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

AWS アカウント管理リファレンスガイドへようこそ

AWS アカウントAWSサービスにアクセスするための基本的な部分です。

an AWS アカウント には次の 2 つの基本機能があります。

- コンテナ — An AWS アカウント は、AWSAWS顧客として作成するすべてのリソースの基本コンテナです。たとえば、Amazon Simple Storage Service (Amazon S3) バケット、Amazon Relational Database Service (Amazon RDS) データベース、および 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、そのアカウントの認証情報を持っているユーザーなら利用できます。

  アカウントで作成できる主なリソースには、ユーザーやロールなどの ID があります。ID には、ユーザーがサインイン (認証) に使用できる認証情報があります。AWSID には、アカウント内のリソースを使用してユーザーが実行できること (承認) を指定するアクセス権限ポリシーもあります。

  セキュリティ上のベストプラクティスとして、AWSアクセス時には一時的な認証情報の使用をユーザーに義務付けています。一時的な認証情報を提供するには、フェデレーションと AWS IAM Identity Center(IAM Identity Center) などの ID プロバイダーを使用できます。会社で既に ID プロバイダーを使用している場合は、そのプロバイダーをフェデレーションと併用すると、社内のリソースへのアクセスを簡単に提供できますAWS アカウント。

  セキュリティのベストプラクティスについては、IAM ユーザーガイドの「IAM における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。

トピック

- 複数は必要ですかAWS アカウント?
- 使用開始: 初めての AWS ユーザーですか?
- AWS アカウントのルートユーザーの使用

複数は必要ですかAWS アカウント?

AWS アカウントの基本的なセキュリティ境界として機能するAWS。これらは、有用な分離レベルを提供するリソースコンテナとして機能します。リソースとユーザーを隔離する能力は、安全で適切に管理された環境を確立するための重要な要件です。

リソースを別々に分離するAWS アカウントは、クラウド環境で次の原則をサポートするのに役立ちます。

- 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を持つことができ、それらの周りに異なる制御ポリシーとメカニズムが必要です。例えば、監査人と話をして、単一のものを指すことができる方がはるかに簡単です。AWS アカウントこれは、対象となるワークロードのすべての要素をホストします。PCI（ペイメントカード業界）セキュリティ基準。
- ISOLATION— あん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の脅威は、AWS アカウント他人に影響を与えずに。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。
- 多くのチーム：チームごとに異なる責任とリソースニーズがあります。チーム同士を別々に移動させることで、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。
- データの隔離— チームを隔離することに加えて、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。これにより、機密性の高いデータへの露出を抑えることができ、欧州連合の一般データ保護規則(GDPR)。
- ビジネスプロセス：ビジネスユニットや製品によって、目的やプロセスがまったく異なる場合があります。複数の場合AWS アカウントでは、ビジネスユニットの特定のニーズをサポートできます。
- Billing (料金)— 課金レベルでアイテムを区切る唯一の真の方法は、アカウントです。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。それでもすべての請求書を単一の支払人に統合することができます（AWS Organizationsおよび一括請求）で明細項目が区切られている間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ものに分けるAWS アカウントお互いのクォータを消費しないようにします。

このドキュメントで説明する推奨事項と手順はすべて、AWSWell-Architected フレームワーク。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、フレームワークのこのガイダンスを遵守

して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、アカウントを管理する計画を策定する必要があります。そのためには、AWS Organizationsは無料ですAWSすべてのサービスを管理するAWS アカウントお客様の組織内で

AWS提供タイプも提供していますAWS Control Towerのレイヤーを加える。AWSOrganizations への自動化を管理し、他の組織と自動的に統合するAWSサービスのようなAWS CloudTrail,AWS ConfigAmazon CloudWatch、AWS Service Catalogなど。これらのサービスには、追加コストが発生する可能性があります。詳細については、AWS Control Tower 料金表を参照してください。

使用開始: 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、AWSAWS アカウント入力した情報を使用してアカウントを作成し、アカウントを割り当てます。を作成したらAWS アカウント、root ユーザーとしてサインインし、root 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。

ステップ

- 前提条件
- ステップ 1:AWS アカウント を作成する
- ステップ 2: ルートユーザーの MFA を有効にする
- ステップ 3: 管理者ユーザーを作成する
- 関連トピック

前提条件

にサインアップするにはAWS アカウント、以下の情報が必要です。

- アカウント名 — アカウントの名前は、請求書、コンソール内の請求情報とコスト管理ダッシュボード、および AWS Organizations コンソールなど複数の場所に表示されます。

  アカウントにわかりやすい名前を付けるために、標準的な方法でアカウントに名前を付けることをおすすめします。企業アカウントには、組織-目的-環境 (例:-監査 AnyCompany-製品) のような命

名規則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」などの命名基準 (例:) の使用を検討してください。paulo-santos-testaccount

アカウント名の変更について詳しくは、「AWS アカウント自分のアカウント名を変更するにはどうすればいいですか?」を参照してください。 。

- 住所 — 連絡先の住所がインドにある場合、AWSアカウントのユーザー契約はインドのローカルセラーである Amazon Internet Services Private Limited (AISPL) とのものです。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。確認プロセスの一環として、AISPL からカードに 2 インドルピー (INR) が請求されます。確認が完了すると、2 INR が AISPL より返金されます。
- メールアドレス — メールアドレスは root ユーザーのサインイン名として使用され、アカウントの復旧に必要です。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。

> **Important**
>
> このアカウントが法人用の場合は、安全な企業配布リスト (などit.admins@example.com) を使用して、AWS アカウント従業員が職務を変えたり退職したりしても会社がそのアカウントにアクセスできるようにしてください。電子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をリセットするために使用される可能性があるため、この配布リストまたはアドレスへのアクセスを保護してください。

- 電話番号 — この番号は、アカウントの所有権を確認するために使用できます。この電話番号で通話を受信できる必要があります。

> **Important**
>
> このアカウントが法人向けである場合は、会社の電話番号を使用して、AWS アカウント従業員が職務を変更したり退職したりした場合でも、会社が引き続きアカウントにアクセスできるようにしてください。

ステップ 1:AWS アカウント を作成する

1. AWSブラウザでホームページを開きます。
2. [Create an AWS アカウント] (作成する) を選択します。

> **Note**
>
> AWSに最近ログインした場合は、[サインイン] を選択します。[Create a new AWS アカウント] (新しく作成する) オプションが表示されない場合、まず [Sign in to a different account] (別のアカウントにサインインする) を選択してから、[Create an AWS アカウント] (作成する) を選択します。

3. アカウント情報を入力し、[メールアドレスを確認] を選択します。これにより、指定したメールアドレスに確認コードが送信されます。
4. 認証コードを入力し、[Verify] を選択します。
5. root ユーザーの強力なパスワードを入力して確認し、[続行] を選択します。 AWSパスワードが以下の条件を満たす必要があります。
   - 8 ~ 128 文字で構成されていること。
   - 英字の大文字と小文字、数字、および ! @ # $ % ^ & * () <> [] {} | _+-= の記号を含める必要があります。
   - AWS アカウント アカウント名またはメールアドレスと同じでないこと。
6. [ビジネス] または [パーソナル] を選択します。これらのオプションの違いは、お客様にお伺いする情報です。どちらのアカウントタイプも同じ機能と機能を備えています。
7. ビジネス情報または個人情報を入力します。メールアドレスと電話番号についての [Prerequisites] (前提条件) セクションの推奨事項を参照してください。
8. AWS カスタマーアグリーメントを読み、同意します。AWS カスタマーアグリーメントの条項を読み、理解していることを確認してください。
9. [続行] を選択します。この時点で、AWS アカウント を使用する準備が完了したことを確認する E メールメッセージが届きます。サインアップ時に指定したメールアドレスとパスワードを使用して、新しいアカウントにサインインできます。ただし、アカウントのアクティベーションが完了するまでいずれのAWSサービスを使用することはできません。
10. 支払い方法に関する情報を入力します。請求目的で別の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。
11. [検証して続行] を選択します。
12. 一覧から国コードまたは地域コードを入力し、数分以内に連絡が取れる電話番号を入力します。CAPTCHAコードを入力し、送信してください。
13. 自動システムから連絡があったら、受信した PIN を入力して送信します。

14. AWS Supportプランを選択します。使用可能なプランの説明については、「AWS Support予定を比較する」を参照してください。
15. [サインアップを完了] 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。
16. アカウントが有効になったことを確認するメールメッセージがメールと迷惑メールフォルダに届いていないか確認してください。アクティベーションには通常数分かかりますが、最長で 24 時間かかることもあります。

    アクティベーションメッセージを受け取ると、AWSすべてのサービスに完全にアクセスできるようになります。

> **Note**
>
> アカウントのアクティベーションに問題がある場合は、を参照してくださいthe section called “アカウント作成の問題”。

ステップ 2: ルートユーザーの MFA を有効にする

ルートユーザーの MFA を有効化することを強くお勧めします。MFA は、誰かがあなたの許可なしにあなたのアカウントにアクセスするリスクを劇的に減らします。

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

   root ユーザーを使用してサインインする方法については、『Sign-In User Guide』の「root AWS Management ConsoleAWSユーザーとしてにサインインする」を参照してください。
2. ルートユーザーの MFA を有効にします。

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

ステップ 3: 管理者ユーザーを作成する

ルートユーザーが実行できる操作を制限することはできないため、ルートユーザーを明示的に必要としない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。代わりに、IAM Identity Center の管理ユーザーに管理アクセスを割り当て、その管理者ユーザーとしてサインインして日常の管理タスクを実行します。

手順については、『IAM Identity Center ユーザーガイド』の「IAM Identity Center AWS アカウント管理ユーザーのアクセス権の設定」を参照してください。

関連トピック

- ルートユーザーの認証情報の保護については、IAM ユーザーガイドの「ルートユーザーの認証情報の保護」を参照してください。
- root ユーザーを必要とするタスクのリストについては、IAM ユーザーガイドの「root ユーザー認証情報を必要とするタスク」を参照してください。

AWS アカウントのルートユーザーの使用

> **Important**
>
> AWS アカウント のユーザー認証情報を持っていればだれでも、請求情報を含む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。

AWS アカウント を作成する場合は、このアカウントのすべての AWS のサービス とリソースに対して完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることによってアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報を保護し、それらを使用してルートユーザーのみが実行できるタスクを実行します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

日常的なタスクに root ユーザーを使わないようにするには、で管理ユーザーを設定する方法を学んでください。AWS IAM Identity Center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、「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AWS アカウント。

root ユーザーのパスワードを変更またはリセットしたり、root 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。root ユーザーを使用してサインインする方法については、『Sign-In User Guide』の「root AWS Management Console AWS ユーザーとしてにサインインする」を参照してください。

管理してくださいAWS アカウント

このセクションでは、AWS アカウント の管理方法について説明します。

> **Note**
>
> もし、あなたのAWS アカウントを使用してインドで作成されましたAmazon Internet Services Private Limited(AISPL)、他にも考慮すべき点があります。詳細については、「インドのアカウント管理」を参照してください。

トピック

スタンドアロンの作成 AWS アカウント

このトピックでは、AWS Organizations によって管理されないスタンドアロン AWS アカウント の作成方法について説明します。が管理する組織に属するアカウントを作成する場合はAWS Organizations、AWS Organizationsユーザーガイドの「組織でのメンバーアカウントの作成」を参照してください。

以下は、インド以外で AWS アカウント を作成する手順です。インドでのアカウントの作成については、「作成AWS アカウントAISPL と」を参照してください。

AWS Management Console

AWS アカウント を作成するには

1. Amazon Web Services ホームページを開きます。
2. [Create an AWS アカウント] (作成する) を選択します。

> **Note**
>
> 最近 AWS にサインインした場合、その選択肢は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。次いで、[Create a new AWS アカウント] (新しく作成する) が表示されない場合、まず Sign in to a different account (別のアカウントにサインインする) を選択してから、Create an AWS アカウント (作成する) を選択します。

3. アカウント情報を入力し、[メールアドレスを確認] を選択します。これにより、指定したメールアドレスに確認コードが送信されます。

> **Important**
>
> アカウントの root ユーザーは重要であるため、個人だけでなくグループがアクセスできるメールアドレスを使用することを強くお勧めします。そうすれば、AWS アカウント を申し込んだ人が会社を辞めても、メールアドレスがアクセス可能なので、AWS アカウント をそのまま使用できます。
> AWS アカウント に関連付けられている E メールアドレスにアクセスできない場合、パスワードを紛失した場合に、アカウントへのアクセスを回復することはできません。

4. 確認コードを入力し、[Verify] を選択します。
5. root ユーザーの強力なパスワードを入力して確認し、[続行] を選択します。 AWSパスワードが以下の条件を満たす必要があります。

   - 8 ~ 128 文字で構成されていること。
   - 英字の大文字と小文字、数字、および ! @ # $ % ^ & * () <> [] {} | _+-= の記号を含める必要があります。
   - AWS アカウント アカウント名またはメールアドレスと同じでないこと。

6. [ビジネス] または [パーソナル] を選択します。個人アカウントとビジネスアカウントは同じ特徴と機能を備えています。
7. 会社または個人情報を入力します。

> **Important**
>
> AWS アカウントビジネスでは、以下を入力するのがベストプラクティスです。
>
> - 個人の電話の番号ではなく、会社の電話番号。
> - アカウントを使用する会社または組織に属するドメイン名の付いた電子メールアドレス。
>
> アカウントのルートユーザーを個人のメールアドレスまたは個人の電話番号で設定すると、アカウントの安全性が低下する可能性があります。

8. AWS カスタマーアグリーメントを読み、同意します。AWS カスタマーアグリーメントの条項を読み、理解していることを確認してください。
9. [続行] を選択します。この時点で、AWS アカウント を使用する準備が完了したことを確認する E メールメッセージが届きます。サインアップ時に指定したメールアドレスとパスワードを使用して、新しいアカウントにサインインできます。ただし、アカウントのアクティベーションが完了するまでいずれのAWSサービスを使用することはできません。
10. お支払い方法に関する情報を入力し、[確認して続行] を選択します。請求情報に別の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。AWS

    有効な支払い方法を追加するまで、サインアッププロセスを進めることはできません。
11. 一覧から国コードまたは地域コードを入力し、数分以内に連絡が取れる電話番号を入力します。
12. CAPTCHAに表示されるコードを入力し、送信してください。
13. 自動システムから連絡があったら、受信した PIN を入力して送信します。
14. AWS Support利用可能なプランを 1 つ選択してください。利用可能な Support プランとその利点の説明については、「AWS Support プランの比較」を参照してください。
15. [サインアップを完了] 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。

16. メールと迷惑メールフォルダをチェックして、アカウントが有効になったことを確認するメールメッセージがないか確認してください。アクティベーションには通常数分かかりますが、最長で 24 時間かかることもあります。

    アクティベーションメッセージを受け取ると、AWSすべてのサービスに完全にアクセスできるようになります。

AWS CLI & SDKs

によって管理されている組織では、AWS OrganizationsCreateAccountその組織の管理アカウントにサインインした状態で操作を実行することで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 操作を使用して、組織外にスタンドアロン AWS アカウント を作成することはできません。

AWS アカウント 識別子の表示

AWS は、各 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

を一意に識別する 012345678901 などの 12 桁の番号 AWS アカウント。多くの AWS リソースには、Amazon リソースネーム (ARNsが含まれています。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 Management Console を使用して にサインインできます。アカウント IDs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、機密情報、重要情報、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 。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 場合は、この ID を使用して を識別できます。の正規ユーザー ID は、ルートユーザーまたは IAM ユーザー AWS アカウント として取得できます。

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サードパーティーに 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。そうすることで、ユーザーと同じアクセス権が付与 AWS アカウント されます。

AWS アカウント ID の検索

AWS アカウント ID は、 AWS Management Console または AWS Command Line Interface () を使用して確認できますAWS CLI。コンソールでのアカウント ID の場所は、ルートユーザーとしてログインしているか、IAM ユーザーとしてログ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ログインしているか IAM ユーザーとしてログ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 Management Console

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は、IAM ユーザーではなく、IAM ロールを持つフェデレーティッドユーザーとしてサインインしている可能性があります。この場合、 アカウント エントリと、その横のアカウント ID 番号を探します。

2. アカウントの詳細セクションのアカウント番号は ID AWS アカウント の横に表示されます。

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 Management Console

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は、IAM ユーザーではなく、IAM ロールを持つフェデレーティッドユーザーとしてサインインしている可能

性があります。この場合、 アカウント エントリと、その横のアカウント ID 番号を探します。

2. ページの上部のアカウントの詳細 の下に、 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 Management Console または AWS アカウント を使用して、 の正規ユーザー ID を検索できます 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 ID を検索する

AWS Management Console

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 Management Console 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は、IAM ユーザーではなく、IAM ロールを持つフェデレーティッドユーザーとしてサインインしている可能性があります。この場合、エントリ Account とその横のアカウント ID 番号を探します。

3. アカウントの詳細セクションでは、正規ユーザー ID が正規ユーザー ID の横に表示されます。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 (ACLs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 コマンドが、 AWS アカウントのルートユーザー、IAM ユーザー、または IAM ロールに対して機能します。

list-buckets コマンドを次のように使用します。

```
$ aws s3api list-buckets \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

IAM ロールを持つフェデレーティッドユーザーとして正規 ID を検索する

AWS Management Console

IAM ロールを持つフェデレーティッド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 ID を検索するには

> **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 Management Console 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、 の正規 ID AWS アカウント 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 コマンドが、 AWS アカウントのルートユーザー、IAM ユーザー、または IAM ロールに対して機能します。

list-buckets コマンドを次のように使用します。

```
$ aws s3api list-buckets \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

ルートユーザー AWS アカウント の名前、E メールアドレス、またはパスワードを更新する

AWS アカウントの名前を編集したり、ルートユーザーのパスワードや E メールアドレスを変更したりするには、次の手順を実行します。この E メールアドレスとパスワードは、 としてサインインするために使用する認証情報です AWS アカウントのルートユーザー。

> **Note**
>
> への変更は、すべての に伝達されるまでに最大 4 時間かかる AWS アカウント 場合があります。

AWS Management Console

AWS アカウント 名前、ルートユーザーパスワード、またはルートユーザーの E メールアドレスを編集するには

> **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。
>
> - としてサインインする必要があります。 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 Management Console 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、アカウント設定 の横にある 編集 を選択します。セキュリティ上の理由から、再認証を求められます。

> **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としてログインしていない可能性があります。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、アカウント設定を変更できません。

4. アカウント設定の更新ページで、更新するフィールドの横にある編集を選択します。

   a. 名前 - アカウント名の更新ページで、新しいアカウント名 に新しいアカウント名を入力し、変更の保存 を選択します。

   > **Note**
   >
   > AWS アカウント 名前を変更できない場合は、 へのアクセスを制限するサービスコントロールポリシー (SCP) account AWS Organizations が に存在するか、 `iam:UpdateAccountName` アクションを拒否するように設定されているかどうかを確認します。

   b. E メールの場合 – E メールアドレスの更新ページで、新しい E メールアドレス 、新しい E メールアドレス の確認、現在のパスワード のフィールドに入力します。次に、[変更の保存] を選択します。から新しい E メールアドレスに検証コードが送信されますno-reply@verify.signin.aws。新しい E メールアドレスの検証 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、変更の保存 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。受信トレイに E メールが表示されない場合は、スパムフォルダと迷惑メールフォルダを確認してください。

   c. パスワード - パスワードの更新ページで、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 のフィールドに入力します。次に、[変更の保存] を選択します。ルートユーザーパスワードの設定に関するベストプラクティスを含むその他のガイダンスについては、IAM ユーザーガイドの「 のパスワードの変更 AWS アカウントのルートユーザー」を参照してください。

5. 変更を行ったら、[完了] を選択します。

AWS CLI & SDKs

このタスクは、 AWS CLI または AWS SDKs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 Management Console。

API 操作モードについて

と連動する API オペレーションAWS アカウントの属性は、常に以下の 2 つの操作モードのいずれかで動作します。

- スタンドアロンコンテキスト— このモードは、アカウントのユーザーまたはロールが同じアカウント。スタンドアロンコンテキストモードは、アカウント管理 `AccountId` または AWS CLI SDK の操作のいずれかを呼び出す際に AWS パラメータを含めずに実行すると自動的に使用されます。
。
- Organizations 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か、それを変更する場合に使用されます。組織コンテキストモードは、次の場合に自動的に使用されます。行うを含む`AccountId`アカウント管理のいずれかを呼び出すときのパラメータAWS CLIまたはAWSSDKオペレーション。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 の操作は、スタンドアロンコンテキストまたは組織コンテキストのいずれでも動作します。

- `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権限を付与する

ほとんどの場合と同様AWSオペレーションでは、アカウント属性を追加、更新、または削除する権限を付与しますAWS アカウントを使用してIAM アクセス権限ポリシー。IAM 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。

AWS アカウント の Amazon リソースネーム形式

- ポリシーステートメントの resource 要素に含めることができる AWS アカウント 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か組織内のアカウントかによって、異なる構成になります。「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
    ```

    スタンドアロンモードで操作を実行する場合は、スタンドアロンモードで操作を実行する場合は、この形式を使用する必要があります。AccountIDパラメータ。
  - 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}
    ```

組織モードでアカウント属性に関する操作を実行する場合は、この形式を使用する必要があります。AccountIDパラメータ。

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 OU へのパスを参照する場合でも、条件キーのプレフィックスは account 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する場合でも、条件キーのプレフィックスは account 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 AWS アカウント にタグをアタッチすることはできません。

を更新AWS アカウント連絡先情報

AWS アカウント のプライマリアカウントの連絡先情報を保存できます。また、以下のように、代替アカウントの連絡先情報の追加または編集を行うこともできます。

- 請求 – 請求に関する代替連絡先では、請求書の有無に関する通知など、請求関連の通知を受信します。
- 操作 – 操作に関する代替連絡先では、操作関連の通知を受信します。
- セキュリティ – セキュリティに関する代替連絡先は、AWS 不正使用対策チームからの通知を含むセキュリティ関連の通知を受信します。

トピック

- の代替連絡先を更新する AWS アカウント
- の主要連絡先を更新する AWS アカウント

の代替連絡先を更新する AWS アカウント

代替連絡先では 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。代替連絡先が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た E メールアドレスに追加されます。プライマリアカウントの連絡先は、ルートアカウントの E メール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 AWS CLI と SDKs 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 組織内の - 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された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 AWS CLI と SDKs 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。この方法については、「組織内の 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。

トピック

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に進む前に、電話番号と E メールアドレスを入力するときに、まず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、および次の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、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次の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 Management Console 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 Management Console 、 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 Management Console

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には)
> - `account:PutAlternateContact` (代替連絡先を設定または更新するため)
> - `account:DeleteAlternateContact` (代替連絡先を削除するには)

1. AWS Management Console 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 までスクロールし、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として、または上記で指定した最小限のアクセス許可を持つユーザーとしてサイン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 の場合 AWS アカウント、個人に属する電話番号とメールアドレスではなく、会社の電話番号と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 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、 AWS または削除できます。

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **メモ**
>
> - 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には)

- PutAlternateContact (代替連絡先を設定または更新するため)
- DeleteAlternateContact (代替連絡先を削除するには)

これらの個々のアクセス許可を使用する場合、一部のユーザーに連絡先情報のみを読み取る権限を付与し、他のユーザーに読み書きの両方の権限を付与できます。

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**
>
> 同じ連絡先タイプ AWS アカウント と同じ連絡先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、 は最初に新しい連絡先を追加し、同じ AWS アカウント と連絡先タイプへの連続するすべての呼び出しによって既存の連絡先が更新されます。

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、以下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。組織が一括請求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の有効化」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、 AWS 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、 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 Management Console

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 の場合 AWS アカウント、個人に属する電話番号とメールアドレスではなく、会社の電話番号と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

> **メモ**
>
> - 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。
> - 操作の呼び出しに使用する組織と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には)
> - `PutAlternateContact` (代替連絡先を設定または更新するため)
> - `DeleteAlternateContact` (代替連絡先を削除するには)
>
> これらの個々のアクセス許可を使用する場合、一部のユーザーに連絡先情報のみを読み取る権限を付与し、他のユーザーに読み書きの両方の権限を付与できます。

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**
>
> 同じ連絡先タイプ AWS アカウント と同じ連絡先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、 は最初に新しい連絡先を追加し、同じ AWS アカウント と連絡先タイプへの連続するすべての呼び出しによって既存の連絡先が更新されます。

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。

アカウント：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 つの請求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。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "account:GetAlternateContact",
            "Resource": [
                "arn:aws:account::123456789012:account/o-aa111bb222/111111111111"
            ],
```

```
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "account:AlternateContactTypes": [
                        "BILLING"
                    ]
                }
            }
        }
    ]
}
```

の主要連絡先を更新する AWS アカウント

連絡先のフルネーム、会社名、郵送先住所、電話番号、ウェブサイトアドレスなど、アカウントに関連付けられている主な連絡先情報を更新できます。

プライマリアカウントの連絡先は、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、異なる方法で編集します。

- 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するか、CLI および 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 アカウントのプライマリ連絡先 を更新する」を参照してください。
- AWS アカウント 組織内の – 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、「組織のAWS アカウントプライマリ連絡先を更新する」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 のプライマリ連絡先を更新する AWS アカウント
- 組織AWS アカウント内の任意の の主要な連絡先を更新する

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に進む前に、電話番号と E メールアドレスを入力するときに、まず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、および次の文字のみを含めることができます：+-( )「」
- 電話番号は、 +および国コードで始まる必要があり、国コードの後に先頭の 0 または追加スペースを含めることはできません。例えば、 +1 (米国/カナダ) や +44 (英国) などです。
- 電話番号には、市外局番、交換コード、およびローカルコード-の間にハイフン「」を含める必要があります。例えば、+1 202-555-0179 などです。

> **Note**
>
> ハイフンなしで電話番号を入力すると、ルートユーザーの MFA デバイスをリセットするときに、電話番号検証プロセス中に通話を受信できなくなる可能性があります。詳細については、AWS「ルートユーザーアカウントの MFA デバイスをリセットするにはどうすればよいですか？」を参照してください。

- セキュリティ上の理由から、電話番号は から SMS を受信できる必要がありますAWS。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、その個人が会社を離れると、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 のプライマリ連絡先を更新する AWS アカウント

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。以下の AWS Management Console の手順は、常にスタンドアロンコンテキストでのみ動作します。を使用してAWS Management Console、 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な連絡先情報のみにアクセスまたは変更できます。

AWS Management Console

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ため)

- `account:PutContactInformation` (主要連絡先の詳細を更新するため)

1. AWS Management Console 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 の同等のオペレーションを使用して、主な連絡先情報を取得、更新、または削除できます。

- GetContactInformation
- PutContactInformation

> **メモ**
>
> - 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`

これらの個々のアクセス許可を使用する場合は、一部のユーザーに連絡先情報のみを読み取る権限を付与し、他のユーザーに読み取りと書き込みの両方の権限を付与できます。

Example

次の例では、呼び出し元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の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AWS アカウント内の任意の の主要な連絡先を更新する

組織AWS アカウント内の任意の で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 コンソールで主要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。組織が一括請求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 アカウント管理用に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 アカウント管理用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 Management Console

組織AWS アカウント内の 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、プライマリ連絡先 、
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 の同等のオペレーションを使用して、主な連絡先情報を取得、更新、または削除できます。

- GetContactInformation
- PutContactInformation

メモ

- 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。
- 操作の呼び出しに使用する組織と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

これらの個々のアクセス許可を使用する場合は、一部のユーザーに連絡先情報のみを読み取る権限を付与し、他のユーザーに読み取りと書き込みの両方の権限を付与できます。

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な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。

セキュリティチャレンジの質問を更新する

セキュリティチャレンジの質問は、アカウント復旧シナリオで以前に ID を検証するために使用された検証方法です。多要素認証 (MFA) など、最新の検証形式よりも安全性が低くなります。現在、 でセキュリティチャレンジの質問が有効になっている場合AWS アカウント、 AWS Supportはこれらを使用して、アカウントの所有者として認証できます。

> **Important**
>
> 2024 年 1 月 5 日以降、 AWSは、まだ有効化および使用していないアカウントのセキュリティチャレンジの質問をサポートしなくなります。これにより、 のアカウントページから新しいセキュリティチャレンジの質問を追加するオプションが削除されますAWS Management Console。セキュリティチャレンジの質問がすでに設定されているか、AWSOrganization の管理アカウントにすでに設定されている場合は、引き続き使用できます。2025 年 1 月 6 日以降、 AWSは、残りのすべてのお客様のセキュリティチャレンジの質問をサポートしなくなります。代わりに MFA を追加することをお勧めします。詳細については、AWS「アカウントはセキュリティチャレンジの質問の使用を中止します」を参照してください。

既存のセキュリティチャレンジの質問を編集して回答を提供するには、次の手順を実行します。

AWS Management Console

のセキュリティチャレンジの質問を編集するには 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:GetChallengeQuestions` (セキュリティチャレンジの質問を見るため)
> - `account:PutChallangeQuestions` (セキュリティチャレンジの質問を設定または更新するため)

1. AWS アカウントのルートユーザー に AWS Management Consoleまたは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. 下にスクロールして「セキュリティチャレンジの質問」セクションに進み、「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として、または上記で指定された最小限のアクセス許可を持つユーザーとしてサイン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。提供された質問のいずれかを選択し、適切な回答を入力できます。
5. 変更を加え終わったら、[Update] (更新) を選択します。

AWS CLI & SDKs

このタスクは AWS CLI 内でも AWS SDK のいずれかによる API 操作でもサポートされません。このタスクは、AWS Management Console を使用してのみ実行できます。

AWS リージョン アカウントで使用できる を指定する

AWS リージョン は、複数のアベイラビリティーゾーン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、それぞれに冗長電源、ネットワーク、接続があり、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。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。

あるリージョンで作成したリソースは、 AWS サービスが提供するレプリケーション機能を明示的に使用しない限り、他のリージョンには存在しません。たとえば、Amazon S3 と Amazon EC2 はクロスリージョンのレプリケーションをサポートしています。 AWS Identity and Access Management (IAM) などの一部のサービスには、リージョンリソースがありません。

アカウントにより、利用できるリージョンが決まります。

- AWS アカウント には複数の リージョンが用意されているため、要件を満たす場所で AWS リソースを起動できます。例えば、欧州の顧客に近い場所に、または法的要件を満たすために、欧州で Amazon EC2 インスタンスを起動したい場合があります。
- AWS GovCloud （ 米国西部) アカウントは、 AWS GovCloud （ 米国西部) リージョンと AWS GovCloud （ 米国東部) リージョンへのアクセスを提供します。詳細については、「AWS GovCloud (US)」を参照してください。
- Amazon AWS （ 中国) アカウントでは、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」(中国でのアマゾン ウェブ サービス) を参照してください。

リージョン名とそれに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。各リージョンでサポートされている AWS サービス (エンドポイントなし) 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、レイテンシーを低減するために、グローバルエンドポイントの代わりにリージョン 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。リージョンの 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、有効に AWS リージョン 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 エンドポイントの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を与える可能性があります。 AWS STS エンドポイントが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 AWS」を参照してください。

トピック

リージョンを有効または無効にする前の考慮事項

リージョンを有効または無効にする前に、次の点を考慮することが重要です。

- 2019 年 3 月 20 日より前に導入されたリージョンはデフォルトで有効になっています。 AWS つまり、最初はすべての新しい AWS リージョン がデフォルトで有効になっています。つまり、これらのリージョンでリソースの作成と管理をすぐに開始できます。デフォルトで有効になっているリージョンは、有効または無効にできません。現在、 がリージョン AWS を追加すると、新しいリージョンはデフォルトで無効になっています。ユーザーが新しいリージョンでリソースを作成および管理できるようにするには、まずそのリージョンを有効にする必要があります。以下のリージョンはデフォルトで無効になっています。

名前	コード
アフリカ (ケープタウン)	af-south-1
アジアパシフィック (香港)	ap-east-1
アジアパシフィック (ハイデラバード)	ap-south-2
アジアパシフィック (ジャカルタ)	ap-southeast-3

名前	コード
アジアパシフィック (メルボルン)	ap-southeast-4
カナダ (カルガリー)	ca-west-1
欧州 (ミラノ)	eu-south-1
欧州 (スペイン)	eu-south-2
欧州 (チューリッヒ)	eu-central-2
イスラエル (テルアビブ)	il-central-1
中東 (バーレーン)	me-south-1
中東 (アラブ首長国連邦)	me-central-1

- 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できます – 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「: 有効化と無効化 AWS リージョンを許可する」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 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は無料 – リージョンを有効にすると料金はかかりません。新しいリソースで作成するリソースに対してのみ、料金がかかります。
- 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。Amazon Elastic Compute Cloud (Amazon EC2) インスタンスなどの AWS リソースがまだ含まれているリージョンを無効にすると、そのリージョン内のリソースへの IAM アクセスが失われます。例えば、 を使用して、無効になっているリージョンの EC2 インスタンスの設定 AWS Management Console を表示または変更することはできません。
- アクティブなリソースの料金は、リージョンを無効にしても継続します。 AWS リソースがまだ含まれているリージョンを無効にすると、それらのリソース (存在する場合) の料金は引き続き標準レートで発生します。例えば、Amazon EC2 インスタンスが含まれているリージョンを無効にした場合、それらのインスタンスはアクセス不可能であっても、引き続き料金のお支払いが必要になります。

- リージョンの無効化は、必ずしもすぐに表示されるとは限りません。リージョンを無効化すると、サービスと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ことがあります。
- リージョンの有効化には数分から数時間かかる場合があります。リージョンを有効にすると、AWS は IAM リソースをリージョンに配布するなど、そのリージョンでアカウントを準備する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数分かかりますが、場合によっては数時間かかることがあります。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。
- 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、組織の完了を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 つのアカウントの 1 つの特定のリージョンの有効または無効のいずれかに等しくなります。
- 1 つのアカウントで、一度に 6 つのリージョンオプトリクエストを実行できます。1 つのリクエストは、1 つのアカウントに対して 1 つの特定のリージョンの有効化または無効化のいずれかに等しくなります。
- Amazon EventBridge 統合 — お客様は、 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 EventBridge。ステータスの変更ごとに 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。
- 式リージョンオプトステータス – オプトインリージョンを有効または無効にする非同期性のため、リージョンオプトリクエストには 4 つの潜在的な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が `ENABLING`または `DISABLING`ステータスの場合、キャンセルすることはできません。そうしないと、 がスロー`ConflictException`されます。完了した (有効/無効) region-opt 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依存します。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`。
- との完全な統合 AWS Organizations — 管理アカウントは、その AWS 組織のメンバーアカウントに対して region-opt を変更または読み取ることができます。メンバーアカウントは、リージョンの状態を読み書きすることもできます。

スタンドアロンアカウントのリージョンを有効または無効にする

が AWS アカウント アクセスできるリージョンを更新するには、以下の手順を実行します。 AWS Management Console 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 Management Console 、 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 Management Console

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、それらが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. 最小限のアクセス許可を持つ IAM ユーザーまたはロールAWS Management Console AWS アカウントのルートユーザー として にサインインします。
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、 セクションまでスクロールしますAWS リージョン。

   > **Note**
   >
   > この情報へのアクセスを承認するよう求められる場合があります。 AWS は、アカウントに関連付けられた E メールアドレスと主要連絡先の電話番号にリクエストを送信します。リクエスト内のリンクを選択してブラウザで開き、アクセスを承認します。

4. アクション列のオプション AWS リージョン がある各 の横にある を有効または無効にするかを選択します。これは、アカウントのユーザーがそのリージョンでリソースを作成およびアクセスできるようにするかどうかによって異なります。
5. プロンプトが表示されたら、選択内容を確認します。

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、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、一覧表示できます。

- `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される アクセス許可が必要です。
>
> - `account:EnableRegion`
> - `account:DisableRegion`
> - `account:GetRegionOptStatus`
> - `account:ListRegions`

これらの個々のアクセス許可を使用する場合、一部のユーザーにリージョンオプト情報のみを読み取る機能を付与し、他のユーザーに読み書きの両方の機能を付与できます。

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された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。

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

```
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。

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、リクエストの最新の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を有効または無効にする

のメンバーアカウントで有効なリージョンを更新するには AWS Organizations、以下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 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、 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**
>
> 組織内の管理アカウントまたは委任された管理者アカウントからこれらのオペレーションをメンバーアカウントで使用する前に、以下を実行する必要があります。
>
> - 組織内のすべての機能を有効にして、メンバーアカウントの設定を管理します。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。組織が一括請求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、「」を参照してくださいAWS アカウント管理用の信頼されたアクセスを有効にする。

AWS Management Console

組織内のリージョンを有効または無効にするには

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 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、有効または無効にオプションを選択します。
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、リージョンを有効化 を選択します。
7. Disable 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、Disable と入力して確認します。次に、Disable region 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の有効化、無効化、読み取り、一覧表示は、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て行うことができます。

- `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される アクセス許可が必要です。
>
> - `account:EnableRegion`
> - `account:DisableRegion`
> - `account:GetRegionOptStatus`

- account:ListRegions

これらの個々のアクセス許可を使用する場合、一部のユーザーにリージョンオプト情報のみを読み取る機能を付与し、他のユーザーに読み書きの両方の機能を付与できます。

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された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。

同じコマンドを使用してリージョンを無効にし、 を enable-regionに置き換えることもできますdisable-region。

```
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**
>
> 組織は、一度に最大 20 のリージョンリクエストしか持つことができません。それ以外の場合は、 を受け取りますTooManyRequestsException。

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、リクエストの最新の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"
  }
```

AWS アカウントエイリアスを作成または更新する

IAM ユーザーの URL に AWS アカウント ID の代わりに会社名 (easy-to-remember または別の識別子) を含めたい場合は、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 アカウントエイリアスの作成、削除、一覧表示」を参照してください。

請求の請求AWS アカウント

請求関連の手続きおよびタスクについては、AWS アカウントについては、の次のトピックを参照してください。AWS Billing and Cost Managementユーザーガイド:

- 請求の支払いに使用する通貨の変更
- 税登録番号の更新と削除
- 税設定の継承の有効化

インドのアカウント管理

新規にサインアップする場合AWS アカウントそして、連絡先にインドを選択してください。ユーザー同意書はAmazon Internet Services Private Limited(AISPL)、ローカルAWSIndia.aispl の出品者が請求を管理し、請求書の合計金額は米ドル (USD) ではなくインドルピー (INR) で表示されます。AISPL でアカウントを作成した後で、連絡先情報の国を変更することはできません。

住所がインドの既存の AWS アカウント がある場合、アカウントの販売者は、アカウントを開いた時期に応じて AWS または AISPL のいずれかとなります。アカウントの販売者が AWS と AISPL のどちらであるか確認するには、「Determining which company your account is with」の手順を参照してください。既存の AWS カスタマーは、引き続き AWS アカウント を使用することができます。AWS アカウント と AISPL アカウントの両方を持つこともできますが、それらを同じ AWS 組織に統合することはできません AWS アカウント アカウントを管理する方法の詳細については、「管理してくださいAWS アカウント」を参照してください。

アカウントの販売者が AISPL である場合、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、AISPL アカウントにサインアップし、AISPL アカウントに関する情報を編集して、Permanent Account Number (PAN) の追加、編集を行う方法について説明します。

サインアップ中のクレジットカードの確認プロセスの一環として、AISPL からクレジットカードに 2 インドルピー (INR) が課金されます。2 INR は、確認完了後に AISPL より返金されます。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

- アカウントがどの会社か確認しましょう
- 作成AWS アカウントAISPL と
- AISPL アカウントを管理する

アカウントがどの会社か確認しましょう

AWS のサービスは、AWS と AISPL の両方から提供されます。アカウントに関連する販売者を判別するには、次の手順を使用します。

AWS Management Console

アカウントに関連する企業を判断するには

> **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。
>
> - この手順では、特別な権限は必要ありません。

1. AWS Management ConsoleAWS Management Console で、を開きます。
2. フッターページで、著作権表記に注目します。著作権が Amazon Web Services を対象にしている場合、アカウントの販売者は AWS です。著作権が Amazon Internet Services Private Ltd. を対象にしている場合、アカウントは AISPL に関連しています。

AWS CLI & SDKs

このタスクは AWS CLI 内でも AWS SDK のいずれかによる API 操作でもサポートされません。このタスクは、AWS Management Console を使用してのみ実行できます。

作成AWS アカウントAISPL と

Ltd (AISPL) はインドの地元 AWS 販売者です。連絡先住所がインドにある場合、AISPL アカウントにサインアップするには、以下の手順を使用します。

AWS Management Console

AISPL にサインアップしてアカウントを作成するには

> **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。

- この操作は AWS アカウント がなくても発生するので、この操作に AWS アクセス許可は必要ありません。

1. AWS Management Console を開いて [Sign In to the Console] (コンソールにサインイン) を選択します。
2. [Sign In] (サインイン) ページで、使用したいメールアドレスを入力します。
3. メールアドレスの下で [I am a new user] (新しいユーザーです) を選択して、[Sign in using our secure server] (安全なサーバーを使用してサインイン) を選択します。
4. 各ログイン認証情報フィールドに情報を入力し、[Create account] (アカウントの作成) を選択します。
5. 各連絡先情報フィールドに情報を入力します。
6. カスタマーアグリーメントの内容を読み、諸条件のチェックボックスをオンにして、[Create Account and Continue] (アカウントを作成して続行) を選択します。
7. [Payment Information] (支払い情報) ページで、使用する支払い方法を入力します。
8. [PAN Information] で、Permanent Account Number (PAN) がないか、後で追加する場合は、[No] を選択します。PAN があり、今すぐ追加する場合は、[Yes] (はい) を選択し、PAN] フィールドに PAN を入力します。
9. [Verify Card and Continue] (カードを検証して続行) を選択します。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。確認プロセスの一環として、AISPL からカードに 2 インドルピー (INR) が請求されます。2 INR は、確認完了後に AISPL より返金されます。
10. [Provide a telephone number] (電話番号の入力) に電話番号を入力します。内線番号がある場合は、[Ext] (内線) に内線番号を入力します。
11. [Call Me Now] を選択します。しばらくすると、4 桁の PIN が画面に表示されます。
12. AISPL からの自動呼び出しに応答します。電話のキーパッドで、画面に表示された 4 桁の PIN を入力します。
13. 自動呼び出しで連絡先の番号が確認されたら、[Continue to Select Your Support Plan] を選択します。
14. [Support Plan] (サポートプラン) ページで、サポートプランを選択し、[Continue] (続行) を選択します。支払い方法が確認され、アカウントがアクティブになると、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。

AWS CLI & SDKs

このタスクは AWS CLI 内でも AWS SDK のいずれかによる API 操作でもサポートされません。このタスクは、AWS Management Console を使用してのみ実行できます。

AISPL 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。管理してくださいAWS アカウント を参照してください。

AWS Management Console を使用して、次のタスクを実行できます。

- 永久口座番号 (PAN) の追加または編集
- 複数の永久口座番号 (PAN) の編集
- 複数の物品サービス税番号 (GST) の編集
- 税金の請求書を表示する

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、このセクションの指示に従っていつでも を閉じることができます。閉鎖後、アカウントを閉鎖した日から 90 日以内に再度開くことができます。アカウントを閉鎖した日から がアカウントを完全に閉鎖するまで AWS の時間間隔は、閉鎖後期間 と呼ばれます。

アカウントを閉鎖する前に知っておくべきこと

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。

- アカウントの解約は、このアカウントのカスタマーアグリーメントの終了 AWS 通知として機能します。
- リソースを閉じる AWS アカウント 前に、 のリソースを削除する必要はありません。ただし、保持するリソースまたは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、そのサービスに適したAWS ドキュメントを参照してください。
- 閉鎖後期間 の間にアカウントを再度開くことができます。アカウント内に残っているサービスの料金は、再度開くと再開されます。また、未払いの請求書、未払いのリザーブドインスタンスおよび Savings Plans引き続き責任を負います。

- お客様は、アカウント閉鎖前に消費されたサービスに対する未払いの料金と料金をすべて負担します。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 日の間に発生した使用料の請求書が 2 月初めに届きます。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てから有効期限が切れるまで引き続き受け取ります。 Savings Plans
- アカウントで以前に利用可能な AWS サービスにアクセスできなくなります。ただし、閉鎖後の AWS アカウント 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、過去の請求情報の表示、アカウント設定へのアクセス、または への問い合わせのみですAWS Support。
- 閉鎖 AWS アカウント 時に に登録されたのと同じ E メールアドレスを、別の のプライマリ E メールとして使用することはできません AWS アカウント。別の に同じ E メールアドレスを使用する場合は AWS アカウント、閉鎖前に更新することをお勧めします。E メールアドレスの更新手順ルートユーザー AWS アカウント の名前、E メールアドレス、またはパスワードを更新するについては、「」を参照してください。
- ルートユーザー で AWS アカウント 多要素認証 (MFA) を有効にしている場合、または IAM ユーザー で MFA デバイスを設定している場合、アカウントを閉鎖しても MFA は自動的に削除されません。閉鎖後 90 日間に MFA を有効にしたままにする場合は、その間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のままにします。ハードウェア TOTP トークンデバイスは、アカウントの永続的な閉鎖後に他のユーザーに関連付けることはできません。後で別のユーザーでハードウェア TOTP トークンを使用する場合は、アカウントを閉鎖する前にハードウェア MFA デバイスを非アクティブ化することができます。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すると、閉鎖後期間 の後まで、そのアカウント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、「閉鎖する前に組織からメンバーアカウントを削除する」を参照してください。
- 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、アカウントの最小閉鎖数は 10 で、最大閉鎖数は 1000 です。Organizations のクォータの詳細については、「 のクォータ AWS Organizations」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。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。
- Route 53 に登録しているドメインは自動的に削除されません。を閉じる前に AWS アカウント、次の 4 つのオプションがあります。
  - 自動更新を無効にすると、登録期間が有効期限切れになったときにドメインが削除されます。詳細については、Amazon Route 53 デベロッパーガイドの「ドメインの自動更新の有効化または無効化」を参照してください。
  - ドメインを別の AWS アカウントに移管できます。詳細については、「異なる AWS アカウントへのドメインの移管」を参照してください。
  - ドメインを別のドメインレジストラに移管できます。詳細については、「Route 53 から別のレジストラへのドメインの移管」を参照してください。
  - アカウントをすでに閉鎖している場合は、 でケースを開いて AWS Supportドメインの移管に役立てることができます。
- 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、AWS アカウントを閉鎖する前にアカウント内の証跡を明示的に削除しない限り、 AWS アカウントを閉鎖した後も引き続き存在し、イベントを配信します。この動作は、管理アカウントまたは委任された管理者によって作成された組織証跡や、組織のメンバーアカウントで作成されたマルチリージョンの組織証跡にも適用されます。詳細については、「 CloudTrail ユーザーガイド」のAWS 「アカウント閉鎖と証跡」を参照してください。

アカウントを閉鎖する方法

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 AWS GovCloud (US)するアカウント [スタンドアロン、メンバー、管理、] 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。

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

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には

1. 閉じる のルートユーザー AWS Management Console 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、アカウントを閉じることはできません。
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、アカウントを閉じる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ます) を入力して、アカウント閉鎖プロセスを読み、理解したことを確認します。
5. アカウントを閉じる 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示す確認メールが届きます。

> **Note**
>
> このタスクは、 AWS CLI または AWS SDKs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 Management Console。

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解約するには

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の名前を探し、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。一括請求モードの組織は、コンソールで閉じるボタンを表示できません。一括請求モードでアカウントを解約するには、スタンドアロンアカウントタブのステップに従う必要があります。

4. アカウント閉鎖ガイダンスを読み、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、アカウントを閉じる を選択してアカウント閉鎖プロセスを開始します。

アカウントページからメンバーアカウントを閉鎖するには

オプションで、 のアカウントページから AWS メンバーアカウントを直接閉鎖できます AWS Management Console。 step-by-step 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指示に従ってください。

AWS CLI および SDKs を使用してメンバーアカウントを解約するには

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 、 の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**
> コンソールから AWS Organizations 管理アカウントを直接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には

1. 閉鎖する管理アカウントのルートユーザー AWS Management Console 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、アカウントを閉じることはできません。
2. 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がアカウント名のSuspended横に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、次のステップに進む前に、メンバーアカウントタブに記載されているアカウント閉鎖ガイダンスに従う必要があります。
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、アカウントを閉じる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ます) を入力して、アカウント閉鎖プロセスを読み、理解したことを確認します。
6. アカウントを閉じる 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示す確認メールが届きます。

> **Note**
>
> このタスクは、 AWS CLI または AWS SDKs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 Management Console。

AWS GovCloud (US) account

AWS GovCloud (US) アカウントは、請求および支払い AWS アカウント の目的で常に単一の標準にリンクされます。

AWS GovCloud (US) アカウントを解約するには

AWS GovCloud (US) アカウントにリンク AWS アカウント されている がある場合は、アカウントを閉鎖する前に標準アカウントを AWS GovCloud (US) 閉鎖する必要があります。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。

アカウントを閉鎖した後の予定

アカウントを閉鎖した直後に、次のことが発生します。

- アカウントの閉鎖を確認するメールがルートユーザーの E メールアドレスに送信されます。この E メールが数時間以内に届かない場合は、「」を参照してください閉鎖に関する問題の AWS アカウント トラブルシューティング。
- 閉鎖したメンバーアカウントには、 AWS Organizations コンソールのアカウント名の横にSUSPENDEDラベルが表示されます。
- の のサービスに他の アカウントにアクセス AWS アカウント するためのアクセス許可を付与している場合、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。

閉鎖後期間

閉鎖後期間は、アカウントを閉鎖した日から が AWS を完全に閉鎖するまでの時間を指します AWS アカウント。閉鎖後期間は 90 日間です。閉鎖後期間中は、アカウントを再度開くことによってのみコンテンツと 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。また 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。アカウントが完全に閉鎖されると、その AWS アカウント ID は再利用できなくなります。

の再開 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、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) できるだけ早く に連絡しAWS Support、(2) アカウントの閉鎖日から 60 日以内に、請求書に指定されている必須情報の提供を含め、未払い残高の全額を受け取る必要があります。

> **Note**
>
> アカウント内に残っているサービスの料金は、再度開くと再開されます。

組織内の AWS 管理アカウントの使用

AWS Organizations は AWS アカウント をグループとして管理するための 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。AWS Organizations の詳細については、「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と、組織のほとんどの管理タスクを組織の管理アカウントだけで実行できるようになります。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。この追加機能を他の AWS サービスに拡張するには、組織とそのサービスの間の信頼されたアクセスを有効にします。信頼されたアクセスは、指定した AWS サービスに対して、組織とそこに含まれるアカウントに関する情報へのアクセス権を付与するものです。アカウント管理のトラステッド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とその管理アカウントに、組織のすべてのメンバーアカウントの主要連絡先情報や代替連絡先情報などのメタデータにアクセスする権限を付与します。

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後、メンバーアカウントのいずれかを 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可能です。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、「に対する委任管理者アカウントの有効化AWSアカウント管理」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 AWS Organizations で管理される組織の一部である場合、組織の管理者はサービスコントロールポリシー (SCP)を適用して、メンバーアカウントのプリンシパルの権限を制限できます。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。

AWS アカウント に適用される SCP の例については、「AWS Organizations サービスコントロールポリシーによるアクセスの制限」を参照してください。

AWS アカウント管理用の信頼されたアクセスを有効にする

AWSアカウント管理へのトラステッド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（たとえば、主要連絡先または代替連絡先の詳細）を変更できます。AWS Organizations詳細については、「AWSアカウント管理」と AWS Organizations「AWS Organizationsユーザーガイド」を参照してください。トラステッドアクセスの仕組みに関する一般的な情報については、「AWS OrganizationsAWS他のサービスとの併用」を参照してください。

トラステッドアクセスを有効にすると、それをサポートするアカウント管理 API `accountID` オペレーションでパラメータを使用できます。このパラメータを正常に使用できるのは、管理アカウントからの認証情報、または組織の委任管理者アカウント（有効にしている場合）からの認証情報を使用して操作を呼び出した場合のみです。詳細については、「に対する委任管理者アカウントの有効化AWSアカウント管理」を参照してください。

以下の手順に従って、組織内のアカウント管理の信頼できるアクセスを有効にします。

> 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 Management Console

AWSアカウント管理への信頼できる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できるアクセスを有効にする」ダイアログボックスで、「enable」と入力して確認し、「信頼できるアクセスを有効にする」を選択します。

AWS CLI & SDKs

AWSアカウント管理への信頼できるアクセスを有効にするには

次のコマンドを実行すると、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 API オペレーションを呼び出すことができます。

- AWS CLI: enable-aws-service-access

  次の例では、呼び出し側アカウントの組織内の AWS アカウント管理用に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。

に対する委任管理者アカウントの有効化AWSアカウント管理

委任された管理者アカウントは、AWS組織内の他のメンバーアカウントのアカウント管理 API オペレーション。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指定するには、以下の手順に従います。

> **最小限必要なアクセス権限**
>
> 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。
>
> - この処理は、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。
> - 必要なもの組織内のアカウント管理で信頼されたアクセスを有効にする。

組織の委任管理者アカウントを指定した後、そのアカウントのユーザおよびロールはAWS CLIそしてAWSの SDK オペレーションaccountオプションをサポートすることで、Organizations モードで動作できる名前空間AccountIdパラメータ。

AWS Management Console

このタスクは、AWSアカウントマネジメントコンソール。このタスクは、AWS CLIまたは、いずれかの API オペレーションAWSSDK。

AWS CLI & SDKs

アカウント管理サービスに委任された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、アカウントマネジメントサービスの委任管理者を有効にすることができます。

以下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:委任された管理者の登録

  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
  ```

  このコマンドが成功した場合、出力は生成されません。

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

AWS Organizations サービスコントロールポリシーによるアクセスの制限

このトピックでは、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で実行できる操作を制限する方法を説明します。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。

```
{
    "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。

```
{
    "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。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": "account:PutAlternateContact",
            "Resource": [
                "arn:aws:account::*:account"
            ],
            "Condition": {
                "ForAnyValue:StringLike": {
                    "account:AccountResourceOrgPath": [
                        "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/",
                        "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/"
                    ]
                }
            }
    ]
```

```
}
```

セキュリティAWSアカウント管理

AWSでは、クラウドのセキュリティが最優先事項です。AWSのお客様は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャから利点を得られます。

セキュリティは、AWSとお客様の間の共有責任です。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、AWS で AWS クラウド サービスを実行するインフラストラクチャを保護する責任を負います。また、AWS は、使用するサービスを安全に提供します。AWS コンプライアンスプログラム[g11]AWSコンプライアンスプログラム[/g11][g10]AWSコンプライアンスプログラム[/g10]の一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。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、を参照してください。AWS のサービスコンプライアンスプログラムによる範囲内。
- クラウド内のセキュリティ–お客様の責任は、使用するAWSのサービスに応じて異なります。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、を使用する際に共有責任モデルを適用する方法を理解するのに役立ちます。AWSアカウント管理。ここでは、セキュリティとコンプライアンスの目標を満たすようにアカウント管理を設定する方法を説明します。また、他の使用方法についても説明します。AWS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のサービス。

トピックス

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

AWS アカウント管理でのデータ保護

AWS 責任共有モデルは、AWS アカウント管理で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、AWS クラウド のすべて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を負います。顧客は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービスのセキュリティ設定と管理タスクにも責任があります。データプライバシーの詳細については、データプライバシーのよくある質問を参照してください。欧州でのデータ保護の詳細については、「AWS セキュリティブログ」に投稿された「AWS 責任共有モデルおよび GDPR」のブログ記事を参照してください。

データを保護するため、AWS アカウント の認証情報を保護し、AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーをセットアップすることをお勧めします。こうすると、それぞれのジョブを遂行するために必要なアクセス許可のみを各ユーザーに付与できます。また、次の方法でデータを保護することをお勧めします。

- 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 および TLS 1.3 をお勧めします。
- AWS CloudTrail で API とユーザーアクティビティログをセットアップします。
- AWS のサービス 内でデフォルトである、すべてのセキュリティ管理に加え、AWS の暗号化ソリューションを使用します。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API を使用して AWS にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

顧客のメールアドレスなどの機密情報やセンシティブ情報は、タグや 名前 フィールドなどの自由形式のフィールドに配置しないことを強くお勧めします。これには、コンソール、API AWS CLI、または AWS SDK AWS のサービス を使用してアカウント管理やその他のユーザーを操作する場合も含まれます。名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーに 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にとってAWSアカウント管理

Amazon Virtual Private Cloud (Amazon VPC) を使用してホストする場合AWSリソースの場合、AWS パブリックインターネットを経由することなく VPC 内からアカウント管理サービス。

Amazon VPC を使用すると、カスタム仮想化ネットワークで 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。Amazon 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VPC を他の VPC に接続できますAWSのサービス。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。

エンドポイントの作成

作成できるAWSVPC 内のアカウント管理エンドポイントAWS Management Consoleとすると、AWS Command Line Interface(AWS CLI)、とAWSSDK、AWSアカウント管理 API、またはAWS CloudFormation。

Amazon VPC コンソールまたは AWS CLI 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、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とき、VPC の接続先のサービスとして Account Management を次の形式を使用して指定します。
>
> ```
> com.amazonaws.us-east-1.account
> ```
>
> 文字列は、示されているとおりに正確に使用する必要があります。us-east-1リージョン。グローバルサービスとして、アカウント管理はそのサービスでのみホストされます。AWS リージョン。

AWS CloudFormation 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 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 エンドポイントのポリシー

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添付することで、複雑な IAM ルールを作成できます。詳細については、以下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
- VPC エンドポイントによるサービスのアクセスコントロールのAWS PrivateLinkGuide。

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

アカウント管理用の Amazon VPC エンドポイントポリシーを作成できます。このポリシーでは以下を指定します。

- 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、任意の代替連絡先情報の取得と変更の両方を許可する Amazon VPC エンドポイントのポリシーを示しています。AWS アカウント。ただし、すべて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。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "account:GetAlternateContact",
                "account:PutAlternateContact"
            ],
            "Resource": "arn:aws::iam:*:account,
            "Effect": "Allow",
            "Principal": {
              "AWS": "arn:aws::iam:123456789012:user/Alice"
```

```
            }
        },
        {
            "Action": "account:DeleteAlternateContact",
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "arn:aws::iam:*:root"
        }
    ]
}
```

の一部であるアカウントへのアクセスを許可する場合AWSOrganization を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設定し、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の詳細については、「」を参照してください。VPC エンドポイントによるサービスのアクセスコントロールのAWS PrivateLinkGuide。

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 AWS のサービス 使用できる です。

トピック

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- 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 アカウント管理でのアイデンティティベースのポリシー (IAM ポリシー) の使用
- AWS アカウント管理のアイデンティティとアクセスのトラブルシューティング

対象者

AWS Identity and Access Management (IAM) の使用方法は、アカウント管理で行う作業によって異なります。

サービスユーザー - コスト管理サービスを使用してジョブを実行する場合は、必要なアクセス許可と認証情報を管理者が用意します。業務に際してさらに多くのアカウント管理機能を使用しようとすると、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。アカウント管理機能にアクセスできない場合、「AWS アカウント管理のアイデンティティとアクセスのトラブルシューティング」を参照してください。

サービス管理者 - 社内のアカウント管理リソースを担当している場合は、通常、アカウント管理へのフルアクセスがあります。サービスユーザーがどのアカウント管理機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。社内でアカウント管理と IAM を併用するには、「AWS アカウント管理と IAM の連携方法」を参照してください。

IAM 管理者 – IAM 管理者である場合は、アカウント管理へのアクセスを管理するポリシーの作成方法の詳細について理解しておくことをお勧めします。IAM で使用できるアカウント管理 ID ベースのポリシーの例を表示するには、「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。

アイデンティティを使用した認証

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

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

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

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

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

AWS アカウント ルートユーザー

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

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、一時的な認証情報を使用して にアクセスするための ID プロバイダーとのフェデレーションの使用を要求 AWS のサービス します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、アイデンティティセンターディレクトリ、または ID ソースを通じて提供された認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッド ID が にアクセスすると AWS アカウント、ロールが引き受けられ、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成することも、独自の ID ソース内のユーザーとグループのセットに接続して同期して、すべての AWS アカウント とアプリケーションで使用することもできます。IAM Identity Center の詳細については、「AWS IAM Identity Center ユーザーガイド」の「What is IAM Identity Center?」(IAM Identity Center 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、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、IAM ユーザーガイドの長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションするを参照してください。

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

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

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。ロール を切り替える AWS Management Console ことで、 で IAM ロールを一時的に引き受けることができます。ロールを引き受けるには、 または AWS API AWS CLI オペレーションを呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの使用」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションの詳細については、「IAM ユーザーガイド」の「Creating a role for a third-party Identity Provider」(サードパーティーアイデンティティプロバイダー向けロールの作成) を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスでき

るものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「アクセス許可セット」を参照してください。

- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、(ロールをプロキシとして使用する代わりに) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。
- クロスサービスアクセス — 一部の は、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリーム サービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。
  - サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。 AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、IAM ユーザーガイドのAmazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与するを参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、IAM ユーザーガイドの(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか?を参照してください。

ポリシーを使用したアクセスの管理

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

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

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

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

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデ

ンティティベースのポリシーを作成する方法については、IAM ユーザーガイドのIAM ポリシーの作成を参照してください。

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

リソースベースのポリシー

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

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

アクセスコントロールリスト (ACL)

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

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

その他のポリシータイプ

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

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。

エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、IAM ユーザーガイドのIAM エンティティのアクセス許可の境界を参照してください。

- サービスコントロールポリシー (SCPs) – SCPs は、 の組織または組織単位 (OU) に対する最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、 AWS アカウント ビジネスが所有する複数の をグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、AWS Organizations ユーザーガイドの「SCP の仕組み」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、IAM ユーザーガイドのセッションポリシーを参照してください。

複数のポリシータイプ

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

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	Yes
ポリシー条件キー	Yes
ACL	なし
ABAC (ポリシー内のタグ)	はい
一時的な認証情報	あり
プリンシパル権限	あり
サービスロール	いいえ
サービスリンクロール	なし

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を把握するには、「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ポリシーをサポートする	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のポリシーを作成する方法については、IAM ユーザーガイドのIAM ポリシーの作成を参照してください。

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。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。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制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、アカウント全体、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。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる にある場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。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に対するサポート	あり

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

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

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

アカウント管理アクションのリストを確認するには、「サービス認証リファレンス」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。例えば、 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

ポリシーリソースに対するサポート	あり

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

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

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

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

アカウント管理サービスは、IAM ポリシーの Resources要素で以下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の 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 アカウント 、 AWS Organizations サービスによって管理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のタイプとその ARNs」のAWS 「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。 どのアクションで各リソースの ARN を指定できるかについては、「 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 AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。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することで、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。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、IAM ユーザーガイドのIAM ポリシーの要素: 変数およびタグを参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。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。

- アカウント：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。

- アカウント：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。

- アカウント：AccountResourceOrgPaths

  この条件キーは、組織内のアカウントを表すワイルドカードを持つ ARN 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 ARN を持つアカウントをターゲットと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。例えば、次の ARN は、指定した組織および指定された組織単位 (OU) のアカウントのみに一致します。

  ```
  arn:aws:account::111111111111:ou/o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*
  ```

- アカウント：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。

アカウント管理条件キーのリストを確認するには、「サービス認証リファレンス」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許可を持つかをコントロールします。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

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 のサポート (ポリシー内のタグ)	はい

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アクセス許可戦略です。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。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、IAM ユーザーガイドのABAC とは?を参照してください。ABAC をセットアップするステップを説明するチュートリアルについては、IAM ユーザーガイドの「属性ベースのアクセスコントロール (ABAC) を使用する」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

一部の AWS のサービス は、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報 AWS のサービス を使用する などの詳細については、IAM ユーザーガイドのAWS のサービス「IAM と連携する 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社の Single Sign-On (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、IAM ユーザーガイドのロールへの切り替え (コンソール)を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用して . AWS recommends にアクセスできます AWS。これは、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推奨しています。詳細については、IAM の一時的セキュリティ認証情報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

フォワードアクセスセッション (FAS) をサポート	あり

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

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	いいえ

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 のサービスにアクセス許可を委任するロールの作成」を参照してください。

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。

サービスリンク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。表の中から、[Service-linked role] (サービスにリンクされたロール) 列に Yes と記載されたサービスを見つけます。サービスリンク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、ユーザーと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はありません。また、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

これらサンプルの 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 ポリシーの作成を参照してください。

各リソースタイプの ARNs」のAWS 「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

- ポリシーのベストプラクティス
- のアカウントページの使用 AWS Management Console
- 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 Management Console
- のアカウントページへのフルアクセスを提供する AWS Management Console

ポリシーのベストプラクティス

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

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

- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイドのIAM でのポリシーとアクセス許可を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、 などの特定の を通じてサービスアクションが使用される場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素:条件) を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイドのIAM Access Analyzer ポリシーの検証を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイドのMFA 保護 API アクセスの設定を参照してください。

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

のアカウントページの使用 AWS Management Console

のアカウントページにアクセスするには AWS Management Console、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、エンティティに `AWSAccountManagementReadOnlyAccess`または `AWSAccountManagementFullAccess` AWS 管理ポリシーを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許可の追加を参照してください。

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

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 Management Console

次の例では、 のアカウントページへの読み取り専用アクセスを IAM ユーザーに付与します AWS アカウント AWS Management Console。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、アカウントページでほとんどの設定を表示するアクセスを許可します。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。

```
{
    "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を提供する AWS Management Console

次の例では、 のアカウントページへのフルアクセスを IAM ユーザーに付与します AWS アカウント AWS Management Console。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。

このポリシー例では、使用可能な各書き込みアクセス許可 (を除く CloseAccount) を追加することで、前述のポリシーの例に基づいて構築されます。これにより、ユーザーは `account:EnableRegion`および アクセス`account:DisableRegion`許可を含むアカウントのほとんどの設定を変更できます。

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

AWS アカウント管理でのアイデンティティベースのポリシー (IAM ポリシー) の使用

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

カスタマーマネージド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「カスタマーマネージドポリシーの編集 (コンソール)」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を許可するアクセス許可をまとめたものです。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 「アカウント管理ポリシーの例」を参照してください。

> **Note**
>
> IAM ユーザーに のアカウントページの特定のアカウント設定への書き込みアクセスを許可するには AWS Management Console、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)	利用可能なリージョンを一覧表示するアクセス許可を付与します。
account:GetAccountInformation	読み取り	アカウントのアカウント情報を取得するアクセス許可を付与します。
account:GetAlternateContact	読み取り	アカウントの代替連絡先を取得するアクセス許可を付与します。
account:GetChallengeQuestions	読み取り	アカウントのチャレンジ質問を取得するアクセス許可を付与します。
account:GetContactInformation	読み取り	アカウントのプライマリ連絡先情報を取得するアクセス許可を付与します。
account:GetRegionOptStatus	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アクセス許可を付与します。
account:AcceptPrimaryEmailUpdate	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
		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:PutChallengeQuestions	書き込み	アカウントのチャレンジ質問を変更する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:PutContactInformation	書き込み	アカウントのプライマリ連絡先情報を更新する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 アカウント管理のアイデンティティとアクセスのトラブルシューティング

以下の情報は、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。

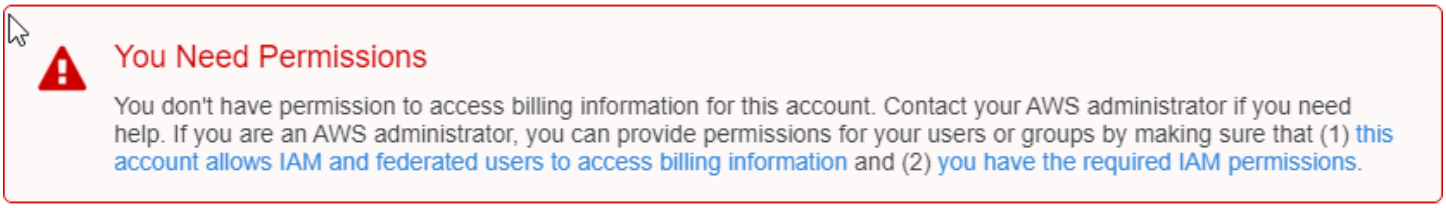
トピック

- アカウントページでアクションを実行する権限がない
- 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アクションを実行する権限がない

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

次の例のエラーは、IAM ユーザーがコンソールを使用して `mateojackson` 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 AWS Management Console しても、 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` アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新してアカウント管理にロールを渡すことができるようにする必要があります。

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

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権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

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

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

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

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でのロールとリソースベースのポリシーの使用の違いについては、IAM ユーザーガイドの「IAM でのクロスアカウントリソースアクセス」を参照してください。

AWS アカウント管理用の AWS マネージドポリシー

現在、AWS アカウント管理には 2 つの AWS マネージドポリシーが用意されています。

- AWS マネージドポリシー: AWSAccountManagementReadOnlyAccess
- AWS マネージドポリシー: AWSAccountManagementFullAccess
- アカウント管理の AWS マネージドポリシーの更新

AWS マネージドポリシーは、AWS が作成および管理するスタンドアロンポリシーです。AWS マネージドポリシーは、多くの一般的なユースケースでアクセス許可を提供できるように設計されているため、ユーザー、グループ、ロールへのアクセス許可の割り当てを開始できます。

AWS マネージドポリシーは、ご利用の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ご注意ください。AWS のすべてのお客様が使用できるようになるのを避け

るためです。ユースケース別にカスタマー管理ポリシーを定義することで、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義したアクセス権限は変更できません。AWS が AWS マネージドポリシーに定義されているアクセス許可を更新すると、更新はポリシーがアタッチされているすべてのプリンシパルアイデンティティ (ユーザー、グループ、ロール) に影響します。新しい AWS のサービスを起動するか、既存のサービスで新しい API オペレーションが使用可能になると、AWS が AWS マネージドポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の「AWS 管理ポリシー」を参照してください。

AWS マネージドポリシー: AWSAccountManagementReadOnlyAccess

`AWSAccountManagementReadOnlyAccess` ポリシーは IAM ID 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。

- AWS アカウント に関するメタデータ
- AWS アカウント について有効または無効になっている AWS リージョン (アカウント内のリージョンのステータス表示は AWS コンソールでのみ可能)

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 の有効と無効を切り替える機能は提供されません。

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 AWS アカウント に関するメタデータ情報を取得できるようにします。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 Management Console を一覧表示できます。

```
{
    "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。

- AWS アカウント に関するメタデータ
- AWS リージョン について有効または無効になっている AWS アカウント (自分のアカウントについてのリージョンのステータス表示または有効と無効の切り替えは AWS コンソールでのみ可能)

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。

許可の詳細

このポリシーには、以下の許可が含まれています。

- account — プリンシパルが AWS アカウント に関するメタデータ情報を表示できるようにします。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 Management Console 内でそれらの有効と無効を切り替えることができます。

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

アカウント管理の AWS マネージドポリシーの更新

アカウント管理用の AWS マネージドポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始した以降の分について表示します。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
新しい AWS マネージドポリシーを伴う AWS アカウント管理が発表され、変更の追跡が開始されました	発表当時のアカウント管理には以下の AWS マネージドポリシーがありました。 • 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

複数の AWS コンプライアンスプログラムの一環として、AWS アカウント で実行できる AWS サービスのセキュリティおよびコンプライアンスは、サードパーティーの監査者により評価されます。具体的には、SOC、PCI、FedRAMP、HIPAA、その他があります。

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

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

AWS アカウント の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は、データの機密性、企業のコンプライアンス目的、適用法規によって決まります。AWS ではコンプライアンスに役立つ以下のリソースを用意しています。

- セキュリティとコンプライアンスのクイックスタートガイド — これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境を AWS にデプロイするためのステップを示します。

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

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

- AWS コンプライアンスのリソース– このワークブックおよびガイドのコレクションは、顧客の業界と拠点に適用されるものである場合があります。
- 「AWS Config デベロッパーガイド」の「ルールでのリソースの評価」 — AWS Config のサービスでは、自社のプラクティス、業界ガイドライン、および規制に対するリソースの設定の準拠状態を評価します。
- AWS Security Hub — この AWS のサービス では、AWS 内のセキュリティ状態が包括的に示されており、セキュリティ業界の標準およびベストプラクティスへの準拠の確認に役立ちます。
- AWS Audit Manager - この AWS のサービス は AWS の使用状況を継続的に監査し、リスクの管理方法やコンプライアンスを業界スタンダードへの準拠を簡素化するために役立ちます。

での耐障害性AWSアカウント管理

-AWSのグローバルインフラストラクチャは構築されますAWS リージョンのアベイラビリティーゾーン。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、耐障害性、および拡張性が優れています。

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

AWS Account Management でのインフラストラクチャセキュリティ

マネージドサービスとして、AWSAWS アカウントAWSユーザーで実行されているサービスはグローバルネットワークセキュリティによって保護されます。AWSセキュリティサービスと AWS がインフラストラクチャを保護する方法については、「AWS クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「セキュリティの柱 - AWS Well-Architected Framework」の「インフラストラクチャ保護」を参照してください。

AWS公開されている API 呼び出しを使用して、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 および TLS 1.3 をお勧めします。
- DHE (Ephemeral Diffie-Hellman) や ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートです。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

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

AWS アカウント管理のモニタリング

モニタリングは、AWS アカウント管理とその他の 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うえで重要な部分です。AWS には、アカウント管理を監視し、問題の発生時に報告し、必要に応じて自動アクションを実行できるように、以下のモニタリングツールが用意されています。

- AWS CloudTrail は、AWS アカウント またはその代行によって発生した API コールや関連イベントを取得し、指定した Amazon Simple Storage Service (Amazon S3) バケットにログファイルを配信します。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対応することで、AWSサービスをさらに自動化します。AWSサービスからのイベントは、 EventBridge ほぼリアルタイムでに配信されます。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。

ログ記録AWSを使用したアカウント管理 API 呼び出しAWS CloudTrail

-AWSアカウント管理 API は、AWS CloudTrailは、ユーザー、ロール、またはによって実行されたアクションの記録を提供するサービスです。AWSアカウント管理オペレーションを呼び出すサービス。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、アカウント管理オペレーションへのすべての呼び出しが含まれます。証跡を作成する場合は、アカウント管理オペレーションのイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。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、アカウント管理オペレーションを呼び出したリクエスト、リクエストに使用した IP アドレス、リクエストしたユーザーとそのタイミング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

CloudTrail は、AWS アカウントアカウント作成時に使用されます。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、他の CloudTrail イベントとともにそのアクティビティを CloudTrail イベントに記録します。AWSのサービスイベントイベント履歴。最近のイベントは、AWS アカウント で表示、検索、ダウンロードできます。詳細については、CloudTrail イベント履歴でのイベントの表示を参照してください。

のイベントの継続的な記録についてはAWS アカウントには、アカウント管理のオペレーションのイベントなど、証跡を作成します。追跡により、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きに使用されます。AWS Management Consoleとすると、トレイルはすべての人に当てはまります。AWS リージョン。追跡は、AWS パーティションのすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。その他の AWS のサービスを設定して、CloudTrail ログで収集されたイベントデータをより詳細に分析し、それに基づく対応を行うことができます。詳細については、以下を参照してください:

- 証跡を作成するための概要
- CloudTrail でサポートされるサービスと統合
- CloudTrail の Amazon SNS 通知の設定
- 複数のリージョンからの CloudTrail ログファイルの受信
- 複数のアカウントからの CloudTrail ログファイルの受信

AWS CloudTrailで検出されたすべてのアカウント管理 API オペレーションをログに記録します。API リファレンスこのガイドの「」セクションについて説明します。例えば `CreateAccount`、`DeleteAlternateContact`、`PutAlternateContact` の各演算へのコールは、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、リクエストの生成者に関する情報が含まれます。同一性情報は以下の判断に役立ちます:

- リクエストが、ルートユーザーと、ルートユーザーとのどちらを使用して送信されたかAWS Identity and Access Management(IAM) ユーザー認証情報
- 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 のサービスによって送信されたかどうか

詳細については、CloudTrail userIdentity 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

追跡は、指定したAmazon S3バケットにイベントをログファイルとして配信するように設定できるものです。CloudTrailのログファイルには、単一か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ー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: への呼び出しの CloudTrail ログエントリの例を以下に示します。GetAlternateContact現在の値を取得するオペレーションOPERATIONSアカウントの代替連絡先。オペレーション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: への呼び出しの CloudTrail ログエントリの例を以下に示します。PutAlternateContact新しいを追加するための操作BILLINGアカウントの代替連絡先。

```
{
  "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: への呼び出しの CloudTrail ログエントリの例を以下に示しま
す。DeleteAlternateContact現在のものを削除する操作OPERATIONS代替連絡先。

```
{
  "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"
}
```


によるアカウント管理イベントの監視 EventBridge

Amazon EventBridge（ CloudWatch 以前はイベントと呼ばれていました）は、特定のイベントをモニタリングし、その他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AWS のサービスからのイベントは、 EventBridge ほぼリアルタイムでに配信されます。

を使用すると EventBridge、受信イベントを照合してターゲットにルーティングして処理するルールを作成できます。

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

アカウント管理イベント

以下の例は、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、リージョンと API CloudTrail 呼び出しの有効化と無効化に固有のイベントのみです。

イベントタイプ

- リージョンを有効または無効にするイベント

リージョンを有効または無効にするイベント

コンソールまたは API からアカウントの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、 CloudTrail ターゲットアカウントに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と、どちらかのプロセスが完了すると、EventBridge 呼び出し元のアカウントにイベントが送信されます。

次のイベント例は、「ap-east-1ENABLEDリージョンがアカウント用だった」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123456789012。2020-09-30

```
{
   "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 によって返されるステータスと一致するステータスは 4 つあります。

- ENABLED— 指定されたリージョンの有効化に成功しました accountId
- ENABLING— accountId 指定されたリージョンの有効化が進行中です
- DISABLED— accountId 指定されたリージョンは正常に無効化されました
- DISABLING— accountId 指定のリージョンは無効化処理中です

以下のサンプルイベントパターンでは、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"
   ]
}
```

次のサンプルイベントパターンでは、ENABLEDDISABLED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"
      ]
   }
}
```

API リファレンス

アカウント管理の API 操作 (account) 名前空間を使用すると、AWS アカウント を変更できるようになります。

すべての AWS アカウント 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をサポートします。これらは、に関連付けられている電子メールアドレスに追加されますルートユーザアカウントの。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、AWS Organizations 管理アカウントの ID からこれらの API 操作を呼び出し、組織のメンバーである AWS アカウント の任意のアカウント ID 番号を指定します。

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、さまざまなプログラム言語およびプラットフォームのライブラリやサンプルコード (Java、Ruby、.NET、iOS、Android など)から成るAWSSDK のひとつを使用できます。SDK は、プログラムによる AWS 組織へのアクセス権を作成するのに便利な方法を提供します。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 SDK のダウンロードおよびインストール方法の詳細については、「Amazon Web Services 用ツール」を参照してください。

AWS SDK を使用してアカウント管理サービスへプログラマティックな API 呼び出しを行う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、以下を参照してください。HTTP クエリリクエストを作成して API を呼び出すアカウント管理ユーザーガイドにあります。組織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ています。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

AWS に HTTP リクエストを送る際、AWS が送信元を特定できるよう、リクエストに署名なければなりません。リクエストには、AWS アクセスキーを使用して署名します。このアクセスキーは、アクセスキー ID とシークレットアクセスキーで構成されています。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、管理者権限を持つ IAM ユーザー用のアクセスキーを作成してください。別のオプションとして、AWS セキュリティトークンサービスを使用して、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 を必要とする操作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。

AWS コマンドラインインターフェイス (AWS CLI) または AWS SDK のいずれかを使用して AWS へのリクエストを作成する場合、これらのツールにより、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が署名されます。

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

リクエストに対する応答としてアカウント管理によって返される JSON は、改行や書式空白を含まない単一の長い文字列として返されます。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

アカウント管理サポートCloudTrail、記録するサービスAWSあなたの API コールAWS アカウントログファイルを Amazon S3 バケットに配信します。によって収集された情報を使用してCloudTrail、Account Management へのどのリクエストが正常に行われたか、誰がリクエストを行ったか、いつ実行されたかなどを判断できます。アカウント管理とそのサポートについての詳細CloudTrail、を参照してくださいログ記録AWSを使用したアカウント管理 API 呼び出しAWS CloudTrail。詳しく知るにはCloudTrail有効にする方法やログファイルを見つける方法については、を参照してください。AWS CloudTrailユーザーガイド。

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
- GetAlternateContact
- GetContactInformation
- GetPrimaryEmail
- GetRegionOptStatus
- ListRegions
- PutAlternateContact
- PutContactInformation
- StartPrimaryEmailUpdate

AcceptPrimaryEmailUpdate

指定されたアカウントのプライマリ 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ます) を更新StartPrimaryEmailUpdateするために 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された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の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**
>
> 管理アカウントは独自の を指定できませんAccountId。

型: 文字列

Pattern: ^\d{12}$

必須：はい

Otp

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

型: 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プライマリ E メールアドレス。StartPrimaryEmailUpdate これは API コールPrimaryEmailの と一致する必要があります。

型: 文字列

長さの制限: 最小長は 5。最大長は 64 文字です。

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

受け入れられたプライマリ 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、「共通エラー」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。

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、現在無効になっているリージョン (DISABLING のステータス) を有効にしようとする場合や、アカウントのルートユーザーの E メールを、既に使用されている E メールアドレスに変更しようとする場合に発生します。

HTTP ステータスコード: 409

InternalServerException

の内部エラーのため、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。

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。

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。

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。

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- 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

代替連絡先操作の使用方法については、「代替連絡先にアクセスまたは更新する」を参照してください。

> **Note**
>
> AWS アカウント が管理する代理連絡先情報を更新する前に AWS Organizations、 AWS まずアカウント管理とOrganizations 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

AWS この操作でアクセスまたは変更するアカウントの 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、オペレーションの呼び出しに使用された ID AWS のアカウントがデフォルトになります。

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。

型: 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、「共通エラー」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。

HTTP ステータスコード: 403

InternalServerException

内部エラーにより操作は失敗しました AWS。後でもう一度操作をお試しください。

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。

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。

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。

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

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

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
```

その他の参照資料

言語固有の AWS SDK の 1 つでこの 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
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go バージョン 2 用 SDK
- AWS Java V2 用 SDK
- AWS V3 用 JavaScript SDK
- AWS PHP V3 用SDK
- AWS Python 用 SDK
- AWS ルビー V3 用 SDK

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**
>
> リージョンを無効にすると、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る 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された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**
>
> 管理アカウントは独自の を指定できませんAccountId。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でこのオペレーションを呼び出すには、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。

型: 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、 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 AWS 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リージョンを有効にすることはできません。

型: 文字列

長さの制限：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、「共通エラー」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。

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、現在無効になっているリージョン (DISABLING のステータス) を有効にしようとする場合や、アカウントのルートユーザーの E メールを、既に使用されている E メールアドレスに変更しようとする場合に発生します。

HTTP ステータスコード: 409

InternalServerException

の内部エラーのため、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。

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。

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。

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

EnableRegion

アカウントの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る 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された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**
>
> 管理アカウントは独自の を指定できませんAccountId。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でこのオペレーションを呼び出すには、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。

型: 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数分かかりますが、数時間かかる場合があります。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リージョンを無効にすることはできません。

型: 文字列

長さの制限：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、「共通エラー」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。

HTTP ステータスコード: 403

ConflictException

リソースの現在のステータスに競合があるため、リクエストを処理できませんでした。例えば、現在無効になっているリージョン (DISABLING のステータス) を有効にしようとする場合や、ア

カウントのルートユーザーの E メールを、既に使用されている E メールアドレスに変更しようとする場合に発生します。

HTTP ステータスコード: 409

InternalServerException

の内部エラーのため、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。

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。

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。

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetAlternateContact

に接続されている指定された代替連絡先を取得します。 AWS アカウント

代替連絡先操作の使用方法については、「代替連絡先にアクセスまたは更新する」を参照してください。

> **Note**
>
> AWS アカウント が管理する代理連絡先情報を更新する前に AWS Organizations、 AWS まずアカウント管理とOrganizations 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

AWS この操作でアクセスまたは変更するアカウントの 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、オペレーションの呼び出しに使用された ID AWS のアカウントがデフォルトになります。

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。

型: 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、「共通エラー」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。

HTTP ステータスコード: 403

InternalServerException

内部エラーにより操作は失敗しました AWS。後でもう一度操作をお試しください。

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。

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。

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。

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"
    }
}
```

その他の参照資料

言語固有の AWS SDK の 1 つでこの 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
- AWS SDK for .NET
- AWS SDK for C++
- AWS Go バージョン 2 用 SDK
- AWS Java V2 用 SDK
- AWS V3 用 JavaScript SDK
- AWS PHP V3 用SDK
- AWS Python 用 SDK
- AWS ルビー V3 用 SDK

GetContactInformation

の主要な連絡先情報を取得します AWS アカウント。

主な問い合わせオペレーションの使用方法の詳細については、「主な連絡先情報と代替連絡先情報の更新」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る 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された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**
>
> 管理アカウントは独自の を指定できませんAccountId。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でこのオペレーションを呼び出すには、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。

型: 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

に関連付けられている主な連絡先情報の詳細が含まれます AWS アカウント。

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、「共通エラー」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。

HTTP ステータスコード: 403

InternalServerException

の内部エラーのため、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。

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。

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。

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。

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
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- 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プライマリ 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された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の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**
>
> 管理アカウントは独自の を指定できませんAccountId。

型: 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プライマリ E メールアドレスを取得します。

型: 文字列

長さの制限: 最小長は 5。最大長は 64 文字です。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」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。

HTTP ステータスコード: 403

InternalServerException

の内部エラーのため、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。

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。

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。

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。

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- 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る 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された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**
>
> 管理アカウントは独自の を指定できませんAccountId。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でこのオペレーションを呼び出すには、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。

型: 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すリージョンのステータスを返します。

型: 文字列

長さの制限：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。

型: 文字列

長さの制限：最小長は 1 です。最大長は 50 です。

RegionOptStatus

リージョンが受ける可能性のあるステータスの 1 つ (有効、有効、無効、無効、有効_By_Default)。

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、「共通エラー」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。

HTTP ステータスコード: 403

InternalServerException

の内部エラーのため、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。

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。

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。

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- 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一覧表示します。オプションで、このリストは 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る 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された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**
>
> 管理アカウントは独自の を指定できませんAccountId。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でこのオペレーションを呼び出すには、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。

型: 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合計数。使用可能な項目の合計数が指定された値より大きい場合、コマンドの出力に NextTokenが指定されます。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、「 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 AWS 」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

ページ分割を開始する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レスポンスNextTokenからの です。使用例については、「 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 AWS 」を参照してください。

型: 文字列

長さの制限: 最小長は 0 です。最大長は 1,000 です。

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、有効化、無効化、無効化、有効化_by_default) のリスト。例えば、ENABLING の値を渡すと、ENABLING のリージョンステータスを持つリージョンのリストのみが返されます。

タイプ：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は、入力されます。これは、 のnext-tokenリクエストパラメータに渡される必要がありますlist-regions。

型: 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、またはフィルタリングされたパラメータが使用されている場合は、 filter パラメータで設定されたフィルター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、「共通エラー」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。

HTTP ステータスコード: 403

InternalServerException

の内部エラーのため、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。

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。

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。

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- 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。

代替連絡先操作の使用方法については、「代替連絡先にアクセスまたは更新する」を参照してください。

> **Note**
>
> によって管理 AWS アカウント されている 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。

型: 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。

型: 文字列

長さの制限：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。

型: 文字列

長さの制限：最小長は 1 です。最大長は 64 文字です。

必須：はい

PhoneNumber

代替連絡先の電話番号を指定します。

型: 文字列

長さの制限：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。

型: 文字列

長さの制限：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、「共通エラー」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。

HTTP ステータスコード: 403

InternalServerException

の内部エラーのため、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。

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。

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。

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutContactInformation

の主な連絡先情報を更新します AWS アカウント。

主な問い合わせオペレーションの使用方法の詳細については、「主要および代替の連絡先情報の更新」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

用される 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された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**
>
> 管理アカウントは独自の を指定できませんAccountId。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でこのオペレーションを呼び出すには、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。

型: 文字列

パターン：`^\d{12}$`

必須: いいえ

ContactInformation

に関連付けられている主な連絡先情報の詳細が含まれます AWS アカウント。

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、「共通エラー」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。

HTTP ステータスコード: 403

InternalServerException

の内部エラーのため、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。

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。

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。

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- 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プライマリ 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された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の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**
>
> 管理アカウントは独自の を指定できませんAccountId。

型: 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プライマリ 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ます) 。

型: 文字列

長さの制限: 最小長は 5。最大長は 64 文字です。

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

プライマリ E メール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、「共通エラー」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。

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、現在無効になっているリージョン (DISABLING のステータス) を有効にしようとする場合や、アカウントのルートユーザーの E メールを、既に使用されている E メールアドレスに変更しようとする場合に発生します。

HTTP ステータスコード: 409

InternalServerException

の内部エラーのため、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。

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。

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。

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。

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

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

その他の関連アクションAWSサービス

以下のオペレーションはに関連しています。AWS Account Managementしかし、の一部はありますAWS Organizations名前空間:

- CreateAccount
- GovCloud アカウントを作成する
- DescribeAccount

CreateAccount

-`CreateAccount`API オペレーションは、によって管理されている組織のコンテキストでのみ使用できます。AWS Organizationsサービス。API オペレーションは、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、「」を参照してください。CreateAccountのAWS OrganizationsAPI リファレンス。

GovCloud アカウントを作成する

-`CreateGovCloudAccount`API オペレーションは、によって管理されている組織のコンテキストでのみ使用できます。AWS Organizationsサービスサービス。API オペレーションは、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、「」を参照してください。GovCloud アカウントを作成するのAWS OrganizationsAPI リファレンス。

DescribeAccount

-`DescribeAccount`API オペレーションは、によって管理されている組織のコンテキストでのみ使用できます。AWS Organizationsサービス。API オペレーションは、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、「」を参照してください。DescribeAccountのAWS OrganizationsAPI リファレンス。

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。

型: 文字列

長さの制限：最小長は 1 です。最大長は 254 です。

Pattern: `^[\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。

型: 文字列

長さの制限：最小長は 1 です。最大長は 64 文字です。

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。

型: 文字列

長さの制限：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。

型: 文字列

長さの制限：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

に関連する主な連絡先情報の詳細が含まれます AWS アカウント。

コンテンツ

AddressLine1

主要連絡先住所の最初の行。

型: 文字列

長さの制限：最小長は 1 です。最大長は 60 です。

必須: はい

City

主要連絡先住所の市区町村。

型: 文字列

長さの制限：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 2 文字の国コード。

型: 文字列

長さの制約:長さは 2 に固定されています。

必須: はい

FullName

主要連絡先住所のフルネーム。

型: 文字列

長さの制限：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。電話番号は認証され、一部の国では有効化が確認されます。

型: 文字列

長さの制限：最小長は 1 です。最大長は 20 です。

Pattern: ^[+][\s0-9()-]+$

必須：はい

PostalCode

主要連絡先住所の郵便番号。

型: 文字列

長さの制限：最小長は 1 です。最大長は 20 です。

必須: はい

AddressLine2

主連絡先住所の 2 行目 (ある場合)。

型: 文字列

長さの制限：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)。

型: 文字列

長さの制限：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)。

型: 文字列

長さの制限：最小長は 1 です。最大長は 50 です。

必須: いいえ

DistrictOrCounty

主要連絡先の地区または郡 (ある場合)。

型: 文字列

長さの制限：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) 内の場合、このフィールドの値は 2 文字の州コード (例:NJ) でも完全な州名 (例:New Jersey) でもかまいません。このフィールドはUS、、、、、CAGBDEJPIN、BRおよびの各国で必須です。

型: 文字列

長さの制限：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 Web サイトの URL (ある場合)。

型: 文字列

長さの制限：最小長は 1 です。最大長は 256 です。

必須：いいえ

その他の参照資料

言語固有の AWS SDK の 1 つでこの 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 Java V2 用 SDK

- AWS ルビー V3 用 SDK

Region

これは特定のアカウントのリージョンを表す構造で、名前とオプトインステータスで構成されます。

コンテンツ

RegionName

特定の地域の地域コード (例:)。`us-east-1`

型: 文字列

長さの制限：最小長は 1 です。最大長は 50 です。

必須: いいえ

RegionOptStatus

リージョンが受ける可能性のあるステータスの1つ ([有効]、[有効化]、[無効]、[無効化]、[Enabled_By_Default])。

型: 文字列

有効な値：`ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

必須：いいえ

その他の参照資料

この API を言語固有の SDK で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

- AWS SDK for C++
- AWS Java V2 用 SDK
- AWS ルビー V3 用 SDK

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。

型: 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。

型: 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「AWSAPI リクエストへの署名」を参照してください。

Action

実行するアクション。

型: 文字列

必須: はい

Version

リクエストが想定している API バージョンである、YYYY-MM-DD 形式で表示されます。

型: 文字列

必須: はい

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 認証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/YYYYYYYYMMDD/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 リクエストを作成する」を参照してください。

条件: HTTP 認証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「AWSAPI 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(AWS STS) を呼び出して取得された一時的セキュリティトークン。から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AWS STS、「IAM ユーザーガイド」の「IAM と連携するサービス」を参照してくださいAWS のサービス。

条件:からの一時的なセキュリティ認証情報を使用する場合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 認証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 リクエストを作成する」を参照してください。

条件: HTTP 認証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

共通エラー

このセクションでは、AWS のすべてのサービスの API アクションに共通の工ラーを一覧表示しています。このサービスの API アクションに固有の工ラーについては、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十分なアクセス権限がありません。

HTTP ステータスコード: 400

IncompleteSignature

リクエストの署名が AWS 基準に適合しません。

HTTP ステータスコード: 400

InternalFailure

リクエストの処理が、不明な工ラー、例外、または障害により実行できませんでした。

HTTP ステータスコード: 500

InvalidAction

リクエストされたアクション、またはオペレーションは無効です。アクションが正しく入力されていることを確認します。

HTTP ステータスコード: 400

InvalidClientTokenId

指定された x.509 証明書、または AWS アクセスキー ID が見つかりません。

HTTP ステータスコード: 403

NotAuthorized

このアクションを実行するにはアクセス許可が必要です。

HTTP ステータスコード: 400

OptInRequired

サービスを利用するためには、AWS アクセスキー ID を取得する必要があります。

HTTP ステータスコード: 403

RequestExpired

リクエストの日付スタンプの 15 分以上後またはリクエストの有効期限 (署名付き URL の場合など) の 15 分以上後に、リクエストが到着しました。または、リクエストの日付スタンプが現在より 15 分以上先です。

HTTP ステータスコード: 400

ServiceUnavailable

リクエストは、サーバーの一時的障害のために実行に失敗しました。

HTTP ステータスコード: 503

ThrottlingException

リクエストは、制限が必要なために実行が拒否されました。

HTTP ステータスコード: 400

ValidationError

入力が、AWS サービスで指定された制約を満たしていません。

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 アカウント管理のためのクエリ API の使用についての一般的な情報を提供します。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、AWS SDK のいずれかを使用できます。AWS SDK は、さまざまなプログラム言語およびプラットフォームのライブラリやサンプルコード (Java、Ruby、.NET、iOS、Android など) から成ります。SDK は、AWS アカウント管理や AWS へのプログラムによるアクセス許可を作成するうえで役立ちます。

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 SDK のダウンロードやインストールなどの詳細については、「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クエリ API の使用、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、HTTPS リクエストであり、実行すべき操作を示す Action パラメータを含む必要があります。AWSアカウント管理は、すべての操作について GET と POST 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 リクエストに署名する

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) AWS リージョン でホストされる単一のグローバル API エンドポイントがあります。

詳細についてはAWSすべてのサービスのエンドポイントとリージョン、を参照してくださいリージョンとエンドポイントに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 リクエストに署名する

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 アカウント管理での日々の作業には、AWS ルートアカウント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 ロールなどで使用する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。Signature Version 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。

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 のセキュリティベストプラクティス— セキュリティ保護に役立つ IAM サービスの使用方法を提案しますAWSリソース (にあるものを含む)AWSアカウント管理。
- 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。

AWS Account Management のクォータ

AWS アカウント には、AWS のサービスごとにデフォルトのクォータ (以前は制限と呼ばれたもの) があります。特に明記されていない限り、クォータは AWS リージョン 固有です。

AWS アカウント ごとにアカウント管理に関係する以下のクォータがあります。

リソース	クォータ
AWS アカウント 内の代替連絡先の数	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数	6
組織ごとの同時リージョンオプトリクエスト数	20
アカウント 1 件あたりのリクエスト数 DeleteAlternateContact	1 秒あたり 1 回、1 秒あたり 6 回にバースト
アカウント 1 DisableRegion 件あたりのリクエスト数	1 秒あたり 1 回、バーストは 1 秒あたり
アカウント 1 EnableRegion 件あたりのリクエスト数	1 秒あたり 1 回、バーストは 1 秒あたり
アカウント 1 GetAlternateContact 件あたりのリクエスト数	毎秒 10 回、バーストは毎秒 15 回まで
アカウント 1 GetContactInformation 件あたりのリクエスト数	毎秒 10 回、バーストは毎秒 15 回まで
アカウント 1 GetRegionOptStatus 件あたりのリクエスト数	1 秒あたり 5 回、バーストは 1 秒あたり 5 回
アカウント 1 ListRegions 件あたりのリクエスト数	1 秒あたり 5 回、バーストは 1 秒あたり 5 回

リソース	クォータ
アカウント 1 PutAlternateContact 件あたりのリクエスト数	毎秒 5 回、バーストは毎秒 8 回まで
アカウント 1 PutContactInformation 件あたりのリクエスト数	毎秒 5 回、バーストは毎秒 8 回まで

AWS アカウント のトラブルシューティング

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のトラブルシューティング」を参照してください。 サインインプロセスの詳細については、AWS アカウント「 サインインユーザーガイド」の「サインインに関する問題のトラブルシューティングAWS」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 の作成に関する問題のトラブルシューティング
- 閉鎖に関する問題の AWS アカウント トラブルシューティング
- AWS アカウント に関する問題のトラブルシューティング

AWS アカウント の作成に関する問題のトラブルシューティング

次の表の参照リンクを使用して、 AWS アカウント新規作成に関する問題の診断と解決に役立ててください。

問題	リファレンスリンク	ソース
登録方法やアカウントの作成方法がわからない	スタンドアロンの作成 AWS アカウント	このガイド
AWS 新しいアカウントを確認するための電話がかかってこなかったり、入力した PIN が機能しない場合はどうすればいいですか？	https://repost.aws/knowledge-center/ phone-verify-no-call	AWS re:Post
AWS アカウント 電話で認証しようとしたときに「最大失敗回数」エラーを解決する方法を教えてください。	https://repost.aws/knowledge-center/ maximum-failed-attempts	AWS re:Post

問題	リファレンスリンク	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-アカウント	AWS re:Post
新しいアカウントを作成したら、そのアカウント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特定の問題に関連するコンテンツを検索することをおすすめします。それでもサポートが必要な場合は、お問い合わせくださいAWS Support。

閉鎖に関する問題の AWS アカウント トラブルシューティング

以下の情報は、アカウント閉鎖プロセス中に発生する一般的な問題の診断や修復に役立ちます。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、「」を参照してくださいを閉じる AWS アカウント。

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
- アカウントページのアカウントを閉じるボタンが表示されない
- アカウントを閉鎖したが、まだ E メールによる確認が届かない
- 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、「」の手順に従いますを閉じる AWS アカウント。

アカウントページのアカウントを閉じ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、アカウントを閉じる ページには表示されません。アカウントを閉鎖するには、ルートユーザー AWS Management Console 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 に関する問題のトラブルシューティング」を参照してください。

アカウントを閉鎖したが、まだ E メールによる確認が届かない

この確認 E メールは、 のルートユーザーの E メールアドレスにのみ送信されます AWS アカウント。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 Management Console として にサインインし、アカウントが閉鎖されていることを確認できます。アカウントが正常に閉鎖されると、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SUSPENDEDで としてラベル付けされているかどうかをチェックして、閉鎖が正常に完了し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、アカウント閉鎖に関する E メールの確認を受け取らない場合、組織にはアクティブなメンバーアカウントがある可能性が最も高くなります。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Suspended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、これは不可能です。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 Management Console 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、「 ユーザーガイド」の「組織内の管理アカウントの解約AWS Organizations 」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 を超えていても、閉鎖できる最小アカウント数は 10 で、閉鎖できる最大アカウント数は 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「 のクォータ AWS Organizations」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、組織内にアクティブなメンバーアカウントがない場合にのみ、管理アカウントを閉鎖できます。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Suspended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。

AWS アカウント に関する問題のトラブルシューティング

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。

問題点

- AWS アカウント のクレジットカードを変更する必要がある
- 不正な AWS アカウント アカウントアクティビティを報告する必要がある
- AWS アカウント を閉じる必要がある

AWS アカウント のクレジットカードを変更する必要がある

AWS アカウント のクレジットカードを変更するには、サインインする必要があります。AWS には保護機能があり、アカウントの所有者であることを証明するように求められます。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。

不正な AWS アカウント アカウントアクティビティを報告する必要がある

AWS アカウント アカウントを使用した不正なアクティビティの疑いがあり、レポートを作成する場合は、「AWS リソースの不正使用の報告方法」を参照してください。

Amazon.com での購入に関する問題については、Amazon カスタマーサービスを参照してください。

AWS アカウント を閉じる必要がある

AWS アカウント の問題を解決するためのヘルプについては、「を閉じる AWS アカウント」を参照してください。

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
新しいプライマリ E APIs	内の任意のメンバーアカウントのルートユーザーの E GetPrimaryEmail メールアドレスを一元的に更新するための新しい StartPrimaryEmailUpdate 、、および AcceptPrimaryEmailUpdate APIs のサポート AWS Organizations。詳細については、「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 メールアドレスの更新」を参照してください。 AWS Organizations	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方法のステップを追加することを含め、閉鎖アカウントトピック全体を完全に見直しました。	2024 年 2 月 1 日
新しいセキュリティチャレンジの質問の追加のサポート終了	新しいチャレンジの質問を追加するオプションがアカウントページから削除されたことに注意する新しいコンテンツを追加しました。	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)	2024 年 1 月 1 日

	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。	
リージョントピックの書き換え	拡張コントロールと折りたたみコントロールの追加を含め、リージョン全体のトピックを完全に見直しました。	2023 年 10 月 8 日
ルートユーザートピックを IAM ユーザーガイドに再配置しました	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クロスリファレンスリンクを追加しました。	2023 年 9 月 18 日
プライマリアカウントの連絡先トピックに新しいセクションが追加されました	新しい電話番号と E メールアドレスの要件セクションを追加しました。	2023 年 9 月 12 日
新しい連絡先情報 APIs	新しい GetContactInformation および PutContactInformation APIsのサポート。	2022 年 7 月 22 日
AWS アカウント管理では、コンソールを使用した代替連絡先の更新がサポートされる AWS Organizations 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 コンソールから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

AWS 用語集

AWS の最新の用語については、「AWS の用語集リファレンス」の「AWS 用語集」を参照してください。

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