンス

アカウント管理 (account) 名前空間の API オペレーションを使用すると、 を変更できます AWS アカウント。

すべての は、アカウントに関連付けられた最大 3 つの代替連絡先に関する情報を含む、アカウントに関する情報を含むメタデータ AWS アカウント をサポートします。これらは、アカウントのルートユーザーに関連付けられている E メールアドレスに加えて指定されます。アカウントに関連付けられている次の各連絡先タイプのいずれか 1 つのみを指定できます。

- 請求に関するお問い合わせ先
- 操作問い合わせ先
- セキュリティ問い合わせ先

デフォルトでは、このガイドで説明する API 操作は、操作を呼び出すアカウントに直接適用されます。操作を呼び出しているアカウントのアイデンティティは、通常 IAM ロールまたは IAM ユーザーがあり、API 操作を呼び出すには IAM ポリシーによって適用されるアクセス権限が必要です。または、管理アカウントの ID からこれらの API オペレーションを AWS Organizations 呼び出し、組織のメンバー AWS アカウント である のアカウント ID 番号を指定することもできます。

API バージョン

このバージョンの「アカウント API リファレンス」には、「アカウント管理 API バージョン 2021-02-01」と記載されています。

> **Note**
>
> API を直接使用する代わりに、 AWS SDKs のいずれかを使用できます。SDK は、さまざまなプログラミング言語とプラットフォーム (Java、Ruby、.NET、iOS、Android など) のライブラリとサンプルコードで構成されます。SDKs を使用すると、アカウント管理へのプログラムによるアクセスを簡単に作成できます。例えば、SDK では暗号を使用して要求に署名したり、エラーを管理したり、要求を自動的に再試行したりすることができます。 AWS SDKs「Amazon Web Services のツール」を参照してください。

アカウント管理サービスに対してプログラムによる API コールを行うには、 AWS SDKs を使用することをお勧めします。ただし、アカウント管理クエリ API を使用して、アカウント管理 Web サー

ビスを直接呼び出すこともできます。アカウント管理クエリ API の詳細については、「アカウント管理ユーザーガイド」の「HTTP クエリリクエストを作成して API を呼び出す」を参照してください。アカウント管理は、すべてのアクションの GET リクエストと POST リクエストをサポートします。つまり、API は、あるアクションに対しては GET を、他のアクションに対しては POST をといった使い分けを必要としません。しかしながら、GET リクエストは URL のサイズに制限があります。したがって、より大きなサイズを必要とする操作の場合は、POST リクエストを使用します。

リクエストへの署名

HTTP リクエストを に送信するときは AWS、 がリクエストを送信したユーザー AWS を識別できるように、リクエストに署名する必要があります。アクセスキー ID とシークレット AWS アクセスキーで構成されるアクセスキーを使用してリクエストに署名します。ルートアカウントのアクセスキーを作成しないことを強くお勧めします。ルートアカウントのアクセスキーを持っていれば誰でも、アカウントのすべてのリソースに無制限にアクセスできます。代わりに、管理権限を持つ IAM ユーザーのアクセスキーを作成します。別のオプションとして、 AWS Security Token Service を使用して一時的なセキュリティ認証情報を生成し、それらの認証情報を使用してリクエストに署名します。

リクエストをサインアップする際には、署名バージョン 4 の使用が推奨されます。Signature バージョン 2 を使用する既存のアプリケーションがある場合は、Signature バージョン 4 を使用するために更新する必要はありません。ただし、一部の操作では、Signature バージョン 4 が必要です。バージョン 4 を必要とするオペレーションのドキュメントには、この要件が示されています。詳細については、IAM ユーザーガイドの AWS API リクエストの署名を参照してください。

コマンドラインインターフェイス (AWS CLI) またはいずれかの AWS SDKs AWS を使用してリクエストを行うと AWS、これらのツールはツールの設定時に指定したアクセスキーを使用して自動的にリクエストに署名します。

アカウント管理のサポートとフィードバック

ご意見をお待ちしております。コメントを feedback-awsaccounts@amazon.com] 宛てに送信するか、アカウント管理サポートフォーラムにフィードバックと質問を掲載してください。 AWS サポートフォーラムの詳細については、「 フォーラムのヘルプ」を参照してください。

例が提示される方法

リクエストに応答して Account Management によって返される JSON は、改行や空白の書式設定のない単一の長い文字列です。読みやすさを向上させるために、このガイドの例には改行と空白の両方を示します。入力パラメータの例で画面を超えて長い文字列が生成される場合は、読みやすさを向上

させるために改行を挿入します。入力は常に 1 つの JSON テキスト文字列として送信する必要があります。

API リクエストの記録

アカウント管理は、 の AWS API コールを記録 AWS アカウント し、ログファイルを Amazon S3 バケットに配信するサービスである CloudTrail をサポートします。 Amazon S3 CloudTrail によって収集された情報を使用して、アカウント管理に対してどのようなリクエストが行われたか (リクエストの実行者、実行日など) を判断できます。アカウント管理と CloudTrail のサポートの詳細については、「を使用した AWS アカウント管理 API コールのログ記録 AWS CloudTrail」を参照してください。CloudTrail の詳細 (有効にする方法、ログファイルを検索する方法を含む) については、AWS CloudTrail ユーザーガイドを参照してください。

アクション

以下のアクションがサポートされています:

- AcceptPrimaryEmailUpdate
- DeleteAlternateContact
- DisableRegion
- EnableRegion
- GetAccountInformation
- GetAlternateContact
- GetContactInformation
- GetGovCloudAccountInformation
- GetPrimaryEmail
- GetRegionOptStatus
- ListRegions
- PutAccountName
- PutAlternateContact
- PutContactInformation
- StartPrimaryEmailUpdate

AcceptPrimaryEmailUpdate

指定されたアカウントの主要な E メールアドレス (ルートユーザーの E メールアドレスとも呼ばれる) を更新するために、StartPrimaryEmailUpdate から発信されたリクエストを受け入れます。

リクエストの構文

```
POST /acceptPrimaryEmailUpdate HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "Otp": "string",
   "PrimaryEmail": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

AccountId

このオペレーションでアクセスまたは変更 AWS アカウント する の 12 桁のアカウント ID 番号を指定します。このパラメータを使用するには、呼び出し元が組織の管理アカウントまたは委任管理者アカウントの ID である必要があります。指定されたアカウント ID は、同じ組織のメンバーアカウントである必要があります。組織はすべての機能を有効にして、アカウント管理サービス用の有効な信頼されたアクセスを持つ必要があり、オプションとして委任管理者アカウントが割り当てられます。

このオペレーションは、メンバーアカウントに対して、組織の管理アカウントまたは委任管理者アカウントからのみ呼び出すことができます。

> **Note**
>
> 管理アカウントは、自身の AccountId を指定することはできません。

タイプ: 文字列

Pattern: \d{12}

必須: はい

Otp

StartPrimaryEmailUpdate API コールで指定された PrimaryEmail に送信される OTP コード。

タイプ: 文字列

Pattern: [a-zA-Z0-9]{6}

必須: はい

PrimaryEmail

指定されたアカウントで使用する新しい主要 E メールアドレス。これは、StartPrimaryEmailUpdate API コールからの PrimaryEmail と一致する必要があります。

タイプ: 文字列

長さの制限: 最小長は 5。最大長 64

必須: はい

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "Status": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

Status

受け入れられた主要 E メール更新リクエストのステータスを取得します。

型: 文字列

有効な値：PENDING | ACCEPTED

エラー

すべてのアクションに共通のエラーについては、「一般的なエラータイプ」を参照してください。

AccessDeniedException

呼び出し元の ID に必要な最小アクセス許可がないため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 403

ConflictException

リソースの現在のステータスが競合しているため、リクエストを処理できませんでした。例えば、現在無効化中 (DISABLING ステータス) のリージョンを有効化しようとした場合や、アカウントのルートユーザーの E メールを、既に使用している E メールアドレスに変更しようとした場合にこれが発生します。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 409

InternalServerException

内部エラーのため、オペレーションが失敗しました AWS。後でもう一度操作をお試しください。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 500

ResourceNotFoundException

見つからないリソースが指定されているため、操作が失敗しました。

errorType

API Gateway によって `x-amzn-ErrorType` レスポンスヘッダーに入力された値。

HTTP ステータスコード: 404

TooManyRequestsException

操作が頻繁に呼び出され、スロットルの制限を超えているため、操作が失敗しました。

errorType

API Gateway によって `x-amzn-ErrorType` レスポンスヘッダーに入力された値。

HTTP ステータスコード: 429

ValidationException

入力パラメータのいずれかが無効であるため、操作が失敗しました。

fieldList

無効なエントリが検出されたフィールド。

message

リクエストのどの部分が無効だったかを知らせるメッセージ。

reason

検証が失敗した理由。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス V2
- AWS SDK for .NET V4
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteAlternateContact

指定された代替連絡先を から削除します AWS アカウント。

代替連絡先オペレーションの使用方法については、「AWS アカウントの代替連絡先を更新する」を参照してください。

> **Note**
>
> AWS アカウント が管理する の代替連絡先情報を更新する前に AWS Organizations、まず AWS アカウント管理と Organizations の統合を有効にする必要があります。詳細については、「AWS アカウント管理用の信頼されたアクセスの有効化」を参照してください。

リクエストの構文

```
POST /deleteAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

AccountId

このオペレーションでアクセスまたは変更するアカウントの 12 桁の AWS アカウント ID 番号を指定します。

このパラメータを指定しない場合、デフォルトで オペレーションの呼び出しに使用される ID の AWS アカウントになります。

このパラメータを使用するには、呼び出し元が組織の管理アカウントまたは委任管理者アカウント、および指定されたアカウント ID は、同じ組織内のメンバーアカウントである必要があります。組織はすべての機能を有効化して、アカウント管理サービス用の有効な信頼されたアクセスを持つ必要があり、オプションとして委任管理者アカウントが割り当てられます。

> **Note**
>
> 管理アカウントは独自の AccountId アカウントを指定できません; これは、AccountId パラメータを含めないことにより、スタンドアロンコンテキストでの操作を呼び出さなければなりません。

組織のメンバーではないアカウントでこの操作を呼び出すには、このパラメータを指定せず、取得または変更する取引先責任者のアカウントに属する ID を使用して操作を呼び出します。

タイプ: 文字列

パターン: \d{12}

必須: いいえ

AlternateContactType

削除する代替連絡先を指定します。

型: 文字列

有効な値 : BILLING | OPERATIONS | SECURITY

必須: はい

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「一般的なエラータイプ」を参照してください。

AccessDeniedException

呼び出し元の ID に必要な最小アクセス許可がないため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 403

InternalServerException

内部エラーのため、オペレーションが失敗しました AWS。後でもう一度操作をお試しください。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 500

ResourceNotFoundException

見つからないリソースが指定されているため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 404

TooManyRequestsException

操作が頻繁に呼び出され、スロットルの制限を超えているため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 429

ValidationException

入力パラメータのいずれかが無効であるため、操作が失敗しました。

fieldList

無効なエントリが検出されたフィールド。

message

リクエストのどの部分が無効だったかを知らせるメッセージ。

reason

検証が失敗した理由。

HTTP ステータスコード: 400

例

例 1

次の例では、操作の呼び出しに使用される認証情報を持つアカウントのセキュリティ代替連絡先を削除します。

リクエスト例

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact

{
   "AccountName":"MyAccount"
}
```

レスポンス例

```
HTTP/1.1 200 OK
Content-Type: application/json
```

例 2

次の例では、組織内の指定されたメンバーアカウントの請求代行連絡先を削除します。組織の管理アカウントまたはアカウント管理サービスの委任管理者アカウントの認証情報を使用する必要があります。

リクエスト例

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact
```

```
{
   "AccountId":"123456789012",
   "AlternateContactType":"BILLING"
}
```

レスポンス例

```
HTTP/1.1 200 OK
Content-Type: application/json
```

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DisableRegion

アカウントの特定のリージョンを無効化 (オプトアウト) します。

> **Note**
>
> リージョンを無効化すると、そのリージョンに存在するリソースへのすべての IAM アクセスが削除されます。

リクエストの構文

```
POST /disableRegion HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

AccountId

このオペレーションでアクセスまたは変更 AWS アカウント する の 12 桁のアカウント ID 番号を指定します。このパラメータを指定しない場合、デフォルトで、オペレーションの呼び出しに使用された ID の Amazon Web Services アカウントになります。このパラメータを使用するには、呼び出し元が組織の管理アカウントまたは委任管理者アカウントの ID である必要があります。指定されたアカウント ID は、同じ組織のメンバーアカウントである必要があります。組織はすべての機能を有効にして、アカウント管理サービス用の有効な信頼されたアクセスを持つ必要があり、オプションとして委任管理者アカウントが割り当てられます。

> **Note**
>
> 管理アカウントは、自身の AccountId を指定することはできません。AccountId パラメータを含めずに、スタンドアロンコンテキストでオペレーションを呼び出す必要があります。

組織のメンバーではないアカウントに対してこのオペレーションを呼び出す場合は、このパラメータを指定しないでください。代わりに、連絡先を取得または変更するアカウントに属する ID を使用してオペレーションを呼び出します。

タイプ: 文字列

パターン: \d{12}

必須: いいえ

RegionName

特定のリージョン名のリージョンコードを指定します (例: af-south-1)。リージョンを無効にすると、 AWS は、リージョン内の IAM リソースを破棄するなど、アカウント内のそのリージョンを非アクティブ化するアクションを実行します。ほとんどのアカウントでは、このプロセスに数分かかりますが、数時間かかることがあります。無効化プロセスが完全に完了するまで、そのリージョンを有効化することはできません。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 50 です。

必須: はい

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「一般的なエラータイプ」を参照してください。

AccessDeniedException

呼び出し元の ID に必要な最小アクセス許可がないため、操作が失敗しました。

errorType

API Gateway によって `x-amzn-ErrorType` レスポンスヘッダーに入力された値。

HTTP ステータスコード: 403

ConflictException

リソースの現在のステータスが競合しているため、リクエストを処理できませんでした。例えば、現在無効化中 (DISABLING ステータス) のリージョンを有効化しようとした場合や、アカウントのルートユーザーの E メールを、既に使用している E メールアドレスに変更しようとした場合にこれが発生します。

errorType

API Gateway によって `x-amzn-ErrorType` レスポンスヘッダーに入力された値。

HTTP ステータスコード: 409

InternalServerException

内部エラーのため、オペレーションが失敗しました AWS。後でもう一度操作をお試しください。

errorType

API Gateway によって `x-amzn-ErrorType` レスポンスヘッダーに入力された値。

HTTP ステータスコード: 500

TooManyRequestsException

操作が頻繁に呼び出され、スロットルの制限を超えているため、操作が失敗しました。

errorType

API Gateway によって `x-amzn-ErrorType` レスポンスヘッダーに入力された値。

HTTP ステータスコード: 429

ValidationException

入力パラメータのいずれかが無効であるため、操作が失敗しました。

fieldList

無効なエントリが検出されたフィールド。

message

リクエストのどの部分が無効だったかを知らせるメッセージ。

reason

検証が失敗した理由。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

EnableRegion

アカウントに対して特定のリージョンを有効化 (オプトイン) します。

リクエストの構文

```
POST /enableRegion HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

AccountId

このオペレーションでアクセスまたは変更 AWS アカウント する の 12 桁のアカウント ID 番号を指定します。このパラメータを指定しない場合、デフォルトで、オペレーションの呼び出しに使用された ID の Amazon Web Services アカウントになります。このパラメータを使用するには、呼び出し元が組織の管理アカウントまたは委任管理者アカウントの ID である必要があります。指定されたアカウント ID は、同じ組織のメンバーアカウントである必要があります。組織はすべての機能を有効にして、アカウント管理サービス用の有効な信頼されたアクセスを持つ必要があり、オプションとして委任管理者アカウントが割り当てられます。

> **Note**
>
> 管理アカウントは、自身の `AccountId` を指定することはできません。`AccountId` パラメータを含めずに、スタンドアロンコンテキストでオペレーションを呼び出す必要があります。

組織のメンバーではないアカウントに対してこのオペレーションを呼び出す場合は、このパラメータを指定しないでください。代わりに、連絡先を取得または変更するアカウントに属する ID を使用してオペレーションを呼び出します。

タイプ: 文字列

パターン: \d{12}

必須: いいえ

RegionName

特定のリージョン名のリージョンコードを指定します (例: af-south-1)。リージョンを有効にすると、そのリージョンへの IAM リソースの配信など、 AWS がそのリージョンでアカウントを準備するためのアクションを実行します。このプロセスは、ほとんどのアカウントでは数分で完了しますが、数時間かかることもあります。このプロセスが完了するまでそのリージョンを使用することはできません。さらに、有効化プロセスが完全に完了するまで、そのリージョンを無効化することはできません。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 50 です。

必須: はい

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「一般的なエラータイプ」を参照してください。

AccessDeniedException

呼び出し元の ID に必要な最小アクセス許可がないため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 403

ConflictException

リソースの現在のステータスが競合しているため、リクエストを処理できませんでした。例えば、現在無効化中 (DISABLING ステータス) のリージョンを有効化しようとした場合や、アカウントのルートユーザーの E メールを、既に使用している E メールアドレスに変更しようとした場合にこれが発生します。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 409

InternalServerException

内部エラーのため、オペレーションが失敗しました AWS。後でもう一度操作をお試しください。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 500

TooManyRequestsException

操作が頻繁に呼び出され、スロットルの制限を超えているため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 429

ValidationException

入力パラメータのいずれかが無効であるため、操作が失敗しました。

fieldList

無効なエントリが検出されたフィールド。

message

リクエストのどの部分が無効だったかを知らせるメッセージ。

reason

検証が失敗した理由。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetAccountInformation

アカウント名、アカウント ID、アカウント作成日時、アカウントの状態など、指定されたアカウントに関する情報を取得します。この API を使用するには、IAM ユーザーまたはロールに `account:GetAccountInformation` IAM アクセス許可が必要です。

リクエストの構文

```
POST /getAccountInformation HTTP/1.1
Content-type: application/json

{
   "AccountId": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

AccountId

このオペレーションでアクセスまたは変更するアカウントの 12 桁の AWS アカウント ID 番号を指定します。

このパラメータを指定しない場合、デフォルトで オペレーションの呼び出しに使用される ID の AWS アカウントになります。

このパラメータを使用するには、呼び出し元が組織の管理アカウントまたは委任管理者アカウント、および指定されたアカウント ID は、同じ組織内のメンバーアカウントである必要があります。組織はすべての機能を有効化して、アカウント管理サービス用の有効な信頼されたアクセスを持つ必要があり、オプションとして委任管理者アカウントが割り当てられます。

> **Note**
>
> 管理アカウントは独自の `AccountId` アカウントを指定できません; これは、`AccountId` パラメータを含めないことにより、スタンドアロンコンテキストでの操作を呼び出さなければなりません。

組織のメンバーではないアカウントでこの操作を呼び出すには、このパラメータを指定せず、取得または変更する取引先責任者のアカウントに属する ID を使用して操作を呼び出します。

タイプ: 文字列

パターン: \d{12}

必須: いいえ

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "AccountCreatedDate": "string",
   "AccountId": "string",
   "AccountName": "string",
   "AccountState": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

AccountCreatedDate

アカウントが作成された日時。

タイプ: タイムスタンプ

AccountId

このオペレーションでアクセスまたは変更 AWS アカウント する の 12 桁のアカウント ID 番号を指定します。このパラメータを使用するには、呼び出し元が組織の管理アカウントまたは委任管理者アカウントの ID である必要があります。指定されたアカウント ID は、同じ組織のメンバーアカウントである必要があります。組織はすべての機能を有効にして、アカウント管理サービス用の有効な信頼されたアクセスを持つ必要があり、オプションとして委任管理者アカウントが割り当てられます。

このオペレーションは、メンバーアカウントに対して、組織の管理アカウントまたは委任管理者アカウントからのみ呼び出すことができます。

> **Note**
>
> 管理アカウントは、自身の AccountId を指定することはできません。

タイプ: 文字列

パターン: \d{12}

AccountName

アカウントの名前。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 50 です。

パターン: [-;=?-~]+

AccountState

アカウントの状態。各アカウントの状態は、アカウントライフサイクルの特定のフェーズを表します。この情報を使用して、アカウントアクセスの管理、ワークフローの自動化、またはアカウントの状態の変更に基づくアクションのトリガーを行います。

有効な値: PENDING_ACTIVATION | ACTIVE | SUSPENDED | CLOSED

型: 文字列

有効な値 : PENDING_ACTIVATION | ACTIVE | SUSPENDED | CLOSED

エラー

すべてのアクションに共通のエラーについては、「一般的なエラータイプ」を参照してください。

AccessDeniedException

呼び出し元の ID に必要な最小アクセス許可がないため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 403

InternalServerException

内部エラーのため、オペレーションが失敗しました AWS。後でもう一度操作をお試しください。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 500

TooManyRequestsException

操作が頻繁に呼び出され、スロットルの制限を超えているため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 429

ValidationException

入力パラメータのいずれかが無効であるため、操作が失敗しました。

fieldList

無効なエントリが検出されたフィールド。

message

リクエストのどの部分が無効だったかを知らせるメッセージ。

reason

検証が失敗した理由。

HTTP ステータスコード: 400

例

例 1

次の例では、オペレーションの呼び出しに使用される認証情報を持つアカウントのアカウント情報を取得します。

リクエスト例

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAccountInformation

{}
```

レスポンス例

```
HTTP/1.1 200 OK
Content-Type: application/json

{
   "AccountId": "123456789012",
   "AccountName": "MyAccount",
   "AccountCreatedDate": "2020-11-30T17:44:37Z",
   "AccountState": "ACTIVE"
}
```

例 2

次の例では、組織内の指定されたメンバーアカウントのアカウント情報を取得します。組織の管理アカウントまたはアカウント管理サービスの委任管理者アカウントの認証情報を使用する必要があります。

リクエスト例

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAccountInformation

{
   "AccountId": "123456789012"
}
```

レスポンス例

```
HTTP/1.1 200 OK
Content-Type: application/json

{
   "AccountId": "123456789012",
```

```
    "AccountName": "MyMemberAccount",
    "AccountCreatedDate": "2020-11-30T17:44:37Z",
    "AccountState": "ACTIVE"
}
```

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetAlternateContact

にアタッチされた指定された代替連絡先を取得します AWS アカウント。

代替連絡先オペレーションの使用方法については、「AWS アカウントの代替連絡先を更新する」を参照してください。

> **Note**
>
> AWS アカウント が管理する の代替連絡先情報を更新する前に AWS Organizations、まず AWS アカウント管理と Organizations の統合を有効にする必要があります。詳細については、「AWS アカウント管理用の信頼されたアクセスの有効化」を参照してください。

リクエストの構文

```
POST /getAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

AccountId

このオペレーションでアクセスまたは変更するアカウントの 12 桁の AWS アカウント ID 番号を指定します。

このパラメータを指定しない場合、デフォルトで オペレーションの呼び出しに使用される ID の AWS アカウントになります。

このパラメータを使用するには、呼び出し元が組織の管理アカウントまたは委任管理者アカウント、および指定されたアカウント ID は、同じ組織内のメンバーアカウントである必要があります。組織はすべての機能を有効化して、アカウント管理サービス用の有効な信頼されたアクセスを持つ必要があり、オプションとして委任管理者アカウントが割り当てられます。

> **Note**
>
> 管理アカウントは独自の AccountId アカウントを指定できません; これは、AccountId パラメータを含めないことにより、スタンドアロンコンテキストでの操作を呼び出さなければなりません。

組織のメンバーではないアカウントでこの操作を呼び出すには、このパラメータを指定せず、取得または変更する取引先責任者のアカウントに属する ID を使用して操作を呼び出します。

タイプ: 文字列

パターン: \d{12}

必須: いいえ

AlternateContactType

取得する代替連絡先を指定します。

型: 文字列

有効な値 : BILLING | OPERATIONS | SECURITY

必須: はい

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "AlternateContact": {
      "AlternateContactType": "string",
      "EmailAddress": "string",
      "Name": "string",
```

```
        "PhoneNumber": "string",
        "Title": "string"
    }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

AlternateContact

指定された代替連絡先の詳細を含む構造体。

型: AlternateContact オブジェクト

エラー

すべてのアクションに共通のエラーについては、「一般的なエラータイプ」を参照してください。

AccessDeniedException

呼び出し元の ID に必要な最小アクセス許可がないため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 403

InternalServerException

内部エラーのため、オペレーションが失敗しました AWS。後でもう一度操作をお試しください。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 500

ResourceNotFoundException

見つからないリソースが指定されているため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 404

TooManyRequestsException

操作が頻繁に呼び出され、スロットルの制限を超えているため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 429

ValidationException

入力パラメータのいずれかが無効であるため、操作が失敗しました。

fieldList

無効なエントリが検出されたフィールド。

message

リクエストのどの部分が無効だったかを知らせるメッセージ。

reason

検証が失敗した理由。

HTTP ステータスコード: 400

例

例 1

次の例では、操作の呼び出しに使用される認証情報を持つアカウントのセキュリティ代替連絡先を取得します。

リクエスト例

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAlternateContact
```

```
{
   "AlternateContactType":"SECURITY"
}
```

レスポンス例

```
HTTP/1.1 200 OK
Content-Type: application/json

{
   "AlternateContact":{
      "Name":"Anika",
      "Title":"COO",
      "EmailAddress":"anika@example.com",
      "PhoneNumber":"206-555-0198",
      "AlternateContactType":"Security"
   }
}
```

例 2

次の例では、組織内の指定されたメンバーアカウントの操作に関する代替連絡先を取得します。組織の管理アカウントまたはアカウント管理サービスの委任管理者アカウントの認証情報を使用する必要があります。

リクエスト例

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAlternateContact

{
   "AccountId":"123456789012",
   "AlternateContactType":"Operations"
}
```

レスポンス例

```
HTTP/1.1 200 OK
Content-Type: application/json

{
   "AlternateContact":{
```

```
        "Name":"Anika",
        "Title":"COO",
        "EmailAddress":"anika@example.com",
        "PhoneNumber":"206-555-0198",
        "AlternateContactType":"Operations"
    }
}
```

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetContactInformation

AWS アカウントの主要連絡先情報を取得します。

主要連絡先オペレーションの使用方法については、「AWS アカウントの主要連絡先情報を更新する」を参照してください。

リクエストの構文

```
POST /getContactInformation HTTP/1.1
Content-type: application/json

{
   "AccountId": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

AccountId

このオペレーションでアクセスまたは変更 AWS アカウント する の 12 桁のアカウント ID 番号を指定します。このパラメータを指定しない場合、デフォルトで、オペレーションの呼び出しに使用された ID の Amazon Web Services アカウントになります。このパラメータを使用するには、呼び出し元が組織の管理アカウントまたは委任管理者アカウントの ID である必要があります。指定されたアカウント ID は、同じ組織のメンバーアカウントである必要があります。組織はすべての機能を有効にして、アカウント管理サービス用の有効な信頼されたアクセスを持つ必要があり、オプションとして委任管理者アカウントが割り当てられます。

> **Note**
>
> 管理アカウントは、自身の AccountId を指定することはできません。AccountId パラメータを含めずに、スタンドアロンコンテキストでオペレーションを呼び出す必要があります。

組織のメンバーではないアカウントに対してこのオペレーションを呼び出す場合は、このパラメータを指定しないでください。代わりに、連絡先を取得または変更するアカウントに属する ID を使用してオペレーションを呼び出します。

タイプ: 文字列

パターン: \d{12}

必須: いいえ

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "ContactInformation": {
      "AddressLine1": "string",
      "AddressLine2": "string",
      "AddressLine3": "string",
      "City": "string",
      "CompanyName": "string",
      "CountryCode": "string",
      "DistrictOrCounty": "string",
      "FullName": "string",
      "PhoneNumber": "string",
      "PostalCode": "string",
      "StateOrRegion": "string",
      "WebsiteUrl": "string"
   }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

ContactInformation

AWS アカウントに関連付けられた主要連絡先情報の詳細が含まれます。

型: ContactInformation オブジェクト

エラー

すべてのアクションに共通のエラーについては、「一般的なエラータイプ」を参照してください。

AccessDeniedException

呼び出し元の ID に必要な最小アクセス許可がないため、操作が失敗しました。

errorType

API Gateway によって `x-amzn-ErrorType` レスポンスヘッダーに入力された値。

HTTP ステータスコード: 403

InternalServerException

内部エラーのため、オペレーションが失敗しました AWS。後でもう一度操作をお試しください。

errorType

API Gateway によって `x-amzn-ErrorType` レスポンスヘッダーに入力された値。

HTTP ステータスコード: 500

ResourceNotFoundException

見つからないリソースが指定されているため、操作が失敗しました。

errorType

API Gateway によって `x-amzn-ErrorType` レスポンスヘッダーに入力された値。

HTTP ステータスコード: 404

TooManyRequestsException

操作が頻繁に呼び出され、スロットルの制限を超えているため、操作が失敗しました。

errorType

API Gateway によって `x-amzn-ErrorType` レスポンスヘッダーに入力された値。

HTTP ステータスコード: 429

ValidationException

入力パラメータのいずれかが無効であるため、操作が失敗しました。

fieldList

無効なエントリが検出されたフィールド。

message

リクエストのどの部分が無効だったかを知らせるメッセージ。

reason

検証が失敗した理由。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetGovCloudAccountInformation

GovCloud アカウント ID と状態など、指定された標準アカウント (存在する場合) にリンクされた GovCloud アカウントに関する情報を取得します。この API を使用するには、IAM ユーザーまたはロールに `account:GetGovCloudAccountInformation` IAM アクセス許可が必要です。

リクエストの構文

```
POST /getGovCloudAccountInformation HTTP/1.1
Content-type: application/json

{
   "StandardAccountId": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

StandardAccountId

このオペレーションでアクセスまたは変更するアカウントの 12 桁の AWS アカウント ID 番号を指定します。

このパラメータを指定しない場合、デフォルトで オペレーションの呼び出しに使用される ID の AWS アカウントになります。

このパラメータを使用するには、呼び出し元が組織の管理アカウントまたは委任管理者アカウント、および指定されたアカウント ID は、同じ組織内のメンバーアカウントである必要があります。組織はすべての機能を有効化して、アカウント管理サービス用の有効な信頼されたアクセスを持つ必要があり、オプションとして委任管理者アカウントが割り当てられます。

> **Note**
>
> 管理アカウントは独自の `AccountId` アカウントを指定できません; これは、`AccountId` パラメータを含めないことにより、スタンドアロンコンテキストでの操作を呼び出さなければなりません。

組織のメンバーではないアカウントでこの操作を呼び出すには、このパラメータを指定せず、取得または変更する取引先責任者のアカウントに属する ID を使用して操作を呼び出します。

タイプ: 文字列

パターン: \d{12}

必須: いいえ

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "AccountState": "string",
   "GovCloudAccountId": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

AccountState

リンクされた GovCloud アカウントのアカウント状態。

型: 文字列

有効な値 : PENDING_ACTIVATION | ACTIVE | SUSPENDED | CLOSED

GovCloudAccountId

リンクされた GovCloud アカウントの 12 桁のアカウント ID 番号。

タイプ: 文字列

パターン: \d{12}

エラー

すべてのアクションに共通のエラーについては、「一般的なエラータイプ」を参照してください。

AccessDeniedException

呼び出し元の ID に必要な最小アクセス許可がないため、操作が失敗しました。

errorType

API Gateway によって `x-amzn-ErrorType` レスポンスヘッダーに入力された値。

HTTP ステータスコード: 403

InternalServerException

内部エラーのため、オペレーションが失敗しました AWS。後でもう一度操作をお試しください。

errorType

API Gateway によって `x-amzn-ErrorType` レスポンスヘッダーに入力された値。

HTTP ステータスコード: 500

ResourceNotFoundException

見つからないリソースが指定されているため、操作が失敗しました。

errorType

API Gateway によって `x-amzn-ErrorType` レスポンスヘッダーに入力された値。

HTTP ステータスコード: 404

ResourceUnavailableException

現在利用できないリソースが指定されているため、オペレーションは失敗しました。

errorType

API Gateway によって `x-amzn-ErrorType` レスポンスヘッダーに入力された値。

HTTP ステータスコード: 424

TooManyRequestsException

操作が頻繁に呼び出され、スロットルの制限を超えているため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 429

ValidationException

入力パラメータのいずれかが無効であるため、操作が失敗しました。

fieldList

無効なエントリが検出されたフィールド。

message

リクエストのどの部分が無効だったかを知らせるメッセージ。

reason

検証が失敗した理由。

HTTP ステータスコード: 400

例

例 1

次の の例では、 オペレーションの呼び出しに認証情報が使用されるアカウントのリンクされた GovCloud アカウント情報を取得します。

リクエスト例

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetGovCloudAccountInformation

{}
```

レスポンス例

```
HTTP/1.1 200 OK
Content-Type: application/json

{
```

```
   "GovCloudAccountId": "123456789012",
   "AccountState": "ACTIVE"
}
```

例 2

次の の例では、組織内の指定されたメンバーアカウントのリンクされた GovCloud アカウント情報を取得します。組織の管理アカウントまたはアカウント管理サービスの委任管理者アカウントの認証情報を使用する必要があります。

リクエスト例

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetGovCloudAccountInformation

{
   "StandardAccountId": "111111111111"
}
```

レスポンス例

```
HTTP/1.1 200 OK
Content-Type: application/json

{
   "GovCloudAccountId": "123456789012",
   "AccountState": "ACTIVE"
}
```

例 3

次の例では、GovCloud アカウントにリンクされていない標準アカウントのリンクされた GovCloud アカウント情報を取得しようとします。

リクエスト例

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetGovCloudAccountInformation

{
   "StandardAccountId": "222222222222"
```

```
}
```

レスポンス例

```
HTTP/1.1 404
Content-Type: application/json

{
   "message":"GovCloud Account ID not found for Standard Account - 222222222222."
}
```

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetPrimaryEmail

指定されたアカウントの主要 E メールアドレスを取得します。

リクエストの構文

```
POST /getPrimaryEmail HTTP/1.1
Content-type: application/json

{
   "AccountId": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

AccountId

このオペレーションでアクセスまたは変更 AWS アカウント する の 12 桁のアカウント ID 番号を指定します。このパラメータを使用するには、呼び出し元が組織の管理アカウントまたは委任管理者アカウントの ID である必要があります。指定されたアカウント ID は、同じ組織のメンバーアカウントである必要があります。組織はすべての機能を有効にして、アカウント管理サービス用の有効な信頼されたアクセスを持つ必要があり、オプションとして委任管理者アカウントが割り当てられます。

このオペレーションは、メンバーアカウントに対して、組織の管理アカウントまたは委任管理者アカウントからのみ呼び出すことができます。

> **Note**
>
> 管理アカウントは、自身の `AccountId` を指定することはできません。

タイプ: 文字列

Pattern: `\d{12}`

必須: はい

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "PrimaryEmail": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

PrimaryEmail

指定されたアカウントに関連付けられている主要 E メールアドレスを取得します。

タイプ: 文字列

長さの制限: 最小長は 5。最大長 64

エラー

すべてのアクションに共通のエラーについては、「一般的なエラータイプ」を参照してください。

AccessDeniedException

呼び出し元の ID に必要な最小アクセス許可がないため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 403

InternalServerException

内部エラーのため、オペレーションが失敗しました AWS。後でもう一度操作をお試しください。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 500

ResourceNotFoundException

見つからないリソースが指定されているため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 404

TooManyRequestsException

操作が頻繁に呼び出され、スロットルの制限を超えているため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 429

ValidationException

入力パラメータのいずれかが無効であるため、操作が失敗しました。

fieldList

無効なエントリが検出されたフィールド。

message

リクエストのどの部分が無効だったかを知らせるメッセージ。

reason

検証が失敗した理由。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetRegionOptStatus

特定のリージョンのオプトインステータスを取得します。

リクエストの構文

```
POST /getRegionOptStatus HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

AccountId

このオペレーションでアクセスまたは変更 AWS アカウント する の 12 桁のアカウント ID 番号を指定します。このパラメータを指定しない場合、デフォルトで、オペレーションの呼び出しに使用された ID の Amazon Web Services アカウントになります。このパラメータを使用するには、呼び出し元が組織の管理アカウントまたは委任管理者アカウントの ID である必要があります。指定されたアカウント ID は、同じ組織のメンバーアカウントである必要があります。組織はすべての機能を有効にして、アカウント管理サービス用の有効な信頼されたアクセスを持つ必要があり、オプションとして委任管理者アカウントが割り当てられます。

> **Note**
>
> 管理アカウントは、自身の `AccountId` を指定することはできません。`AccountId` パラメータを含めずに、スタンドアロンコンテキストでオペレーションを呼び出す必要があります。

組織のメンバーではないアカウントに対してこのオペレーションを呼び出す場合は、このパラメータを指定しないでください。代わりに、連絡先を取得または変更するアカウントに属する ID を使用してオペレーションを呼び出します。

タイプ: 文字列

パターン: \d{12}

必須: いいえ

RegionName

特定のリージョン名のリージョンコードを指定します (例: af-south-1)。この関数は、このパラメータに渡されたリージョンのステータスを返します。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 50 です。

必須: はい

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "RegionName": "string",
   "RegionOptStatus": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

RegionName

渡されたリージョンコード。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 50 です。

RegionOptStatus

リージョンが取り得るステータスの 1 つ (有効、有効化中、無効、無効化中、デフォルトで有効)。

型: 文字列

有効な値 : ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT

エラー

すべてのアクションに共通のエラーについては、「一般的なエラータイプ」を参照してください。

AccessDeniedException

呼び出し元の ID に必要な最小アクセス許可がないため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 403

InternalServerException

内部エラーのため、オペレーションが失敗しました AWS。後でもう一度操作をお試しください。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 500

TooManyRequestsException

操作が頻繁に呼び出され、スロットルの制限を超えているため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 429

ValidationException

入力パラメータのいずれかが無効であるため、操作が失敗しました。

fieldList

無効なエントリが検出されたフィールド。

message

リクエストのどの部分が無効だったかを知らせるメッセージ。

reason

検証が失敗した理由。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListRegions

特定のアカウントのすべてのリージョンと、それぞれのオプトインステータスをリストします。オプションで、このリストを region-opt-status-contains パラメータでフィルタリングできます。

リクエストの構文

```
POST /listRegions HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "MaxResults": number,
   "NextToken": "string",
   "RegionOptStatusContains": [ "string" ]
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

AccountId

このオペレーションでアクセスまたは変更 AWS アカウント する の 12 桁のアカウント ID 番号を指定します。このパラメータを指定しない場合、デフォルトで、オペレーションの呼び出しに使用された ID の Amazon Web Services アカウントになります。このパラメータを使用するには、呼び出し元が組織の管理アカウントまたは委任管理者アカウントの ID である必要があります。指定されたアカウント ID は、同じ組織のメンバーアカウントである必要があります。組織はすべての機能を有効にして、アカウント管理サービス用の有効な信頼されたアクセスを持つ必要があり、オプションとして委任管理者アカウントが割り当てられます。

> **Note**
>
> 管理アカウントは、自身の AccountId を指定することはできません。AccountId パラメータを含めずに、スタンドアロンコンテキストでオペレーションを呼び出す必要があります。

組織のメンバーではないアカウントに対してこのオペレーションを呼び出す場合は、このパラメータを指定しないでください。代わりに、連絡先を取得または変更するアカウントに属する ID を使用してオペレーションを呼び出します。

タイプ: 文字列

パターン: \d{12}

必須: いいえ

MaxResults

コマンドの出力で返される項目の総数。使用可能な項目の総数が指定された値を上回る場合、コマンドの出力で NextToken が提供されます。ページ分割を再開するには、後続コマンドの starting-token 引数で NextToken 値を指定します。 AWS CLI の外部でNextTokenレスポンス要素を直接使用しないでください。使用例については、 AWS 「 コマンドラインインターフェイスユーザーガイド」の「ページ分割」を参照してください。

タイプ: 整数

有効範囲: 最小値 は 1 です。最大値は 50 です。

必須: いいえ

NextToken

ページ分割の開始場所を指定するために使用されるトークン。これは、以前に切り捨てられた応答からの NextToken です。使用例については、 AWS 「 コマンドラインインターフェイスユーザーガイド」の「ページ分割」を参照してください。

タイプ: 文字列

長さの制約: 最小長は 0 です。最大長 1,000

必須: いいえ

RegionOptStatusContains

特定のアカウントのリージョンのリストをフィルタリングするために使用するリージョンステータス (有効化中、有効、無効化中、無効、デフォルトで有効) のリスト。例えば、値 ENABLING を渡すと、リージョンステータスが ENABLING であるリージョンのリストのみが返されます。

型: 文字列の配列

有効な値: ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT

必須：いいえ

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Regions": [
      {
         "RegionName": "string",
         "RegionOptStatus": "string"
      }
   ]
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

NextToken

返されるデータがさらにある場合、これが設定されます。list-regions の next-token リクエストパラメータに渡す必要があります。

タイプ: 文字列

Regions

これは、特定のアカウントのリージョンのリストです。あるいは、フィルタリングされたパラメータが使用された場合は、filter パラメータで設定されたフィルタ条件に一致するリージョンのリストです。

型: Region オブジェクトの配列

エラー

すべてのアクションに共通のエラーについては、「一般的なエラータイプ」を参照してください。

AccessDeniedException

呼び出し元の ID に必要な最小アクセス許可がないため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 403

InternalServerException

内部エラーのため、オペレーションが失敗しました AWS。後でもう一度操作をお試しください。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 500

TooManyRequestsException

操作が頻繁に呼び出され、スロットルの制限を超えているため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 429

ValidationException

入力パラメータのいずれかが無効であるため、操作が失敗しました。

fieldList

無効なエントリが検出されたフィールド。

message

リクエストのどの部分が無効だったかを知らせるメッセージ。

reason

検証が失敗した理由。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutAccountName

指定されたアカウントのアカウント名を更新します。この API を使用するには、IAM プリンシパルに account:PutAccountName IAM アクセス許可が必要です。

リクエストの構文

```
POST /putAccountName HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AccountName": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

AccountId

このオペレーションでアクセスまたは変更するアカウントの 12 桁の AWS アカウント ID 番号を指定します。

このパラメータを指定しない場合、デフォルトで オペレーションの呼び出しに使用される ID の AWS アカウントになります。

このパラメータを使用するには、呼び出し元が組織の管理アカウントまたは委任管理者アカウント、および指定されたアカウント ID は、同じ組織内のメンバーアカウントである必要があります。組織はすべての機能を有効化して、アカウント管理サービス用の有効な信頼されたアクセスを持つ必要があり、オプションとして委任管理者アカウントが割り当てられます。

> **Note**
>
> 管理アカウントは独自の AccountId アカウントを指定できません; これは、AccountId パラメータを含めないことにより、スタンドアロンコンテキストでの操作を呼び出さなければなりません。

組織のメンバーではないアカウントでこの操作を呼び出すには、このパラメータを指定せず、取得または変更する取引先責任者のアカウントに属する ID を使用して操作を呼び出します。

タイプ: 文字列

パターン: `\d{12}`

必須: いいえ

AccountName

アカウントの名前。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 50 です。

パターン: `[ -;=?-~]+`

必須: はい

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「一般的なエラータイプ」を参照してください。

AccessDeniedException

呼び出し元の ID に必要な最小アクセス許可がないため、操作が失敗しました。

errorType

API Gateway によって `x-amzn-ErrorType` レスポンスヘッダーに入力された値。

HTTP ステータスコード: 403

InternalServerException

内部エラーのため、オペレーションが失敗しました AWS。後でもう一度操作をお試しください。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 500

TooManyRequestsException

操作が頻繁に呼び出され、スロットルの制限を超えているため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 429

ValidationException

入力パラメータのいずれかが無効であるため、操作が失敗しました。

fieldList

無効なエントリが検出されたフィールド。

message

リクエストのどの部分が無効だったかを知らせるメッセージ。

reason

検証が失敗した理由。

HTTP ステータスコード: 400

例

例 1

次の例では、オペレーションの呼び出しに使用される認証情報を持つアカウント名を更新します。

リクエスト例

```
POST / HTTP/1.1
```

```
X-Amz-Target: AWSAccountV20210201.PutAccountName

{
   "AccountName":"MyAccount"
}
```

レスポンス例

```
HTTP/1.1 200 OK
Content-Type: application/json
```

例 2

次の例では、組織内の指定されたメンバーアカウントのアカウント名を更新します。組織の管理アカウントまたはアカウント管理サービスの委任管理者アカウントの認証情報を使用する必要があります。

リクエスト例

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.PutAccountName

{
   "AccountId": "123456789012",
   "AccountName": "MyMemberAccount"
}
```

レスポンス例

```
HTTP/1.1 200 OK
Content-Type: application/json
```

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス V2
- AWS SDK for .NET V4
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutAlternateContact

にアタッチされている指定された代替連絡先を変更します AWS アカウント。

代替連絡先オペレーションの使用方法については、「AWS アカウントの代替連絡先を更新する」を参照してください。

> **Note**
>
> AWS アカウント が管理する の代替連絡先情報を更新する前に AWS Organizations、まず AWS アカウント管理と Organizations の統合を有効にする必要があります。詳細については、「AWS アカウント管理用の信頼されたアクセスの有効化」を参照してください。

リクエストの構文

```
POST /putAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string",
   "EmailAddress": "string",
   "Name": "string",
   "PhoneNumber": "string",
   "Title": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

AccountId

このオペレーションでアクセスまたは変更するアカウントの 12 桁の AWS アカウント ID 番号を指定します。

このパラメータを指定しない場合、デフォルトで オペレーションの呼び出しに使用される ID の AWS アカウントになります。

このパラメータを使用するには、呼び出し元が組織の管理アカウントまたは委任管理者アカウント、および指定されたアカウント ID は、同じ組織内のメンバーアカウントである必要があります。組織はすべての機能を有効化して、アカウント管理サービス用の有効な信頼されたアクセスを持つ必要があり、オプションとして委任管理者アカウントが割り当てられます。

> **Note**
>
> 管理アカウントは独自の AccountId アカウントを指定できません; これは、AccountId パラメータを含めないことにより、スタンドアロンコンテキストでの操作を呼び出さなければなりません。

組織のメンバーではないアカウントでこの操作を呼び出すには、このパラメータを指定せず、取得または変更する取引先責任者のアカウントに属する ID を使用して操作を呼び出します。

タイプ: 文字列

パターン: `\d{12}`

必須: いいえ

AlternateContactType

作成または更新する代替連絡先を指定します。

型: 文字列

有効な値 : `BILLING | OPERATIONS | SECURITY`

必須: はい

EmailAddress

代替連絡先の電子メールアドレスを指定します。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 254 です。

パターン: `[\s]*[\w+=.#|!&-]+@[\w.-]+\.[\w]+[\s]*`

必須: はい

Name

代替連絡先の名前を指定します。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長 64

必須: はい

PhoneNumber

代替連絡先の電話番号を指定します。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 25 です。

パターン: `[\s0-9()+-]+`

必須: はい

Title

代替連絡先のタイトルを指定します。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 50 です。

必須: はい

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「一般的なエラータイプ」を参照してください。

AccessDeniedException

呼び出し元の ID に必要な最小アクセス許可がないため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 403

InternalServerException

内部エラーのため、オペレーションが失敗しました AWS。後でもう一度操作をお試しください。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 500

TooManyRequestsException

操作が頻繁に呼び出され、スロットルの制限を超えているため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 429

ValidationException

入力パラメータのいずれかが無効であるため、操作が失敗しました。

fieldList

無効なエントリが検出されたフィールド。

message

リクエストのどの部分が無効だったかを知らせるメッセージ。

reason

検証が失敗した理由。

HTTP ステータスコード: 400

例

例 1

次の例では、操作の呼び出しに使用される認証情報を持つアカウントの請求代行連絡先を設定します。

リクエスト例

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.PutAlternateContact

{
    "AlternateContactType": "Billing",
    "Name": "Carlos Salazar",
    "Title": "CFO",
    "EmailAddress": "carlos@example.com",
    "PhoneNumber": "206-555-0199"
}
```

レスポンス例

```
HTTP/1.1 200 OK
Content-Type: application/json
```

例 2

次の例では、組織内の指定されたメンバーアカウントの請求代行連絡先を設定または上書きします。組織の管理アカウントまたはアカウント管理サービスの委任管理者アカウントの認証情報を使用する必要があります。

リクエスト例

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.PutAlternateContact

{
    "AccountId": "123456789012",
    "AlternateContactType": "Billing",
    "Name": "Carlos Salazar",
    "Title": "CFO",
    "EmailAddress": "carlos@example.com",
```

```
    "PhoneNumber": "206-555-0199"
}
```

レスポンス例

```
HTTP/1.1 200 OK
Content-Type: application/json
```

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutContactInformation

AWS アカウントの主要連絡先情報を更新します。

主要連絡先オペレーションの使用方法については、「AWS アカウントの主要連絡先情報を更新する」を参照してください。

リクエストの構文

```
POST /putContactInformation HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "ContactInformation": {
      "AddressLine1": "string",
      "AddressLine2": "string",
      "AddressLine3": "string",
      "City": "string",
      "CompanyName": "string",
      "CountryCode": "string",
      "DistrictOrCounty": "string",
      "FullName": "string",
      "PhoneNumber": "string",
      "PostalCode": "string",
      "StateOrRegion": "string",
      "WebsiteUrl": "string"
   }
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

AccountId

このオペレーションでアクセスまたは変更 AWS アカウント する の 12 桁のアカウント ID 番号を指定します。このパラメータを指定しない場合、デフォルトで、オペレーションの呼び出しに使用された ID の Amazon Web Services アカウントになります。このパラメータを使用するに

は、呼び出し元が組織の管理アカウントまたは委任管理者アカウントの ID である必要があります。指定されたアカウント ID は、同じ組織のメンバーアカウントである必要があります。組織はすべての機能を有効化して、アカウント管理サービス用の有効な信頼されたアクセスを持つ必要があり、オプションとして委任管理者アカウントが割り当てられます。

> **Note**
>
> 管理アカウントは、自身の AccountId を指定することはできません。AccountId パラメータを含めずに、スタンドアロンコンテキストでオペレーションを呼び出す必要があります。

組織のメンバーではないアカウントに対してこのオペレーションを呼び出す場合は、このパラメータを指定しないでください。代わりに、連絡先を取得または変更するアカウントに属する ID を使用してオペレーションを呼び出します。

タイプ: 文字列

パターン: \d{12}

必須: いいえ

ContactInformation

AWS アカウントに関連付けられた主要連絡先情報の詳細が含まれます。

型: ContactInformation オブジェクト

必須: はい

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「一般的なエラータイプ」を参照してください。

AccessDeniedException

呼び出し元の ID に必要な最小アクセス許可がないため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 403

InternalServerException

内部エラーのため、オペレーションが失敗しました AWS。後でもう一度操作をお試しください。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 500

TooManyRequestsException

操作が頻繁に呼び出され、スロットルの制限を超えているため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 429

ValidationException

入力パラメータのいずれかが無効であるため、操作が失敗しました。

fieldList

無効なエントリが検出されたフィールド。

message

リクエストのどの部分が無効だったかを知らせるメッセージ。

reason

検証が失敗した理由。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

StartPrimaryEmailUpdate

指定されたアカウントの主要 E メールアドレスを更新するプロセスを開始します。

リクエストの構文

```
POST /startPrimaryEmailUpdate HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "PrimaryEmail": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

AccountId

このオペレーションでアクセスまたは変更 AWS アカウント する の 12 桁のアカウント ID 番号を指定します。このパラメータを使用するには、呼び出し元が組織の管理アカウントまたは委任管理者アカウントの ID である必要があります。指定されたアカウント ID は、同じ組織のメンバーアカウントである必要があります。組織はすべての機能を有効にして、アカウント管理サービス用の有効な信頼されたアクセスを持つ必要があり、オプションとして委任管理者アカウントが割り当てられます。

このオペレーションは、メンバーアカウントに対して、組織の管理アカウントまたは委任管理者アカウントからのみ呼び出すことができます。

> **Note**
>
> 管理アカウントは、自身の AccountId を指定することはできません。

タイプ: 文字列

Pattern: \d{12}

必須: はい

PrimaryEmail

指定されたアカウントで使用する新しい主要 E メールアドレス (ルートユーザーの E メールアドレスとも呼ばれる)。

タイプ: 文字列

長さの制限: 最小長は 5。最大長 64

必須: はい

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "Status": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

Status

主要 E メールの更新リクエストのステータス。

型: 文字列

有効な値：PENDING | ACCEPTED

エラー

すべてのアクションに共通のエラーについては、「一般的なエラータイプ」を参照してください。

AccessDeniedException

呼び出し元の ID に必要な最小アクセス許可がないため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 403

ConflictException

リソースの現在のステータスが競合しているため、リクエストを処理できませんでした。例えば、現在無効化中 (DISABLING ステータス) のリージョンを有効化しようとした場合や、アカウントのルートユーザーの E メールを、既に使用している E メールアドレスに変更しようとした場合にこれが発生します。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 409

InternalServerException

内部エラーのため、オペレーションが失敗しました AWS。後でもう一度操作をお試しください。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 500

ResourceNotFoundException

見つからないリソースが指定されているため、操作が失敗しました。

errorType

API Gateway によって x-amzn-ErrorType レスポンスヘッダーに入力された値。

HTTP ステータスコード: 404

TooManyRequestsException

操作が頻繁に呼び出され、スロットルの制限を超えているため、操作が失敗しました。

errorType

API Gateway によって `x-amzn-ErrorType` レスポンスヘッダーに入力された値。

HTTP ステータスコード: 429

ValidationException

入力パラメータのいずれかが無効であるため、操作が失敗しました。

fieldList

無効なエントリが検出されたフィールド。

message

リクエストのどの部分が無効だったかを知らせるメッセージ。

reason

検証が失敗した理由。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

他の AWS サービスの関連アクション

以下のオペレーションは に関連しています AWS アカウント管理 が、 AWS Organizations 名前空間の一部です。

- CreateAccount
- CreateGovCloudAccount
- DescribeAccount

CreateAccount

`CreateAccount` API オペレーションは、 AWS Organizations サービスによって管理される組織のコンテキストでのみ使用できます。API 操作は、そのサービスの名前空間に定義されています。

詳細については、AWS Organizations API リファレンスの「CreateAccount」を参照してください。

CreateGovCloudAccount

`CreateGovCloudAccount` API オペレーションは、 AWS Organizations サービスによって管理される組織のコンテキストでのみ使用できます。API 操作は、そのサービスの名前空間に定義されています。

詳細については、AWS Organizations API リファレンスの「CreateGovCloudAccount」を参照してください。

DescribeAccount

`DescribeAccount` API オペレーションは、 AWS Organizations サービスによって管理される組織のコンテキストでのみ使用できます。API 操作は、そのサービスの名前空間に定義されています。

詳細については、AWS Organizations API リファレンスの「DescribeAccount」を参照してください。

データ型

以下のデータ型 (タイプ) がサポートされています。

- AlternateContact

- ContactInformation
- Region
- ValidationExceptionField

AlternateContact

AWS アカウントに関連付けられた代替連絡先の詳細を含む構造

内容

AlternateContactType

代替連絡先のタイプ。

型: 文字列

有効な値 : `BILLING | OPERATIONS | SECURITY`

必須 : いいえ

EmailAddress

この代替連絡先に関連付けられているメールアドレス。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 254 です。

パターン: `[\s]*[\w+=.#|!&-]+@[\w.-]+\.[\w]+[\s]*`

必須: いいえ

Name

この代替連絡先に関連付けられている名前。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長 64

必須: いいえ

PhoneNumber

この代替連絡先に関連付けられている電話番号。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 25 です。

パターン: `[\s0-9()+-]+`

必須: いいえ

Title

この代替連絡先に関連付けられているタイトル。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 50 です。

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ContactInformation

AWS アカウントに関連付けられた主要連絡先情報の詳細が含まれます。

内容

AddressLine1

主要連絡先住所の最初の行。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 60 です。

必須: はい

City

主要連絡先住所の都市。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 50 です。

必須: はい

CountryCode

主要連絡先住所の ISO-3166 の 2 文字の国コード。

タイプ: 文字列

長さの制限: 固定長は 2 です。

必須: はい

FullName

主要連絡先住所の正式名称。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 50 です。

必須: はい

PhoneNumber

主要連絡先情報の電話番号。この番号は検証され、一部の国では有効化の確認も行われます。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 20 です。

パターン: `[+][\s0-9()-]+`

必須: はい

PostalCode

主要連絡先住所の郵便番号。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 20 です。

必須: はい

AddressLine2

主要連絡先住所の 2 行目 (ある場合)。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 60 です。

必須: いいえ

AddressLine3

主要連絡先住所の 3 行目 (ある場合)。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 60 です。

必須: いいえ

CompanyName

主要連絡先情報に関連付けられている会社の名前 (ある場合)。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 50 です。

必須: いいえ

DistrictOrCounty

主要連絡先住所の地区または郡 (ある場合)。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 50 です。

必須: いいえ

StateOrRegion

主要連絡先住所の都道府県または地域。郵送先住所が米国 (US) 内にある場合、このフィールドの値は 2 文字の州コード (例: `NJ`) または州の正式名称 (例: `New Jersey`) のいずれかを使用できます。このフィールドは、`US`、`CA`、`GB`、`DE`、`JP`、`IN`、および `BR` の各国では必須です。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 50 です。

必須: いいえ

WebsiteUrl

主要連絡先情報に関連付けられているウェブサイトの URL (ある場合)。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 256 です。

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2

- AWS SDK for Ruby V3

Region

これは、特定のアカウントのリージョンを表す構造であり、名前とオプトインステータスで構成されています。

内容

RegionName

特定のリージョンのリージョンコード (例: `us-east-1`)。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 50 です。

必須: いいえ

RegionOptStatus

リージョンが取り得るステータスの 1 つ (有効、有効化中、無効、無効化中、デフォルトで有効)。

型: 文字列

有効な値 : `ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ValidationExceptionField

入力が、指定されたフィールドで AWS サービスによって指定された制約を満たせませんでした。

内容

message

検証例外に関するメッセージ。

タイプ: 文字列

必須: はい

name

無効なエントリが検出されたフィールド名。

タイプ: 文字列

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

共通パラメータ

次のリストには、すべてのアクションが署名バージョン 4 リクエストにクエリ文字列で署名するために使用するパラメータを示します。アクション固有のパラメータは、アクションのトピックに示されています。署名バージョン 4 の詳細については、IAM ユーザーガイドの AWS API リクエストの署名を参照してください。

X-Amz-Algorithm

リクエストの署名を作成するのに使用したハッシュアルゴリズム。

条件: HTTP 認可ヘッダーではなくクエリ文字列に認証情報を含める場合は、このパラメータを指定します。

型: 文字列

有効な値：AWS4-HMAC-SHA256

必須: 条件による

X-Amz-Credential

認証情報スコープの値で、アクセスキー、日付、対象とするリージョン、リクエストしているサービス、および終了文字列 ("aws4_request") を含む文字列です。値は次の形式で表現されます: [access_key/YYYYMMDD/リージョン/サービス/aws4_request]。

詳細については、IAM ユーザーガイドの「署名付き AWS API リクエストの作成」を参照してください。

条件: HTTP 認可ヘッダーではなくクエリ文字列に認証情報を含める場合は、このパラメータを指定します。

型: 文字列

必須: 条件による

X-Amz-Date

署名を作成するときに使用する日付です。形式は ISO 8601 基本形式の YYYYMMDD'T'HHMMSS'Z' でなければなりません。例えば、日付 20120325T120000Z は、有効な X-Amz-Date の値です。

条件: X-Amz-Date はすべてのリクエストに対してオプションです。署名リクエストで使用する日付よりも優先される日付として使用できます。ISO 8601 ベーシック形式で日付ヘッダーが指定されている場合、X-Amz-Date は必要ありません。X-Amz-Date を使用すると、常に Date ヘッダーの値よりも優先されます。詳細については、IAM ユーザーガイドの AWS API リクエスト署名の要素を参照してください。

タイプ: 文字列

必須: 条件による

X-Amz-Security-Token

AWS Security Token Service () の呼び出しによって取得された一時的なセキュリティトークン AWS STS。 AWS STSの一時的なセキュリティ認証情報をサポートするサービスのリストについては、「IAM ユーザーガイド」の「IAM と連携するAWS のサービス」を参照してください。

条件: の一時的なセキュリティ認証情報を使用している場合は AWS STS、セキュリティトークンを含める必要があります。

タイプ: 文字列

必須: 条件による

X-Amz-Signature

署名する文字列と派生署名キーから計算された 16 進符号化署名を指定します。

条件: HTTP 認可ヘッダーではなくクエリ文字列に認証情報を含める場合は、このパラメータを指定します。

型: 文字列

必須: 条件による

X-Amz-SignedHeaders

正規リクエストの一部として含まれていたすべての HTTP ヘッダーを指定します。署名付きヘッダーの指定の詳細については、IAM ユーザーガイドの「署名付き AWS API リクエストの作成」を参照してください。

条件: HTTP 認可ヘッダーではなくクエリ文字列に認証情報を含める場合は、このパラメータを指定します。

型: 文字列

必須: 条件による

一般的なエラータイプ

このセクションでは、この AWS サービスが返す可能性のある一般的なエラータイプを一覧表示します。すべてのサービスが、ここにリストされているすべてのエラータイプを返すわけではありませ

ん。このサービスの API アクションに固有のエラーについては、その API アクションのトピックを参照してください。

AccessDeniedException

このアクションを実行するためのアクセス許可がありません。IAM ポリシーに必要なアクセス許可が含まれていることを確認します。

HTTP ステータスコード: 403

ExpiredTokenException

リクエストに含まれるセキュリティトークンの有効期限が切れています。新しいセキュリティトークンをリクエストして、もう一度試してください。

HTTP ステータスコード: 403

IncompleteSignature

リクエスト署名が AWS 標準に準拠していません。有効な AWS 認証情報を使用し、リクエストの形式が適切であることを確認します。SDK を使用している場合は、最新の状態であることを確認します。

HTTP ステータスコード: 403

InternalFailure

内部サーバーの問題のため、リクエストは現在処理できません。後でもう一度お試しください。問題が解決しない場合は、 AWS サポートにお問い合わせください。

HTTP ステータスコード: 500

MalformedHttpRequestException

リクエスト本文を処理できません。これは通常、指定されたコンテンツエンコーディングアルゴリズムを使用してリクエストボディを解凍できない場合に発生します。コンテンツエンコーディングヘッダーが、使用される圧縮形式と一致していることを確認します。

HTTP ステータスコード: 400

NotAuthorized

このアクションを実行するアクセス許可がありません。IAM ポリシーに必要なアクセス許可が含まれていることを確認します。

HTTP ステータスコード: 401

OptInRequired

AWS アカウントには、このサービスのサブスクリプションが必要です。アカウントでサービスが有効になっていることを確認します。

HTTP ステータスコード: 403

RequestAbortedException

リクエストは、レスポンスが返される前に中止されました。これは通常、クライアントが接続を閉じたときに発生します。

HTTP ステータスコード: 400

RequestEntityTooLargeException

リクエストエンティティが大きすぎます。リクエスト本文のサイズを小さくして、もう一度試してください。

HTTP ステータスコード: 413

RequestTimeoutException

リクエストがタイムアウトしました。サーバーは、予想される期間内に完全なリクエストを受信しませんでした。もう一度試してください。

HTTP ステータスコード: 408

ServiceUnavailable

サービスが一時的に使用できません 後でもう一度お試しください。

HTTP ステータスコード: 503

ThrottlingException

リクエストの頻度が多すぎます。 AWS SDKsこの例外を受け取るリクエストを自動的に再試行します。リクエストの頻度を少なくしてください。

HTTP ステータスコード: 400

UnknownOperationException

アクションまたはオペレーションは認識されません。アクション名のスペルが正しく、使用している API バージョンでサポートされていることを確認します。

HTTP ステータスコード: 404

UnrecognizedClientException

指定した X.509 証明書または AWS アクセスキー ID がレコードに存在しません。有効な認証情報を使用し、有効期限が切れていないことを確認します。

HTTP ステータスコード: 403

ValidationError

入力が必要な形式または制約を満たしていません。すべての必須パラメータが含まれ、値が有効であることを確認します。

HTTP ステータスコード: 400

HTTP クエリリクエストを作成して API を呼び出す

このセクションでは、 AWS アカウント管理用の クエリ API の使用に関する一般的な情報について説明します。API 操作とエラーの詳細については、「API リファレンス」を参照してください。

> **Note**
>
> AWS アカウント管理クエリ API を直接呼び出す代わりに、いずれかの AWS SDKs を使用できます。 AWS SDKs は、さまざまなプログラミング言語とプラットフォーム (Java、Ruby、.NET、iOS、Android など) 用のライブラリとサンプルコードで構成されています。SDKs を使用すると、 AWS アカウント管理と へのプログラムによるアクセスを簡単に作成できます AWS。例えば、SDK は要求への暗号を使用した署名、エラーの管理、要求の自動的な再試行などのタスクを処理します。 AWS SDKs「Amazon Web Services のツール」を参照してください。

AWS アカウント管理用の Query API を使用すると、サービスアクションを呼び出すことができます。クエリ API リクエストは、実行するオペレーションを示す `Action`パラメータを含む必要がある HTTPS リクエストです。 AWS アカウント管理は、すべてのオペレーションの `GET` および `POST`リクエストをサポートします。つまり、API は、あるアクションには `GET`、別のアクションには `POST` というような使い分けを必要としません。ただし、`GET` リクエストには URL サイズの制限があります。この制限はブラウザによって異なり、通常は 2,048 バイトです。したがって、大きなサイズを必要とするクエリ API リクエストでは、`POST` リクエストを使用する必要があります。

レスポンスは XML 文書です。レスポンスの詳細については、API リファレンス の個々のアクションページを参照してください。

トピック

- エンドポイント
- HTTPS の必要性
- AWS アカウント管理 API リクエストの署名

エンドポイント

AWS アカウント管理には、米国東部 (バージニア北部) でホストされている単一のグローバル API エンドポイントがあります AWS リージョン。

すべてのサービスの AWS エンドポイントとリージョンの詳細については、の「リージョンとエンドポイント」を参照してくださいAWS 全般のリファレンス。

HTTPS の必要性

クエリ API は、セキュリティ認証情報などの機密情報を返す可能性があるので、必ず HTTPS を使用してすべての API リクエストを暗号化する必要があります。

AWS アカウント管理 API リクエストの署名

リクエストには、アクセスキー ID およびシークレットアクセスキーによる署名が必要です。 AWS アカウント管理の日常業務には、 AWS ルートアカウントの認証情報を使用しないことを強くお勧めします。 AWS Identity and Access Management (IAM) ユーザーの認証情報、または IAM ロールで使用する などの一時的な認証情報を使用できます。

API リクエストに署名するには、 AWS 署名バージョン 4 を使用する必要があります。署名バージョン 4 の使用の詳細については、IAM ユーザーガイドの AWS API リクエストの署名を参照してください。

詳細については次を参照してください:

- AWS セキュリティ認証情報 - AWSへのアクセスに使用できる認証情報の種類に関する一般的な情報を提供します。
- IAM のセキュリティのベストプラクティス – IAM サービスを使用して、 AWS アカウント管理のリソースを含む AWS リソースを保護するための提案を提供します。

- IAM での一時的なセキュリティ認証情報 - 一時的なセキュリティ認証情報の作成方法と使用方法を説明します。

のクォータ AWS アカウント管理

AWS アカウント には、サービスごとに AWS 、以前は制限と呼ばれていたデフォルトのクォータがあります。特に明記されていない限り、各クォータは AWS リージョン固有です。

各 AWS アカウント には、アカウント管理に関連する次のクォータがあります。

[リソース]	クォータ
ターゲットアカウントあたりの StartPrimaryEmailUpdate リクエストの最大数	30 秒あたり 3
の代替連絡先の数 AWS アカウント	3 - BILLING、SECURITY、および OPERATIONS に 1 つずつ
アカウントあたりの同時リージョンオプトリクエストの数	6
組織あたりの同時リージョンオプトリクエストの数	50
呼び出し元アカウントごとの AcceptPrimaryEmailUpdate リクエストのレート	毎秒 1 回、バーストは毎秒 1 回まで
アカウントごとの DeleteAlternateContact リクエストのレート	毎秒 1 回、バーストは毎秒 6 回まで
アカウントごとの DisableRegion リクエストのレート	毎秒 1 回、バーストは毎秒 1 回まで
アカウントごとの EnableRegion リクエストのレート	毎秒 1 回、バーストは毎秒 1 回まで
呼び出し元アカウントごとの GetAccountInformation リクエストのレート	毎秒 3 回、バーストは毎秒 3 回まで
アカウントごとの GetAlternateContact リクエストのレート	毎秒 10 回、バーストは毎秒 15 回まで

[リソース]	クォータ
アカウントごとの GetContactInformation リクエストのレート	毎秒 10 回、バーストは毎秒 15 回まで
アカウントごとの GetGovCloudAccountInformation リクエストのレート	毎秒 3 回、バーストは毎秒 5 回まで
呼び出し元アカウントごとの GetPrimaryEmail リクエストのレート	毎秒 3 回、バーストは毎秒 3 回まで
アカウントごとの GetRegionOptStatus リクエストのレート	毎秒 5 回、バーストは毎秒 5 回まで
アカウントごとの ListRegions リクエストのレート	毎秒 5 回、バーストは毎秒 5 回まで
呼び出し元アカウントごとの PutAccountName リクエストのレート	毎秒 1 回、バーストは毎秒 1 回まで
アカウントごとの PutAlternateContact リクエストのレート	毎秒 5 回、バーストは毎秒 8 回まで
アカウントごとの PutContactInformation リクエストのレート	毎秒 5 回、バーストは毎秒 8 回まで
呼び出し元アカウントごとの StartPrimaryEmailUpdate リクエストのレート	毎秒 1 回、バーストは毎秒 1 回まで

インドでのアカウントの管理

新しい にサインアップ AWS アカウント し、連絡先と請求先住所としてインドを選択した場合、ユーザー契約はインドの現地 AWS 販売者である Amazon Web Services India Private Limited (AWS インド) と締結されます。 AWS インドが請求を管理し、請求書の合計は米ドル (USD) ではなくインドルピー (INR) で表示されます。の管理の詳細については AWS アカウント、「」を参照してくださいを設定する AWS アカウント。

アカウントが AWS India にある場合は、このトピックの手順に従ってアカウントを管理します。このトピックでは、 AWS インドアカウントにサインアップし、 AWS インドアカウントに関する情報を編集し、顧客確認を管理し、永続アカウント番号 (PAN) を追加または編集する方法について説明します。

サインアップ時のクレジットカード検証の一環として、 AWS インドはクレジットカードに 2 INR を請求します。 AWS インドは、検証が完了した後に 2 INR を返金します。確認プロセス中に、お客様の銀行にリダイレクトされる場合があります。

トピック

- India AWS アカウント で を作成する AWS
- 顧客検証情報の管理

India AWS アカウント で を作成する AWS

AWS India は、インドの の現地販売 AWS 者です。連絡先と請求先住所がインドにあり、アカウントを作成する場合は、次の手順を使用して AWS India アカウントにサインアップします。

AWS India アカウントにサインアップするには

1. Amazon Web Services ホームページを開きます。
2. の作成 AWS アカウント を選択します。

> **Note**
>
> AWS 最近 にサインインした場合、そのオプションは存在しない可能性があります。[Sign in to the Console] (コンソールにサインインする) を選択します。それでも [新

しい AWS アカウントの作成] が表示されない場合は、[別のアカウントにサインイン] を選択し、その後に [新しい AWS アカウントの作成] を選択します。

3. アカウント情報を入力し、E メールアドレスを確認し、アカウント用の強力なパスワードを選択します。
4. [ビジネス] または [個人] を選択します。個人アカウントとプロフェッショナルアカウントの機能は同じです。
5. 会社または個人の連絡先情報を入力します。連絡先または請求先住所がインドにある場合、インドのコンピュータ緊急対応チーム (CERT-In) の規制に従って、 AWS は、 AWS サービスへのアクセスを許可する前にお客様の ID 情報を収集して検証する必要があります。

   連絡先情報または請求情報から選択する名前は、顧客検証に使用する予定のドキュメントに表示される名前と完全に一致する必要があります。例えば、設立証明証を使用してビジネスアカウントを確認する予定の場合は、そのドキュメントに記載されている事業名を提供する必要があります。受け入れられたドキュメントタイプのリストについては、「the section called “顧客確認用にインドで受け入れられるドキュメント”」を参照してください。
6. カスタマーアグリーメントを読んだら、利用規約のチェックボックスを選択し、[続行] を選択します。
7. [請求情報] ページで、使用する支払い方法を入力します。検証プロセスの一部として CVV を指定する必要があります。
8. [PAN はありますか?] で、税務請求書に表示したい納税者番号 (PAN) がある場合は [はい] を選択して PAN を入力します。PAN がない場合、またはサインアップ後に追加する場合は、[いいえ] を選択します。
9. Verify and continue を選択します。 AWS India は、検証プロセスの一環としてカード 2 INR を請求します。 AWS India は、検証が完了した後に 2 INR を返金します。
10. [本人確認] ページで、アカウント登録の主な目的を選択します。
11. アカウントの所有者を最も適切に表す所有権タイプを選択します。所有権タイプとして会社、組織、またはパートナーシップを選択する場合は、主要な管理担当者の名前を入力します。主要な管理担当者には、取締役、業務責任者、または事業の運営責任者を指定できます。
12. 選択した所有権タイプに応じて、検証に使用する承認済みのインドのドキュメントタイプを選択し、ドキュメント情報を入力します。

> **Note**
>
> 個人アカウントを持っており、インド連邦による発行ではない運転免許証を使用する予定の場合は、検証用に別のタイプの個人ドキュメントを使用することをお勧めします。

13. 顧客検証に使用する名前を選択します。

    請求情報や連絡先情報にインドの住所が関連付けられている場合、その名前が選択肢として表示されます。選択した名前が、顧客検証に使用する予定のドキュメントタイプに記載された名前と一致していることを確認してください。請求先または連絡先の住所に関連付けられている名前を変更する必要がある場合は、アカウントのサインアップを完了した後に変更できます。

14. 検証のために情報を提出することに同意し、[続行] をクリックします。

    アカウントのサインアップが完了すると、顧客検証の結果が E メールで通知されます。また、アカウント設定の顧客確認ページまたは後で AWS ヘルスダッシュボードでステータスを確認することもできます。 AWS サービスにアクセスするには、顧客検証に合格する必要があります。

15. 携帯電話番号の検証方法として、[テキストメッセージ (SMS)] または [音声通話] のいずれかを選択します。
16. 国とリージョンコードを選択し、携帯電話番号を入力します。
17. セキュリティチェックを完了してください。
18. [SMS を送信] または [今すぐ電話する] を選択します。しばらくすると、携帯電話に SMS または自動通話で 4 桁の PIN が届きます。
19. [本人確認] ページで、受け取った PIN を入力し、[続行] を選択します。
20. [サポートプランの選択] ページでサポートプランを選択し、[サインアップを完了] を選択します。支払い方法と顧客検証が検証されると、アカウントがアクティブ化され、アカウントのアクティブ化を確認する E メールが送信されます。

> **Note**
>
> 顧客検証の完了後に、以前に本人確認に使用した名前、住所、またはドキュメントを編集する場合は、再度顧客検証を更新して完了する必要がある場合があります。詳細については、「the section called “顧客検証情報の編集”」を参照してください。

顧客検証情報の管理

インドのコンピュータ緊急対応チーム (CERT-In) の規制に従い、 AWS は、 AWS サービスへの新規または継続的なアクセスを許可する前に、ID 情報を収集して検証する必要があります。入力したインドの請求先住所または連絡先住所に記載されている名前を使用して本人確認を行う必要があります。検証中、 AWS はドキュメント番号が有効かどうか、および指定した名前が顧客検証に使用するドキュメントに関連付けられた名前と一致するかどうかを確認します。連絡先情報または請求情報から選択した名前は、ドキュメントに記載されている名前と完全に一致する必要があります。

請求名と住所を更新するには、「お支払いの詳細設定」ページを参照してください。連絡先の名前と住所を更新するには、「the section called “のプライマリ連絡先を更新する AWS アカウント”」を参照してください。請求先情報や連絡先情報の名前やインドの住所など、以前に顧客検証に使用した情報を編集する場合、顧客検証情報を更新して再提出する必要がある場合があります。

顧客検証ステータスの確認

顧客検証ステータスは、いつでも [顧客検証] ページで確認できます。検証ステータスが [検証が必要です] または [検証に失敗しました] の場合は、顧客検証情報を作成または更新して、検証のために提出してください。

顧客検証情報の作成

顧客検証を完了するには、承認済みのインドのドキュメントからの情報を提供する必要があります。受け入れられたドキュメントタイプのリストについては、「the section called “顧客確認用にインドで受け入れられるドキュメント”」を参照してください。

1. AWS マネジメントコンソール にサインインします。
2. 右上隅のナビゲーションバーで、アカウント名 (またはエイリアス) を選択し、[アカウント] を選択します。
3. [その他の設定] で [顧客確認] を選択します。

   以前に顧客検証情報を提供していない場合は、[お客様の本人確認情報を作成] ページが表示されます。
4. 顧客検証に使用する予定のドキュメントに記載された名前と正確に一致する名前を選択します。例えば、設立証明証を使用してビジネスアカウントを確認する予定の場合は、そのドキュメントに記載されている事業名を提供する必要があります。
5. このページでリクエストされている残りの情報を入力します。選択したドキュメントタイプによっては、ドキュメントの表面と裏面の両方のコピーをアップロードする必要がある場合があり

ます。画像ファイルをアップロードする場合は、ドキュメント内のすべての情報が認識でき、判読可能であることを確認してください。

6. [Submit] を選択してください。

   顧客検証の結果と次のステップについては、E メールまたは AWS Health Dashboard で通知されます。

顧客検証情報の編集

アカウント登録の主な目的や組織タイプ、および検証に使用する名前、ドキュメントタイプ、ドキュメントアップロード、またはドキュメント情報など、顧客検証情報を編集できます。

顧客検証に使用する名前やドキュメントタイプを編集する、またはドキュメント情報を更新する場合、変更を保存するには再度本人確認を行う必要があります。

1. AWS マネジメントコンソール にサインインします。
2. 右上隅のナビゲーションバーで、アカウント名 (またはエイリアス) を選択し、[アカウント] を選択します。
3. [その他の設定] で [顧客確認] を選択します。
4. [編集] を選択し、変更する情報を更新します。

   情報を更新する際には、次のガイダンスに注意してください。

   - 別の名前を選択する場合、その名前は顧客検証に使用する予定のドキュメントに記載されている名前と完全に一致する必要があります。例えば、設立証明証を使用してビジネスアカウントを確認する予定の場合は、そのドキュメントに記載されている事業名を提供する必要があります。
   - 別のドキュメントタイプを選択する場合は、ドキュメントの表面と裏面 (該当する場合) のコピーをアップロードする必要があります。ドキュメントアップロードに含まれるすべての情報が認識でき、判読可能である必要があります。
   - 個人アカウントを持っており、インド連邦による発行ではない運転免許証を使用する予定の場合は、検証用に別のタイプの個人ドキュメントを使用することをお勧めします。

     受け入れられたドキュメントタイプのリストについては、「the section called “顧客確認用にインドで受け入れられるドキュメント”」を参照してください。

5. [Submit] を選択してください。

保存した変更のタイプによって再度本人確認を行う必要がある場合は、顧客検証の結果と次の手順が E メールで通知されます。また、顧客検証ページに戻るか、 AWS ヘルスダッシュボードで結果を表示することもできます。

顧客確認用にインドで受け入れられるドキュメント

インド政府が発行した以下の種類のドキュメントを顧客確認に使用できます。

> **Note**
>
> 以下に示されているリンクは、政府によって変更される可能性があります。

- PAN カード - 納税者番号 (PAN) カードは、デジタルと物理の両方の形式で提供されており、個人、企業、および団体に対してインドの所得税局が発行する一意の英数字識別子が含まれています。PAN は、文字と数字を含む 10 文字の形式 (**AAAAA1111A**) で構成されます。このドキュメントを検証に使用する場合は、PAN ドキュメントに記載されている生年月日 (個人の場合) または法人設立日 (ビジネスの場合) も入力し、カードの表面をアップロードする必要があります。PAN の有効性を確認するには、所得税局の公式ウェブサイトにアクセスしてください。
- 有権者 ID カード/EPIC - 有権者 ID カードは写真付き選挙人 ID カード (EPIC) とも呼ばれ、インド選挙委員会によってインドの適格な有権者に発行される一意の識別番号が含まれています。有権者 ID/EPIC 番号は、文字と数字を含む 10 文字で構成されます。インド選挙委員会の公式ウェブサイトにアクセスして、投票者 ID の有効性を確認できます。このドキュメントを検証に使用するには、カードの表面と裏面の両方をアップロードする必要があります。
- 運転免許証 - 運転免許証がインド連邦によって発行されたものではない場合は、検証に別のドキュメントタイプを使用することをお勧めします。運転免許証番号は、文字、数字、スペース、ハイフンを含む 12～16 文字で構成されます。このドキュメントを検証に使用するには、生年月日を入力し、カードの表面と裏面の両方をアップロードする必要があります。運転免許証の有効性を確認するには、道路交通省の Parivahan Sewa のサイトにアクセスしてください。
- 設立証明証 - 設立証明書は、企業省 (MCA) によって発行されるドキュメントであり、企業が法人として登録された日付を示します。この証明書は、インドで登録されている企業を一意に識別し、追跡するために使用されます。各証明書には企業識別番号 (CIN) が含まれています。これは、文字と数字を含む 21 文字で構成される一意の英数字識別子です。このドキュメントを検証に使用するには、設立証明書ドキュメントをアップロードする必要があります。CIN の有効性を確認するには、企業省のポータルにアクセスしてください。

個人アカウントとビジネスアカウントでは、インドのさまざまなドキュメントタイプが受け入れられます。

- 個人アカウントの場合 - PAN カード、有権者 ID カード/EPIC、運転免許証。
- ビジネスアカウントの場合 - PAN カードと設立証明書。

AWS India アカウントを管理する

以下のタスクを除き、アカウントを管理する手順は、インド国外で作成されたアカウントと同じです。アカウントの管理に関する一般情報については、「アカウントの設定」を参照してください。

を使用して、次のタスク AWS マネジメントコンソール を実行します。

- 納税者番号の追加または編集
- 複数の納税者番号の編集
- the section called “顧客検証情報の管理”
- 複数の物品サービス税 (GST) 番号の編集
- 税金請求書の表示

アカウント管理ユーザーガイドのドキュメント履歴

次の表に、 AWS アカウント管理のドキュメントリリースを示します。

変更	説明	日付
新しいアカウント名 API	アカウント名を表示または変更するための新しい GetAccountInformation および PutAccountName API のサポート。	2025 年 4 月 22 日
秘密の質問の編集のサポート終了	サポートが終了したため、「秘密の質問の編集」トピックをガイドから削除しました。	2025 年 1 月 6 日
新しい主要 E メール API	AWS Organizations内の任意のメンバーアカウントのルートユーザーの E メールアドレスと を一元的に更新するための新しい GetPrimaryEmail 、StartPrimaryEmailUpdate 、および AcceptPrimaryEmailUpdate API のサポート。詳細については、「AWS Organizations ユーザーガイド」の「メンバーアカウントのルートユーザーの E メールアドレスと の更新」を参照してください。	2024 年 6 月 6 日
アカウント閉鎖トピックの書き換え	メンバーアカウントと管理アカウントを閉鎖する手順を追加するなど、アカウント閉鎖	2024 年 2 月 1 日

	トピック全体が完全に見直されました。	
新しい秘密の質問の追加のサポート終了	[アカウント] ページから新しい秘密の質問を追加するオプションが削除されたことを記載した新しいコンテンツが追加されました。	2024 年 1 月 5 日
aws-portal 名前空間のサポート終了	AWS Identity and Access Management アカウントの管理に以前使用されていた (IAM) アクション (aws-portal:ModifyAccount や などaws-portal:ViewAccount) は、標準サポートが終了しました。	2024 年 1 月 1 日
リージョントピックの書き換え	展開コントロールと折りたたみコントロールの追加など、リージョントピック全体が完全に見直されました。	2023 年 10 月 8 日
「IAM ユーザーガイド」へのルートユーザートピックの移動	ルートユーザーに関する説明を 1 つのトピックに統合し、「IAM ユーザーガイド」に移動されたルートユーザートピックへの相互参照リンクが追加されました。	2023 年 9 月 18 日
主要アカウント連絡先トピックへの新しいセクションの追加	新たに「Phone number and email address requirements」セクションが追加されました。	2023 年 9 月 12 日

新しい連絡先情報 API	新しい GetContactInformation API および PutContactInformation API のサポート。	2022 年 7 月 22 日
AWS アカウント管理では、AWS Organizations コンソールを介した代替連絡先の更新がサポートされるようになりました。	更新された AWS Organizations 管理ポリシーによって提供されるアカウント API アクセス許可を使用して、 AWS Organizations コンソールを介して組織の代替連絡先を更新できるようになりました。	2022 年 2 月 8 日
初回リリース	AWS アカウント管理リファレンスガイドの初回リリース	2021 年 9 月 30 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。