ユーザーガイド

AWS Organizations

AWS Organizations: ユーザーガイド

Table of Contents

とは AWS Organizations 1
機能 1
ユースケース 3
用語と概念 4
利用可能な機能セット 5
組織構造 5
招待とハンドシェイク 8
組織ポリシー 9
クォータとサービス制限 11
命名ガイドライン 11
考慮事項 11
最大値および最小値 11
ハンドシェイクの有効期限 16
1 つのエンティティにアタッチできるポリシーの数 16
スロットリングの制限 18
リージョンのサポート 22
使用可能なリージョンのリスト 23
請求と料金 27
支払い責任 28
支払い構造 28
サポートとフィードバック 28
その他の AWS リソース 28
ベストプラクティス 30
アカウントと認証情報 30
ルートアクセス管理を有効にして、メンバーアカウントのルートユーザー認証情報の管理を簡素化する 30
連絡先の電話番号を最新の状態に保つ 31
ルートアカウントにグループメールアドレスを使用する 31
組織構造とワークロード 31
アカウントを 1 つの組織内で管理する 31
報告体制ではなく、ビジネス目的に基づいてワークロードをグループ化する 32
複数のアカウントを使用してワークロードを整理する 32
サービスとコスト管理 32

AWS サービスコンソールまたは API/CLI オペレーションを使用して組織レベルでサービスを有効にする ... 32
請求ツールを使用してコストを追跡し、リソースの使用を最適化する ... 32
組織リソース全体でのタグ付け戦略とタグの適用を計画する ... 33
入門 ... 34
にサインアップする AWS ... 34
にサインアップする AWS アカウント ... 34
管理アクセスを持つユーザーを作成する ... 35
アクセス AWS Organizations ... 36
チュートリアル: 組織の作成と設定 ... 38
前提条件 ... 39
ステップ 1: 組織を作成する ... 39
ステップ 2: 組織単位を作成する ... 42
ステップ 3: サービスコントロールポリシーを作成する ... 44
ステップ 4: 組織のポリシーをテストする ... 49
チュートリアル: Amazon EventBridge を使用して、組織をモニタリングする ... 50
前提条件 ... 51
ステップ 1: 証跡およびイベントセレクターを設定する ... 52
ステップ 2: Lambda 関数を設定する ... 53
ステップ 3: 受信者に E メールを送信する Amazon SNS トピックを作成する ... 54
ステップ 4: Amazon EventBridge ルールを作成する ... 55
ステップ 5: Amazon EventBridge ルールをテストする ... 55
クリーンアップ: 不要になったリソースを削除する ... 57
AWS SDKs の使用 ... 58
組織全体の管理 ... 60
組織の作成 ... 60
組織を作成する ... 60
E メールアドレスの検証 ... 65
E メールアドレスを検証する ... 65
検証 E メールの再送信 ... 65
E メールアドレスの変更 ... 66
すべての機能の有効化 ... 66
考慮事項 ... 67
標準移行プロセス ... 68
アシスト移行プロセス ... 78
組織の詳細の表示 ... 79

組織の削除 80
考慮事項 81
組織を削除する 82
組織内のアカウント管理 85
管理アカウント 85
管理アカウントのベストプラクティス 86
管理アカウントの閉鎖 87
メンバーアカウント 88
メンバーアカウントのベストプラクティス 89
メンバーアカウントを作成する 92
メンバーアカウントへのアクセス 97
メンバーアカウントの閉鎖 104
メンバーアカウントが閉鎖されないように保護する 106
メンバーアカウントの削除 108
メンバーアカウントから組織を脱会する 113
メンバーアカウントのアカウント名の更新 117
メンバーアカウントのルートユーザー E メール メールの更新 117
アカウント招待 118
考慮事項 119
招待の送信 121
保留中の招待の管理 124
招待の承諾または拒否 129
アカウントの移行 133
移行前 133
移行 137
移行後 137
アカウントの詳細を表示する 138
アカウントの詳細をエクスポートする 140
組織のすべての AWS アカウント のリストをエクスポートする 140
アカウントの代替連絡先を更新する 141
アカウントのプライマリ連絡先を更新する 142
AWS リージョン アカウントの の更新 142
組織単位 (OUs) 143
OU のベストプラクティス 144
について AWS Organizations 144
推奨される基本 OU 145

推奨される追加の OU 145
結論 147
ルートとツリーの操作 147
OU の詳細の表示 148
OU の作成 150
OU の名前変更 154
OU のタグ付け 156
OU 間のアカウントの移動 157
ルートの詳細の表示 159
OU の削除 160
組織ポリシー 164
ポリシータイプ 164
承認ポリシー 165
管理ポリシー 165
承認ポリシー 167
SCPs と RCPsの違い 167
SCPs と RCPs 168
サービスコントロールポリシー 170
リソースコントロールポリシー 222
管理ポリシー 239
前提条件とアクセス許可 239
ポリシーの継承について 241
有効なポリシーの表示 256
無効なポリシーアラート 260
宣言ポリシー 262
バックアップポリシー 283
タグポリシー 325
チャットアプリケーションポリシー 443
AI サービスのオプトアウトポリシー 458
Security Hub ポリシー 468
の委任管理者 AWS Organizations 479
リソースベースの委任ポリシーを作成する 479
リソースベースの委任ポリシーを更新する 484
リソースベースの委任ポリシーを表示する 489
リソースベースの委任ポリシーを削除する 490
ポリシータイプの有効化 491

ポリシータイプの無効化 492
考慮事項 492
ポリシータイプを無効にする 493
ポリシーの作成 494
サービスコントロールポリシー (SCP) を作成する 495
リソースコントロールポリシー (RCP) を作成する 500
宣言ポリシーを作成する 504
バックアップポリシーを作成する 507
タグポリシーを作成する 511
チャットアプリケーションポリシーを作成する 516
AI サービスのオプトアウトポリシーを作成する 520
Security Hub ポリシーを作成する 522
ポリシーの更新 524
サービスコントロールポリシー (SCP) を更新する 525
リソースコントロールポリシー (RCP) を更新する 528
宣言ポリシーを更新する 531
バックアップポリシーを更新する 532
タグポリシーを更新する 536
チャットアプリケーションポリシーを更新する 539
AI サービスのオプトアウトポリシーを更新する 540
Security Hub ポリシーを更新する 543
ポリシーにアタッチされたタグを編集する 545
サービスコントロールポリシー (SCP) にアタッチされたタグを編集する 546
リソースコントロールポリシー (RCP) にアタッチされたタグを編集する 547
宣言ポリシーにアタッチされたタグを編集する 548
バックアップポリシーにアタッチされたタグを編集する 550
タグポリシーにアタッチされたタグを編集する 551
チャットアプリケーションポリシーにアタッチされたタグを編集する 552
AI サービスのオプトアウトポリシーにアタッチされたタグを編集する 554
Security Hub ポリシーにアタッチされたタグを編集する 555
ポリシーのアタッチ 557
ポリシーをアタッチする 557
ポリシーのデタッチ 569
ポリシーをデタッチする 569
ポリシーの詳細情報の取得 582
すべてのポリシーの一覧表示 582

アタッチされたポリシーの一覧表示 ... 587
すべての添付ファイルを一覧表示する ... 588
ポリシーの詳細の取得 ... 590
ポリシーの削除 ... 593
ポリシーを削除する ... 593
リソースのタグ付け ... 601
考慮事項 ... 601
タグの使用 ... 602
タグの追加、更新、削除 ... 602
リソースの作成時にタグを追加する ... 603
既存のリソースにタグを追加または更新する ... 603
マルチパーティー承認 ... 606
他の の使用 AWS のサービス ... 607
信頼されたアクセスを有効にするために必要なアクセス許可 ... 608
信頼されたアクセスを無効にするために必要なアクセス許可 ... 609
信頼されたアクセスを有効または無効にする方法 ... 610
AWS Organizations およびサービスにリンクされたロール ... 613
AWSServiceRoleForDeclarativePoliciesEC2Report サービスにリンクされたロールの使用 ... 614
Organizations と連携するサービス ... 614
AWS アカウント管理 ... 670
AWS Application Migration Service ... 674
AWS Artifact ... 679
AWS Audit Manager ... 682
AWS Backup ... 686
AWS Billing and Cost Management ... 689
AWS CloudFormation StackSets ... 691
AWS CloudTrail ... 695
Amazon CloudWatch ... 700
AWS Compute Optimizer ... 705
AWS Config ... 709
AWS Cost Optimization Hub ... 712
AWS Control Tower ... 716
Amazon Detective ... 718
Amazon DevOps Guru ... 722
AWS Directory Service ... 727
Amazon Elastic Compute Cloud ... 729

Amazon Elastic Kubernetes Service ... 732
AWS Firewall Manager ... 734
Amazon GuardDuty ... 738
AWS Health ... 741
AWS Identity and Access Management ... 745
Amazon Inspector ... 747
AWS License Manager ... 752
AWS Managed Services (AMS) セルフサービスレポート (SSR) ... 755
Amazon Macie ... 757
AWS Marketplace ... 760
AWS Marketplace プライベートマーケットプレイス ... 763
AWS Marketplace 調達インサイトダッシュボード ... 767
AWS ネットワークマネージャー ... 771
Amazon Q Developer ... 774
AWS Resource Access Manager ... 775
AWS Resource Explorer ... 780
AWS Security Hub ... 784
Amazon S3 Storage Lens ... 786
AWS セキュリティインシデント対応 ... 790
Amazon Security Lake ... 795
AWS Service Catalog ... 800
Service Quotas ... 804
AWS IAM Identity Center ... 805
AWS Systems Manager ... 810
AWS User Notifications ... 815
タグポリシー ... 817
AWS Trusted Advisor ... 819
AWS Well-Architected Tool ... 822
Amazon VPC IP Address Manager (IPAM) ... 826
Amazon VPC Reachability Analyzer ... 829
統合 の委任管理者 AWS のサービス ... 833
委任管理者アカウントに付与された権限 ... 834
セキュリティ ... 836
AWS PrivateLink ... 836
for の制限と制限 AWS PrivateLinkAWS Organizations ... 837
VPC エンドポイントの作成 ... 837

VPCエンドポイントポリシーの作成 838
Identity and Access Management 839
対象者 839
アイデンティティを使用した認証 840
ポリシーを使用したアクセスの管理 843
が IAM と AWS Organizations 連携する方法 846
組織へのアクセス許可の管理 853
アイデンティティベースのポリシーの例 862
リソースベースのポリシーの例 869
AWS 管理ポリシー 875
タグによる属性ベースのアクセスコントロール 879
トラブルシューティング 885
ログ記録とモニタリング 887
AWS CloudTrail 887
Amazon EventBridge 900
コンプライアンス検証 900
耐障害性 901
インフラストラクチャセキュリティ 902
トラブルシューティング 903
一般的な問題のトラブルシューティング 903
へのリクエスト時に「アクセス拒否」メッセージが表示される AWS Organizations 903
一時的なセキュリティ認証情報を使用してリクエストを送信すると「アクセスが拒否されました」というメッセージが表示される 904
組織をメンバーアカウントとして残したり、メンバーアカウントを管理アカウントとして削除しようとすると、「アクセスが拒否されました」というメッセージが表示されます。 904
組織にアカウントを追加しようとすると「クォータを超えました」というメッセージが表示される 905
アカウントを追加または削除するときに「このオペレーションでは待機期間が必要です」というメッセージが表示される 905
組織にアカウントを追加しようとすると「組織がまだ初期化中です」というメッセージが表示される 905
組織にアカウントを招待しようとすると、「招待は無効になっています」というメッセージが表示される。 906
変更がすぐに表示されない 906
既に組織の一部であるアカウントにアクセスしようとすると、「サインアップの完了」というメッセージが表示される 906

HTTP クエリリクエストの作成 907
エンドポイント 908
HTTPS の必要性 908
AWS Organizations API リクエストの署名 908
コードの例 909
基本 909
アクション 910
ドキュメント履歴 948
..... cmlxiii

とは AWS Organizations

AWS リソースをスケールしながら環境を一元管理する

AWS Organizations は、 AWS リソースの拡大とスケーリングに合わせて環境を一元管理および管理するのに役立ちます。Organizations を使用すると、アカウントの作成、リソースの割り当て、ワークロードを整理するためのアカウントのグループ化、ガバナンスへのポリシーの適用、すべてのアカウントに単一の支払い方法を使用した請求の簡素化が可能になります。

Organizations は他の と統合 AWS のサービス されているため、組織内のアカウント間で中央設定、セキュリティメカニズム、監査要件、リソース共有を定義できます。詳細については、「を他の AWS Organizations で使用する AWS のサービス」を参照してください。

次の図は、 AWS Organizationsの使用方法の概要を示しています。

- アカウントを追加する
- アカウントをグループ化する
- ポリシーを適用する
- 有効にします AWS のサービス。

トピック

- の機能 AWS Organizations
- のユースケース AWS Organizations
- の用語と概念 AWS Organizations
- のクォータとサービス制限 AWS Organizations
- のリージョンサポート AWS Organizations
- の請求と料金 AWS Organizations
- のサポートとフィードバック AWS Organizations

の機能 AWS Organizations

AWS Organizations には以下の機能があります。

の管理 AWS アカウント

AWS アカウント は、アクセス許可、セキュリティ、コスト、ワークロードの自然な境界です。マルチアカウント環境は、クラウド環境をスケーリングするときに推奨されるベストプラクティスです。 AWS Command Line Interface （ AWS CLI ）、SDKs、または APIs を使用して新しいアカウントをプログラムで作成し、AWS CloudFormation StackSets を使用してそれらのアカウントに推奨されるリソースとアクセス許可を一元的にプロビジョニングすることで、アカウントの作成を簡素化できます。

組織の定義と管理

新しいアカウントを作成するときに、それらを組織単位 (OU) または単一のアプリケーションまたはサービスを提供するアカウントのグループにグループ化できます。タグポリシーを適用して、組織内のリソースを分類または追跡し、ユーザーまたはアプリケーションに属性ベースのアクセスコントロールを提供します。さらに、サポートされている の責任を AWS のサービス アカウントに委任して、ユーザーが組織に代わって管理できるようにします。

アカウントの保護とモニタリング

セキュリティチームが組織に代わって、セキュリティニーズを管理するためのツールとアクセスを一元的に提供することができます。例えば、アカウント間で読み取り専用のセキュリティアクセスを提供し、Amazon GuardDuty を使用して脅威を検出して緩和し、IAM Access Analyzer を使用してリソースへの意図しないアクセスを確認し、Amazon Macie を使用して機密データを保護することができます。

アクセスとアクセス許可を制御する

アクティブディレクトリを使用して AWS アカウント および リソースにアクセスできるように AWS IAM Identity Center を設定し、個別のジョブロールに基づいてアクセス許可をカスタマイズします。ユーザー、アカウント、または OU に組織ポリシーを適用することもできます。たとえば、サービスコントロールポリシー (SCPs) を使用すると、組織内の AWS リソース、サービス、リージョンへのアクセスを制御できます。リソースコントロールポリシー (RCPs) を使用すると、 AWS リソースの意図しない使用を一元的に防止できます。チャットアプリケーションポリシーを使用すると、Slack や Microsoft Teams などのチャットアプリケーションから組織のアカウントへのアクセスを制御できます。

アカウント間でリソースを共有する

AWS Resource Access Manager （ AWS RAM ） を使用して、組織内で AWS リソースを共有できます。例えば、Amazon Virtual Private Cloud (Amazon VPC) サブネットを 1 回作成し、組織全体で共有できます。また、AWS License Manager とのソフトウェアライセンスに一元的に同意

し、AWS Service Catalog アカウント間で IT サービスとカスタム製品のカタログを共有することもできます。

コンプライアンスの環境を監査する

アカウント AWS CloudTrail 間でアクティブ化できます。これにより、メンバーアカウントではオフまたは変更できないクラウド環境内のすべてのアクティビティのログが作成されます。さらに、 を使用して指定した頻度でバックアップを適用するポリシーを設定したりAWS Backup、アカウント間および AWS リージョン でリソースの推奨構成設定を定義したりできますAWS Config。

請求とコストを一元管理

Organizations では、単一の統合された請求書が提供されます。さらに、AWS Cost Explorer を使用してアカウント間でリソースの使用状況を表示し、コストを追跡したり、AWS Compute Optimizer を使用してコンピューティングリソースの使用を最適化たりできます。

のユースケース AWS Organizations

以下は、いくつかのユースケースです AWS Organizations。

ワークロードの作成 AWS アカウント と分類を自動化する

の作成を自動化 AWS アカウント して、新しいワークロードをすばやく起動できます。アカウントをユーザー定義グループに追加して、即時セキュリティポリシーアプリケーション、タッチレスインフラストラクチャデプロイ、監査を行います。個別のグループを作成して開発アカウントと本番稼働アカウントを分類し、AWS CloudFormation StackSets を使用して各グループにサービスとアクセス許可をプロビジョニングします。

監査ポリシーとコンプライアンスポリシーを定義して適用する

サービスコントロールポリシー (SCP) を適用して、ユーザーがセキュリティおよびコンプライアンス要件を満たすアクションのみを実行できるようにします。AWS CloudTrail を使用して、組織全体で実行されたすべてのアクションの中央ログを作成します。 AWS リージョン を使用して、アカウント間および 間で標準リソース設定を表示および適用しますAWS Config。AWS Backup を使用して、定期的なバックアップを自動的に適用します。を使用してAWS Control Tower、AWS ワークロードのセキュリティ、運用、コンプライアンスにパッケージ化されたガバナンスルールを適用します。

開発を奨励しながら、セキュリティチームにツールとアクセスを提供する

セキュリティグループを作成し、すべてのリソースへの読み取り専用アクセスを提供し、セキュリティ上の懸念を特定して軽減します。そのグループが Amazon GuardDuty を管理できるようにすることで、ワークロードに対する脅威を積極的にモニタリングして軽減し、IAM Access Analyzer でリソースへの意図しないアクセスをすばやく特定できます。

アカウント間で共通リソースを共有する

Organizations を使用すると、アカウント間で重要なセントラルリソースを簡単に共有できます。例えば、セントラル AWS Directory Service for Microsoft Active Directory を共有して、アプリケーションがセントラル ID ストアにアクセスするようにできます。

アカウント間で重要なセントラルリソースを共有する

AWS Directory Service for Microsoft Active Directory をアプリケーションのセントラル ID ストアとして共有します。AWS Service Catalog を使用して、指定されたアカウントで IT サービスを共有し、ユーザーが承認されたサービスをすばやく検出してデプロイできるようにします。Amazon Virtual Private Cloud (Amazon VPC) サブネットにアプリケーションリソースが作成されていることを確認します。アプリケーションリソースは 1 回一元的に定義し、AWS Resource Access Manager (AWS RAM) を使用して組織全体で共有します。

の用語と概念 AWS Organizations

このトピックでは、 の主要な概念について説明します AWS Organizations。

次の図は、組織を示しています。この組織は、5 つのアカウントで構成されており、そのアカウントは、ルートを親として、4 つの組織単位 (OU) に分類されています。この組織には、複数のポリシーがあり、OU の一部、またはアカウントに直接アタッチされています。

これらの各項目の詳細については、このトピックの定義を参照してください。

トピック

- 利用可能な機能セット
- 組織構造
- 招待とハンドシェイク
- 組織ポリシー

利用可能な機能セット

すべての機能 (推奨)

すべての機能は、 で使用できるデフォルトの機能セットです AWS Organizations。組織全体の一元的なポリシーと設定要件の設定、組織内のカスタムアクセス許可や機能の作成、1 回の請求でアカウントの管理と整理、組織に代わって他のアカウントに責任を委任できます。また、他の AWS のサービス と統合することで、組織内のすべてのメンバーアカウントにわたる中央設定、セキュリティメカニズム、監査要件、リソース共有を定義することもできます。詳細については、「を他の AWS Organizations で使用する AWS のサービス」を参照してください。

すべての機能モードには、一括請求のすべての機能と管理機能が用意されています。

一括請求

一括請求は、共有請求機能を提供する機能セットですが、より高度な機能は含まれていません AWS Organizations。例えば、他の AWS のサービスが組織と統合してすべてのアカウントで動作するようにしたり、ポリシーを使用して異なるアカウントのユーザーとロールが実行できる操作を制限したりすることはできません。

組織の設定を一括請求機能 (コンソリデーティッドビリング) のみのサポートからすべての機能のサポートに変更することができます。すべての機能を有効にするには、招待済みのすべてのメンバーアカウントを使用して、管理アカウントでプロセスを開始する際に送信される招待を承認し、変更を承認する必要があります。詳細については、「を使用して組織のすべての機能を有効にする AWS Organizations」を参照してください。

組織構造

組織

組織とは、一元的に管理し、上部にルートがあり、ルートの下にネストされた組織単位を持つ階層的な木のような構造に整理できる AWS アカウントのコレクションです。各アカウントは、ルートに直接含めるか、階層内の OU のいずれかに配置することができます。

各組織は以下で構成されます。

- 管理アカウント
- ゼロ以上のメンバーアカウント
- ゼロ以上の組織単位 (OU)

- ゼロ以上のポリシー。

組織には、有効にする機能セットによって決定された機能を含みます。

ルート

管理ルート (ルート) は管理アカウントに含まれ、AWS アカウントを整理するための出発点です。ルートは、組織の階層で最上位のコンテナです。このルートでは、組織単位 (OU) を作成してアカウントを論理的にグループ化し、ニーズに最適な階層 OU に整理できます。

管理ポリシーをルートに適用する場合は、組織の管理アカウントを含む、すべての組織単位 (OU) とアカウントに適用されます。

承認ポリシー (サービスコントロールポリシー (SCP) など) をルートに適用すると、組織内のすべての組織単位 (OU) とメンバーアカウントに適用されます。組織の管理アカウントには適用されません。

> **Note**
>
> 組織の作成時に AWS Organizations ルートを自動的に作成できるのは 1 つの root のみです。

組織単位 (OU)

組織単位 (OU) は、組織内の AWS アカウントのグループです。OU には、階層を作成できる他の OU を含めることもできます。例えば、同じ部門に属するすべてのアカウントを部門 OU にグループ化できます。同様に、セキュリティサービスを実行しているすべてのアカウントをセキュリティ OU にグループ化できます。

OU は、組織内のアカウントのサブセットに同じコントロールを適用する必要がある場合に役立ちます。OU ネストすると、管理単位が小さくなります。例えば、ワークロードごとに OU を作成し、ワークロード OU ごとにネストされた OU を 2 つ作成して、本番ワークロードを本番稼働前から分割できます。これらの OU は、チームレベルの OU に直接割り当てられたコントロールに加えて、親 OU からポリシーを継承します。最も低い OUs に AWS アカウント 作成されたルートと を含めると、階層の深さは 5 レベルになります。

AWS アカウント

AWS アカウント は、 AWS リソースのコンテナです。で AWS リソースを作成および管理すると AWS アカウント、 はアクセスと請求のための管理機能 AWS アカウント を提供します。

複数の を使用すること AWS アカウント は、環境をスケーリングするためのベストプラクティスです。これは、コストの請求境界を提供し、セキュリティのためにリソースを分離し、新しいプロセスに適応できるだけでなく、柔軟性や個人やチームも提供するためです。

> **Note**
>
> AWS アカウントはユーザーとは異なります。ユーザーは、 AWS Identity and Access Management (IAM) を使用して作成する ID で、長期の認証情報を持つ IAM ユーザーか、短期の認証情報を持つ IAM ロールのどちらかの形態をとります。1 つの AWS アカウントには、多数のユーザーとロールを含めることができ、通常は含めることができます。

組織は 2 種類のアカウントで構成されます。一つは管理アカウントとして指定された単一のアカウント、もう一つは 1 つ以上のメンバーアカウントです。

管理アカウント

管理アカウントは、組織の作成 AWS アカウント に使用する です。管理アカウントから、以下のことができます。

- 組織内の他のアカウントを作成する
- 他のアカウントを組織に参加するよう招待し、招待を管理する
- 委任管理者アカウントを指定する
- 組織からアカウントを削除する
- ルート、組織単位 (OU)、組織内のアカウントなどのエンティティにポリシーをアタッチする
- サポートされている AWS サービスとの統合を有効にして、組織内のすべてのアカウントでサービス機能を提供します。

管理アカウントは組織の最終的な所有者であり、セキュリティ、インフラストラクチャ、財務ポリシーを最終的に制御します。このアカウントには支払者アカウントの役割があり、組織内のアカウントによって発生したすべての料金を支払う責任があります。

> **Note**
>
> 組織内のアカウントを管理アカウントに変更することはできません。

メンバーアカウント

メンバーアカウントは AWS アカウント、組織の一部である管理アカウント以外の です。組織の管理者であれば、組織内にメンバーアカウントを作成したり、既存のアカウントを組織に招待して参加させることができます。メンバーアカウントにポリシーを適用することもできます。

> **Note**
>
> メンバーアカウントは、一度に 1 つの組織のみに所属できます。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できます。

委任管理者

管理アカウントとそのユーザーおよびロールは、そのアカウントで実行する必要のあるタスクのみに使用することをおすすめします。 AWS リソースを組織内の他のメンバーアカウントに保存し、管理アカウントからは切り離すことをおすすめします。これは、Organizations のサービスコントロールポリシー (SCP) などのセキュリティ機能は、管理アカウントのどのユーザーやどのロールにも制限を加えることができないためです。また、リソースを管理アカウントから分離することで、請求書に記載される請求額が理解しやすくなります。組織の管理アカウントから、1 つ以上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と、この推奨事項を実施するうえで役立ちます。委任管理者には次の 2 種類があります。

- Organizations の委任管理者:これらのアカウントからは、組織のポリシーを管理したり、組織内のエンティティ(ルート、OU、またはアカウント)にポリシーをアタッチしたりできます。管理アカウントは、委任権限をきめ細かく制御できます。詳細については、「の委任管理者 AWS Organizations」を参照してください。
- AWS サービスの委任管理者: これらのアカウントから、Organizations と統合する AWS サービスを管理できます。管理アカウントは、必要に応じて異なるメンバーアカウントをさまざまなサービスの委任管理者として登録できます。これらのアカウントには、特定のサービスの管理者権限と、Organizations の読み取り専用アクションの権限があります。詳細については、Organizations と連携 AWS のサービス する の委任管理者を参照してください。

招待とハンドシェイク

招待

招待は、組織の管理アカウントが別のアカウントに対して行うリクエストです。例えば、スタンドアロンアカウントに組織への参加を依頼するプロセスは招待です。

招待はハンドシェイクとして実装されます。 AWS Organizations コンソールで作業している場合、ハンドシェイクが表示されないことがあります。ただし、 AWS CLI または AWS Organizations API を使用する場合は、ハンドシェイクを直接操作する必要があります。

ハンドシェイク

ハンドシェイクは、送信者と受信者の 2 つの AWS アカウント間で安全に情報を交換することです。

次のハンドシェイクがサポートされています。

- INVITE: ハンドシェイクが送信者の組織に加わるためにスタンドアロンアカウントに送信されました。
- ENABLE_ALL_FEATURES: 招待されたメンバーアカウントにハンドシェイクが送信され、組織のすべての機能が有効になります。
- APPROVE_ALL_FEATURES: 招待されたすべてのメンバーアカウントがすべての機能を有効にすることを承認したときに、ハンドシェイクが管理アカウントに送信されます。

通常、ハンドシェイクと直接やり取りする必要があるのは、 AWS Organizations API や などのコマンドラインツールを使用する場合のみです AWS CLI。

組織ポリシー

ポリシーは、グループに適用するコントロールを定義する 1 つ以上のステートメントを含む「ドキュメント」です AWS アカウント。 は、認可ポリシーと管理ポリシー AWS Organizations をサポートしています。

承認ポリシー

認可ポリシーは、組織全体の のセキュリティ AWS アカウント を一元管理するのに役立ちます。

サービスコントロールポリシー (SCP)

サービスコントロールポリシーは、組織内の IAM ユーザーと IAM ロールが利用できる最大アクセス許可を一元的に制御できるようにするポリシーの一種です。

つまり、SCPsプリンシパル中心のコントロールを指定します。SCPs は、アクセス許可ガードレールを作成するか、メンバーアカウントのプリンシパルが使用できるアクセス許可の上限を設定します。SCP は、組織内のプリンシパルに対して一貫したアクセスコントロールを一元的に適用する場合に使用します。

これには、IAM ユーザーと IAM ロールがアクセスできるサービス、アクセスできるリソース、またはリクエストを実行できる条件 (特定のリージョンやネットワークなど) の指定が含まれます。詳細については、SCPs」を参照してください。

リソースコントロールポリシー (RCP)

リソースコントロールポリシーは、組織内のリソースに対して使用可能なアクセス許可の最大数を一元的に制御するポリシーの一種です。

つまり、RCPsリソース中心のコントロールを指定します。RCPs は、メンバーアカウントのリソースで使用できる最大アクセス許可に対してアクセス許可ガードレールを作成するか、制限を設定します。組織内のリソース間で一貫したアクセスコントロールを一元的に適用する場合は、RCP を使用します。

これには、組織に属する ID のみがアクセスできるようにリソースへのアクセスを制限することや、組織外部の ID がリソースにアクセスできる条件を指定することが含まれます。詳細については、RCPs」を参照してください。

管理ポリシー

管理ポリシーは、組織全体で AWS のサービス とその機能を一元的に設定および管理するのに役立ちます。

宣言ポリシー

宣言型ポリシーは、組織全体で大規模 AWS のサービス に特定の に必要な設定を一元的に宣言して適用できるようにするポリシーの一種です。アタッチされると、サービスが新機能または APIs「宣言ポリシー」を参照してください。

バックアップポリシー

バックアップポリシーは、バックアッププランを一元管理し、組織のアカウント全体の AWS リソースに適用できるようにするポリシーのタイプです。詳細については、「 バックアップポリシー」を参照してください。

タグポリシー

タグポリシーは、組織のアカウントの AWS リソースにアタッチされたタグを標準化できるポリシーのタイプです。詳細については、「タグポリシー」を参照してください。

チャットアプリケーションポリシー

チャットアプリケーションポリシーは、Slack や Microsoft Teams などのチャットアプリケーションから組織のアカウントへのアクセスを制御できるようにするポリシーの一種です。詳細については、「チャットアプリケーションポリシー」を参照してください。

AI サービスのオプトアウトポリシー

AI サービスのオプトアウトポリシーは、組織内のすべてのアカウントの AWS AI サービスのデータ収集を制御できるポリシーの一種です。詳細については、「AI サービスのオプトアウトポリシー」を参照してください。

のクォータとサービス制限 AWS Organizations

このトピックでは、 のクォータとサービス制限について説明します AWS Organizations。

命名ガイドライン

以下は、アカウント名 AWS Organizations、組織単位 (OUs)、ルート、ポリシーなど、 で作成する名前のガイドラインです。

- 名前は Unicode 文字で構成されている必要があります。
- 名前の最大文字列長は、オブジェクトによって異なります。各オブジェクトの実際の制限の詳細については、「AWS Organizations API リファレンス」を参照し、オブジェクトを作成する API オペレーションを検索して、そのオペレーションの Name パラメータの詳細をご確認ください。例: アカウント名または OU 名。

考慮事項

サービスクォータコードは、更新により時間の経過とともに変更される可能性があります。これは、クォータ値または名前には影響しません。特定のクォータのクォータコードを検索するには、ListServiceQuotas オペレーションを使用して、必要なクォータの出力でQuotaCodeレスポンスを探します。

最大値および最小値

のエンティティのデフォルトの最大値を次に示します AWS Organizations。

> **Note**
>
> AWS Organizations クォータに関する次の情報を考慮してください。
>
> - Service Quotas コンソールを使用して、これらの値の一部を引き上げるよう要求できます。
> - AWS Organizations 特に指定がない限り、 の制限は組織レベルで適用されます。多くのクォータは、管理アカウントから AWS Organizations 実行されるアクションにのみ適用されます。
> - AWS Organizations は、米国東部 (バージニア北部) リージョン () で物理的にホストされるグローバルサービスですus-east-1。したがって、Service Quotas コンソール、、 AWS CLIまたは AWS SDK を使用する場合は、 us-east-1を使用してこれらのクォータにアクセスする必要があります。

説明	[制限]
デフォルトの最大アカウント数	10 — 組織で許容されるアカウントのデフォルトの最大数。このクォータは調整可能で、Service Quotas コンソールを使用して増やすことができます。 注: このクォータ引き上げリクエストを送信できるのは、組織の管理アカウントのみです。制限引き上げは、顧客の資格と要件に基づいて最大 10,000 アカウントまで許可できます。新しく作成されたアカウントや Organizations では、デフォルトの 10 アカウントを下回るクォータが発生する可能性があります。 アカウントに送信された招待はこのクォータに対してカウントされます。招待されたアカウントが拒否された場合、管理アウントが招待をキャンセルした場合、または招待状の有効期限が切れた場合は、カウントが返されます。 アカウントが閉鎖されても、アカウントが完全に閉鎖されるまで、このクォータに対するカウントは停止されません。アカウントが完全に閉鎖された場合の詳細については、「AWS アカウント管理 リファレンスガイド」の「閉鎖後期間」を参照してください。

説明	[制限]
	一部のサービスには、組織で許可されるアカウントの最大数とは別にアカウント制限があります。詳細については、AWS 「サービス別の制限」を参照してください。
作成したアカウントの削除の最小期間	サポートされている各リージョン: 7 — 組織から削除する前に、作成されたアカウントが存在する必要がある最小日数。
組織の root の数	1
組織の OU の数	2000
組織の各タイプのポリシーの数	サービスコントロールポリシー: 10,000 リソースコントロールポリシー: 1000 宣言ポリシー: 1000 バックアップポリシー: 1,000 タグポリシー: 1000 チャットアプリケーションポリシー: 1000 AI サービスのオプトアウトポリシー: 1,000 Security Hub ポリシー: 1000

説明	[制限]
ポリシードキュメントの最大サイズ	サービスコントロールポリシー: 5120 文字 リソースコントロールポリシー: 5120 文字 宣言ポリシー: 10,000 文字 バックアップポリシー: 10,000 文字 チャットアプリケーションポリシー: 10,000 文字 AI サービスのオプトアウトポリシー: 2500 文字 タグポリシー: 10,000 文字 Security Hub ポリシー: 10,000 文字 注： を使用してポリシーを保存すると AWS Management Console、JSON 要素と引用符の外側の間の余分な空白 (スペースや改行など) が削除され、カウントされません。SDK オペレーションまたは を使用してポリシーを保存すると AWS CLI、指定したとおりにポリシーが保存され、文字の自動削除は行われません。
ルート内の OU 最大ネスト数	ルート以下に 5 レベルの OU 深。
24 時間以内に試行できる招待の最大回数	20 または組織で許可される最大アカウント数のいずれか大きい方です。承諾済みの招待は、このクォータに対してカウントされません。1 つの招待が承諾されるとすぐ、同じ日に別の招待を送信できます。 組織で許可される最大アカウント数が 20 未満の場合、組織に含めることができるアカウント数を超えてアカウントを招待しようとすると、「アカウント制限を超えました」という例外が発生します。ただし、招待をキャンセルして、1 日に最大 20 回まで新しい招待を送信することができます。
同時に作成できるメンバーアカウントの数	5 - 1 つが終了するとすぐに他を開始できますが、一度に進行できるのは 5 つのみです。

説明	[制限]
30 日以内に閉鎖できるアカウントの数	組織内のメンバーアカウントの 10% (上限 1,000)。これは調整可能なクォータではありません。 • 100 アカウント未満 — 最大 10 人のメンバーアカウントを閉鎖できます • 100 ~ 10,000 アカウント – メンバーアカウントの最大 10% を閉鎖できます • > 10,000 アカウント – 最大 1,000 人のメンバーアカウントを閉鎖できます この上限に達すると、追加のアカウントを閉鎖できます。また、上限数がリセットされるまで待ちます。詳細については、「AWS アカウント管理ガイド」の「アカウントを閉じる」を参照してください。AWS
同時に閉鎖できるメンバーアカウントの数	3 – 同時に実行できるアカウント閉鎖は 3 つだけです。1 つが終了するとすぐに、別のアカウントを閉鎖できます。
ポリシーをアタッチできるエンティティの数	無制限
ルート、OU、またはアカウントにアタッチできるタグの数	50
リソースベースの委任ポリシーの最大サイズ	40,000 文字

AWS サービス別の制限

ほとんどの は、組織内で保持できるアカウントの最大数 AWS のサービス をサポートしています。ただし、一部のサービスには、組織で許可されるアカウントの最大数とは別にアカウント制限があります。

次の表は、個別のアカウント制限があるサービスを示しています。

AWS サービス	[制限]	引き上げ可能
AWS IAM Identity Center	3000	はい
AWS Application Migration Service	5000	いいえ
AWS Directory Service	250	はい

詳細については、「IAM Identity Center ユーザーガイド」の「AWS IAM Identity Center quotas」と「Application Migration Service User Guide」の「AWS MGN service quota limits」を参照してください。

ハンドシェイクの有効期限

以下は、ハンドシェイクのタイムアウトです AWS Organizations。

説明	[制限]
組織に参加するための招待	15 日間
組織内のすべての機能を有効にするリクエスト	90 日間
ハンドシェイクが削除され、リストに表示されなくなる	ハンドシェイクの完了から 30 日後

1 つのエンティティにアタッチできるポリシーの数

最小値および最大値は、ポリシータイプとポリシーをアタッチするエンティティよって異なります。次の表では、各ポリシータイプおよび各タイプにアタッチできるエンティティの数を示します。

> **Note**
>
> これらの数は、OU またはアカウントに直接アタッチされたポリシーにのみ適用されます。継承によって OU またはアカウントに影響を与えるポリシーは、これらの制限にはカウントされません。すべてのポリシー制限はハード制限です。

ポリシータイプ	エンティティにアタッチされる最小数	ルートにアタッチされる最大値	OU あたりの最大アタッチ数	アカウントあたりの最大アタッチ数
サービスコントロールポリシー	1 — SCP を有効にするときは、すべてのエンティティに少なくとも 1 つの SCPsアタッチされている必要があります。エンティティから最後の SCP を削除することはできません。	5	5	5
リソースコントロールポリシー	1 — RCP を有効にすると、`RCPFullAWSAccess` ポリシーはルート、すべての OU、および組織内のすべてのアカウントに自動的にアタッチされます。 RCPs このポリシーはデタッチできず、5 つのポリシークォータにカウントされます。	5	5	5
宣言ポリシー	0	10	10	10

ポリシータイプ	エンティティにアタッチされる最小数	ルートにアタッチされる最大値	OU あたりの最大アタッチ数	アカウントあたりの最大アタッチ数
バックアップポリシー	0	10	10	10
タグポリシー	0	10	10	10
チャットアプリケーションポリシー	0	5	5	5
AI サービスのオプトアウトポリシー	0	5	5	5
Security Hub ポリシー	0	10	10	10

> **Note**
>
> ルートは組織に 1 つのみ持つことができます。

スロットリングの制限

次の表に、管理カテゴリ別の AWS Organizations APIs と、アカウントおよび組織レベルでのそれぞれのスロットルレートを示します。

AWS Organizations はトークンバケットアルゴリズムを使用して API スロットリングを実装します。このアルゴリズムでは、アカウントには、特定の数のトークンを保持するバケットがあります。バケット内のトークンの数は、特定の秒におけるスロットリングクォータを表します。

Rate は、トークンが 1 秒あたりにトークンバケットに追加される固定ペースです。

バーストは、追加できるトークンの最大数と、1 秒あたりに使用できるトークンの最大数です。

例えば、DescribeAccountAPI はベースラインレートとして 1 秒あたり 1 AWS アカウント ~20 リクエスト、バーストレートとして 1 秒あたり 30 リクエストに制限されます。1 秒あたり 30 リクエストのバーストレートでは、1 秒あたり 20 リクエストのベースラインレートを一時的に超えることができます。

1 秒あたり 20 件のリクエストを行うことができます。これはベースラインレートです。次の 1 秒で、ベースラインを超える 30 件のリクエストを実行できますが、バーストレートは 30 のままです。ただし、3 秒目に 20 件を超えるリクエストを実行しようとすると、ベースラインレートを超え、バースト容量が使用されているため、スロットリングされます。

バーストレートを使用すると、1 秒あたりの平均リクエスト数が時間の経過とともにベースライン制限内であれば、スロットリングなしでトラフィックの一時的な急増を処理できます。

アカウント管理の制限

次の表に、 AWS Organizations APIs を示します。

AWS Organizations API	アカウントあたりの制限 (レート、バースト)	組織あたりの制限 (レート、バースト)
CloseAccount	.05、1	
CreateAccount 、CreateGovCloudAccount	0.1、3	
DescribeAccount	20、30	24、36
DescribeCreateAccountStatus	2、2	2、3
LeaveOrganization	1、1	
ListCreateAccountStatus	5、8	6、10

ハンドシェイク管理の制限

次の表に、アカウントハンドシェイク AWS Organizations APIs を示します。

AWS Organizations API	アカウントあたりの制限 (レート、バースト)	組織あたりの制限 (レート、バースト)
AcceptHandshake	1、2	5、5
DescribeHandshake	1、2	6、10
CancelHandshake	2、3	
DeclineHandshake	1、1	5、5
InviteAccountToOrganization	3、5	
ListHandshakesForAccount、ListHandshakesForOrganization	5、8	6、10

組織管理の制限

次の表に、 AWS Organizations APIs を示します。

AWS Organizations API	アカウントあたりの制限 (レート、バースト)	組織あたりの制限 (レート、バースト)
CreateOrganization、DeleteOrganization、EnableFullControl	1、1	
CreateOrganizationalUnit、DescribeOrganization	1、2	
MoveAccount、UpdateOrganizationalUnit、DeleteOrganizationalUnit	2、3	
DescribeOrganizationalUnit	2、2	2、3
ListAccounts	8、12	9、15
ListChildren	6、10	7、12

AWS Organizations API	アカウントあたりの制限 (レート、バースト)	組織あたりの制限 (レート、バースト)
ListParents、ListAccountsForParent、ListOrganizationalUnitsForParent	5、8	6、10
ListRoots	1、2	1、3
ListTagsForResource	10、15	12、18
RemoveAccountFromOrganization	2、2	
TagResource、UntagResource	4、6	

ポリシー管理の制限

次の表に、 AWS Organizations APIs を示します。

AWS Organizations API	アカウントあたりの制限 (レート、バースト)	組織あたりの制限 (レート、バースト)
CreatePolicy、DeletePolicy、AttachPolicy、DetachPolicy	2、3	
DescribePolicy	2、2	2、3
DisablePolicyType、EnablePolicyType	1、1	
ListPolicies、ListPoliciesForTarget、ListTargetsForPolicy	5、8	6、10
UpdatePolicy	2、3	

サービス管理の制限

次の表に、 AWS Organizations APIs を示します。

AWS Organizations API	アカウントあたりの制限 (レート、バースト)	組織あたりの制限 (レート、バースト)
EnableAWSServiceAccess、DisableAWSServiceAccess	1、2	
ListAWSServiceAccessForOrganization、ListDelegatedServicesForAccount	1、3	1、4
ListDelegatedAdministrators	5、8	6、10
RegisterDelegatedAdministrator、DeregisterDelegatedAdministrator	1、2	

のリージョンサポート AWS Organizations

AWS Organizations は、すべての AWS 商用リージョン AWS GovCloud (US) Regions、および中国リージョンで利用できます。

の機能の違いのリストについては AWS GovCloud (US) Regions、「」のAWS OrganizationsAWS GovCloud (US)「」を参照してください。

中国リージョンの機能の違いの一覧については、AWS Organizations 中国での「」を参照してください。

Organizations のサービスエンドポイントは次の場所にあります。

- 米国東部 (バージニア北部) 商業組織向け
- AWS GovCloud (US) 組織の In AWS GovCloud (米国西部)
- 中国 (寧夏) 中国組織向け。Ningxia Western Cloud Data Technology Co. Ltd (NWCD) が運営。

(AWS Identity and Access Management IAM) の現在の仕組みと同様に、中国で管理されている組織を除き、すべての組織エンティティにグローバルにアクセスできます。組織を作成および管理 AWS リージョン するときに を指定する必要はありませんが、中国で使用するアカウント用に別の組織を作成する必要があります。のユーザーは AWS アカウント 、そのサービスが利用可能な任意の地理的リージョン AWS のサービス で を使用できます。

> **Note**
>
> タグポリシーは、リージョンのサブセットでのみサポートされています
> タグポリシーはポリシーの一種で、組織のアカウント内のリソース間でタグを標準化するのに役立ちます。タグポリシーは、Organizations がサポートされているリージョンのサブセットでのみサポートされます。タグポリシーがサポートされているリージョンのリストについては、「Tag policies | Support Regions」を参照してください。

使用可能な のリスト AWS リージョン

次の表では使用できるすべての AWS リージョンを示します。

リージョン名	リージョン	エンドポイント	プロトコル
米国東部 (オハイオ)	us-east-2	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
米国東部 (バージニア北部)	us-east-1	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
米国西部 (北カリフォルニア)	us-west-1	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
米国西部 (オレゴン)	us-west-2	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS

リージョン名	リージョン	エンドポイント	プロトコル	
アフリカ (ケープタウン)	af-south-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
アジアパシフィック (香港)	ap-east-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
アジアパシフィック (ハイデラバード)	ap-south-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
アジアパシフィック (ジャカルタ)	ap-southeast-3	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
アジアパシフィック (マレーシア)	ap-southeast-5	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
アジアパシフィック (メルボルン)	ap-southeast-4	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
アジアパシフィック (ムンバイ)	ap-south-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	

リージョン名	リージョン	エンドポイント	プロトコル	
アジアパシフィック (大阪)	ap-northeast-3	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
アジアパシフィック (ソウル)	ap-northeast-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
アジアパシフィック (シンガポール)	ap-southeast-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
アジアパシフィック (シドニー)	ap-southeast-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
アジアパシフィック (台北)	ap-east-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
アジアパシフィック (タイ)	ap-southeast-7	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
アジアパシフィック (東京)	ap-northeast-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
カナダ (中部)	ca-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	

リージョン名	リージョン	エンドポイント	プロトコル
カナダ西部 (カルガリー)	ca-west-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
欧州 (フランクフルト)	eu-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
欧州 (アイルランド)	eu-west-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
欧州 (ロンドン)	eu-west-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
ヨーロッパ (ミラノ)	eu-south-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
欧州 (パリ)	eu-west-3	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
欧州 (スペイン)	eu-south-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
欧州 (ストックホルム)	eu-north-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
欧州 (チューリッヒ)	eu-central-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS

リージョン名	リージョン	エンドポイント	プロトコル
イスラエル (テルアビブ)	il-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
メキシコ (中部)	mx-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
中東 (バーレーン)	me-south-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
中東 (アラブ首長国連邦)	me-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
南米 (サンパウロ)	sa-east-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
AWS GovCloud (米国東部)	us-gov-east-1	organizations.us-gov-west-1.amazonaws.com	HTTPS
AWS GovCloud (米国西部)	us-gov-west-1	organizations.us-gov-west-1.amazonaws.com	HTTPS

の請求と料金 AWS Organizations

AWS Organizations は追加料金なしで提供されます。メンバーアカウントのユーザーとロールが使用する AWS リソースに対してのみ課金されます。例えば、メンバーアカウントのユーザーまたはロー

ルが使用する Amazon EC2 インスタンスの標準料金が請求されます。他のサービスの料金については AWS 、AWS 「 料金表」を参照してください。

組織内の AWS メンバーアカウントのユーザーによって発生した使用量に対して誰が支払いますか？

管理アカウントの所有者は、組織内のアカウントが使用するすべての使用状況、データ、リソースに対して支払いを行います。

請求書には、組織内で作成した組織単位構造が反映されますか?

請求書には、組織で定義した構造が反映されません。コスト配分タグを個々の で使用 AWS アカウント して、 AWS コストを分類および追跡できます。この配分は、組織の一括請求に表示されます。

のサポートとフィードバック AWS Organizations

ご意見をお待ちしております。feedback-awsorganizations@amazon.com にコメントを送信することができます。また、AWS Organizations サポートフォーラムにフィードバックと質問を掲載することができます。 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。

その他の AWS リソース

- AWS トレーニングとコース – スキルを磨き AWS 、実践的な経験を積むのに役立つ、役割ベースのコースや専門コース、セルフペースラボへのリンクです。
- AWS デベロッパーツール - AWSを使用して革新的なアプリケーションを構築する際に役立つ、ドキュメント、サンプルコード、リリースノート、その他の情報を提供するデベロッパーツールとリソースへのリンクです。
- AWS サポート センター – AWS サポートケースを作成および管理するためのハブ。フォーラム、技術上のよくある質問、サービスヘルスステータス、 AWS Trusted Advisor などの便利なリソースへのリンクも含まれています。
- AWS サポート – AWS クラウドでのアプリケーションの構築と実行に役立つ one-on-one の迅速な対応のサポートチャネルである サポートに関する情報のプライマリウェブページ。
- お問い合わせ — AWS 請求、アカウント、イベント、不正使用、その他の問題に関するお問い合わせの受付窓口です。

- AWS サイト規約 – 当社の著作権と商標、お客様のアカウント、ライセンス、サイトアクセス、およびその他のトピックに関する詳細情報。

マルチアカウント環境におけるベストプラクティス

マルチアカウント環境のセットアップと管理については、以下の推奨事項に従ってください AWS Organizations。

トピック

- アカウントと認証情報
- 組織構造とワークロード
- サービスとコスト管理

アカウントと認証情報

ルートアクセス管理を有効にして、メンバーアカウントのルートユーザー認証情報の管理を簡素化する

メンバーアカウントのルートユーザー認証情報のモニタリングと削除に役立つルートアクセス管理を有効にすることをお勧めします。ルートアクセス管理は、ルートユーザーの認証情報の復旧を防ぎ、組織内のアカウントセキュリティを向上させます。

- メンバーアカウントのルートユーザー認証情報を削除して、ルートユーザーへのサインインを防止します。これにより、メンバーアカウントによるルートユーザーの復旧も防止されます。
- メンバーアカウントで次のタスクを実行する特権セッションを想定します。
  - すべてのプリンシパルが Amazon S3 バケットにアクセスすることを拒否する、誤って設定されたバケットポリシーを削除します。
  - すべてのプリンシパルによる Amazon SQS キューへのアクセスを拒否する Amazon Simple Queue Service リソースベースのポリシーを削除します。
  - メンバーアカウントにルートユーザーの認証情報の復元を許可します。メンバーアカウントのルートユーザーの E メールAmazon メール受信トレイにアクセスできるユーザーは、ルートユーザーのパスワードをリセットし、メンバーアカウントのルートユーザーとしてサインインできます。

ルートアクセス管理を有効にすると、新しく作成されたメンバーアカウントはsecure-by-defaultになり、ルートユーザーの認証情報がないため、プロビジョニング後の MFA などの追加のセキュリティが不要になります。

詳細については、「 AWS Identity and Access Management 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認証情報を一元化する」を参照してください。

連絡先の電話番号を最新の状態に保つ

へのアクセスを回復するには AWS アカウント、テキストメッセージや通話を受信できる有効でアクティブな連絡先電話番号を用意することが重要です。アカウントのサポートと復旧の目的で AWS からお客様に連絡できるように、専用の電話番号を使用することをお勧めします。または Account Management APIs を使用して、 AWS Management Console アカウントの電話番号を簡単に表示および管理できます。

がお客様に AWS 確実に連絡できるように、専用の電話番号を取得するにはさまざまな方法があります。専用の SIM カードと電話機を入手することを強くおすすめします。電話番号をアカウントの復旧に使用できるように、電話機と SIM を長期間安全に保管します。また、携帯電話料金の請求処理を担当するチームが、この番号が長期間使用されない場合でも重要な番号であることを理解していることを確認してください。この電話番号は、さらなる保護のために、組織内で秘密にしておくことが不可欠です。

AWS 連絡先情報コンソールページに電話番号を記録し、その詳細を組織内の特定のチームと共有します。このアプローチは、電話番号を別の SIM に転送する際に生じるリスクを最小限に抑えるのに役立ちます。電話は、既存の情報セキュリティポリシーに従って保管します。ただし、保管場所は、関連する他の認証情報と同じにしてはなりません。電話機とその保存場所へのアクセスはすべてログに記録し、モニタリングする必要があります。アカウントに関連付けられている電話番号が変更された場合は、既存のドキュメントに記載の電話番号を更新するプロセスを実施してください。

ルートアカウントにグループメールアドレスを使用する

会社が管理するメールアドレスを使用します。受信したメッセージをユーザーのグループに直接転送するメールアドレスを使用します。がアクセスを確認するためにアカウントの所有者に連絡 AWS する必要がある場合、E メールメッセージは複数の当事者に配信されます。こうすることで、誰かが休暇中や病欠であるか、あるいはすでに退職している場合でも、応答の遅延のリスクを軽減できます。

組織構造とワークロード

アカウントを 1 つの組織内で管理する

1 つの組織を作成し、その組織内ですべてのアカウントを管理することをおすすめします。組織は、環境のアカウント間の一貫性を維持するためのセキュリティ境界です。組織のアカウントに対し、ポリシーやサービスレベルの設定を一元的に適用できます。マルチアカウント環境全体で一貫したポリ

シー、一元的な可視性、プログラムによる制御を実現したい場合は、単一の組織内で実現するのが最適です。

報告体制ではなく、ビジネス目的に基づいてワークロードをグループ化する

本番環境のワークロード環境とデータを、最上位のワークロード指向の OU に分離することをおすすめします。OU は、会社の報告体制を反映するのではなく、共通のコントロールセットに基づいて作成する必要があります。本番環境の OU とは別に、ワークロードの開発とテストに使用されるアカウントとワークロード環境を含む非本番環境の OU を 1 つ以上定義することがおすすめです。追加のガイダンスについては、「ワークロード指向の OU を構成する」を参照してください。

複数のアカウントを使用してワークロードを整理する

AWS アカウント は、 AWS リソースの自然なセキュリティ、アクセス、請求の境界を提供します。複数のアカウントを使用することには、アカウントレベルのクォータと API リクエストレートの制限を分散できるというメリットがあります。その他にも、こちらに記載されているようなメリットがあります。セキュリティ、ログ、インフラストラクチャ用のアカウントなど、組織全体の基本アカウントを複数使用することをおすすめします。ワークロードアカウントの場合、本番用ワークロードとテスト/開発用ワークロードを別々のアカウントに分ける必要があります。

サービスとコスト管理

AWS サービスコンソールまたは API/CLI オペレーションを使用して組織レベルでサービスを有効にする

ベストプラクティスとして、そのサービスのコンソール、または API オペレーション/CLI コマンドに相当するもの AWS Organizations を使用して、 と統合するサービスを 間で有効または無効にすることをお勧めします。この方法を使用すると、 AWS サービスを無効にするときに、必要なリソースの作成やリソースのクリーンアップなど、組織に必要なすべての初期化ステップを実行できます。AWS アカウント管理 は、 AWS Organizations コンソールまたは APIs を使用して有効にする必要がある唯一のサービスです。と統合されているサービスのリストを確認するには AWS Organizations、「」を参照してくださいAWS のサービス で使用できる AWS Organizations。

請求ツールを使用してコストを追跡し、リソースの使用を最適化する

組織を管理する場合、組織内のアカウントのすべての料金が網羅的にまとめられた一括請求書が届きます。コストを可視化する必要のあるビジネスユーザーには、請求ツールやコストツールを確認

するために、読み取り専用の制限つき権限ロールを管理アカウントに割り当てることができます。たとえば、請求レポートへのアクセスを許可する権限セットを作成したり、 AWS Cost Explorer Service (経時的なコスト傾向を表示するツール)を使用したり、Amazon S3 ストレージレンズ、AWS Compute Optimizer などのコスト効率化サービスを使用したりできます。

組織リソース全体でのタグ付け戦略とタグの適用を計画する

アカウントやワークロードがスケールしてくると、コスト追跡、アクセス制御、リソースの整理にタグが役立ちます。命名戦略のタグ付けについては、「 AWS リソースのタグ付け」のガイダンスに従ってください。リソースの他にも、組織のルート、アカウント、OU、およびポリシーにタグを作成することができます。詳しくは、「タグ付け戦略の構築」を参照してください。

の開始方法 AWS Organizations

次のトピックでは、 AWS Organizationsの使用の開始に役立つ情報を提供します。以下のチュートリアルを使用して、 AWS Organizationsを使用してタスクの実行を開始することもできます。

チュートリアル: 組織の作成と設定

組織の作成、最初のメンバーアカウントの招待、アカウントを含む OU 階層の作成、サービスコントロールポリシー (SCP) の適用に関する手順を実行します。

チュートリアル: Amazon EventBridge を使用して、組織の重要な変更をモニタリングする

組織内で指定したアクションが発生した場合に、E メール、SMS テキストメッセージ、またはログエントリの形式でアラームをトリガーするように Amazon EventBridge を設定し、組織での主要な変更をモニタリングします。例えば、多くの組織は、アカウントの作成日時や、アカウントが登録解除された日時を必要としています。

トピック

- にサインアップする AWS
- アクセス AWS Organizations
- チュートリアル: 組織の作成と設定
- チュートリアル: Amazon EventBridge を使用して、組織の重要な変更をモニタリングする
- AWS SDK AWS Organizations での の使用

にサインアップする AWS

トピック

- にサインアップする AWS アカウント
- 管理アクセスを持つユーザーを作成する

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

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

   サインアップ手順の一環として、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザー が作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、ルートユーザーアクセスが必要なタスクの実行にはルートユーザーのみを使用するようにしてください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、日常的なタスクにルートユーザーを使用しないように AWS アカウントのルートユーザー、 を保護し AWS IAM Identity Center、 を有効にして管理ユーザーを作成します。

を保護する AWS アカウントのルートユーザー

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

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

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

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。

2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

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

管理アクセス権を持つユーザーとしてサインインする

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

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

追加のユーザーにアクセス権を割り当てる

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

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

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

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

アクセス AWS Organizations

は、次のいずれか AWS Organizations の方法で使用できます。

AWS Management Console

AWS Organizations コンソールは、組織と AWS リソースの管理に使用できるブラウザベースのインターフェイスです。コンソールを使用して、組織内の任意のタスクを実行できます。

AWS コマンドラインツール

AWS コマンドラインツールを使用すると、システムのコマンドラインでコマンドを発行して、AWS Organizations および AWS タスクを実行できます。コマンドラインを使用すると、コンソールよりも高速かつ便利になります。コマンドラインツールは、 AWS のタスクを実行するスクリプトを作成する場合に便利です。

AWS には、次の 2 セットのコマンドラインツールが用意されています。

- AWS Command Line Interface

  AWS Command Line Interface （ AWS CLI) は、 を管理するための統合ツールです AWS のサービス。ダウンロードと設定のツールを 1 つだけ使用すると、コマンドライン AWS のサービス から複数の を制御し、スクリプトを使用して自動化できます。

  のインストールと使用の詳細については AWS CLI、 AWS Command Line Interface ユーザーガイドを参照してください。

- AWS Tools for Windows PowerShell

  Tools for Windows PowerShell を使用すると、開発者と管理者は PowerShell スクリプト環境で AWS のサービス とリソースを管理できます。Windows、Linux、MacOS 環境の管理に使用するのと同じ PowerShell ツールで AWS リソースを管理できます。

  Tools for Windows PowerShell のインストールおよび使用の方法については、AWS Tools for PowerShell ユーザーガイドを参照してください。

AWS SDK

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

AWS Organizations HTTPS クエリ API

AWS Organizations HTTPS クエリ API を使用すると、 AWS Organizations と にプログラムでアクセスできます AWS。HTTPS クエリ API を使用すると、HTTPS リクエストを直接サービスに

発行できます。HTTPS API を使用する場合は、認証情報を使用してリクエストにデジタル署名するコードを含める必要があります。詳細については、HTTP クエリリクエストを作成して API を呼び出す、および AWS Organizations API リファレンスを参照してください。

チュートリアル: 組織の作成と設定

このチュートリアルでは、組織を作成し、2 つの AWS メンバーアカウントで設定します。組織のメンバーアカウントのいずれかを作成し、お客様の組織に参加する他のアカウントを招待します。次に、許可リストの手法を使用して、アカウント管理者が明示的にリストされたサービスとアクションだけを委任できるように指定します。これにより、管理者は、 AWS によって導入された新しいサービスを、社内の他のユーザーが使用することを許可する前に検証できます。これにより、 が新しいサービス AWS を導入した場合、管理者が適切なポリシーの許可リストにサービスを追加するまで禁止されたままになります。このチュートリアルでは、拒否リストを使用して、メンバーアカウントのユーザーが が AWS CloudTrail 作成する監査ログの設定を変更できないようにする方法も示します。

次の図は、チュートリアルの主なステップを示しています。

ステップ 1: 組織を作成する

このステップでは、現在の を管理アカウント AWS アカウント として持つ組織を作成します。また、組織に参加する AWS アカウント ように招待し、メンバーアカウントとして 2 番目のアカウントを作成します。

ステップ 2: 組織単位を作成する

次に、新しい組織に 2 つの組織単位 (OU) を作成し、それらの OU にメンバーアカウントを配置します。

ステップ 3: サービスコントロールポリシーを作成する

サービスコントロールポリシー (SCP) を使用して、メンバーアカウントのユーザーおよびロールに委任できるアクションを制限することができます。このステップでは、2 つの SCP を作成し、それらを組織の OU にアタッチします。

ステップ 4: 組織のポリシーをテストする

各テストアカウントからユーザーとしてサインインし、SCP がアカウントに及ぼす影響を確認することができます。

このチュートリアルのどのステップでも、 AWS 請求書にコストはかかりません。 AWS Organizations は無料サービスです。

前提条件

このチュートリアルでは、2 つの既存の AWS アカウント（ このチュートリアルの一部として 3 番目の を作成する) にアクセスできること、および各 に管理者としてサインインできることを前提としています。

このチュートリアルでは、アカウントを次のように参照します。

- 111111111111 - 組織を作成するために使用するアカウント。このアカウントが管理アカウントになります。このアカウントの所有者には、E メールアドレス OrgAccount111@example.com があります。
- 222222222222 - メンバーアカウントとして組織に参加するように招待されたアカウント。このアカウントの所有者には、E メールアドレス member222@example.com があります。
- 333333333333 - 組織のメンバーとして作成するアカウント。このアカウントの所有者には、E メールアドレス member333@example.com があります。

上記の値をテストアカウントに関連付けられた値に置き換えます。このチュートリアルでは、本番稼働用アカウントを使用しないことをお勧めします。

ステップ 1: 組織を作成する

このステップでは、管理者としてアカウント 111111111111 にサインインし、そのアカウントを管理アカウントとして組織を作成し、メンバーアカウントとして参加するように既存カウント 222222222222 を招待します。

AWS Management Console

1. アカウント 111111111111 の管理者 AWS として にサインインし、 AWS Organizations コンソールを開きます。
2. 概要ページで、[Create an organization] (組織を作成する) を選択します。
3. 確認ダイアログボックスで、[Create an organization] (組織を作成する) を選択します。

> **Note**
>
> デフォルトでは、組織はすべての機能を有効にして作成されます。また、一括請求機能のみを有効にした組織を作成することもできます。

AWS は組織を作成し、AWS アカウントページを表示します。別のページが表示されている場合は、左側のナビゲーションペインで AWS アカウント を選択します。

これまでに、ご利用のアカウントのメールアドレスが認証されたことがない場合は、管理アカウントに関連付けられたアドレスに、検証用の E メールが AWSによって自動的に送信されます。検証 E メールの受信には時間がかかる場合があります。

4. 24 時間以内に E メールアドレスを検証します。詳細については、「による E メールアドレスの検証 AWS Organizations」を参照してください。

これで、メンバーだけのアカウントを持つ組織ができました。これは、組織の管理アカウントです

組織に参加するために既存のアカウントを招待する

現在組織がありますので、アカウントの入力を開始できます。このセクションのステップでは、参加する既存のアカウントを組織のメンバーとして招待します。

AWS Management Console

参加する既存のアカウントを招待するには

1. AWS アカウントページに移動し、[Add an AWS アカウント] (AWS アカウントの追加) を選択します。
2. 「 AWS アカウントの追加」ページで、「既存の を招待する AWS アカウント」を選択します。
3. [Email address or account ID of an AWS アカウント to invite] (招待する AWS アカウント の E メールアドレスまたはアカウント ID) ボックスに、招待するアカウントの所有者の E メールアドレスを **`member222@example.com`** のように入力します。または、 AWS アカウント ID 番号がわかっている場合は、代わりに入力することもできます。
4. [Message to include in the invitation email message] (招待 E メールのメッセージに含めるメッセージ) ボックスに、必要なテキストを入力します。このテキストに含まれているアカウントの所有者に E メールが送信されます。

5. 「招待を送信する」を選択します。 AWS Organizations は招待をアカウント所有者に送信します。

> **Important**
>
> エラーがある場合、エラーメッセージを展開します。組織のアカウント制限を超過したことを示すエラーが発生した場合、または組織がまだ初期化中であるためアカウントを追加できない場合は、組織を作成してから 1 時間後にもう一度試してください。それでもエラーが解決しない場合は、AWS サポートまでお問い合わせください。

6. このチュートリアルでは、独自の招待を受け入れる必要があります。次のいずれかを実行して、コンソールの [Invitations] ページに移動します。

   - 管理アカウントから AWS 送信された E メールを開き、招待を受け入れるリンクを選択します。サインインするように求められたら、招待されたメンバーアカウントの管理者としてログインします。
   - AWS Organizations コンソールを開き、[Invitations] (招待) ページに移動します。

7. AWS アカウント ページで、[Accept] (許可)、[Confirm] (確認) の順に選択します。

> **Tip**
>
> 招待の送信が遅れることがあるため、招待を受信するまで待つ必要がある場合があります。

8. メンバーアカウントからサインアウトし、管理アカウントの管理者ユーザーとして再度サインインします。

メンバーアカウントを作成する

このセクションのステップでは、自動的に組織のメンバー AWS アカウント となる を作成します。このチュートリアルでは、このアカウントを 333333333333 とします。

AWS Management Console

メンバーアカウントを作成するには

1. AWS Organizations コンソールのAWS アカウントページで、追加 AWS アカウント を選択します。
2. [Add an AWS アカウント] (の追加) ページで、[Create an AWS アカウント] (の作成) を選択します。
3. [AWS アカウント name] (AWS アカウント 名) には、**MainApp Account** などのアカウント名を入力します。
4. [Email address of the account's root user] (アカウントのルートユーザーの E メールアドレス) には、アカウントに代わって通信を受信する個人の E メールアドレスを入力します。この値は、グローバルで一意であることが必要です。2 つのアカウントで同じ E メールアドレスを使用することはできません。たとえば、**mainapp@example.com** のようなものを使用できます。
5. [IAM role name] の場合は、このフィールドを空白のままにしてデフォルトのロール名 `OrganizationAccountAccessRole` を自動的に使用するか、独自の名前を付けることができます。このロールを使用すると、管理アカウントで IAM ユーザーとしてサインインしたときに、新しいメンバーアカウントにアクセスできます。このチュートリアルでは、ブランクのままにして、 AWS Organizations にデフォルト名のロールを作成するよう指示します。
6. [作成] AWS アカウント を選択します。新しいアカウントが AWS アカウント ページに表示されるのを確認するには、しばらく待ってからページを更新する必要があります。

> **Important**
>
> 組織のアカウント制限を超過したことを示すエラーが発生した場合、または組織がまだ初期化中であるためアカウントを追加できない場合は、組織を作成してから 1 時間待つか、もう一度試してください。それでもエラーが解決しない場合は、AWS サポートまでお問い合わせください。

ステップ 2: 組織単位を作成する

このセクションのステップでは、組織単位 (OU) を作成し、メンバーアカウントを配置します。完了すると、階層は次の図のようになります。管理アカウントはルートのままになります。1 つのメンバーアカウントは本稼働の OU に移動され、他のメンバーアカウントは本番稼働用の子である MainApp OU に移動されます。

AWS Management Console

OU を作成して設定するには

> **Note**
>
> 次の手順では、オブジェクト自体の名前またはオブジェクトの横にあるラジオボタンのいずれかを選択するため、オブジェクトを操作します。
>
> - オブジェクトの名前を選択すると、オブジェクトの詳細を表示する新しいページが開きます。
> - オブジェクトの横にあるラジオボタンをクリックすると、オプションメニューの選択など、別のアクションによって処理されるオブジェクトが表示されます。
>
> 次のステップでは、ラジオボタンをクリックしてメニューを選択し、関連するオブジェクトを処理します。

1. AWS Organizations コンソールで、AWS アカウント ページに移動します。
2. ルートコンテナの横にあるチェックボックス

   をオンにします。
3. [アクション] ドロップダウンを選択し、[組織単位] で [新規作成] を選択します。
4. [Create organizational unit in Root] (ルートでの組織単位の作成) ページで、[Organizational unit name] (組織単位名) に **`Production`** と入力し、[Create organizational unit] (組織単位の作成) を選択します。
5. 新しいProduction OU の横にあるチェックボックス

   をオンにします。
6. [Actions] (アクション) を選択し、[Organizational unit] (組織単位) で [Create new] (新規作成) を選択します。
7. [Create organizational unit in Production] (本番環境での組織単位の作成) ページで、2 番目の OU の名前として **`MainApp`** を入力し、[Create organizational unit] (組織単位の作成) を選択します。

これで、メンバーアカウントをこれらの OU に移動できます。

8. AWS アカウントページに戻り、[Production OU] (運用 OOU) の横にある三角形

   をクリックして、その下のツリーを展開します。これにより、[MainApp] OU が [Production] の子として表示されます。

9. [333333333333] の横にあるチェックボックス

   をオンにし (名前ではない)、[アクション] を選択してから、AWS アカウント の下の [移動] を選択します。

10. Move AWS アカウント '333333333333' ページで、Production の横にある三角形を選択して展開します。MainApp の横にあるラジオボタン

    を選択してから (名前ではない)、[AWS アカウントを移動] を選択します。

11. [222222222222] の横にあるチェックボックス

    をオンにし (名前ではない)、[アクション] を選択してから、AWS アカウント の下の [移動] を選択します。

12. Move AWS アカウント '222222222222' ページの Production の横にあるラジオボタン (名前ではない) を選択し、Move AWS アカウントを選択します。

ステップ 3: サービスコントロールポリシーを作成する

このセクションのステップでは、3 つのサービスコントロールポリシー (SCP) を作成し、それらを root と OU にアタッチして、組織のアカウントのユーザーの実行範囲を制限します。最初の SCP は、メンバーアカウントのすべてのユーザーが、設定した AWS CloudTrail ログを作成または変更することを禁止します。管理アカウントは SCP の影響を受けません。したがって、CloudTrail SCP を適用した後、管理アカウントのログを作成する必要があります。

組織のサービスコントロールポリシータイプを有効にする

いずれかのタイプのポリシーをルートまたはルート内の任意の OU にアタッチするには、その組織のポリシータイプを有効にする必要があります。ポリシータイプは、デフォルトでは有効になっていません。このセクションのステップでは、組織のサービスコントロールポリシー (SCP) タイプを有効にする方法を示します。

AWS Management Console

組織の SCP を有効にするには

1. ポリシーページに移動し、[サービスコントロールポリシー] を選択します。
2. サービスコントロールポリシー ページで、[サービスコントロールポリシーを有効にする] を選択します。

   緑色のバナーが表示され、組織で SCP を作成できるようになりました。

SCP の作成

組織のサービスコントロールポリシーが有効になったので、このチュートリアルに必要な 3 つのポリシーを作成できます。

AWS Management Console

CloudTrail 設定アクションをブロックする最初の SCP を作成するには

1. ポリシーページに移動し、[サービスコントロールポリシー] を選択します。
2. サービスコントロールポリシーページで、[ポリシーの作成] を選択します。
3. [ポリシー名] に「**Block CloudTrail Configuration Actions**」と入力します。
4. [ポリシー] セクションで、右側のサービスのリストで、CloudTrail を選択します。次に、以下のアクションを選択します。[AddTags]、[CreateTrail]、[DeleteTrail]、[RemoveTags]、[StartLogging]、[StopLogging]、[UpdateTrail]。
5. 引き続き右側のペインで、[リソースの追加] を選択し、[CloudTrail] および [すべてのリソース] を指定します。[リソースの追加] を選択します。

   左側のポリシーステートメントは次のようになります。

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1234567890123",
            "Effect": "Deny",
            "Action": [
```

```
                "cloudtrail:AddTags",
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:RemoveTags",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. [Create policy] (ポリシーの作成) を選択します。

2 番目のポリシーは、Production OU のユーザーとロールが使用できるすべてのサービスとアクションの許可リストを定義します。終了したら、本稼働の OU のユーザーはリストにあるサービスとアクションのみにアクセスすることができます。

AWS Management Console

Production OU の承認されたサービスを許可する第 2 のポリシーを作成するには

1. サービスコントロールポリシーページから、[Create policy] (ポリシーの作成) を選択します。
2. [ポリシー名] に「**Allow List for All Approved Services**」と入力します。
3. カーソルの右ペインの [ポリシー] セクションに合わせ、次のようにポリシーを貼り付けます。

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1111111111111",
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:*",
                "elasticloadbalancing:*",
                "codecommit:*",
                "cloudtrail:*",
                "codedeploy:*"
              ],
            "Resource": [ "*" ]
        }
    ]
}
```

4. [Create policy] (ポリシーの作成) を選択します。

最後のポリシーは、MainApp OU での使用がブロックされているサービスの拒否リストを提供します。このチュートリアルでは、MainApp OU にあるすべてのアカウントの Amazon DynamoDB へのアクセスをブロックします。

AWS Management Console

MainApp OU で使用できないサービスへのアクセスを拒否する 3 番目のポリシーを作成するには

1. サービスコントロールポリシーページから、[Create policy] (ポリシーの作成) を選択します。
2. [ポリシー名] に「**Deny List for MainApp Prohibited Services**」と入力します。
3. 左側の [Policy] (ポリシー) セクションで、サービスに [Amazon DynamoDB] を選択します。アクションでは、[すべてのアクション] を選択します。
4. 引き続き左側のペインで、[Add resource](リソースの追加) を選択し、[DynamoDB] および [All Resources] (すべてのリソース) を指定します。[リソースの追加] を選択します。

   右側の更新ポリシーステートメントは次のようになります。

   JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [ "dynamodb:*" ],
      "Resource": [ "*" ]
```

```
    }
  ]
}
```

5. [ポリシーの作成] を選択して SCP を保存します。

SCP を OU にアタッチする

これで SCP はルートに対して有効になったため、ルートおよび OU にアタッチすることができます。

AWS Management Console

root と OU にポリシーをアタッチするには

1. AWS アカウント ページに移動します。
2. AWS アカウントページで、[Root] (ラジオボタンではなく名前) を選択し、詳細ページに移動します。
3. [Root] (ルート) の詳細ページで [Policies] (ポリシー) を選択してから、[Service Control Policies] (サービスコントロールポリシー) で [Attach] (アタッチ) を選択します
4. [Attach a service control policy] (サービスコントロールポリシーのアタッチ) ページで、SCP の横にある `Block CloudTrail Configuration Actions` というラジオボタンをクリックし、[Attach] (アタッチ) を選択します。このチュートリアルでは、サービスコントロールポリシーをルートにアタッチして、すべてのメンバーアカウントに影響を与え、CloudTrail の設定方法を誰にも変更されないようにします。

   [Root] (ルート) の詳細ページの [Policies] (ポリシー) タブで、2 つの SCP (アタッチした SCP とデフォルトの `FullAWSAccess` SCP) がルートにアタッチされていることが確認できました。
5. AWS アカウントページに戻り、[Production OU] (ラジオボタンではなく名前) を選択して、詳細ページに移動します。
6. [Production OU] の詳細ページで、[Policies] (ポリシー) タブを選択します。
7. [Service Control Policies] (サービスコントロールポリシー) で [Attach] (アタッチ) を選択します。
8. [Attach a service control policy] (サービスコントロールポリシーのアタッチ) ページで、`Allow List for All Approved Services` の横にあるラジオボタンをクリックし

てから [Attach] (アタッチ) を選択します。これにより、Production OUのメンバーアカウントのユーザーまたはロールが、承認されたサービスにアクセスできるようになります。

9. [ポリシー] タブを再度選択して、2 つの SCP が OU にアタッチされていることを確認します。先ほどアタッチした SCPと、デフォルトの `FullAWSAccess` SCPです。ただし、`FullAWSAccess` SCP はすべてのサービスとアクションを許可する許可リストでもあるため、承認されたサービスのみが許可されるように、今はこの SCP をデタッチする必要があります。
10. Production OU からデフォルトのポリシーを削除するには、[FullAWSAccess] のラジオボタンをクリックし、[Detach] (デタッチ) を選択してから、確認ダイアログボックスで [Detach policy] (ポリシーのデタッチ) を選択します。

    このデフォルトポリシーを削除すると、Production OU のすべてのメンバーアカウントは、直前のステップでアタッチした、許可リスト SCP にないすべてのアクションとサービスにすぐにアクセスできなくなります。Allow List for All Approved Services SCP に含まれていないアクションを使用するリクエストはすべて拒否されます。これは、アカウントの管理者が、メンバーアカウントのいずれかのユーザーに IAM アクセス許可ポリシーをアタッチして別のサービスへのアクセスを許可する場合にも当てはまります。
11. `Deny List for MainApp Prohibited services` という名前の SCP をアタッチして、MainApp OU 内のアカウントの誰も制限付きサービスを使用できないように制限できるようになりました。

    これを行うには、AWS アカウントページに移動し、三角形のアイコンを選択して [Production OU] のブランチを展開してから、[MainApp] OU (ラジオボタンではなく名前) を選択して、その内容に移動します。
12. MainApp の詳細ページで、[Policies] (ポリシー) タブを選択します。
13. [Service Control Policies] (サービスコントロールポリシー) で [Attach] (アタッチ) を選択し、使用可能なポリシーのリストで、[Deny List for MainApp Prohibited Services] (MainApp で禁止されたサービスの拒否リスト) の横にあるラジオボタンをクリックしてから、[Attach policy] (ポリシーのアタッチ) を選択します。

ステップ 4: 組織のポリシーをテストする

これで、メンバーアカウントのいずれかのユーザーでサインインし、さまざまな AWS アクションを実行できるようになりました。

- 管理アカウントでユーザーとしてサインインすると、IAM アクセス許可ポリシーで許可されているオペレーションを実行することができます。SCP は、アカウントがどのルートまたは OU に属していても、管理アカウントのユーザーまたはロールに影響を与えません。
- アカウント 222222222222 でユーザーとしてサインインすると、許可リストで許可されているアクションを実行できます。 は、許可リストに含まれていないサービスでアクションを実行しようとする試み AWS Organizations を拒否します。また、 AWS Organizations は CloudTrail 設定アクションのいずれかの実行を拒否します。
- アカウント 333333333333 でユーザーとしてサインインすると、許可リストで許可され、拒否リストでブロックされていないアクションはすべて実行できます。 AWS Organizations は、許可リストポリシーにないアクションと拒否リストポリシーにあるアクションを実行しようとするすべての試みを拒否します。また、 AWS Organizations は CloudTrail 設定アクションのいずれかの実行を拒否します。

チュートリアル: Amazon EventBridge を使用して、組織の重要な変更をモニタリングする

このチュートリアルでは、組織の変更をモニタリングできるように Amazon EventBridge (旧 Amazon CloudWatch Events) を設定する方法を紹介します。まず、ユーザーが特定の AWS Organizations 操作を呼び出したときにトリガーされるルールを設定します。次に、ルールがトリガーされたときに AWS Lambda 関数を実行するように Amazon EventBridge を設定し、イベントに関する詳細を含む E メールを送信するように Amazon SNS を設定します。

次の図は、チュートリアルの主なステップを示しています。

ステップ 1: 証跡およびイベントセレクターを設定する

証跡と呼ばれるログを作成します AWS CloudTrail。すべての API コールをキャプチャするように設定します。

ステップ 2: Lambda 関数を設定する

イベントの詳細を S3 バケットに記録する AWS Lambda 関数を作成します。

ステップ 3: 受信者に E メールを送信する Amazon SNS トピックを作成する

受信者に E メールを送信する Amazon SNS トピックを作成し、自分自身でトピックをサブスクライブします。

ステップ 4: Amazon EventBridge ルールを作成する

指定された API コールの詳細を Lambda 関数および SNS トピックのサブスクライバーに渡すよう Amazon EventBridge に指示するルールを作成します。

ステップ 5: Amazon EventBridge ルールをテストする

監視対象の操作の 1 つを実行して新しいルールをテストします。このチュートリアルでは、監視対象の操作で、組織単位 (OU) を作成しています。Lambda 関数が作成するログエントリを表示し、Amazon SNS が受信者に送信する E メールを表示します。

> **ヒント**
>
> このチュートリアルを、アカウントの作成が完了した際のメール通知を送信など、類似したオペレーションを設定するガイドとして使用することもできます。アカウントの作成は非同期オペレーションであるため、デフォルトでは完了時に通知されません。 AWS CloudTrail と Amazon EventBridge を で使用する方法の詳細については AWS Organizations、「」を参照してくださいでの口グ記録とモニタリング AWS Organizations。

前提条件

このチュートリアルでは、次のことを前提としています。

- 組織の管理アカウントから IAM ユーザー AWS Management Console として にサインインできます。IAM ユーザーには、CloudTrail の口グ、Lambda の関数、Amazon SNS のトピック、Amazon EventBridge のルールを作成および設定するためのアクセス許可が必要です。アクセス許可を付与する方法の詳細については、IAM ユーザーガイドの「アクセス管理」または、アクセスを設定するサービスのガイドを参照してください。
- ステップ 1 で設定した CloudTrail ログを受信するための既存の Amazon Simple Storage Service (Amazon S3) バケットにアクセスできます (または、バケットを作成するアクセス許可があります)。

> **Important**
>
> 現在、 AWS Organizations は米国東部 (バージニア北部) リージョンでのみホストされています (グローバルに利用可能ですが) 。このチュートリアルのステップを実行するには、そのリージョンを使用する AWS Management Console ように を設定する必要があります。

ステップ 1: 証跡およびイベントセレクターを設定する

このステップでは、管理アカウントにサインインして、 AWS CloudTrailでログ (証跡と呼ばれる) を設定します。また、Amazon EventBridge がトリガーを呼び出すように、証跡でイベントセレクターを設定し、すべての読み取り/書き込み API コールをキャプチャします。

証跡を作成するには

1. 組織の管理アカウントの管理者 AWS として にサインインし、 で CloudTrail コンソールを開きますhttps://console.aws.amazon.com/cloudtrail/。
2. コンソールウィンドウの右上隅にあるナビゲーションバーで、米国東部 (バージニア北部) リージョンを選択します。別のリージョンを選択した場合、Amazon EventBridge AWS Organizations 設定ではオプションとして表示されず、CloudTrail は情報をキャプチャしませんAWS Organizations。
3. ナビゲーションペインで、[Trails] (追跡) を選択します。
4. [追跡の作成]を選択します。
5. [Trail name] (証跡名) に、**`My-Test-Trail`** と入力します。
6. CloudTrail がログを配信する場所を指定するには、次のいずれかのオプションを実行します。
   - バケットを作成する必要がある場合は、[Create a new S3 bucket] (新しい S3 バケットの作成) を選択し、[Trail log bucket and folder] (Trail ログバケットとフォルダ) に新しいバケットの名前を入力します。

     > **Note**
     >
     > S3 バケット名は、グローバルに 一意である必要があります。

   - 既にバケットがある場合、[Use existing S3 bucket] (既存の S3 バケットを使用) を選択し、次に S3 バケット リストからバケット名を選択します。
7. [Next (次へ)] を選択します。

8. [Choose log events] (ログイベントの選択) ページの [Management events] (管理イベント) セクションで、[Read] (読み取り) と [Write] (書き込み) を選択します。
9. [Next (次へ)] を選択します。
10. 場所を確認して [Create function] (関数の作成) を選択します。

Amazon EventBridge では、アラームルールが着信 API コールと一致したときに、アラートを送信する複数の異なる方法から選択できます。このチュートリアルでは、2 つの方法について説明します。API コールをログに記録できる Lambda 関数を呼び出す方法、およびトピックの受信者へ E メールまたはテキストメッセージを送信する Amazon SNS トピックに情報を送信する方法です。次の 2 つのステップでは、必要なコンポーネントである Lambda 関数および Amazon SNS トピックを作成します。

ステップ 2: Lambda 関数を設定する

このステップでは、後で設定する Amazon EventBridge ルールによって送信される API アクティビティをログに記録する Lambda 関数を作成します。

Amazon EventBridge イベントをログに記録する Lambda 関数を作成するには

1. で AWS Lambda コンソールを開きますhttps://console.aws.amazon.com/lambda/。
2. Lambda を初めて利用する場合は、ようこそページの [Get Started Now] (今すぐ始める) を選択するか、[Create function] (関数を作成) を選択します。
3. [Create function] (関数の作成) ページで、[Blueprints] (設計図) を選択します。
4. [設計図] 検索ボックスでは、フィルターに **`hello`** を入力し、[hello-world] 設計図を選択します。
5. [設定] を選択します。
6. [基本的な情報] ページでは、以下を実行します。
   a. [Name] (名前) テキストボックスに、Lambda 関数名として **`LogOrganizationEvents`** を入力します。
   b. [Role] で、[Create a new role with basic Lambda permissions] を選択します。このロールは、必要なデータにアクセスし、出力ログを書き込むために Lambda 関数にアクセス許可を付与します。
7. 次の例に示すように、 Lambda 関数のコードを編集します。

```
console.log('Loading function');
```

```
exports.handler = async (event, context) => {
    console.log('LogOrganizationsEvents');
    console.log('Received event:', JSON.stringify(event, null, 2));
    return event.key1;  // Echo back the first key value
    // throw new Error('Something went wrong');
};
```

このサンプルコードでは、「**LogOrganizationEvents**」マーカー文字列の後にイベントを構成する JSON 文字列を続けてイベントをログに記録します。

8. [Create function (関数の作成)] を選択します。

ステップ 3: 受信者に E メールを送信する Amazon SNS トピックを作成する

このステップでは、受信者に E メールで情報を送信する Amazon SNS トピックを作成します。このトピックを、後で作成する Amazon EventBridge ルールのターゲットにします。

受信者に E メールを送信する Amazon SNS トピックを作成するには

1. https://console.aws.amazon.com/sns/v3/ で Amazon SNS コンソールを開きます。
2. ナビゲーションペインで、[トピック] を選択します。
3. [Create new topic] を選択します。
   a. [トピック名] に **OrganizationsCloudWatchTopic** と入力します。
   b. [Display name (表示名)] に **OrgsCWEvnt** と入力します。
   c. [トピックの作成] を選択してください。
4. トピックのサブスクリプションを作成できるようになりました。先ほど作成したトピックの ARN を選択します。
5. [Create subscription] を選択します。
   a. [Create subscription] ページの [Protocol] で [Email] を選択します。
   b. [エンドポイント] に E メールアドレスを入力します。
   c. サブスクリプションの作成 を選択します。 AWS は、前のステップで指定した E メールアドレスに E メールを送信します。E メールが送信されたら、[サブスクリプションを確認] リンクを選択して、E メールを正常に受信したことを確認します。

d. コンソールに戻り、ページを更新します。[Pending confirmation] メッセージが表示されなくなり、現在有効なサブスクリプション ID に置き換えられます。

ステップ 4: Amazon EventBridge ルールを作成する

必要な Lambda 関数がアカウントに存在するようになったので、ルールの基準が満たされた場合にそのルールを呼び出す Amazon EventBridge ルールを作成します。

EventBridge ルールを作成するには

1. https://console.aws.amazon.com/events/ で[Amazon EventBridge console] (Amazon EventBridge コンソール) を開きます。
2. コンソールを米国東部 (バージニア北部)リージョンに設定しないと、Organizations に関する情報は利用できません。コンソールウィンドウの右上隅にあるナビゲーションバーで、米国東部 (バージニア北部) リージョンを選択します。
3. ルールの作成手順については、「Amazon EventBridge ユーザーガイド」の「Amazon EventBridge のルール」を参照してください。 EventBridge

ステップ 5: Amazon EventBridge ルールをテストする

このステップでは、組織単位 (OU) を作成して Amazon EventBridge ルールを確認し、ログエントリを生成して、イベントに関する詳細を E メールで送信します。

AWS Management Console

OU を作成するには

1. AWS Organizations コンソールを開き、 AWS アカウントページに移動します。
2. [
Root] (ルート) OU のチェックボックスをオンにし、[Action] (アクション) を選択してから、[Organizational unit] (組織単位) で [Create new] (新規作成) を選択します。
3. OU の名前では、**`TestCWEOU`** と入力してから、[Create organizational unit (組織単位の作成)] を選択します。

EventBridge ログエントリを表示するには

1. https://console.aws.amazon.com/cloudwatch/ にある CloudWatch コンソールを開きます。

2. ナビゲーションページで [Logs] (ログ) を選択します。
3. [Log Groups] (ロググループ) で、Lambda 関数 [/aws/lambda/LogOrganizationEvents] に関連付けられているグループを選択します。
4. 各グループには 1 つ以上のストリームがあり、今日のための 1 つのグループがあります。これを選択します。
5. ログを表示します。次のような行が表示されます。

6. エントリの中央の行を選択すると、受信したイベントの完全な JSON テキストが表示されます。API リクエストのすべての詳細は、出力の `requestParameters` および `responseElements` で確認できます。

```
2017-03-09T22:45:05.101Z 0999eb20-051a-11e7-a426-cddb46425f16 Received event:
{
    "version": "0",
    "id": "123456-EXAMPLE-GUID-123456",
    "detail-type": "AWS API Call via CloudTrail",
    "source": "aws.organizations",
    "account": "123456789012",
    "time": "2017-03-09T22:44:26Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventVersion": "1.04",
        "userIdentity": {
            ...
        },
        "eventTime": "2017-03-09T22:44:26Z",
        "eventSource": "organizations.amazonaws.com",
        "eventName": "CreateOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.168.0.1",
        "userAgent": "AWS Organizations Console, aws-internal/3",
        "requestParameters": {
            "parentId": "r-exampleRootId",
            "name": "TestCWEOU"
        },
        "responseElements": {
            "organizationalUnit": {
                "name": "TestCWEOU",
                "id": "ou-exampleRootId-exampleOUId",
```

```
                "arn": "arn:aws:organizations::1234567789012:ou/o-exampleOrgId/ou-
exampleRootId-exampeOUId"
            }
        },
        "requestID": "123456-EXAMPLE-GUID-123456",
        "eventID": "123456-EXAMPLE-GUID-123456",
        "eventType": "AwsApiCall"
    }
}
```

7. E メールアカウントで、[OrgsCWEvnt] (Amazon SNS トピックの表示名) からのメッセージを確認します。E メールの本文には、前のステップで示されたログエントリと同じ JSON テキスト出力が含まれます。

クリーンアップ: 不要になったリソースを削除する

料金が発生しないようにするには、このチュートリアルの一部として作成した、保持したくない AWS リソースをすべて削除する必要があります。

AWS 環境をクリーンアップするには

1. CloudTrail コンソールを使用して、ステップ 1 で作成した **My-Test-Trail** という名前の証跡を削除します。
2. ステップ 1 で Amazon S3 バケットを作成した場合は、Amazon S3 コンソールを使用して削除します。
3. Lambda コンソールを使用して、ステップ 2 で作成した **LogOrganizationEvents** という名前の関数を削除します。
4. Amazon SNS コンソールを使用して、ステップ 3 で作成した **OrganizationsCloudWatchTopic** という名前の Amazon SNS トピックを削除します。
5. CloudWatch コンソールを使用して、ステップ 4 で作成した **OrgsMonitorRule** という名前の EventBridge ルールを削除します。
6. 最後に、Organizations コンソールを使用して、ステップ 5 で作成した **TestCWEOU** という名前の OU を削除します。

これで完了です。このチュートリアルでは、組織の変更をモニタリングできるように EventBridge を設定しました。ユーザーが特定の AWS Organizations オペレーションを呼び出したときにトリガー

されるルールを設定しました。ルールによって、イベントを記録した Lambda 関数が実行され、イベントに関する詳細を含む E メールが送信されました。

AWS SDK AWS Organizations での の使用

AWS Software Development Kit (SDKsは、多くの一般的なプログラミング言語で利用できます。各 SDK には、デベロッパーが好みの言語でアプリケーションを簡単に構築できるようにする API、コード例、およびドキュメントが提供されています。

SDK ドキュメント	コード例
AWS SDK for C++	AWS SDK for C++ コード例
AWS CLI	AWS CLI コード例
AWS SDK for Go	AWS SDK for Go コード例
AWS SDK for Java	AWS SDK for Java コード例
AWS SDK for JavaScript	AWS SDK for JavaScript コード例
AWS SDK for Kotlin	AWS SDK for Kotlin コード例
AWS SDK for .NET	AWS SDK for .NET コード例
AWS SDK for PHP	AWS SDK for PHP コード例
AWS Tools for PowerShell	AWS Tools for PowerShell コード例
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) コード例
AWS SDK for Ruby	AWS SDK for Ruby コード例
AWS SDK for Rust	AWS SDK for Rust コード例
AWS SDK for SAP ABAP	AWS SDK for SAP ABAP コード例
AWS SDK for Swift	AWS SDK for Swift コード例

可用性の例

必要なものが見つからなかった場合。このページの下側にある [Provide feedback (フィードバックを送信)] リンクから、コードの例をリクエストしてください。

を使用した組織の管理 AWS Organizations

組織は、一元的に管理し、上部にルートがあり、ルートの下にネストされた組織単位を持つ階層的なツリーのような構造に整理 AWS アカウント できる のコレクションです。各アカウントは、ルートに直接含めるか、階層内の OU のいずれかに配置することができます。

各組織は以下で構成されます。

- 管理アカウント
- ゼロ以上のメンバーアカウント
- ゼロ以上の組織単位 (OU)
- ゼロ以上のポリシー。

組織には、有効にする機能セットによって決定された機能を含みます。

トピック

- を使用した組織の作成 AWS Organizations
- による E メールアドレスの検証 AWS Organizations
- で検証 E メールを再送信する AWS Organizations
- を使用して組織の E メールアドレスを変更する AWS Organizations
- を使用して組織のすべての機能を有効にする AWS Organizations
- 管理アカウントを使用した組織の詳細の表示
- を使用した組織の削除 AWS Organizations

を使用した組織の作成 AWS Organizations

を管理アカウント AWS アカウント として組織を作成できます。組織を作成する際、この組織がすべての機能 (推奨) をサポートする、または一括請求のみをサポートするかを選択できます。デフォルトでは、作成した組織はすべての機能をサポートします。

組織を作成する

組織を作成するには、 を使用するか、 AWS Management Console または SDK APIs AWS CLI のいずれかのコマンドを使用します。

最小アクセス許可

現在の で組織を作成するには AWS アカウント、次のアクセス許可が必要です。

- `organizations:CreateOrganization`
- `iam:CreateServiceLinkedRole`

  このアクセス許可は、サービスプリンシパルだけに制限できます`organizations.amazonaws.com`。

AWS Management Console

組織を作成するには

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. デフォルトでは、組織はすべての機能を有効にして作成されます。ただし、次のいずれかのステップを選択できます。

   - すべての機能が有効な組織を作成するには、概要ページで [Create an organization] (組織を作成する) を選択します。
   - 一括請求 (コンソリデーティッドビリング) 機能のみを持つ組織を作成するには、概要ページの [Create an organization] (組織を作成する) で一括請求 (コンソリデーティッドビリング) 機能を選択してから、[Create an organization] (組織を作成する) を選択します。

   オプションの選択を間違えた場合は、すぐに設定ページに移動して [Delete organization] (組織の削除) を選択し、もう一度やり直してください。
3. 組織が作成され、AWS アカウント ページが表示されます。存在するアカウントは管理アカウントのみで、この時点ではルート組織単位 (OU) に保存されています。

   必要に応じて、Organizations により、管理アカウントに関連付けられたアドレスに検証メールが自動的に送信されます。検証 E メールの受信には時間がかかる場合があります。24 時間以内に E メールアドレスを検証します。詳細については、「による E メールアドレスの検証 AWS Organizations」を参照してください。管理アカウントのメールアドレスを検証しなくても、組

織内に新しいアカウントを作成することは可能です。ただし、既存のアカウントを招待するには、その前にメールの検証が完了している必要があります。

> **Note**
>
> 以前にそのアカウントのメールアドレスの検証が行われていた場合は、そのアカウントを使用して組織を作成した際にメールの検証が再度求められることはありません。

AWS CLI & AWS SDKs

以下のコード例は、`CreateOrganization` の使用方法を示しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates an organization in AWS Organizations.
/// </summary>
public class CreateOrganization
{
    /// <summary>
    /// Creates an Organizations client object and then uses it to create
    /// a new organization with the default user as the administrator, and
    /// then displays information about the new organization.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
```

```
            var response = await client.CreateOrganizationAsync(new
CreateOrganizationRequest
            {
                FeatureSet = "ALL",
            });

            Organization newOrg = response.Organization;

            Console.WriteLine($"Organization: {newOrg.Id} Main Accoount:
{newOrg.MasterAccountId}");
        }
    }
```

- API の詳細については、AWS SDK for .NET API リファレンスの「CreateOrganization」を参照してください。

CLI

AWS CLI

例 1: 新しい組織を作成するには

Bill は、アカウント 111111111111 の認証情報を使用して組織を作成したいと考えています。次の例は、このアカウントが新しい組織のマスターアカウントになることを示しています。Bill は機能セットを指定していないため、新しい組織ではデフォルトですべての機能が有効になり、サービスコントロールポリシーがルート上で有効になります。

```
aws organizations create-organization
```

出力には、新しい組織に関する詳細を含む組織オブジェクトが含まれます。

```
{
        "Organization": {
                "AvailablePolicyTypes": [
                        {
                                "Status": "ENABLED",
                                "Type": "SERVICE_CONTROL_POLICY"
                        }
                ],
```

```
                "MasterAccountId": "111111111111",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "FeatureSet": "ALL",
                "Id": "o-exampleorgid",
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid"
        }
}
```

例 2: 一括決済機能のみを有効にした新しい組織を作成するには

次の例では、一括決済機能のみをサポートする組織を作成します。

```
aws organizations create-organization --feature-set CONSOLIDATED_BILLING
```

出力には、新しい組織に関する詳細を含む組織オブジェクトが含まれます。

```
{
        "Organization": {
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
                "AvailablePolicyTypes": [],
                "Id": "o-exampleorgid",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "MasterAccountId": "111111111111",
                "FeatureSet": "CONSOLIDATED_BILLING"
        }
}
```

詳細については、「AWS Organizations ユーザーガイド」の「Creating an Organization」を参照してください。

- API の詳細については、AWS CLI コマンドリファレンスの「CreateOrganization」を参照してください。

組織を作成した後、管理アカウントから以下の方法で組織にアカウントを追加できます。

- 自動的に組織のメンバーアカウントとして追加される AWS アカウントを別途作成する

- E メールアドレスを検証後、組織のメンバーアカウントとして参加するよう既存の AWS アカウントを招待する。

による E メールアドレスの検証 AWS Organizations

組織を作成したら、アカウントを招待する前に、組織の管理アカウントから提供されたメールアドレスを所有していることを検証する必要があります。

組織を作成するときに、管理アカウントが以前に検証されていない場合、 は指定された E メールアドレスに検証 E メール AWS を自動的に送信します。検証 E メールの受信には時間がかかる場合があります。

E メールアドレスを検証する

24 時間以内に E メール内の指示に従って、E メールアドレスを検証します。24 時間以上経過している場合は、「Resending the verification email」を参照してください。

で検証 E メールを再送信する AWS Organizations

24 時間以内にメールアドレスを検証しない場合、検証リクエストを再送信します。E メールアドレスを確認したら、他の AWS アカウント を組織に招待できます。検証 E メールが受信されない場合には、E メールアドレスが正しいことを確認し、必要に応じて変更します。

- 管理アカウントに関連付けられたメールアドレスを確認するには、管理アカウントを使用した組織の詳細の表示 を参照してください。
- 管理アカウントに関連付けられたメールアドレスを変更するには、AWS Billing ユーザーガイドの AWS アカウントの管理を参照してください。

AWS Management Console

検証リクエストを再送信するには

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. 設定ページに移動し、[Send verification request] (確認リクエストの送信) を選択します。このオプションは、管理アカウントが検証されていない場合にのみ表示されます。

3. 24 時間以内に E メールアドレスを検証します。

メールアドレスを検証したら、別の AWS アカウント を組織に招待できます。詳細については、「を使用したアカウント招待の管理 AWS Organizations」を参照してください。

を使用して組織の E メールアドレスを変更する AWS Organizations

管理アカウントに関連付けられている E メールアドレスを変更するには、「 AWS アカウント管理リファレンスガイド」の「ルートユーザー AWS アカウント の名前、E メールアドレス、またはパスワードの更新」を参照してください。

管理アカウントのメールアドレスを変更する場合、アカウントは「メール未検証」の状態に戻るため、新しいメールアドレスに対して検証プロセスを実施する必要があります。

> **Note**
>
> 管理アカウントのメールアドレスの変更前に組織への招待をアカウントに送り、その招待が未承諾の場合、管理アカウントの新しいメールアドレスを検証するまでは、招待は承諾可能になりません。まず、検証リクエストを再送信する必要があります。送られてきたメールの内容に沿ってプロセスを完了すると、招待されたアカウントで招待が承諾できるようになります。

を使用して組織のすべての機能を有効にする AWS Organizations

AWS Organizations には 2 つの利用可能な機能セットがあります。

- すべての機能 – この機能セットは優先され、デフォルトの操作方法であり AWS Organizations、請求を統合するすべての機能が含まれています。組織を作成する際、デフォルトではすべての機能が有効化されています。すべての機能を有効にすると、サポートされている AWS サービスや組織ポリシーとの統合など、Organizations で利用できる高度なアカウント管理機能を使用できます。???
- 一括請求機能 – この機能セットは、組織全体で 1 つの請求を生成することに限定されています。一括請求では、他の管理機能は利用できません。

一括請求機能セットを使用して組織を作成する場合、後ですべての機能を有効にできます。ただし、すべての機能が有効化された後は、すべての機能から一括請求に移行することはできません。

標準移行とアシスト移行

すべての機能に移行するための 2 つのアプローチは、標準移行とアシスト移行です。

標準移行は、すべての AWS Organizations お客様がすべての機能モードを有効にするために利用できるセルフサービスプロセスです。

アシスト移行は、エンタープライズサポートプランのお客様が組織をユーザーに代わってすべての機能モード AWS に移行するようにリクエストするプロセスです。

> **Note**
>
> 一方向プロセスとロールバックプロセス
>
> - 一括請求からすべての機能への移行は一方向です。すべての機能を有効にした組織を、統合された一括請求機能のみに切り替えることはできません。
> - アシスト移行プロセスを開始した後は、ロールバックできません。代わりに標準プロセスを実行する場合は、プロセスの有効期限が切れるまで 90 日間待つ必要があります。

トピック

- 考慮事項
- Organizations ですべての機能を有効にする標準移行プロセス
- Organizations ですべての機能を有効にするための移行プロセスを支援

考慮事項

一括請求のみをサポートする組織からすべての機能をサポートする機能に変更する前に、以下の点を考慮してください。

招待されたアカウントは移行を承認する必要があります

すべての機能を有効にするプロセスを開始すると、 は組織に参加するように招待したすべてのメンバーアカウントにリクエスト AWS Organizations を送信します。すべての招待されたアカウントは、すべての機能を有効にするリクエストを受け入れて承認する必要があります。その場合にのみ、

プロセスを完了して組織内のすべての機能を有効にします。アカウントがリクエストを拒否した場合は、組織からアカウントを削除するか、リクエストを再送信する必要があります。すべての機能を有効にするプロセスを完了する前に、リクエストを受け入れる必要があります。 を使用して作成した AWS Organizations アカウントは、追加のコントロールを承認する必要がないため、リクエストを取得しません。

招待されたアカウントには、現在有効になっている機能セットが通知されます

招待されたアカウントの所有者には、招待されている組織で有効なのは一括請求 (コンソリデーティッドビリング) だけか、それともすべての機能かが、招待時に通知されます。組織へのアカウントの招待は、すべての機能が有効になっている状態でも継続できます。

すべての機能の有効化プロセスの進行中にアカウントを招待した場合、招待には、組織はすべての機能が有効なものとして記載されます。アカウントが招待を承諾する前に、すべての機能の有効化プロセスをキャンセルすると、その招待はキャンセルされます。一括請求 (コンソリデーティッドビリング) 機能のみの組織として、再度招待する必要があります。

すべての機能の有効化プロセスの開始前にアカウントを招待し、招待が未承諾の場合、その招待はプロセスの開始時にキャンセルされます。これは、招待には一括請求 (コンソリデーティッドビリング) 機能のみの組織であると記載されているためです。すべての機能が有効になっている組織として、再度招待する必要があります。

組織でアカウントを作成するプロセスは、移行の影響を受けません。

組織内のアカウントの作成を継続できます。このプロセスがこうした変更の影響を受けることはありません。

サービスにリンクされたロール **AWSServiceRoleForOrganizations** が必要

AWS Organizations は、すべてのメンバーアカウントに という名前のサービスにリンクされたロールがあることを確認しますAWSServiceRoleForOrganizations。すべての機能を有効にするには、このロールがすべてのアカウントで必須です。招待したアカウントでこのロールが削除されている場合は、すべての機能を有効にするために招待を承諾するとロールが再作成されます。を使用して作成されたアカウントのロールを削除した場合 AWS Organizations、そのアカウントは、そのロールを再作成するための招待を受け取ります。組織ですべての機能を有効にする処理を完了するには、これらの招待をすべて受諾する必要があります。

Organizations ですべての機能を有効にする標準移行プロセス

このトピックでは、標準の移行プロセスですべての機能を有効にする方法について説明します。

ステップ 1: 招待されたアカウントに移行を承認するようにリクエストする (管理アカウント)

組織の管理アカウントにサインインすると、すべての機能の有効化プロセスを開始できます。そのためには、以下の手順を完了します。

> **最小アクセス許可**
>
> 組織内のすべての機能を有効にするには、次のアクセス権限が必要です。
>
> - `organizations:EnableAllFeatures`
> - `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要

AWS Management Console

招待されたメンバーアカウントに、組織内のすべての機能を有効にすることに同意するよう依頼する

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. [設定] ページで、[すべての機能の有効化プロセスの開始] を選択します。
3. [すべての機能の有効化] ページで、[すべての機能の有効化プロセスの開始] を選択して切り替えた後、一括請求機能のみの設定には戻れないことを理解していることを確認します。

   AWS Organizations は、組織内のすべての招待された (作成されていない) アカウントに対して、組織内のすべての機能を有効にするための承認を求めるリクエストを送信します。を使用して作成されたアカウントがあり AWS Organizations 、メンバーアカウント管理者が という名前のサービスにリンクされたロールを削除した場合`AWSServiceRoleForOrganizations`、 はそのアカウントに対してロールの再作成リクエスト AWS Organizations を送信します。

   コンソールには、招待されたアカウントのリクエストの承認ステータスリストが表示されます。

> **Tip**
>
> 後でこのページに戻るには、[Settings] (設定) ページを開き、[Request sent date] (リクエストの送信日) セクションで [View status] (ステータスを表示) を選択します。

4. [Enable all features] (すべての機能の有効化) ページには、組織内の各アカウントに対するリクエストの現在のステータスが表示されます。リクエストに同意したアカウントのステータスは、[ACCEPTED] (承諾済み) と表示されます。まだ同意していないアカウントのステータスは、[OPEN] (オープン) と表示されます。

AWS CLI & AWS SDKs

招待されたメンバーアカウントに、組織内のすべての機能を有効にすることに同意するよう依頼する

組織のすべての機能を有効にするには、次のいずれかのコマンドを使用します。

- AWS CLI: enable-all-features

  次のコマンドを実行すると、すべての機能の有効化プロセスが組織で開始されます。

```
$ aws organizations enable-all-features
{
    "Handshake": {
        "Id": "h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ],
        "State": "REQUESTED",
        "RequestedTimestamp": "2020-11-19T16:21:46.995000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:21:46.995000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-a1b2c3d4e5",
                "Type": "ORGANIZATION"
```

```
            }
        ]
    }
}
```

出力には、招待されたメンバーアカウントが同意する必要があるハンドシェイクの詳細が表示されます。

- AWS SDKs: EnableAllFeatures

> **メモ**
>
> - リクエストがメンバーアカウントに送信されると、90 日のカウントダウンが開始されます。すべてのアカウントは期間内にリクエストを承認する必要があり、承認されない場合リクエストの有効期限が切れます。リクエストの有効期限が切れると、この試行に関連するすべてのリクエストがキャンセルされます。この場合はステップ 2 からやり直す必要があります。
> - すべての機能の有効化をリクエストすると、受理されていない既存のアカウントへの招待はキャンセルされます。
> - すべての機能の移行プロセス中でも、新しいアカウントの招待を開始したり、新しいアカウントを作成したりすることができます。

すべてのアカウントがリクエストを承認したら、プロセスを終了してすべての機能を有効化できます。組織に招待されたメンバーアカウントがない場合は、プロセスをすぐに終了することもできます。プロセスを終了するには、ステップ 3: 移行プロセスを完了してすべての機能を有効にする (管理アカウント) の手順を実施してください。

ステップ 2: リクエストを承認してすべての機能を有効にする、またはサービスにリンクされたロールを再作成する (招待アカウント)

組織の招待されたメンバーアカウントのいずれかにサインインすると、管理アカウントからのリクエストを承認できます。アカウントが元は組織に参加するように招待されたものである場合、招待はすべての機能を有効にするものであり、必要に応じた `AWSServiceRoleForOrganizations` ロールの再作成の黙示的な承認を含んでいます。アカウントが代わりに を使用して作成 AWS Organizations され、`AWSServiceRoleForOrganizations`サービスにリンクされたロールを削除

した場合、ロールを再作成するための招待のみが送信されます。そのためには、以下の手順を完了します。

> **Important**
>
> 次のすべての機能を有効にすると、組織の管理アカウントはメンバーアカウントにポリシーベースのコントロールを適用できます。これらのコントロールは、ユーザーはもちろん、管理者として自分がアカウント内で実行できることも制限できます。こうした制限により、アカウントが組織を離れるのを禁止することも可能になります。

> **最小アクセス許可**
>
> メンバーアカウントのすべての機能を有効にするリクエストを承認するには、次のアクセス許可が必要です。
>
> - `organizations:AcceptHandshake`
> - `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要
> - `organizations:ListHandshakesForAccount` - Organizations コンソールを使用する場合にのみ必要
> - `iam:CreateServiceLinkedRole` - メンバーアカウントで `AWSServiceRoleForOrganizations` ロールを再作成する必要がある場合にのみ必要

AWS Management Console

組織内のすべての機能を有効にするためのリクエストに同意するには

1. AWS Organizations コンソールで AWS Organizations コンソールにサインインします。メンバーアカウントで、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. 組織内のすべての機能のリクエストの受け入れがあなたのアカウントのものであることを確認した後、[Accept] を選択します。このページでは、組織内のすべてのアカウントがリクエストを承認し、管理アカウントの管理者がプロセスを終了するまで、プロセスが未完了であると表示されます。

AWS CLI & AWS SDKs

組織内のすべての機能を有効にするためのリクエストに同意するには

リクエストに同意するには、"Action": "APPROVE_ALL_FEATURES" でハンドシェイクを承諾する必要があります。

- AWS CLI:
  - accept-handshake
  - list-handshakes-for-account

  次の例は、アカウントで使用可能なハンドシェイクを一覧表示する方法を示しています。"Id" の値 (出力の 4 行目) は、次のコマンドに必要な値です。

```
$ aws organizations list-handshakes-for-account
{
    "Handshakes": [
        {
            "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "111122223333",
                    "Type": "ACCOUNT"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
            "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
            "Action": "APPROVE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "c440da758cab44068cdafc812EXAMPLE",
                    "Type": "PARENT_HANDSHAKE"
                },
                {
                    "Value": "o-aa111bb222",
```

```
                    "Type": "ORGANIZATION"
                },
                {
                    "Value": "111122223333",
                    "Type": "ACCOUNT"
                }
            ]
        }
    ]
}
```

次の例では、前のコマンドのハンドシェイク ID を使用して、そのハンドシェイクを受け入れます。

```
$ aws organizations accept-handshake --handshake-id h-
a2d6ecb7dbdc4540bc788200aEXAMPLE
{
    "Handshake": {
        "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "111122223333",
                "Type": "ACCOUNT"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
        "Action": "APPROVE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "c440da758cab44068cdafc812EXAMPLE",
                "Type": "PARENT_HANDSHAKE"
            },
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
```

```
            },
            {
                "Value": "111122223333",
                "Type": "ACCOUNT"
            }
        ]
    }
}
```

- AWS SDKs:
  - list-handshakes-for-account
  - AcceptHandshake

ステップ 3: 移行プロセスを完了してすべての機能を有効にする (管理アカウント)

招待されたメンバーアカウントすべてが全機能を有効にするリクエストを承認する必要があります。組織に招待されたメンバーアカウントがない場合、[Enable all features progress] ページにはプロセスを終了できる緑色のバナーが表示されます。

> **最小アクセス許可**
>
> 組織のすべての機能を有効にするためのプロセスを終了するには、次のアクセス権限が必要です。
>
> - `organizations:AcceptHandshake`
> - `organizations:ListHandshakesForOrganization`
> - `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要

AWS Management Console

すべての機能を有効にするプロセスを終了するには

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. すべての機能の有効化のリクエストがすべての招待されたアカウントによって承認されると、[Settings] (設定) ページの上部に緑色のボックスが表示されます。緑色のボックスで、[Go to finalize] (終了処理に進む) を選択します。
3. [Enable all features] (すべての機能の有効化) ページで [Finalize] (終了する) を選択し、確認ダイアログボックスでもう一度 [Finalize] (終了する) を選択します。
4. 現在、組織は、すべての機能が有効になっています。

AWS CLI & AWS SDKs

すべての機能を有効にするプロセスを終了するには

プロセスを終了するには、["Action": "ENABLE_ALL_FEATURES"] でハンドシェイクを承諾する必要があります。

- AWS CLI:
  - list-handshakes-for-organization
  - accept-handshake

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
            "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
            "Action": "ENABLE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                }
```

```
            ]
        }
    ]
}
```

次の例は、組織で使用可能なハンドシェイクを一覧表示する方法を示しています。"Id" の値 (出力の 4 行目) は、次のコマンドに必要な値です。

```
$ aws organizations accept-handshake \
    --handshake-id h-43a871103e4c4ee399868fbf2EXAMPLE
{
    "Handshake": {
        "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
        "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```

- AWS SDKs:
  - ListHandshakesForOrganization
  - AcceptHandshake

Organizations ですべての機能を有効にするための移行プロセスを支援

エンタープライズのお客様は、管理するアカウントが多いため、標準の移行プロセスを完了することが難しい場合があります。例えば、大規模な組織で招待されたすべてのアカウントを移行するための承認を取得できない場合があります。

エンタープライズサポートプランのお客様が、ユーザーに代わって組織をすべての機能 AWS に移行するようにリクエストできるようにすることで、移行がこのプロセスを支援しました。このプロセスでは、すべてのアカウントを所有し、その後に 14 日間の待機期間があることを確認する契約書に署名する必要があります。この待機期間により、アカウントがすべての機能への移行を有効にする前に組織を離れる時間を確保できます。

AWS Management Console

アシスト移行を使用してすべての機能に移行するには

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. 設定ページで、[すべての機能を有効にする] を選択し、[アシスト移行] を選択します。
3. 契約の利用規約を読み、[承諾] を選択し、[すべての機能を有効にするプロセスを開始する] を選択して、移行を開始します。

> **Note**
>
> アシスト移行プロセスを開始すると、標準の移行プロセスが上書きされます
> 現在、標準の移行プロセスを使用してすべての機能を有効にしている場合、その機能はキャンセルされ、アシスト移行プロセスが開始されます。
> アシスト移行プロセスは一方向であり、ロールバックできません
> アシスト移行プロセスを開始した後は、ロールバックできません。代わりに標準プロセスを実行する場合は、プロセスの有効期限が切れるまで 90 日間待つ必要があります。

アシスト移行を使用する場合、すべての機能への移行を受け入れるために、ルートユーザーとして招待されたアカウントにアクセスすることを心配する必要はありません。

アシスト移行の正確な詳細、進捗状況、タイムラインについては、テクニカルアカウントマネージャー (TAM) にお問い合わせください。

管理アカウントを使用した組織の詳細の表示

AWS Organizations コンソールで組織の管理アカウントにサインインすると、組織の詳細を表示できます。

> **最小アクセス許可**
>
> 組織の詳細を表示するには、次のアクセス権限が必要です。
>
> - `organizations:DescribeOrganization`

AWS Management Console

組織の詳細を表示するには

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. 設定ページに移動します。このページには、組織 ID や、組織の管理アカウントに割り当てられているアカウント名と電子メールアドレスなどの組織の詳細が表示されます。

AWS CLI & AWS SDKs

組織の詳細を表示するには

組織の詳細を表示するには、次のいずれかのコマンドを使用します。

- AWS CLI: describe-organization

  次の例は、このコマンドの出力に含まれる情報を示しています。

```
$ aws organizations describe-organization
{
    "Organization": {
        "Id": "o-aa111bb222",
```

```
        "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
        "FeatureSet": "ALL",
        "MasterAccountArn": "arn:aws:organizations::128716708097:account/o-
aa111bb222/123456789012",
        "MasterAccountId": "123456789012",
        "MasterAccountEmail": "admin@example.com",
        "AvailablePolicyTypes": [ ...DEPRECATED - DO NOT USE... ]
    }
}
```

> **Important**
>
> `AvailablePolicyTypes` フィールドは非推奨であり、組織で有効になっているポリシーに関する正確な情報が含まれません。組織で実際に有効になっているすべてのポリシータイプの正確な一覧を確認するには、`ListRoots` コマンドを使用します。詳しくは、次のセクションの AWS CLI に関する部分を参照してください。

- AWS SDKs: DescribeOrganization

を使用した組織の削除 AWS Organizations

不要になった組織は削除できます。組織を削除しても管理アカウントは閉鎖されません。管理アカウントが組織から削除され、組織自体も削除されます。

以前の管理アカウント AWS アカウント は、 によって管理されなくなったスタンドアロンアカウントになります AWS Organizations。次に 3 つの選択肢があります。

- スタンドアロンアカウントとして引き続き使用できます。
- これを使用して別の組織を作成できます。
- 別の組織からの招待を受け入れて、その組織にメンバーアカウントとしてアカウントを追加できます。

トピック

- 考慮事項
- 組織を削除する

考慮事項

削除された組織は復元できません

組織を削除した場合、その組織は復元できません。組織内にポリシーを作成していた場合、それらのポリシーも削除され、復元はできません。

Organizations を削除できるのは、すべてのメンバーアカウントが削除された後のみです。

組織からすべてのメンバーアカウントを消去した場合に限り、組織を削除できます。を使用して一部のメンバーアカウントを作成した場合 AWS Organizations、それらのアカウントの削除がブロックされる可能性があります。スタンドアロンの AWS アカウントとして動作するために必要な情報すべてがある場合に限り、メンバーアカウントを削除できます。その情報を提供してアカウントを削除する方法について詳しくは、を使用してメンバーアカウントから組織を退出する AWS Organizations を参照してください。

「一時停止」状態のメンバーアカウントは組織から削除できません

組織から削除する前にメンバーアカウントを閉鎖した場合、そのアカウントは一定期間「停止」状態になり、完全に閉鎖されるまでは組織から削除することができません。この処理には最大 90 日かかります。すべてのメンバーアカウントが完全に閉鎖されるまでは、組織を削除できない場合があります。

組織を削除することで組織から管理アカウントを削除すると、そのアカウントに次の影響が及びます。

- このアカウントは独自の料金のみを支払うことになり、他のアカウントの料金を支払う責任はなくなります。
- 他のサービスとの統合が無効になる場合があります。例えば、 AWS IAM Identity Center では組織を運用する必要があるため、IAM Identity Center をサポートする組織からアカウントを削除すると、そのアカウントのユーザーはそのサービスを使用できなくなります。

組織の管理アカウントが SCP (サービスコントロールポリシー) の影響を受けることはないので、SCP を利用できなくなってもアクセス許可が変更されることはありません。

すべてのレポートをバックアップする

管理アカウント、特に請求レポートからレポートをエクスポートまたはバックアップしてください。組織を削除すると、組織レベルのレポートと履歴は保存されません。すべてのコストデータ (Cost

Explorer データセットなど) が削除されます。すべての請求履歴を完全にエクスポートすることをお勧めします。

詳細については、「Cost and Usage Reports」、「Cost Explorer Reports」、「Savings Plans Reports」、「Reserved Instance (RI) utilization and coverage」を参照してください。

組織を削除する

以前の管理アカウントを、 によって管理されなくなったスタンドアロンに戻す組織を削除するには AWS アカウント 、次の手順に従います AWS Organizations。

> **最小アクセス許可**
>
> 組織を削除するには、管理アカウントのユーザーまたはロールとしてサインインし、次の許可を付与される必要があります。
>
> - `organizations:DeleteOrganization`
> - `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要

AWS Management Console

組織を削除するには

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. 組織を削除する前に、すべてのアカウントを組織から削除する必要があります。詳細については、「を使用して組織からメンバーアカウントを削除する AWS Organizations」を参照してください。
3. [Settings] (設定) ページに移動し、[Delete organization] (組織の削除) を選択します。
4. [Delete organization] (組織の削除) 確認ダイアログボックスで、テキストボックスの上の行に表示されている組織の ID を入力します。次に、[Delete organization] (組織の削除) を選択します。

> **Important**
>
> この操作では管理アカウントは閉鎖されず、スタンドアロンの AWS アカウント に戻ります。アカウントを閉鎖するには、を使用して組織のメンバーアカウントを閉鎖する AWS Organizations の手順に従ってください。

AWS CLI & AWS SDKs

次のサンプルコードは、DeleteOrganization を使用する方法を説明しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing organization using the AWS
/// Organizations Service.
/// </summary>
public class DeleteOrganization
{
    /// <summary>
    /// Initializes the Organizations client and then calls
    /// DeleteOrganizationAsync to delete the organization.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();
```

```
            var response = await client.DeleteOrganizationAsync(new
DeleteOrganizationRequest());

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine("Successfully deleted organization.");
            }
            else
            {
                Console.WriteLine("Could not delete organization.");
            }
        }
    }
```

- API の詳細については、AWS SDK for .NET API リファレンスの「DeleteOrganization」を参照してください。

CLI

AWS CLI

組織を削除するには

次の例は、組織を削除する方法を示しています。この操作を実行するには、組織のマスターアカウントの管理者である必要があります。この例では、組織からメンバーアカウント、OU、ポリシーをすべて削除済みであることを前提としています。

```
aws organizations delete-organization
```

- API の詳細については、AWS CLI コマンドリファレンスの「DeleteOrganization」を参照してください。

を使用した組織内のアカウントの管理 AWS Organizations

AWS アカウント は、 AWS リソースのコンテナです。で AWS リソースを作成および管理します AWS アカウント。

このトピックでは、 アカウントを管理する方法について説明します AWS Organizations。

トピック

- を使用した管理アカウントの管理 AWS Organizations
- を使用したメンバーアカウントの管理 AWS Organizations
- を使用したアカウント招待の管理 AWS Organizations
- を使用してアカウントを別の組織に移行する AWS Organizations
- でアカウントの詳細を表示する AWS Organizations
- 内のすべてのアカウントの詳細をエクスポートする AWS Organizations
- でアカウントの代替連絡先を更新する AWS Organizations
- でアカウントのプライマリ連絡先情報を更新する AWS Organizations
- での アカウントの の更新 AWS リージョンAWS Organizations

を使用した管理アカウントの管理 AWS Organizations

管理アカウントは、組織の作成 AWS アカウント に使用する です。

管理アカウントは組織の最終的な所有者であり、セキュリティ、インフラストラクチャ、財務ポリシーを最終的に制御します。このアカウントには支払者アカウントの役割があり、組織内のアカウントによって発生したすべての料金を支払う責任があります。

このトピックでは、 を使用して管理アカウントを管理する方法について説明します AWS Organizations。

トピック

- 管理アカウントのベストプラクティス
- 組織の管理カウントの閉鎖

管理アカウントのベストプラクティス

AWS Organizationsの管理アカウントのセキュリティを保護するため、以下の推奨事項に従います。これらの推奨事項は、厳密に必要とするタスクにのみルートユーザーを使用するというベストプラクティスを遵守していることを前提としています。

トピック

- 管理アカウントにアクセスできるユーザーを制限する
- 誰がアクセスできるかを確認、追跡する
- 管理アカウントは、管理アカウントが必要なタスクにのみ使用してください
- 組織の管理アカウントにワークロードをデプロイすることを避ける
- 分散化のために管理アカウント外に責任を委任する

管理アカウントにアクセスできるユーザーを制限する

管理アカウントは、アカウント管理、ポリシー、他の AWS サービスとの統合、一括請求など、前述のすべての管理タスクにとって重要です。そのため、管理アカウントへのアクセスは、組織に変更を加える権限を必要とする管理者ユーザーのみに制限する必要があります。

誰がアクセスできるかを確認、追跡する

管理アカウントへのアクセスを維持するには、そのアカウントと関連付けられたメールアドレス、パスワード、MFA、電話番号に社内の誰がアクセスできるかを定期的に確認する必要があります。確認は既存のビジネス上の手続きに則って行うことができます。担当者だけに適切なアクセスを限定できるよう、月ごとや四半期ごとにこの情報を確認してください。ルートユーザーの認証情報へのアクセスを回復またはリセットするプロセスが、特定の個人に依存しないようにしてください。すべてのプロセスは、誰かが不在だったとしても問題なく進められるよう設計します。

管理アカウントは、管理アカウントが必要なタスクにのみ使用してください

管理アカウントとそのユーザーおよびロールは、そのアカウントで実行する必要のあるタスクのみに使用することをおすすめします。すべての AWS リソースを組織 AWS アカウント 内の他の に保存し、管理アカウントから遠ざけます。リソースを他のアカウントで保持する重要な理由の一つは、管理アカウントのユーザーとロールに対する制限に Organizations サービスコントロールポリシー (SCP) を使用できないためです。また、リソースを管理アカウントから分離することで、請求書に記載される請求額が理解しやすくなります。

管理アカウントから呼び出す必要があるタスクのリストについては、「Operations you can call from only the organization's management account」を参照してください。

組織の管理アカウントにワークロードをデプロイすることを避ける

特権操作は組織の管理アカウント内で実行でき、SCP は管理アカウントには適用されません。そのため、管理アカウントに含まれるクラウドリソースとデータは、管理アカウントで管理する必要があるものだけに制限する必要があります。

分散化のために管理アカウント外に責任を委任する

可能ならば、責任とサービスを管理アカウント外に委任することをおすすめします。チームにチーム自身の権限を提供することで、管理アカウントにアクセスすることなく、各自のアカウントから組織のニーズを管理できます。さらに、組織全体でソフトウェアを共有する場合や、スタックを作成およびデプロイ AWS Service Catalog するための AWS CloudFormation StackSets など、この機能をサポートするサービスに複数の委任管理者を登録できます。

詳細については、「セキュリティリファレンスアーキテクチャ」、「複数のアカウントを使用して AWS 環境を整理する」、および「さまざまな AWS サービスの委任管理者としてメンバーアカウントを登録する方法の提案AWS のサービス で使用できる AWS Organizations」を参照してください。

委任管理者の設定の詳細については、「AWS アカウント管理 の委任管理者アカウントの有効化」および の委任管理者 AWS Organizations を参照してください。

組織の管理カウントの閉鎖

組織内の管理アカウントを閉鎖するには、まず、組織内のすべてのメンバーアカウントを閉鎖または削除する必要があります。管理アカウントを閉鎖する行為により、閉鎖後期間が経過した後に、その組織内で作成した AWS Organizations のインスタンスとポリシーも削除されます。

管理アカウントを閉鎖する

以下の手順に従って、管理アカウントを閉鎖します。

> **Important**
>
> 管理アカウントを閉鎖する前に、考慮事項を確認し、アカウントを閉鎖した場合の影響を理解しておくことを強くお勧めします。詳細については、「AWS Account Management Guide」の「What you need to know before closing your account」と「What to expect after you close your account」を参照してください。

AWS Management Console

アカウントページから管理アカウントを閉鎖するには

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

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、アカウントを閉鎖できません。
2. 組織内にアクティブなメンバーアカウントが残っていないことを確認します。これを行うには、 AWS Organizations コンソールに移動します。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組織からメンバーアカウントを削除する前に、を使用して組織のメンバーアカウントを閉鎖する AWS Organizations「」または「」に記載されている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、[アカウントを閉鎖] ボタンを選択します。アカウント閉鎖ガイダンスを読んで、理解していることを確認します。
5. [アカウント閉鎖] ボタンを選択して、アカウント閉鎖プロセスを開始します。
6. 数分以内に、アカウントが閉鎖されたことを確認する E メールが届きます。

AWS CLI & AWS SDKs

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

を使用したメンバーアカウントの管理 AWS Organizations

メンバーアカウントは AWS アカウント、組織の一部である管理アカウント以外の です。

このトピックでは、 を使用してメンバーアカウントを管理する方法について説明します AWS Organizations。

トピック

- メンバーアカウントのベストプラクティス
- を使用した組織内のメンバーアカウントの作成 AWS Organizations
- を使用して組織のメンバーアカウントにアクセスする AWS Organizations
- を使用して組織のメンバーアカウントを閉鎖する AWS Organizations
- によるメンバーアカウントの閉鎖からの保護 AWS Organizations
- を使用して組織からメンバーアカウントを削除する AWS Organizations
- を使用してメンバーアカウントから組織を退出する AWS Organizations
- でメンバーアカウントのアカウント名を更新する AWS Organizations
- でメンバーアカウントのルートユーザーの E メールアドレスの更新AWS Organizations

メンバーアカウントのベストプラクティス

組織内のメンバーアカウントのセキュリティを保護するために、以下の推奨事項に従ってください。これらの推奨事項は、厳密に必要とするタスクにのみルートユーザーを使用するというベストプラクティスを遵守していることを前提としています。

トピック

- アカウント名と属性を定義する
- 環境とアカウントの使用量を効率的にスケールする
- ルートアクセス管理を有効にして、メンバーアカウントのルートユーザー認証情報の管理を簡素化する

アカウント名と属性を定義する

メンバーアカウントには、アカウントの使用状況を反映した命名構造とメールアドレスを使用してください。たとえば、WorkloadsFooADev に「Workloads+fooA+dev@domain.com」、WorkloadsFooBDev に「Workloads+fooB+dev@domain.com」などです。組織でカスタムタグを定義している場合は、アカウントの使用方法、コストセンター、環境、およびプロジェクトを反映したアカウントにそれらのタグを割り当てることをおすすめします。これにより、アカウントの識別、整理、検索が容易になります。

環境とアカウントの使用量を効率的にスケールする

スケールするときは、新しいアカウントを作成する前に、不要な重複を避けるために、同様のニーズのアカウントがまだ存在しないことを確認してください。 AWS アカウント は一般的なアクセス要

件に基づいている必要があります。サンドボックスアカウントや同等のアカウントを再利用する予定がある場合は、そのアカウントの不要なリソースやワークロードをクリーンアップし、後で使用できるようにアカウントを保存しておくことをおすすめします。

アカウントを閉鎖する際には、アカウント閉鎖クォータ制限が適用されることに注意してください。詳細については、「のクォータとサービス制限 AWS Organizations」を参照してください。可能であれば、アカウントを閉鎖して新しいアカウントを作成するのではなく、クリーンアッププロセスを実行してアカウントを再利用することを検討してください。これにより、リソースを実行することによるコストの発生や CloseAccount API の上限に達することを回避できます。

ルートアクセス管理を有効にして、メンバーアカウントのルートユーザー認証情報の管理を簡素化する

メンバーアカウントのルートユーザー認証情報のモニタリングと削除に役立つルートアクセス管理を有効にすることをお勧めします。ルートアクセス管理は、ルートユーザー認証情報の復旧を防ぎ、組織内のアカウントセキュリティを向上させます。

- メンバーアカウントのルートユーザー認証情報を削除して、ルートユーザーへのサインインを防止します。これにより、メンバーアカウントのルートユーザーの復旧も防止されます。
- メンバーアカウントで次のタスクを実行する特権セッションを引き受けます。
  - すべてのプリンシパルが Amazon S3 バケットにアクセスすることを拒否する、誤って設定されたバケットポリシーを削除します。
  - すべてのプリンシパルによる Amazon SQS キューへのアクセスを拒否する Amazon Simple Queue Service リソースベースのポリシーを削除します。
  - メンバーアカウントにルートユーザーの認証情報の復元を許可します。メンバーアカウントのルートユーザー E メールAmazon 受信トレイにアクセスできるユーザーは、ルートユーザーのパスワードをリセットし、メンバーアカウントのルートユーザーとしてサインインできます。

ルートアクセス管理を有効にすると、新しく作成されたメンバーアカウントはsecure-by-defaultになり、ルートユーザーの認証情報がないため、プロビジョニング後の MFA などの追加のセキュリティが不要になります。

詳細については、「 AWS Identity and Access Management 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認証情報を一元化する」を参照してください。

SCPを使用し、メンバーアカウントのルートユーザーで行えることを制限する

サービスコントロールポリシー (SCP) を組織内に作成して組織のルートにアタッチし、すべてのメンバーアカウントに適用されるようにすることをお勧めします。詳細については、「Organizations アカウントのルートユーザー認証情報を保護する」を参照してください。

メンバーアカウントで実行する必要がある特定のルート限定アクションを除いて、すべてのルートアクションを拒否できます。例えば、次の SCP は、メンバーアカウントのルートユーザーが AWS サービス API コールを実行できないようにします。ただし、「誤って設定された S3 バケットポリシーを更新し、すべてのプリンシパルへのアクセスを拒否する」 (ルート認証情報を必要とするアクションの 1 つ) は除きます。詳細については、「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。

JSON

```
{
 "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "NotAction":[
            "s3:GetBucketPolicy",
            "s3:PutBucketPolicy",
            "s3:DeleteBucketPolicy"
                 ],
            "Resource": "*",
            "Condition": {
 "ArnLike": { "aws:PrincipalArn": "arn:aws:iam::*:root" }
            }
        }
    ]
 }
```

多くの場合、どのような管理タスクも、関連する管理者用アクセス許可を持つメンバーアカウントの AWS Identity and Access Management (IAM) ロールで実行することが可能です。このようなロールには、アクティビティの制限、ログ、モニタリングを行えるよう、適切なコントロールが適用されている必要があります。

を使用した組織内のメンバーアカウントの作成 AWS Organizations

このトピックでは、 で組織 AWS アカウント 内に を作成する方法について説明します AWS Organizations。単一の を作成する方法については AWS アカウント、「入門リソースセンター」を参照してください。

メンバーアカウントを作成する前に考慮すべき事項

Organizations はメンバーアカウントの IAM ロール **OrganizationAccountAccessRole** を自動的に作成する

組織でメンバーアカウントを作成すると、Organizations は (IAM) ロール `OrganizationAccountAccessRole` をメンバーアカウントで自動的に作成します。このロールにより、管理アカウントのユーザーおよびロールがメンバーアカウントを完全に管理コントロールを実行できるようになります。同じマネージドポリシーに関連付けられた追加アカウントは、ポリシーが更新されるたびに自動的に更新されます。このロールは、メンバーアカウントに適用されるすべてのサービスコントロールポリシー (SCP) の対象となります。

Organizations は、メンバーアカウントのサービスにリンクされたロールを自動的に作成します**AWSServiceRoleForOrganizations**。

組織内にメンバーアカウントを作成すると、Organizations はメンバーアカウントにサービスにリンクされたロール `AWSServiceRoleForOrganizations` を自動的に作成し、一部の AWS サービスとの統合を可能にします。統合を許可するように他のサービスを設定する必要があります。詳細については、「AWS Organizations およびサービスにリンクされたロール」を参照してください。

メンバーアカウントは組織のルートでのみ作成可能

組織のメンバーアカウントは、組織のルートでのみ作成できます。組織のメンバーアカウントルートを作成したら、OU 間で移動できます。詳細については、「を使用して組織単位 (OU) またはルートと OUsする AWS Organizations」を参照してください。

ルートにアタッチされたポリシーはすぐに適用される

ルートにアタッチされたポリシーがある場合、それらのポリシーは即時、作成されたアカウントのすべてのユーザーおよびロールに適用されます。

AWS 組織の別のサービスのサービス信頼を有効にしている場合、その信頼されたサービスは、サービスにリンクされたロールを作成したり、作成したアカウントを含む組織内の任意のメンバーアカウントでアクションを実行したりできます。

メンバーアカウントは、マーケティング E メールを受信するにはオプトインする必要がある

組織の一部として作成したメンバーアカウントは、 AWS マーケティング E メールに自動的にサブスクライブされません。マーケティングメールを受信するようアカウントをオプトインするには、https://pages.awscloud.com/communication-preferences を参照してください。

によって管理される組織のメンバーアカウントは、 で作成 AWS Control Tower する必要があります。 AWS Control Tower

組織が によって管理されている場合は AWS Control Tower、 AWS Control Tower コンソールの AWS Control Tower Account Factory または AWS Control Tower APIsを使用してメンバーアカウントを作成することをお勧めします。

組織が によって管理されているときに Organizations でメンバーアカウントを作成すると AWS Control Tower、そのアカウントは に登録されません AWS Control Tower。詳細については、AWS Control Tower ユーザーガイドの AWS Control Tower外のリソースを参照するを参照してください。

メンバーアカウントを作成する

組織の管理アカウントにサインインすると、組織に属するよう、メンバーアカウントを作成することができます。

次の手順を使用してアカウントを作成すると、 は管理アカウントから新しいメンバーアカウントに次の主要連絡先情報 AWS Organizations を自動的にコピーします。

- 電話番号
- 会社名
- ウェブサイトの URL
- Address

Organizations は、管理アカウントから通信言語と Marketplace 情報 (一部の アカウントのベンダー AWS リージョン) もコピーします。

> **最小アクセス許可**
>
> 組織にメンバーアカウントを作成するには、次のアクセス権限が必要です。
>
> - `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要

- `organizations:CreateAccount`
- `iam:CreateServiceLinkedRole`

AWS Management Console

自動的に組織の一部 AWS アカウント となる を作成するには

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 (非推奨) としてサインインする必要があります。
2. AWS アカウント ページで、[Add an AWS アカウント] (を追加) を選択します。
3. [Add an AWS アカウント] (を追加) ページで、[Create an AWS アカウント] (を作成) を選択します (デフォルトで選択されています)。
4. [Create an AWS アカウント] (を作成) ページの [AWS アカウント name] (名) に、アカウントに割り当てる名前を入力します。この名前は、アカウントを組織内の他のアカウントと区別する際に役立ちます。IAM エイリアスや所有者のメールの名前とは異なります。
5. [Email address of the account's owner] (アカウント所有者のメールアドレス) に、アカウントの所有者のメールアドレスを入力します。この E メールアドレスは、アカウントのルートユーザーのユーザー名認証情報になる AWS アカウント ため、既に別の に関連付けることはできません。
6. (オプション) 新しいアカウント内に自動で作成される IAM ロールに割り当てる名前を指定します。このロールは、組織の管理アカウントに、新しく作成されたメンバーアカウントへのアクセス許可を付与します。名前を指定しない場合、 はロールにデフォルトの名前 AWS Organizations を付与します`OrganizationAccountAccessRole`。一貫性を保つため、すべてのアカウントでデフォルトの名前を使用することをお勧めします。

   > **Important**
   >
   > このロールの名前を忘れないでください。後で、管理アカウントのユーザーおよびロールの新しいアカウントにアクセス権限を付与する際に必要になります。

7. (オプション) [タグ] セクションで、[タグの追加] を選択してキーとオプションの値を入力し、新しいアカウントに 1 つ以上のタグを追加します。値を空白のままにすると、空の文字列が設定され、`null` にはなりません。1 つのアカウントに最大 50 個のタグをアタッチできます。
8. [作成] AWS アカウント を選択します。

- 組織のアカウントクォータを超えたことを示すエラーが表示された場合は、組織にアカウントを追加しようとすると「クォータを超えました」というメッセージが表示される を参照してください。
- 組織がまだ初期化中であるため、アカウントを追加できないことを示すエラーが表示された場合は 1 時間待ってから、もう一度試してください。
- アカウントの作成が成功したかどうかについては、 AWS CloudTrail ログを確認することもできます。詳細については、「での口グ記録とモニタリング AWS Organizations」を参照してください。
- エラーが引き続き発生する場合は、AWS サポート までお問い合わせください。

AWS アカウント ページが表示され、新しいアカウントがリストに追加されます。

9. これで、管理アカウントのユーザーに管理者アクセスを付与する IAM ロールを持つアカウントができました。このアカウントにアクセスするには、を使用して組織のメンバーアカウントにアクセスする AWS Organizations のステップを実施します。

AWS CLI & AWS SDKs

次のサンプルコードは、`CreateAccount` を使用する方法を説明しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new AWS Organizations account.
/// </summary>
```

```
    public class CreateAccount
    {
        /// <summary>
        /// Initializes an Organizations client object and uses it to create
        /// the new account with the name specified in accountName.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var accountName = "ExampleAccount";
            var email = "someone@example.com";

            var request = new CreateAccountRequest
            {
                AccountName = accountName,
                Email = email,
            };

            var response = await client.CreateAccountAsync(request);
            var status = response.CreateAccountStatus;

            Console.WriteLine($"The staus of {status.AccountName} is
{status.State}.");
        }
    }
```

- API の詳細については、AWS SDK for .NET API リファレンスの「CreateAccount」を参照してください。

CLI

AWS CLI

自動的に組織の一部となるメンバーアカウントを作成するには

次の例は、組織のメンバーアカウントを作成する方法を示しています。メンバーアカウントは、「プロダクションアカウント」という名前と E メールアドレス (susan@example.com) で構成されます。roleName パラメータが指定されていないため、Organizations では OrganizationAccountAccessRole というデフォルト名を使用して IAM ロールが自動的に作成されます。また、IamUserAccessToBilling パラメータが指定されていないため、必要な権

限を持つ IAM ユーザーまたはロールにアカウントの請求データへのアクセスを許可する設定には、デフォルト値 ALLOW が使用されます。Organizations は、スーザンに「ようこそ AWS」という E メールを自動的に送信します。

```
aws organizations create-account --email susan@example.com --account-
name "Production Account"
```

出力には、ステータスが現在の IN_PROGRESS 状態であることを示すリクエストオブジェクトが含まれます。

```
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
}
```

describe-create-account-status コマンドに Id レスポンス値を create-account-request-id parameter の値として指定することで、後でリクエストの現在のステータスをクエリすることができます。

詳細については、「 Organizations ユーザーガイド」の「組織での AWS アカウントの作成」を参照してください。 AWS

- API の詳細については、AWS CLI コマンドリファレンスの「CreateAccount」を参照してください。

を使用して組織のメンバーアカウントにアクセスする AWS Organizations

組織でアカウントを作成すると、ルートユーザーに加えて、OrganizationAccountAccessRole というデフォルト名の IAM ロールがAWS Organizations によって自動的に作成されます。作成時に別の名前を指定できますが、すべてのアカウントで一貫して名前を付けることをお勧めします。AWS Organizations は他のユーザーやロールを作成しません。

組織のアカウントにアクセスするには、次のいずれかの方法を使用する必要があります。

> **最小アクセス許可**
>
> 組織内の他のアカウント AWS アカウント から にアクセスするには、次のアクセス許可が必要です。

- `sts:AssumeRole` - `Resource` 要素は、アスタリスク (*) に設定するか、新しいメンバーアカウントにアクセスする必要のあるユーザーが含まれるアカウントのアカウント ID 番号に設定する必要があります。

Using the root user (Not recommended for everyday tasks)

組織に新しいメンバーアカウントを作成すると、アカウントにはデフォルトでルートユーザー認証情報がありません。メンバーアカウントは、アカウントリカバリが有効になっていない限り、ルートユーザーにサインインしたり、ルートユーザーのパスワードリカバリを実行したりすることはできません。

メンバーアカウントのルートアクセスを一元化して、組織内の既存のメンバーアカウントのルートユーザー認証情報を削除できます。ルートユーザーの認証情報を削除すると、ルートユーザーのパスワード、アクセスキー、署名証明書が削除され、多要素認証 (MFA) が無効になります。これらのメンバーアカウントはルートユーザー認証情報を持っておらず、ルートユーザーとしてサインインできず、ルートユーザーのパスワードをリカバリできません。Organizations で作成した新しいアカウントには、デフォルトでルートユーザー認証情報はありません。

ルートユーザー認証情報が存在しないメンバーアカウントでルートユーザー認証情報を必要とするタスクを実行する必要がある場合は、管理者にお問い合わせください。

ルートユーザーとしてメンバーアカウントにアクセスするには、パスワード復旧のプロセスを実行する必要があります。詳細については、「AWS サインインユーザーガイド」の「AWS アカウントアカウント のルートユーザーパスワードを忘れてしまった」を参照してください。

ルートユーザーを使用してメンバーアカウントにアクセスする必要がある場合は、次のベストプラクティスに従ってください。

- アクセス許可がより限定された他のユーザーとロールを作成する場合を除き、ルートユーザーを使用して アカウントにアクセスしないでください。復旧プロセスが完了したら、ユーザーまたはロールでサインインします。
- ルートユーザーで多要素認証 (MFA) を有効にします。パスワードをリセットし、root ユーザーに MFA デバイスを割り当てることができます。

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。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、IAM ユーザーガイドの「 のルートユーザーのベストプラクティス AWS アカウント」を参照してください。

Using trusted access for IAM Identity Center

で IAM Identity Center の信頼されたアクセスを使用AWS IAM Identity Centerおよび有効にしますAWS Organizations。これにより、ユーザーは会社の認証情報を使用して AWS アクセスポータルにサインインし、割り当てられた管理アカウントまたはメンバーアカウントのリソースにアクセスできます。

詳細については、AWS IAM Identity Center ユーザーガイドのマルチアカウント許可を参照してください。IAM Identity Center への信頼されたアクセス設定については、「AWS IAM Identity Center および AWS Organizations」を参照してください。

Using the IAM role OrganizationAccountAccessRole

の一部として提供されるツールを使用してアカウントを作成する場合 AWS Organizations、この方法で作成するすべての新しいアカウントに存在する `OrganizationAccountAccessRole` という名前の事前設定済みロールを使用してアカウントにアクセスできます。詳細については、「で OrganizationAccountAccessRole を持つメンバーアカウントにアクセスする AWS Organizations」を参照してください。

既存のアカウントを組織に招待し、そのアカウントによって招待が承諾されると、招待されたメンバーアカウントへのアクセスを管理アカウントに許可する IAM ロールを作成できるようになります。このロールは、 AWS Organizationsで作成されたアカウントに自動的に追加されるロールと同一であることを意図しています。

このロールの作成については、「で招待されたアカウントの OrganizationAccountAccessRole を作成する AWS Organizations」を参照してください。

ロールの作成が完了したら、「で OrganizationAccountAccessRole を持つメンバーアカウントにアクセスする AWS Organizations」のステップを使用してアクセスできます。

トピック

- で招待されたアカウントの OrganizationAccountAccessRole を作成する AWS Organizations
- で OrganizationAccountAccessRole を持つメンバーアカウントにアクセスする AWS Organizations

で招待されたアカウントの OrganizationAccountAccessRole を作成する AWS Organizations

デフォルトでは、組織の一部としてメンバーアカウントを作成すると、そのアカウントに AWS が自動的に作成するロールにより、そのロールを引き受けることができる管理アカウントの IAM ユーザーに、管理者用のアクセス許可が付与されます。デフォルトでは、そのロールの名前は `OrganizationAccountAccessRole` です。詳細については、「で OrganizationAccountAccessRole を持つメンバーアカウントにアクセスする AWS Organizations」を参照してください。

しかし、組織に招待するメンバーアカウントに、管理者ロールが自動的に作成されることはありません。次の手順に従って、手動で行います。これにより、ロールはコピーされ、作成されたアカウントに自動的に設定されます。一貫性と覚えやすさの点から、手動で作成したロールには、同一の名前 (`OrganizationAccountAccessRole`) を使用されることをお勧めします。

AWS Management Console

メンバーアカウントに AWS Organizations 管理者ロールを作成するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) にサインインします。メンバーアカウントで、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。使用するユーザーまたはロールには、IAM ロールとポリシーを作成するアクセス許可が必要です。
2. IAM コンソールで、[ロール] に移動し、[ロールの作成] を選択します。
3. を選択しAWS アカウント、別の AWS アカウント を選択します。
4. 管理者権限を付与する管理アカウントの 12 桁のアカウント ID 番号を入力します。[オプション]で、次の点に注意してください。

   - このロールの場合、アカウントは会社内部で使用するため、[Require external ID] (外部 ID が必要) は選択しないでください。外部 ID オプションの詳細については、「IAM ユーザーガイド」の「外部 ID が適している状況」を参照してください。
   - MFA が有効化され設定されている場合は、オプションで、MFA デバイスを使用した認証を求めるように設定できます。MFA の詳細については、「IAM ユーザーガイド」の「Using multi-factor authentication (MFA) in AWS」を参照してください。
5. [Next (次へ)] を選択します。
6. [アクセス許可を追加する] のページで、`AdministratorAccess` という名前の AWS 管理ポリシーを選択し、[次へ] を選択します。

7. [名前、確認、および作成] ページで、ロール名とオプションの説明オプションを指定します。新しいアカウントのロールに割り当てられたデフォルト名との整合性を保つために、`OrganizationAccountAccessRole` を使用されることをお勧めします。変更をコミットするには、[ロールの作成] を選択します。
8. 新しいロールが、使用可能なロールのリストに表示されます。新しいロールの名前を選択して詳細を表示します。その際、表示されるリンクの URL に注意します。ロールへのアクセスが必要なメンバーアカウントのユーザーにこの URL を通知します。また、ステップ 15 で必要になる [ロール ARN] も書き留めます。
9. IAM コンソール (https://console.aws.amazon.com/iam/) にサインインします。今回は、ポリシーを作成し、そのポリシーをユーザーまたはグループに割り当てるアクセス許可を持つ管理アカウントのユーザーとしてサインインします。
10. [ポリシー] に移動し、[ポリシーの作成] を選択します。
11. [Service] で、[STS] を選択します。
12. [Actions] (アクション) で、[Filter] (フィルター) ボックスに「**`AssumeRole`**」と入力し始め、表示されたら、横のチェックボックスをオンにします。
13. [リソース] で、[指定] が選択されていることを確認して、[ARN の追加] を選択します。
14. AWS メンバーアカウント ID 番号を入力し、ステップ 1 ~ 8 で以前に作成したロールの名前を入力します。[ARN を追加] を選択します。
15. 複数のメンバーアカウントのロールを引き受けるためのアクセス権限を付与する場合は、アカウントごとにステップ 14 と 15 を繰り返します。
16. [Next (次へ)] を選択します。
17. [確認と作成] ページで、新しいポリシーの名前を入力し、[ポリシーの作成] を選択し、変更を保存します。
18. ナビゲーションペインで [ユーザーグループ] を選択し、メンバーアカウントの管理を委任するグループの名前 (チェックボックスではない) を選択します。
19. [アクセス許可] タブを選択します。
20. [アクセス許可を追加する] を選択し、[ポリシーのアタッチ] を選択し、次に、ステップ 11 ~ 18 で作成したポリシーを選択します。

選択したグループのメンバーであるユーザーは、ステップ 9 で取得した URL より、各メンバーアカウントのロールにアクセスできるようになりました。こうしたメンバーアカウントには、組織内に作成したアカウントにアクセスする場合と同様にアクセスすることができます。メンバーアカウントを管理するロールの使用の詳細については、「で OrganizationAccountAccessRole を持つメンバーアカウントにアクセスする AWS Organizations」を参照してください。

で OrganizationAccountAccessRole を持つメンバーアカウントにアクセスする AWS Organizations

AWS Organizations コンソールを使用してメンバーアカウントを作成すると、 はアカウントOrganizationAccountAccessRole内に という名前の IAM ロール AWS Organizations を自動的に作成します。このロールには、メンバーアカウントの完全な管理権限が含まれます。このロールのアクセスの範囲には、管理アカウント内のすべてのプリンシパルが含まれます。これにより、ロールは組織の管理アカウントにそのアクセスを許可するように構成されます。

招待されたメンバーアカウントと同一のロールを作成するには、「で招待されたアカウントの OrganizationAccountAccessRole を作成する AWS Organizations」のステップを実行します。

このロールを使用してメンバーアカウントにアクセスするには、ロールを引き受けるアクセス許可を持つ管理アカウントのユーザーでサインインする必要があります。このアクセス権限を設定するには、次の手順を行います。メンテナンスしやすいように、アクセス権限は、ユーザーではなくグループに付与することをお勧めします。

AWS Management Console

管理アカウントの IAM グループのメンバーにアクセス許可を付与して、ロールにアクセスするには

1. IAM コンソール (https://console.aws.amazon.com/iam/) に管理者用のアクセス許可を持つ管理アカウントのユーザーとしてサインインします。これは、メンバーアカウントのロールにアクセスするユーザーが属する IAM グループにアクセス許可を委任するために必要です。
2. まず、後で必要になる管理ポリシーを ??? で作成します。

   ナビゲーションペインで、[Policies (ポリシー)] を選択し、[Create Policy (ポリシーの作成)] を選択します。
3. [ビジュアルエディタ] タブで、[サービスの選択] を選択し、検索ボックスに「**STS**」と入力してリストをフィルタリングし、[STS] オプションを選択します。
4. [アクション] セクションで、検索ボックスに「**assume**」と入力してリストをフィルタリングし、[AssumeRole] オプションを選択します。
5. [リソース] セクションで、[特定の] を選択し、[ARN を追加] を選択します。
6. [ARN を指定 (複数可)] セクションで、リソースの [その他のアカウント] を選択します。
7. 作成したメンバーアカウントの ID を入力します。

8. [パス を持つリソースロール名] には、前のセクションで作成したロールの名前を入力します (`OrganizationAccountAccessRole` という名前を付けることをお勧めします)。
9. ダイアログボックスに正しい ARN が表示されたら、[ARN を追加] を選択します。
10. (オプション) 多要素認証 (MFA) が必要な場合や、指定された IP アドレス範囲からロールへのアクセスを制限する場合、[リクエスト条件] セクションを展開し、適用するオプションを選択します。
11. [Next (次へ)] を選択します。
12. [確認と作成] ページで、新しいポリシーの名前を入力します。例: **`GrantAccessToOrganizationAccountAccessRole`**。オプションとして説明を追加することもできます。
13. [ポリシーの作成] を選択してポリシーを保存します。
14. ポリシーが使用可能になったので、グループにアタッチできます。

    ナビゲーションペインで、[ユーザーグループ] を選択してから、メンバーアカウントのロールを引き受けるメンバーが属するグループの名前 (チェックボックスではない) を選択します。必要に応じて、新しいグループを作成できます。
15. [アクセス許可] タブを選択し、[アクセス許可の追加] を選択してから、[ポリシーの添付] を選択します。
16. (オプション) [検索] ボックスに、ポリシー名を入力し始めると、「Step 2」から「Step 13」で作成したポリシーの名前が表示されるまで、リストをフィルタリングできます。[ポリシータイプ]、[カスタマー管理ポリシー] の順に選択すると、すべての AWS 管理ポリシーをフィルタリングできます。
17. ポリシーの横にあるチェックボックスをオンにし、[ポリシーのアタッチ] を選択します。

グループのメンバーである IAM ユーザーには、次の手順を使用して AWS Organizations コンソールで新しいロールに切り替えるアクセス許可が付与されるようになりました。

AWS Management Console

メンバーのアカウントのロールに切り替えるには

ロールを使用する際、ユーザーは、新しいメンバーアカウントの管理者権限が付与されます。グループのメンバーである IAM ユーザーに、以下を実行して新しいロールに切り替えるように指示します。

1. AWS Organizations コンソールの右上から、現在のサインイン名を含むリンクを選択し、ロールの切り替えを選択します。
2. 管理者から提供されたアカウント ID 番号とロール名を入力します。
3. [表示名] で、ロール使用時にユーザー名の代わりに右上隅のナビゲーションバーに表示する文字列を入力します。オプションで色を選択することもできます。
4. [Switch Role] (ロールの切り替え) を選択します。これで、実行するアクションはすべて、切り替えたロールに付与されているアクセス権限で行われるようになりました。切り替えを戻さない限り、元の IAM ユーザーに関連付けられているアクセス許可を使用することはできません。
5. ロールのアクセス許可を必要とするアクションの実行が完了したら、通常の IAM ユーザーにもう一度切り替えることができます。右上隅のロール名 ([表示名] として指定した名前) を選択して、[***#####*** に戻る] を選択します。

を使用して組織のメンバーアカウントを閉鎖する AWS Organizations

組織に不要になったメンバーアカウントがある場合は、このトピックの手順に従って、AWS Organizations コンソールからそのアカウントを閉鎖することができます。組織がすべての機能モードの場合にのみ、 AWS Organizations コンソールを使用してメンバーアカウントを閉鎖できます。

ルートユーザーとしてサインイン AWS Management Console した後、 のアカウントページ AWS アカウント から直接 を閉じることもできます。ステップバイステップの手順については、「AWS Account Management Guide」の「Close an AWS アカウント」を参照してください。

管理アカウントを閉鎖するには、「組織の管理カウントの閉鎖」を参照してください。

メンバーアカウントの閉鎖

組織の管理アカウントにサインインすると、組織に属しているメンバーアカウントを閉鎖できます。そのためには、以下の手順を完了します。

> **Important**
>
> メンバーアカウントを閉鎖する前に、考慮事項を確認し、アカウントを閉鎖した場合の影響を理解しておくことを強くお勧めします。詳細については、「AWS Account Management Guide」の「What you need to know before closing your account」と「What to expect after you close your account」を参照してください。

AWS Management Console

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

1. AWS Organizations コンソール にサインインします。IAM ユーザーとしてサインインするか、組織の管理アカウントのルートユーザー (非推奨) としてサインインする必要があります。
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。このオプションは、組織がすべての機能モードの場合にのみ AWS 使用できます。

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

4. アカウント閉鎖ガイダンスを読んで、理解していることを確認します。
5. メンバーアカウント ID を入力し、[アカウントの閉鎖] をクリックします。

> **Note**
>
> 閉じたメンバーアカウントは、元の終了日から最大 90 日間、 AWS Organizations コンソールのアカウント名の横に SUSPENDED ラベルがに表示されます。90 日後、メンバーアカウントは AWS Organizationsに表示されなくなります。

アカウントページからメンバーアカウントを閉じるには

必要に応じて、 のアカウントページから直接 AWS メンバーアカウントを閉鎖できます AWS Management Console。ステップバイステップのガイダンスについては、「AWS Account Management Guide」の「Close an AWS アカウント」の指示に従ってください。

AWS CLI & AWS SDKs

を閉じるには AWS アカウント

次のいずれかのコマンドを使用して AWS アカウントを閉鎖できます。

- AWS CLI: close-account

```
$ aws organizations close-account \
    --account-id 123456789012
```

このコマンドが成功した場合、出力は生成されません。

- AWS SDKs: CloseAccount

によるメンバーアカウントの閉鎖からの保護 AWS Organizations

誤って閉鎖されないようにメンバーアカウントを保護するには、除外するアカウントを指定する IAM ポリシーを作成します。このポリシーは、保護されたメンバーアカウントの閉鎖を防ぎます。

次のいずれかの方法を使用してアカウント閉鎖を拒否する IAM ポリシーを作成します。

- ARN を使用して、ポリシーの `Resource`要素内の保護されたアカウントを明示的に一覧表示します。 ARNs
- 個々のアカウントにタグ付けし、`aws:ResourceTag`グローバル条件キーを使用して、タグ付けされたアカウントが閉鎖されないようにします。

> **サービスコントロールポリシーがメンバーアカウントを保護できない**
>
> SCP は管理アカウントの IAM プリンシパルには影響しないため、サービスコントロールポリシー (SCPs) は計算されたメンバーアカウントには影響しません。

メンバーアカウントが閉鎖されないようにする IAM ポリシーの例

次のコード例では、メンバーアカウントがアカウントを閉鎖するのを制限するために使用できる方法を 2 つ紹介します。

Prevent member accounts with tags from getting closed

管理アカウントの ID に次のポリシーをアタッチできます。このポリシーにより、管理アカウントのプリンシパルは、`aws:ResourceTag` タググローバル条件キー、`AccountType` キー、および `Critical` タグ値がタグ付けされているメンバーアカウントを閉鎖できなくなります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccountForTaggedAccts",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/AccountType": "Critical"}
            }
        }
    ]
}
```

Prevent member accounts listed in this policy from getting closed

管理アカウントの ID に次のポリシーをアタッチできます。このポリシーにより、管理アカウントのプリンシパルは、Resource エレメントで明示的に指定されたメンバーアカウントを閉鎖できなくなります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccount",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": [
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789012",
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789014"
            ]
        }
    ]
}
```

を使用して組織からメンバーアカウントを削除する AWS Organizations

メンバーアカウントを削除してもアカウントは閉鎖されません。そのメンバーアカウントは組織から削除されます。以前のメンバーアカウント AWS アカウント は、 によって管理されなくなったスタンドアロンアカウントになります AWS Organizations。

その後、そのアカウントにはポリシーが適用されなくなり、請求書の支払いはそのアカウントの責任となります。アカウントが組織から削除された後は、そのアカウントで発生した費用については、組織の管理アカウントには請求されなくなります。

考慮事項

管理アカウントによって作成された IAM アクセスロールは自動的に削除されません

メンバーアカウントを組織から削除しても、組織の管理アカウントによるアクセスを有効にするために作成された IAM ロールは自動的に削除されません。以前の組織の管理アカウントからアクセスされないようにするには、その IAM ロールを手動で削除する必要があります。ロールを削除する方法について詳しくは、IAM ユーザーガイドのロールまたはインスタンスプロファイルの削除を参照してください。

アカウントがスタンドアロンアカウントとして機能するために必要な情報を持っている場合に限り、組織からアカウントを削除できる

アカウントがスタンドアロンアカウントとして動作するために必要な情報を持っている場合に限り、組織からアカウントを削除できます。 AWS Organizations コンソール、API、または AWS CLI コマンドを使用して組織でアカウントを作成する場合、スタンドアロンアカウントに必要なすべての情報は自動的に収集されません。

スタンドアロンにするアカウントごとに、サポートプランを選択し、必要な連絡先情報を指定して検証し、現在の支払い方法を指定する必要があります。 は、アカウントが組織にアタッチされていない間に発生する請求対象 (AWS 無料利用枠ではない) AWS アクティビティに対して課金するために支払い方法 AWS を使用します。この情報がないアカウントを削除するには、「を使用してメンバーアカウントから組織を退出する AWS Organizations」の手順に従ってください。

アカウントが作成されてから少なくとも 7 日間待つ必要がある

組織内に作成したアカウントを削除するには、アカウントが作成されてから 7 日以上が経過している必要があります。招待されたアカウントの場合には、7 日間待つ必要はありません。

退出するアカウントの所有者が、発生したすべての新しいコストを負担する

アカウントが組織を正常に離れた時点で、 の所有者 AWS アカウント は発生したすべての新しい AWS コストの負担となり、アカウントの支払い方法が使用されます。そのとき以降、組織の管理アカウントが責任を負うことはありません。

アカウントは、組織で有効になっている AWS サービスの委任管理者アカウントにすることはできません

削除するアカウントは、組織で有効になっている AWS サービスの委任管理者アカウントであってはなりません。アカウントが代理管理者である場合は、まずその代理管理者アカウントを組織に残る別のアカウントに変更する必要があります。 AWS サービスの委任管理者アカウントを無効化または変更する方法の詳細については、そのサービスのドキュメントを参照してください。

アカウントがコストと使用状況データにアクセスできなくなる

メンバーアカウントが組織を離れると、そのアカウントは組織のメンバーであったときのコストと使用状況のデータにアクセスできなくなります。ただし、組織の管理アカウントは引き続きデータにアクセスできます。再度組織に加わった場合、アカウントは再びデータにアクセスできます。

アカウントにアタッチされたタグは削除される

メンバーアカウントが組織を離れると、そのアカウントにアタッチされていたタグはすべて削除されます。

アカウントのプリンシパルは組織のポリシーの影響を受けなくなる

アカウントのプリンシパルは組織で適用されていたポリシーの影響を受けなくなります。つまり、SCP によって課せられていた制限がなくなり、そのアカウントのユーザーとロールに以前より多くのアクセス許可が付与される可能性があります。その他の組織ポリシータイプが適用または処理されることはなくなります。

アカウントは組織契約の対象ではない

メンバーアカウントが組織から削除されると、そのメンバーアカウントは組織契約の対象範囲ではなくなります。管理アカウントの管理者は、メンバーアカウントが必要に応じて新しい契約を用意できるよう、メンバーアカウントを組織から削除する前に、そのことをメンバーアカウントに通達するべきです。アクティブな組織契約のリストは、AWS Artifact 組織契約ページの AWS Artifact コンソールで表示できます。

他のサービスとの統合が無効になる場合がある

他のサービスとの統合が無効になる場合があります。 AWS サービスとの統合が有効になっている組織からアカウントを削除すると、そのアカウントのユーザーはそのサービスを使用できなくなります。

組織からメンバーアカウントを削除する

組織の管理アカウントにサインインすると、不要になったメンバーアカウントを組織から削除できます。これを行うには、以下の手順を完了します。この手順はメンバーアカウントのみに適用されます。管理アカウントを削除するには、組織を削除する必要があります。

最小アクセス許可

組織から 1 つ以上のメンバーアカウントを削除するには、次の許可がある管理アカウントのユーザーまたはロールとしてサインインする必要があります。

- `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要
- `organizations:RemoveAccountFromOrganization`

ステップ 5 でメンバーアカウントのユーザーまたはロールとしてサインインを選択した場合、そのユーザーまたはロールには次の許可が必要となります。

- `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要です。
- `organizations:LeaveOrganization` - 組織の管理者は、このアクセス許可を削除するポリシーをアカウントに適用し、組織からアカウントを削除することを禁止できます。
- IAM ユーザーとしてサインインし、アカウントに支払い情報がない場合、そのユーザーには `aws-portal:ModifyBilling` 許可と `aws-portal:ModifyPaymentMethods` 許可 (アカウントがきめ細かな許可に移行されていない場合)、または `payments:CreatePaymentInstrument` 許可と `payments:UpdatePaymentPreferences` 許可 (アカウントがきめ細かな許可に移行されている場合) のどちらか一方が必要になります。また、メンバーアカウントでは、請求への IAM ユーザーアクセスが有効になっている必要があります。有効になっていない場合は、AWS Billing ユーザーガイドの Billing and Cost Management コンソールへのアクセスを有効にするを参照してください。

AWS Management Console

組織からメンバーアカウントを削除するには

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. AWS アカウント ページで、組織から削除するメンバーアカウントを探し、その横にあるチェックボックス

   をオンにします。OU 階層を移動するか、表示 AWS アカウント のみを有効にして、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。アカウントが多い場合、削除対象をすべて見つけるにはリスト下部の [Load more accounts in 'ou-name'] ('ou-name' のアカウントをさらに読み込む) を選択する必要がある場合があります。

   AWS アカウント ページで、組織から削除するメンバーアカウントの名前を探し、選択します。場合によっては、目的のアカウントを見つけるには OU を展開
   (
   を選択) する必要があります。
3. [Actions] (アクション) を選択し、[AWS アカウント] で [Remove from organization] (組織から削除する) を選択します。
4. [Remove account 'account-name' (#account-id-num) from organization?] (アカウント 'account-name' (#account-id-num) を組織から削除しますか?) ダイアログボックスで、[Remove account] (アカウントを削除する) を選択します。
5. が 1 つ以上のアカウントを削除 AWS Organizations できなかったのは、通常、アカウントがスタンドアロンアカウントとして動作するために必要なすべての情報を提供していないためです。以下のステップを実行します。

   a. 失敗したアカウントにサインインします。メンバーアカウントには、[Copy link] を選択してから、新しい incognito ブラウザウィンドウのアドレスバーに貼り付けてサインインすることをお勧めします。[リンクのコピー] が表示されない場合は、「このリンク」を使用して [AWSにサインアップ] ページに移動し、不足している登録ステップを完了します。シークレットウィンドウを使用しない場合は、管理アカウントからサインアウトされ、このダイアログボックスに戻ることができなくなります。

   b. ブラウザを使用すると、このアカウントで実行していなかったステップを完了するためのサインアッププロセスが直接表示されます。示されたすべてのステップを実行します。これには次のものが含まれます。

- 連絡先情報を指定する
- 有効な支払い方法の指定
- 電話番号を検証する
- サポートプランオプションを選択する

c. 最後のサインアップステップを完了すると、 AWS は自動的にブラウザをメンバーアカウントの AWS Organizations コンソールにリダイレクトします。[Leave organization] を選択し、確認ダイアログボックスで、その選択を確認します。 AWS Organizations コンソールの [Getting Started] ページにリダイレクトされます。そこで、招待が保留中のアカウントを表示して、他の組織に参加することができます。

d. アカウントへのアクセスを付与する IAM ロールを組織から削除します。

> **Important**
>
> 組織で作成されたアカウントの場合、組織の管理アカウントによるアクセスを有効にするための IAM ロールが、Organizations によってアカウントに自動的に作成されています。招待されたアカウントの場合、Organizations によってこのようなロールが自動で作成されることはありませんが、ご自身または別の管理者が同じメリットを得るためにロールを作成している可能性があります。いずれの場合も、組織からアカウントを削除した場合に、このようなロールは自動的に削除されません。以前の組織の管理アカウントからアクセスされないようにするには、この IAM ロールを手動で削除する必要があります。ロールを削除する方法について詳しくは、IAM ユーザーガイドのロールまたはインスタンスプロファイルの削除を参照してください。

AWS CLI & AWS SDKs

組織からメンバーアカウントを削除するには

メンバーアカウントを作成するには、次のいずれかのコマンドを使用します。

- AWS CLI: remove-account-from-organization

```
$ aws organizations remove-account-from-organization \
    --account-id 123456789012
```

このコマンドが成功した場合、出力は生成されません。

- AWS SDKs: RemoveAccountFromOrganization

メンバーアカウントが組織から削除されたら、アカウントへのアクセスを付与する IAM ロールを組織から削除します。

> **Important**
>
> 組織で作成されたアカウントの場合、組織の管理アカウントによるアクセスを有効にするための IAM ロールが、Organizations によってアカウントに自動的に作成されています。招待されたアカウントの場合、Organizations によってこのようなロールが自動で作成されることはありませんが、ご自身または別の管理者が同じメリットを得るためにロールを作成している可能性があります。いずれの場合も、組織からアカウントを削除した場合に、このようなロールは自動的に削除されません。以前の組織の管理アカウントからアクセスされないようにするには、この IAM ロールを手動で削除する必要があります。ロールを削除する方法について詳しくは、IAM ユーザーガイドのロールまたはインスタンスプロファイルの削除を参照してください。

メンバーアカウントは、代わりに Leave-Organization を使用して自身のアカウントを削除することができます。詳細については、「を使用してメンバーアカウントから組織を退出する AWS Organizations」を参照してください。

を使用してメンバーアカウントから組織を退出する AWS Organizations

メンバーアカウントにサインインすると、組織を離れることができます。管理アカウントは、この方法で組織を離れることはできません。管理アカウントを削除するには、組織を削除する必要があります。

考慮事項

組織に対するアカウントのステータスは、表示できるコストと使用状況のデータに影響する

メンバーアカウントが組織を離れてスタンドアロンアカウントになると、そのアカウントは組織のメンバーであったときのコストと使用状況のデータにアクセスできなくなります。アカウントがアクセスできるのは、スタンドアロンアカウントとして生成されたデータのみです。

メンバーアカウントが組織 A を離れ組織 B に参加すると、そのアカウントは組織 A のメンバーであったときのコストと使用状況のデータにアクセスできなくなります。アカウントがアクセスできるのは、組織 B のメンバーとして生成されたデータのみです。

アカウントが以前に属していた組織に再参加すると、そのアカウントはコストと使用状況データの履歴へのアクセスを再び許可されます。

アカウントは、そのアカウントに代わって承諾された組織契約の対象ではなくなる

組織を離れると、メンバーアカウントを代表して組織の管理アカウントによって受諾されていた組織契約は適用されなくなります。これらの組織契約のリストは、AWS Artifact 組織契約ページの AWS Artifact コンソールで確認できます。組織を離れる前に、(必要に応じて、法務、プライバシー、またはコンプライアンスチームの支援を得て) 新しい契約を結ぶ必要があるかどうか判断してください。

メンバーアカウントから組織を脱会する

組織を脱会する、次の手順を実行します。

最小アクセス許可

組織を登録解除する場合は、次のアクセス権限が必要です:

- `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要です。
- `organizations:LeaveOrganization` - 組織の管理者は、このアクセス許可を削除するポリシーをアカウントに適用し、組織からアカウントを削除することを禁止できます。
- IAM ユーザーとしてサインインし、アカウントに支払い情報がない場合、そのユーザーには `aws-portal:ModifyBilling` 許可と `aws-portal:ModifyPaymentMethods` 許可 (アカウントがきめ細かな許可に移行されていない場合)、または `payments:CreatePaymentInstrument` 許可と `payments:UpdatePaymentPreferences` 許可 (アカウントがきめ細かな許可に移行されている場合) のどちらか一方が必要になります。また、メンバーアカウントでは、請求への IAM ユーザーアクセスが有効になっている必要があります。有効になっていない場合は、AWS Billing ユーザーガイドの Billing and Cost Management コンソールへのアクセスを有効にするを参照してください。

AWS Management Console

メンバーアカウントから組織を退会するには

1. AWS Organizations コンソールで AWS Organizations コンソールにサインインします。メンバーアカウントで、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。

   デフォルトでは、 を使用して作成されたメンバーアカウントのルートユーザーパスワードにアクセスすることはできません AWS Organizations。必要に応じて、「 でのルートユーザーの使用 (日常的なタスクでは推奨されません) 」の手順に従って、ルートユーザーのパスワードを復元しますを使用して組織のメンバーアカウントにアクセスする AWS Organizations。
2. Organizations ダッシュボードページで、[この組織を離れる] を選択します。
3. [組織を離れることを確認する] ダイアログボックスで、[組織を離れる] を選択します。プロンプトが表示されたら、アカウントの削除を確認します。確認後、 AWS Organizations コンソールの開始方法ページにリダイレクトされ、アカウントが他の組織に参加するための保留中の招待を表示できます。

   [まだ組織を離れることはできません] というメッセージが表示される場合、アカウントにはスタンドアロンアカウントとして運営するために必要なすべての情報が揃っていません。この場合は、次のステップに進みます。
4. [組織を離れることを確認する] ダイアログボックスに [まだ組織を離れることはできません] というメッセージが表示される場合、[アカウントのサインアップステップを完了する] というリンクを選択します。

   [アカウントサインアップ手順の完了] リンクが表示されない場合は、「このリンク」を使用して [AWSへのサインアップ] ページに移動し、不足している登録手順を完了します。
5. [AWS にサインアップする] ページで、スタンドアロンアカウントになるために必要な情報をすべて入力します。これには、以下の種類の情報が含まれる場合があります。

   - 連絡先名と住所
   - 有効な支払い方法
   - 電話番号による確認
   - サポートプランオプション
6. サインアッププロセスが完了したことを示すダイアログボックスが表示されたら、[Leave organization] を選択します。

確認のダイアログボックスが表示されます。アカウントを削除するには、その選択を確認します。 AWS Organizations コンソールの開始方法ページにリダイレクトされ、アカウントが他の組織に参加するための保留中の招待を表示できます。

7. アカウントへのアクセスを付与する IAM ロールを組織から削除します。

> **Important**
>
> 組織で作成されたアカウントの場合、組織の管理アカウントによるアクセスを有効にするための IAM ロールが、Organizations によってアカウントに自動的に作成されています。招待されたアカウントの場合、Organizations によってこのようなロールが自動で作成されることはありませんが、ご自身または別の管理者が同じメリットを得るためにロールを作成している可能性があります。いずれの場合も、組織からアカウントを削除した場合に、このようなロールは自動的に削除されません。以前の組織の管理アカウントからアクセスされないようにするには、この IAM ロールを手動で削除する必要があります。ロールを削除する方法について詳しくは、IAM ユーザーガイドのロールまたはインスタンスプロファイルの削除を参照してください。

AWS CLI & AWS SDKs

メンバーアカウントとして組織を離れるには

組織を登録解除するには、次のいずれかのコマンドを使用します。

- AWS CLI: leave-organization

  次の例では、アカウントの認証情報を使用し、組織を離れるコマンドを実行しています。

  ```
  $ aws organizations leave-organization
  ```

  このコマンドが成功した場合、出力は生成されません。

- AWS SDKs: LeaveOrganization

メンバーアカウントが組織を離れたら、アカウントへのアクセスを付与する IAM ロールを組織から削除します。

> **Important**
>
> 組織で作成されたアカウントの場合、組織の管理アカウントによるアクセスを有効にするための IAM ロールが、Organizations によってアカウントに自動的に作成されています。招待されたアカウントの場合、Organizations によってこのようなロールが自動で作成されることはありませんが、ご自身または別の管理者が同じメリットを得るためにロールを作成している可能性があります。いずれの場合も、組織からアカウントを削除した場合に、このようなロールは自動的に削除されません。以前の組織の管理アカウントからアクセスされないようにするには、この IAM ロールを手動で削除する必要があります。ロールを削除する方法について詳しくは、IAM ユーザーガイドのロールまたはインスタンスプロファイルの削除を参照してください。

代わりの方法として、メンバーアカウントは、管理アカウントのユーザーが remove-account-from-Organization を使用して削除することもできます。詳細については、「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。

でメンバーアカウントのアカウント名を更新する AWS Organizations

組織の管理アカウントにサインインすると、メンバーアカウントのアカウント名を更新できます。メンバーアカウント名を更新する方法については、「 AWS アカウント管理 リファレンスガイド」の「組織 AWS アカウント 内の のアカウント名を更新する」の手順に従います。

でメンバーアカウントのルートユーザーの E メールアドレスの更新AWS Organizations

セキュリティと管理のレジリエンスを高めるため、管理アカウントの IAM プリンシパル (必要な IAM アクセス許可を持つ) は、各アカウントに個別にサインインすることなく、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 (プライマリ E メールアドレスとも呼ばれます) を一元的に更新できます。これにより、管理アカウント (または委任管理者アカウント) の管理者は、メンバーアカウントをより細かく制御できます。また、ルートユーザーの E メールアドレスは、元のルートユーザーの E メールアドレスまたは管理者認証情報にアクセスできなくなった場合でも、 全体の任意のメンバーアカウントから最新の状態に保つ AWS Organizations ことができます。

ルートユーザーの E メールアドレスを管理アカウント管理者が一元的に変更する場合、パスワードと MFA 設定の両方が変更前と同じままになります。MFA は、アカウントのルートユーザーの E

メールアドレスと主要連絡先の電話番号を制御できるユーザーがバイパスできることに注意してください。

組織内のメンバーアカウントのルートユーザーの E メールアドレスを更新する、組織で以前にすべての機能モードが有効になっている必要があります。一括請求モードまたは組織の一部ではないアカウント AWS Organizations では、ルートユーザーの E メールアドレスを一元的に更新することはできません。API でサポートされていないアカウントのルートユーザーの E メールアドレスを変更するは、引き続き請求コンソールを使用してルートユーザーの E メールアドレスを管理する必要があります。

メンバーアカウントのルートユーザーの E メールアドレスアマゾン を更新する手順 step-by-step については、「 AWS アカウント管理 リファレンスガイド」の「組織 AWS アカウント 内の のルートユーザーの E メール メールを更新する」を参照してください。

を使用したアカウント招待の管理 AWS Organizations

組織を作成し、管理アカウントに関連付けられた E メールアドレスを所有していることを確認したら、既存の AWS アカウント を組織に招待できます。 AWS Organizations コンソールを使用して、他のアカウントに送信する招待を開始および管理します。別のアカウントへの招待は、組織の管理アカウントからのみ送信できます。

アカウントを招待すると、 はアカウント所有者に招待 AWS Organizations を送信します。アカウント所有者は招待を承諾または拒否できます。

の管理者は AWS アカウント、組織からの招待を承諾または拒否することもできます。受諾する場合は、アカウントがその組織のメンバーになります。

組織の一部としてアカウントを作成するには、「を使用した組織内のメンバーアカウントの作成 AWS Organizations」を参照してください。

> **Important**
>
> 組織内のすべてのアカウントは、管理アカウントと同じ AWS パーティションから取得する必要があります。商用 AWS リージョン パーティションのアカウントは、中国リージョン パーティションのアカウントまたはリージョンパーティションのアカウントを持つ組織内に存在することはできません AWS GovCloud (US) 。

トピック

- 考慮事項
- を使用したアカウント招待の送信 AWS Organizations
- を使用した保留中のアカウント招待の管理 AWS Organizations
- によるアカウント招待の承諾または拒否 AWS Organizations

考慮事項

1 日あたりに送信できる招待数の制限

1 日に送信できる招待の数については、「最大値および最小値」を参照してください。承諾済みの招待は、このクォータに対してカウントされません。1 つの招待が承諾されるとすぐ、同じ日に別の招待を送信できます。各招待は、15 日以内に応答する必要があります。応答しない場合は期限切れとなります。

アカウントへ送られた招待は、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。招待が辞退された場合や、管理アカウントによってキャンセルされた場合、または招待の有効期限が切れた場合、カウントはリセットされます。

アカウントは 1 つの組織にのみ参加できます

アカウントは 1 つの組織にのみ参加できます。複数の招待を受け取った場合は、1 つのみ受け入れることができます。

請求履歴とレポートは管理アカウントに保持されます

すべてのアカウントの請求履歴とレポートは、組織内の管理アカウントに残ります。アカウントを新しい Organization に移動する前に、保持するメンバーアカウントの請求履歴とレポート履歴をエクスポートまたはバックアップしてください。これには、「Cost and Usage Reports」、「Cost Explorer Reports」、「Savings Plans Reports」、「Reserved Instance (RI) utilization and coverage」が含まれます。

管理アカウントは、すべてのメンバーアカウントの料金の支払い責任を負う

アカウントが組織への招待を受け入れた後、組織の管理アカウントは、新しいメンバーアカウントに発生するすべての課金に対して責任を負うことになります。そのメンバーアカウントにそれまで適用されていた支払い方法は使用されなくなります。代わりに、メンバーアカウントに発生したすべての課金の支払いは、組織の管理アカウントに適用されている支払い方法に基づいて行われます。

Organizations はサービスにリンクされたロール **AWSServiceRoleForOrganizations** を自動的に作成する

AWS Organizations は、 AWS Organizations と他の AWS のサービスの統合をサポートするために`AWSServiceRoleForOrganizations`、 というサービスにリンクされたロールを作成します。詳細については、「AWS Organizations およびサービスにリンクされたロール」を参照してください。組織がすべての機能をサポートする場合、招待されたアカウントにはこのロールが必要です。組織が一括請求機能セットのみをサポートしている場合は、このロールは削除できます。このロールを削除し、後で組織内のすべての機能を有効にすると、 はアカウントのこのロール AWS Organizations を再作成します。

Organizations は自動的に IAM ロール **`OrganizationAccountAccessRole`** を作成しない

招待されたメンバーアカウントの場合、IAM ロール は自動的に作成 AWS Organizations されません`OrganizationAccountAccessRole`。このロールは、メンバーアカウントへの管理アクセスを管理アカウントのユーザーに付与します。招待されたアカウントにこのレベルの管理上のコントロールを有効にする場合は、ロールを手動で追加します。詳細については、「で招待されたアカウントの OrganizationAccountAccessRole を作成する AWS Organizations」を参照してください。

> **Note**
>
> 既存のアカウントを招待するのではなく、組織内にアカウントを作成すると、 は`OrganizationAccountAccessRole`デフォルトで IAM ロール AWS Organizations を自動的に作成します。

アカウントを含むルートまたは OU にアタッチされたポリシーがすぐに適用される

招待されたアカウントを含むルートまたは組織単位 (OU) にアタッチされたポリシーがある場合、それらのポリシーは招待されたアカウントのすべてのユーザーとロールに直ちに適用されます。

組織の別のサービスの AWS サービス信頼を有効にできます。これを行うと、その信頼されたサービスは、招待されたアカウントを含め、組織内の任意のメンバーアカウントで、サービスにリンクされた役割を作成したり、アクションを実行したりできます。

一括請求機能セットのみを持つ Organizations は、引き続きアカウントを招待できる

一括請求 (コンソリデーティッドビリング) 機能のみが有効になっている組織に参加するようアカウントを招待できます。後で組織のすべての機能を有効にする場合は、招待されたアカウントが変更を承認する必要があります。

を使用したアカウント招待の送信 AWS Organizations

組織にアカウントを招待するには、まず管理アカウントに関連付けられたメールアドレスを所有していることを検証する必要があります。詳細については、「による E メールアドレスの検証 AWS Organizations」を参照してください。メールアドレスを検証したら、次のステップを実施してアカウントを組織に招待します。

最小アクセス許可

AWS アカウント を組織に招待するには、次のアクセス許可が必要です。

- `organizations:DescribeOrganization` (コンソールのみ)
- `organizations:InviteAccountToOrganization`

AWS Management Console

別のアカウントを組織に招待するには

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. で E メールアドレスをすでに検証している場合は AWS、このステップをスキップします。

   まだメールアドレスを検証していない場合には、組織の作成から 24 時間以内に E メールアドレスの検証の手順を実施します。検証メールが届くまでには時間がかかる場合があります。メールアドレスの検証が完了したら、アカウントを組織に招待できます。
3. [AWS アカウント] ページに移動し、[Add an AWS account] (AWS アカウントを追加する) を選択します。
4. [Add an AWS アカウント] (AWS アカウントを追加する) ページで、[Invite an existing AWS account] (既存の AWS アカウントを招待する) を選択します。
5. 既存のページの招待 AWSで、招待 AWS アカウント する の E メールアドレスまたはアカウント ID に、招待するアカウントに関連付けられた E メールアドレス、またはそのアカウント ID 番号を入力します。
6. (オプション) [Message to include in the invitation email message] (招待メールに含めるメッセージ) で、招待するアカウントの所有者に送る、メールによる招待に含める文章を入力します。

7. (オプション) [Add tags] (タグの追加) セクションで、招待がアカウント管理者によって承諾されたときに自動的にアカウントに適用する 1 つ以上のタグを指定します。これを行うには、[Add tag] (タグの追加) を選択してから、キーとオプションの値を入力します。値を空白のままにすると、空の文字列が設定され、null にはなりません。1 つの AWS アカウントに最大 50 個のタグをアタッチできます。
8. [Send invitation] (招待の送信) を選択します。

   > **Important**
   >
   > 組織内のアカウントのクォータを超過した、または組織がまだ初期化中であるためアカウントを追加できないというメッセージが表示された場合は、AWS サポート までお問い合わせください。

9. コンソールは自動的に [Invitations] (招待) ページに移動します。このページで、保留中または承諾済みのすべての招待を確認できます。作成した招待がリストの上部に表示され、ステータスが OPEN に設定されます。

   AWS Organizations は、組織に招待したアカウントの所有者の E メールアドレスに招待を送信します。この E メールメッセージには、アカウント所有者が詳細を表示し、招待を承諾または拒否することを選択できる AWS Organizations コンソールへのリンクが含まれています。または、招待されたアカウントの所有者は、E メールメッセージをバイパスし、 AWS Organizations コンソールに直接移動して招待を表示し、承諾または拒否できます。

   このアカウントへの招待は、組織内で保持できるアカウントの上限数に対してすぐにカウントされます。 AWS Organizations は、アカウントが招待を承諾するまで待ちません。招待が辞退された場合は、管理アカウントはその招待をキャンセルします。招待されたアカウントが指定された期間内に応答しない場合、招待は期限切れになります。どちらの場合も、招待はクォータに対してカウントされなくなります。

AWS CLI & AWS SDKs

別のアカウントを組織に招待するには

他のアカウントを参加するよう組織を招待するには、次のいずれかのコマンドを使用します。

- AWS CLI: invite-account-to-organization

```
$ aws organizations invite-account-to-organization \
    --target '{"Type": "EMAIL", "Id": "juan@example.com"}' \
```

```
    --notes "This is a request for Juan's account to join Bill's organization."
{
    "Handshake": {
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                 "Type": "ORGANIZATION"
            },
            {
                 "Id": "juan@example.com",
                 "Type": "EMAIL"
            }
        ],
        "RequestedTimestamp": 1481656459.257,
        "Resources": [
            {
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                         "Type": "MASTER_NAME",
                         "Value": "Management Account"
                    },
                    {
                         "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "FULL"
                    }
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "OPEN"
```

```
    }
}
```

- AWS SDKs: InviteAccountToOrganization

を使用した保留中のアカウント招待の管理 AWS Organizations

管理アカウントにサインインすると、組織にリンクされているすべての AWS アカウント の表示と、保留中 (オープン) の招待のキャンセルが可能です。そのためには、以下の手順を完了します。

> **最小アクセス許可**
>
> 組織の保留中の招待を管理するには、次のアクセス権限が必要です。
>
> - `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要
> - `organizations:ListHandshakesForOrganization`
> - `organizations:CancelHandshake`

AWS Management Console

組織から別のアカウントへ送信される招待を表示またはキャンセルするには

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. [Invitations] (招待) ページに移動します。

   組織から送信されたすべての招待と、各招待の現在のステータスが表示されます。

   招待が表示されない場合は、招待されたアカウントが別の組織の管理アカウントであるかどうかを確認します。招待を受信できるのは、メンバーアカウントとスタンドアロンアカウントのみです。管理アカウントは招待を受信できません。

   別の組織の管理アカウントであるアカウントを招待する場合は、そのアカウントをスタンドアロンアカウントにすることをお勧めします。

> **Note**
>
> 承諾済み、キャンセル、および拒否された招待は、30 日間リストに表示され続けます。その後は削除され、リストに表示されなくなります。

3. キャンセルする招待の横にあるラジオボタン

   を選択してから、[Cancel invitation] (招待をキャンセルする) を選択します。ラジオボタンが灰色で表示されている場合、その招待はキャンセルできません。

   招待のステータスが [OPEN] (オープン) から [CANCELED] (キャンセル済み) に変更されます。

   AWS は、招待をキャンセルしたことを示す E メールメッセージをアカウント所有者に送信します。新しく招待を送信しない限り、対象アカウントで組織に参加することはできません。

AWS CLI & AWS SDKs

組織から別のアカウントへ送信される招待を表示またはキャンセルするには

招待を表示またはキャンセルするには、次のコマンドを使用します。

- AWS CLI: list-handshakes-for-organization、cancel-handshake
- 以下は、組織から他のアカウントに送信された招待の例です。

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Action": "INVITE",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1482952459.257,
            "Id": "h-examplehandshakeid111",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
```

```
                {
                    "Id": "juan@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1481656459.257,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type": "MASTER_EMAIL",
                            "Value": "bill@amazon.com"
                        },
                        {
                            "Type": "MASTER_NAME",
                            "Value": "Management Account"
                        },
                        {
                            "Type": "ORGANIZATION_FEATURE_SET",
                            "Value": "FULL"
                        }
                    ],
                    "Type": "ORGANIZATION",
                    "Value": "o-exampleorgid"
                },
                {
                    "Type": "EMAIL",
                    "Value": "juan@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Juan's account to join
 Bill's organization."
                }
            ],
            "State": "OPEN"
        },
        {
            "Action": "INVITE",
            "State":"ACCEPTED",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1.471797437427E9,
            "Id": "h-examplehandshakeid222",
```

```
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "anika@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1.469205437427E9,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type":"MASTER_EMAIL",
                             "Value":"bill@example.com"
                        },
                        {
                            "Type":"MASTER_NAME",
                            "Value":"Management Account"
                        }
                    ],
                    "Type":"ORGANIZATION",
                    "Value":"o-exampleorgid"
                },
                {
                    "Type":"EMAIL",
                    "Value":"anika@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Anika's account to join
 Bill's organization."
                }
            ]
        }
    ]
}
```

次の例は、アカウントへの招待をキャンセルする方法を示しています。

```
$ aws organizations cancel-handshake --handshake-id h-examplehandshakeid111
```

```
{
    "Handshake": {
        "Id": "h-examplehandshakeid111",
        "State":"CANCELED",
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "susan@example.com",
                "Type": "EMAIL"
            }
        ],
        "Resources": [
            {
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid",
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@example.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                        "Value": "CONSOLIDATED_BILLING"
                    }
                ]
            },
            {
                "Type": "EMAIL",
                "Value": "anika@example.com"
            },
            {
                "Type": "NOTES",
                "Value": "This is a request for Susan's account to join Bob's
 organization."
```

```
            }
        ],
        "RequestedTimestamp": 1.47008383521E9,
        "ExpirationTimestamp": 1.47137983521E9
    }
}
```

- AWS SDKs: ListHandshakesForOrganization、CancelHandshake

によるアカウント招待の承諾または拒否 AWS Organizations

組織への参加するための招待を受け取った場合は、招待を承諾または拒否できます。

考慮事項

組織に対するアカウントのステータスは、表示できるコストと使用状況のデータに影響する

メンバーアカウントが組織を離れてスタンドアロンアカウントになると、そのアカウントは組織のメンバーであったときのコストと使用状況のデータにアクセスできなくなります。アカウントがアクセスできるのは、スタンドアロンアカウントとして生成されたデータのみです。

メンバーアカウントが組織 A を離れ組織 B に参加すると、そのアカウントは組織 A のメンバーであったときのコストと使用状況のデータにアクセスできなくなります。アカウントがアクセスできるのは、組織 B のメンバーとして生成されたデータのみです。

アカウントが以前に属していた組織に再参加すると、そのアカウントはコストと使用状況データの履歴へのアクセスを再び許可されます。

メンバーアカウントおよびスタンドアロンアカウントのみが、招待を承諾または拒否することが可能

メンバーアカウントおよびスタンドアロンアカウントのみが、組織への招待を承諾または拒否することができます。メンバーアカウントに招待が送信されたら、そのアカウントは現在の組織を離れてから招待を承諾する必要があります。既に組織の一部である管理アカウントに招待が送信された場合、そのアカウントは組織からすべてのメンバーアカウントを削除して組織を削除するまで招待を表示できません。

アカウントの招待を承諾または拒否する

招待を承諾または拒否するには、次の手順を実行します。

最小アクセス許可

組織への招待を承認または拒否するには、次のアクセス権限が必要です。

- `organizations:ListHandshakesForAccount` – AWS Organizations コンソールで招待のリストを表示するために必要です。
- `organizations:AcceptHandshake`.
- `organizations:DeclineHandshake`.
- `iam:CreateServiceLinkedRole` – 招待を承諾する際に、他の AWS のサービスとの統合をサポートするためにサービスにリンクされたロールをアカウント内に作成する必要がある場合にのみ必須です。詳細については、「AWS Organizations およびサービスにリンクされたロール」を参照してください。

AWS Management Console

招待を承諾または辞退するには

1. 組織への招待は、アカウント所有者の Eメールアドレスに送信されます。アカウント所有者が招待メールを受け取ったら、そのメール内の手順に従うか、ブラウザで AWS Organizations コンソールに移動し、[Invitations] (招待) を選択します。または、[member account's Invitation] (メンバーアカウントの招待) ページに直接移動することもできます。
2. プロンプトが表示されたら、招待されたアカウントに 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、アカウントのルートユーザー (推奨されません) としてサインインします。
3. メンバーアカウントの招待ページには、保留中の組織への招待が表示されます。

   必要に応じて [Accept invitation] (招待を承諾) または [Decline invitation] (招待を辞退) を選択します。

   - 前のステップで [Accept invitation] (招待を承諾) を選択した場合、コンソールは自動的に組織の概要ページにリダイレクトされます。このページで、メンバーアカウントになることを承諾した組織についての詳細を確認できます。組織の ID および所有者の Eメールアドレスが表示されます。

> **Note**
>
> 承諾済みの招待は、30 日間リストに表示され続けます。その後は削除されリストに表示されなくなります。

AWS Organizations は、 AWS Organizations と他の の統合をサポートするために、新しいメンバーアカウントにサービスにリンクされたロールを自動的に作成します AWS のサービス。詳細については、「AWS Organizations およびサービスにリンクされたロール」を参照してください。

AWS は、招待を承諾したことを示す E メールメッセージを組織の管理アカウントの所有者に送信します。また、メンバーアカウントの所有者に、組織のメンバーになったことがメールで通知されます。

- 前述のステップで辞退を選択した場合、アカウントは、その他の保留中の招待が表示されているメンバーアカウントの招待ページにそのまま表示され続けます。

  AWS は、招待を拒否したことを示す E メールメッセージを組織の管理アカウントの所有者に送信します。

> **Note**
>
> 拒否された招待は、30 日間リストに表示され続けます。その後は削除されリストに表示されなくなります。

AWS CLI & AWS SDKs

招待を承諾または辞退するには

招待を承諾または拒否するには、次のコマンドを使用します。

- AWS CLI: accept-handshake、decline-handshake

  次の例は、組織への招待を承諾する方法を示しています。

```
$ aws organizations accept-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
```

```
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "RequestedTimestamp": 1481656459.257,
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "juan@example.com",
                "Type": "EMAIL"
            }
        ],
        "Resources": [
            {
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "ALL"
                    }
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "ACCEPTED"
    }
}
```

次の例は、組織への招待を辞退する方法を示しています。

- AWS SDKs: AcceptHandshake、DeclineHandshake

を使用してアカウントを別の組織に移行する AWS Organizations

は、ある組織 AWS アカウント から別の組織にいつでも移行できます。例えば、複数の組織 AWS アカウント から 1 つ以上の組織を 1 つの組織に統合する必要がある場合に、合併と買収の場合には、アカウントを移行すると便利です。

ユースケースに関係なく、組織間でアカウントを移行するには、古い組織からアカウントを削除し、アカウントをスタンドアロンアカウントとし、アカウントが新しい組織からの招待を受け入れて新しい組織に参加する必要があります。ワークロードとサービスは、移行中もお客様の仕様に従って動作し続けます。ただし、組織内の依存関係に注意することが重要です。

> **Note**
>
> 閉鎖または停止されたアカウントは移行できません
> 閉鎖または停止されたアカウントは移行できません。アカウントをリアクティブにするには、サポートにお問い合わせください。
> 7 日間の待機要件
> 組織内に作成したアカウントを移行するには、アカウントが作成されてから 7 日以上が経過している必要があります。招待されたアカウントの場合には、7 日間待つ必要はありません。
> アカウント間のデータのレプリケート
> 次の AWS 規範ガイダンスでは、 AWS アカウントリソースレプリケーションまたは移行の AWS アカウント 間でデータをレプリケートするための戦略について説明します。

アカウントを移行する前にする必要があること

をある組織 AWS アカウント から別の組織に移行する前に、次のステップを完了していることを確認してください。

ステップ 1: アカウントを移行するために必要な IAM アクセス許可があることを確認する

ステップ 1

アカウントをそれぞれの組織に移行するために必要なアクセス許可が適用されていることを確認してください。

組織を登録解除する場合は、次のアクセス権限が必要です:

- `organizations:DescribeOrganization` (コンソールのみ)
- `organizations:LeaveOrganization`

詳細については、「メンバーアカウントから組織を退会する」を参照してください。

AWS アカウント を組織に招待するには、次のアクセス許可が必要です。

- `organizations:DescribeOrganization` (コンソールのみ)
- `organizations:InviteAccountToOrganization`

詳細については、「 AWS アカウント を組織に招待する」を参照してください。

アカウントを移行するには、移行を妨げる IAM ポリシーまたはサービスコントロールポリシーを持つことはできません

管理アカウントまたは委任管理者である場合は、組織内の IAM ID (ユーザー、グループ、ロール) にアクセス許可ポリシーをアタッチすることで、 AWS リソースへのアクセスを制御できます。詳細については、「IAM policies for AWS Organizations」を参照してください。

アカウントを移行する前に。

- アカウントの移行を妨げる IAM ポリシーまたはサービスコントロールポリシー (SCP) がないことを確認します。
- アカウントを移行する組織でレプリケートする必要がある既存の IAM ポリシーとサービスコントロールポリシー (SCP) を特定します。
- 組織 ID を指定する既存の IAM ポリシーを特定します。例えば、`aws:PrincipalOrgID`。

詳細については、「IAM ユーザーガイド」の「IAM ポリシーを管理する」および「サービスコントロールポリシー (SCP)」を参照してください。

ステップ 2: 古い管理アカウントへのアクセスを有効にする IAM アクセス許可が削除されていることを確認します。

ステップ 2

`OrganizationAccountAccessRole` などの古い管理アカウントへのアクセスを有効にする IAM アクセス許可が削除されていることを確認します。

メンバーアカウントを組織から削除しても、組織の管理アカウントによるアクセスを有効にするために作成された IAM ロールは自動的に削除されません。以前の組織の管理アカウントからアクセスされないようにするには、その IAM ロールを手動で削除する必要があります。

ロールを削除する方法について詳しくは、IAM ユーザーガイドのロールまたはインスタンスプロファイルの削除を参照してください。

ステップ 3: 電話の検証と支払い方法を確認する

ステップ 3

移行アカウントは、新しい組織に移行する前に、一定期間スタンドアロンアカウントとして機能する必要があります。

アカウントをスタンドアロンアカウントとして機能させるには、以下を確認してください。

- 電話の検証が最新であることを確認します。
- アカウントの移行中に発生した料金に対処するために、アカウントに有効な支払い方法が追加されていることを確認してください。
- 支払い方法に請求を使用する場合は、請求書が最新であることを確認します。

ステップ 4: すべてのレポートをバックアップする

ステップ 4

管理アカウント、特に請求レポートからレポートをエクスポートまたはバックアップしてください。組織レベルのレポートと履歴は、アカウントを移行するときに保存されません。すべての請求履歴を完全にエクスポートすることをお勧めします。 AWS CloudTrail イベント履歴やアカウント請求履歴など、メンバーアカウントのレポートには引き続きアクセスできます。

> **Important**
>
> 管理アカウントの組織請求情報など、すべての組織レベルのレポートと履歴は、アカウントが組織から削除された後に削除されます。

詳細については、「Cost and Usage Reports」、「Cost Explorer Reports」、「Savings Plans Reports」、「Reserved Instance (RI) utilization and coverage」を参照してください。

ステップ 5: 組織の依存関係を確認する

ステップ 5

移行するアカウントに組織関連の依存関係がないことを確認します。

確認する依存関係:

- アカウントが委任された管理者である場合は、アカウントを移行する前に委任された管理者のアクセス許可の登録を解除する必要があります。詳細については、「 で使用できるサービス AWS Organizations」を参照してください。
- アカウントが管理アカウントである場合は、移行する前に組織からすべてのメンバーアカウントを削除し、組織を削除する必要があります。組織を削除すると、管理アカウントはスタンドアロンアカウントとして機能します。移行後、管理アカウントは新しい組織のメンバーアカウントになります。詳細については、「Deleting an organization」を参照してください。
- IAM アクセス許可がアカウントに依存する場合は、古い組織が以前と同じように機能するために、アカウントを新しい組織に移行した後に、古い組織のアクセス許可を調整する必要があります。詳細については、「Managing access permissions for your organization」を参照してください。
- アカウントまたは組織単位 (OU) タグを使用している場合は、新しい組織でタグを再作成する必要があります。

(オプション) ステップ 6: を使用する場合はガイダンスを確認する AWS Control Tower

(オプション) ステップ 6

によって管理されている組織との間でアカウントを移行する場合は AWS Control Tower、次の AWS 規範ガイダンスを参照してください。AWS メンバーアカウントを から に移行 AWS Organizations します AWS Control Tower。

アカウントの移行に必要なこと

移行プロセスでは、新しい組織が移行アカウントへの招待を送信し、古い組織が移行アカウントを削除し、移行アカウントが新しい組織からの招待を受け入れて新しい組織に参加する必要があります。

アカウントを移行するには

1. 新しい組織の管理アカウントから移行アカウントに招待を送信します。アカウントが古い組織を離れる前に、招待をそのアカウントに送信する必要があります。これにより、移行アカウントがスタンドアロンアカウントとして一時的に動作するときに発生するコストを最小限に抑えることができます。アカウントを招待する方法については、「 AWS アカウント を組織に招待する」を参照してください。
2. 古い組織から移行アカウントを削除します。管理アカウントを使用して組織からメンバーアカウントを削除するか、メンバーアカウントとして組織を離れることができます。
3. 新しい組織に参加するための招待を受け入れます。詳細については、「Accepting an invitation from an organization」を参照してください。ある組織から別の組織に移行するアカウントは、新しい組織のルートに自動的に追加されます。新しい組織の組織単位 (OU) にアカウントを移動する前に、移行するアカウントに適切な組織ポリシーと OU アクセス許可があることを確認することをお勧めします。
4. 管理アカウントを移行する場合は、管理アカウントを新しい組織に移行する前に、組織からすべてのメンバーアカウントを削除し、組織を削除する必要があります。古い組織を削除すると、管理アカウントはスタンドアロンアカウントとして機能し、新しい組織からの招待を受け入れて新しい組織に参加できます。招待を受け入れると、管理アカウントは新しい組織のメンバーアカウントになります。

アカウントの移行後に実行する必要があること

アカウントをある組織から別の組織に移行したら、次のステップを完了していることを確認してください。

移行後レビュー

1. コストカテゴリ、予算、請求アラームなど、移行されたアカウントのすべての請求ツール設定を評価します。
2. ある組織から別の組織に移行したアカウントについて、次の金額情報を確認して更新します。
   a. 必要に応じて、アカウントの税金設定を更新します。
   b. アカウントの移行 サポート 計画が、新しい組織の支払者アカウントと一致していることを確認してください。
   c. 移行したアカウントに適用する可能性のある免税を確認します。
3. 移行されたアカウントの既存の IAM ポリシーとサービスコントロールポリシー (SCP) を検証して確認します。例えば、一部の IAM ポリシーの組織 ID を更新して、新しい組織を反映する必要がある場合があります。
4. アカウントを移行した新しい組織のコスト配分タグを更新します。移行したアカウントによって収集された以前のすべてのコスト配分タグを更新する必要があります。
5. リザーブドインスタンスと Savings Plans は、アカウントとともに移行されます。これらは古い組織には保持されません。 サポート これらを古い組織に転送する必要がある場合は、 にお問い合わせください。

でアカウントの詳細を表示する AWS Organizations

AWS Organizations コンソールで組織の管理アカウントにサインインすると、メンバーアカウントの詳細を表示できます。

> **最小アクセス許可**
>
> の詳細を表示するには AWS アカウント、次のアクセス許可が必要です。
>
> - `organizations:DescribeAccount`
> - `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要
> - `organizations:ListAccounts` - Organizations コンソールを使用する場合にのみ必要

AWS Management Console

の詳細を表示するには AWS アカウント

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の 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 (非推奨) としてサインインする必要があります。
2. AWS アカウント ページに移動し、調べたいアカウントの名前 (ラジオボタンではなく) を選択します。目的のアカウントが子 OU である場合は、親 OU の横の三角形のアイコン

   を選択して展開し、子 OU を表示します。アカウントが見つかるまで繰り返します。

   [Account details] (アカウントの詳細) ボックスに、アカウントに関する情報が表示されます。

AWS CLI & AWS SDKs

の詳細を表示するには AWS アカウント

次のいずれかのコマンドを使用して、アカウントの詳細を表示できます。

- AWS CLI:
  - list-accounts - 組織のすべてのアカウントの詳細を一覧表示します。
  - describe-account - 指定したアカウントの詳細のみを一覧表示します。

どちらのコマンドでも、レスポンスに含まれる詳細情報は同じです。

次の例は、指定したアカウントの詳細を取得する方法を示しています。

```
$ aws organizations describe-account --account-id 123456789012

{
    "Account": {
        "Id": "123456789012",
        "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "Email": "admin@example.com",
        "Name": "Example.com Organization's Management Account",
        "Status": "ACTIVE",
        "JoinedMethod": "INVITED",
```

```
        "JoinedTimestamp": "2020-11-20T09:04:20.346000-08:00"
    }
}
```

- AWS SDKs:
  - ListAccounts
  - DescribeAccount

内のすべてのアカウントの詳細をエクスポートする AWS Organizations

を使用すると AWS Organizations、組織の管理アカウントユーザーと委任管理者は、組織内のすべてのアカウント詳細を含む .csv ファイルをエクスポートできます。その結果、組織管理者は、アカウントを簡単に表示し、ステータス (ACTIVE、SUSPENDED、または PENDING) でフィルターできます。組織に多数のアカウントがある場合、.csv ファイルのダウンロードオプションを使用すると、スプレッドシートのアカウントの詳細の表示と並べ替えを容易に行うことができます。

> **Note**
>
> アカウントリストをダウンロードできるのは、管理アカウントのプリンシパルのみです。

組織のすべての AWS アカウント のリストをエクスポートする

組織の管理アカウントにサインインすると、組織に属するすべてのアカウントのリストを .csv ファイルとして取得できます。リストには個々のアカウントの詳細が含まれますが、アカウントが属する組織単位 (OU) は示されません。

.csv ファイルには、各アカウントの次の情報が含まれています。

- アカウント ID - 数値のアカウント識別子。例: 123456789012。
- ARN - アカウントの Amazon リソースネーム。例: `arn:aws:organizations::123456789012account/o-o1gb0d1234/123456789012`
- Email - アカウントに関連付けられている E メールアドレス。例: marymajor@example.com。
- 名前 - アカウント作成者によって提供されたアカウント名。例: stage testing account。
- ステータス - 組織内のアカウントのステータス。値は、PENDING、ACTIVE、または SUSPENDED です。

- 参加方法 - アカウントがどのように作成されたかを示します。値は `INVITED` または `CREATED` です。
- 参加タイムスタンプ - アカウントが組織に参加した日付と時刻。

> **最小アクセス許可**
>
> 組織内のすべてのメンバーアカウントを含む .csv ファイルをエクスポートするには、以下のアクセス許可が必要です。
>
> - `organizations:DescribeOrganization`
> - `organizations:ListAccounts`

AWS Management Console

組織 AWS アカウント 内のすべての の .csv ファイルをエクスポートするには

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 (非推奨) としてサインインする必要があります。
2. [アクション] を選択し、[AWS アカウント] で [アカウントリストをエクスポート] を選択します。ページ上部の青いバナーは、エクスポートが進行中であることを示します。
3. ファイルの準備ができたら、バナーが緑色に変わり、ダウンロードの準備ができたことを示します。[CSV のダウンロード] を選択します。ファイル `Organization_accounts_information.csv` がデバイスにダウンロードされます。

AWS CLI & AWS SDKs

アカウントの詳細を含む .csv ファイルをエクスポートする唯一の方法は、 AWS Management Consoleを使用することです。 AWS CLIを使用してアカウントリストの .csv ファイルをエクスポートすることはできません。

でアカウントの代替連絡先を更新する AWS Organizations

Organizations コンソールを使用して AWS 、または CLI または AWS SDKs AWS を使用してプログラムで、組織内のアカウントの代替連絡先を更新できます。代替連絡先を更新する方法については、

「 AWS アカウント管理リファレンス」の「組織 AWS アカウント 内の任意の の代替連絡先を更新する」を参照してください。

でアカウントのプライマリ連絡先情報を更新する AWS Organizations

Organizations コンソールを使用して AWS 、または CLI または AWS SDKs AWS を使用してプログラムで、組織内のアカウントの主要な連絡先情報を更新できます。主な連絡先情報を更新する方法については、「 AWS アカウント管理リファレンス」の「組織 AWS アカウント 内の任意の のプライマリ連絡先を更新する」を参照してください。

での アカウントの の更新 AWS リージョンAWS Organizations

AWS Organizations コンソールを使用して、組織内のアカウント AWS リージョン で有効になっている を更新できます。有効に更新する方法については AWS リージョン、「 アカウント AWS 管理リファレンス」の「 アカウント AWS リージョン で有効または無効にする」を参照してください。

を使用した組織単位 (OUsの管理 AWS Organizations

組織単位 (OU) を使用すると、アカウントをまとめてグループ化し、単一の単位として管理できます。その結果、アカウントの管理は大幅に簡略化されます。たとえば、ポリシーベースの制御を OU に付与すると、OU 内のすべてのアカウントに自動的に OU ポリシーが継承されます。OU は、1 つの組織に複数作成することができるため、その他の OU 内にも OU を作成することができます。各 OU には、複数のアカウントを含めることができるだけでなく、OU から別の OU へアカウントを移動することもできます。ただし、OU の名前は、親 OU またはルート内で一意である必要があります。

次の図は、基本的な組織を示しています。この組織は、7 つのアカウントで構成されており、そのアカウントは、ルートを親として、4 つの OU に分類されています。組織には、OU に適用されるポリシーも一部存在します。

> **Note**
>
> 組織には 1 つのルートがあり、組織を初めてセットアップするときに AWS Organizations によって作成されます。

トピック

- で組織単位 (OUsを管理するためのベストプラクティス AWS Organizations
- を使用したルートおよび組織単位 (OU) 階層のナビゲーション AWS Organizations
- を使用した組織単位 (OU) の詳細の表示 AWS Organizations
- を使用した組織単位 (OU) の作成 AWS Organizations
- を使用した組織単位 (OU) の名前変更 AWS Organizations
- を使用した組織単位 (OU) のタグ付け AWS Organizations
- を使用して組織単位 (OU) またはルートと OUsする AWS Organizations
- を使用したルートの詳細の表示 AWS Organizations
- を使用した組織単位 (OU) の削除 AWS Organizations

で組織単位 (OUsを管理するためのベストプラクティス AWS Organizations

組織単位 (OUs) AWS Organizations を使用して でマルチアカウント環境を管理する手順については、以下の推奨事項に従ってください。

トピック

- について AWS Organizations
- 推奨される基本組織単位 (OU)
- 推奨される追加の組織単位 (OU)
- 結論

について AWS Organizations

適切に設計されたマルチアカウント AWS 環境の基礎は です。これにより AWS Organizations、複数のアカウントを一元管理できます。組織単位 (OU) は、組織内のアカウントの論理的なグループ化です。OU を使用すると、アカウントを階層に整理し、管理コントロールを適用できます。Organizations ポリシーは、グループに適用できるコントロールを定義します AWS アカウント。例えば、サービスコントロールポリシー (SCP) は、組織内のアカウントが実行できる Amazon EC2 Run Instance などの AWS のサービス アクションを定義するポリシーです。

1 つのアカウントで AWS ジャーニーを開始する場合もありますが、 AWS では、ワークロードのサイズと複雑さが増すにつれて、複数のアカウントを設定することをお勧めします。マルチアカウント環境を使用することは、いくつかの利点をもたらす AWS ベストプラクティスです。

- さまざまな要件による迅速なイノベーション: 社内のさまざまなチーム、プロジェクト、製品 AWS アカウント に を割り当てて、それぞれのセキュリティ要件を考慮しながら、迅速にイノベーションを行うことができます。
- 請求の簡素化: 複数の を使用すると AWS アカウント 、どの製品やサービスのラインが AWS 料金の原因となっているかを特定できるため、 AWS コストの割り当て方法を簡素化できます。
- 柔軟なセキュリティコントロール: 複数の を使用して AWS アカウント 、特定のセキュリティ要件を持つワークロードやアプリケーションを分離したり、HIPAA や PCI などのコンプライアンスに関する厳格なガイドラインを満たす必要がある場合に使用できます。
- ビジネスプロセスへの適応: 運用 AWS アカウント 、規制、予算の要件が異なる会社のビジネスプロセスの多様なニーズを最もよく反映した方法で複数の を整理できます。

推奨される基本組織単位 (OU)

組織単位 (OU) は、会社のレポート構造をミラーリングするのではなく、関数または一般的な一連のコントロールに基づいている必要があります。 AWS では、セキュリティとインフラストラクチャを念頭に置いて開始することをお勧めします。ほとんどのビジネスには、これらのニーズに応じて組織全体に対応する一元化されたチームがあります。これらの特定の機能のために、一連の基礎的な OU を作成することをお勧めします。

- セキュリティ: セキュリティサービスに使用されます。ログアーカイブ、セキュリティ読み取り専用アクセス、セキュリティツール、ブレークグラスのアカウントを作成します。
- インフラストラクチャ: ネットワークや IT サービスなどの共有インフラストラクチャサービスに使用されます。必要なインフラストラクチャサービスのタイプごとにアカウントを作成します。

ほとんどの企業では、本番稼働ワークロードのポリシー要件が異なるため、インフラストラクチャとセキュリティには、非本番稼働 (SDLC) と本番稼働 (Prod) 用のネストされた OU がある可能性があります。SDLC OU のアカウントは非本番ワークロードをホストし、他のアカウントからの本番依存関係があってはなりません。ライフサイクルステージ間で OU ポリシーにばらつきがある場合、SDLC は複数の OU (開発や事前生産など) に分割できます。Prod OU のアカウントは、本番ワークロードをホストします。

OU レベルでポリシーを適用して、要件に従って Prod 環境と SDLC 環境を管理します。一般に、ポリシー管理と潜在的なトラブルシューティングを簡素化するため、OU レベルでポリシーを適用する方が、個々のアカウントレベルよりも実践的です。

次の図は、セキュリティとインフラストラクチャの基本的な OU (Prod と SDLC) を示しています。

推奨される追加の組織単位 (OU)

中央サービスが導入されたら、製品やサービスの構築または実行に直接関連する OU を作成することをお勧めします。多くの AWS お客様は、基盤を確立した後に次の OUsを構築します。

- サンドボックス: 個々のデベロッパー AWS アカウント が実験に使用できるものを保持します AWS のサービス。これらのアカウントを内部ネットワークからデタッチできることを確認します。
- ワークロード: 外部向けアプリケーションサービスをホスト AWS アカウント する が含まれています。本番環境ワークロードを分離して厳密に制御するには、SDLC および Prod 環境 (基盤 OU に似ています) の下に OU を構成する必要があります。

また、特定のニーズに応じて、メンテナンスと継続的な拡張のために OU を追加することをお勧めします。以下は、既存の AWS お客様のプラクティスに基づく一般的なテーマです。

- ポリシーステージング: 提案されたポリシーの変更を組織全体に適用する前にテストできる AWS アカウントを保持します。まず、目的の OU のアカウントレベルで変更を実装し、他のアカウント、OU、および組織全体で徐々に作業します。
- 停止: 閉じ AWS アカウント られ、組織から削除されるのを待っている が含まれます。すべてのアクションを拒否する SCP をこの OU にアタッチします。アカウントを復元する必要がある場合は、トレーサビリティの詳細がタグ付けされていることを確認してください。
- 個々のビジネスユーザー: レポートやファイルをパートナーと共有するために S3 バケットを設定するなど、ビジネス生産性関連のアプリケーションを作成する必要があるビジネスユーザー (デベロッパーではない) AWS アカウント 向けの を含む制限付きアクセス OU。
- 例外: ワークロード OU で定義されているものとは異なる、高度にカスタマイズされたセキュリティ要件または監査要件を持つビジネスユースケース AWS アカウント に使用されるホールド。例えば、機密性の高い新しいアプリケーションや機能用に AWS アカウント を特別にセットアップします。カスタマイズされたニーズを満たすために、アカウントレベルで SCP を使用します。Amazon EventBridge と AWS Config ルールを使用して、Detect and React システムを設定することを検討してください。
- デプロイ: 継続的インテグレーションと継続的デリバリー/デプロイ (CI/CD デプロイ) AWS アカウント を目的とした が含まれています。この OU は、ワークロード OU (Prod および SDLC) のアカウントとは異なる CI/CD デプロイのガバナンスモデルと運用モデルがある場合に作成できます。CI/CD の配布は、中央チームが運用する共有 CI/CD 環境への組織的な依存を減らすのに役立ちます。ワークロード OU 内の AWS アカウント アプリケーションの SDLC/Prod のセットごとに、デプロイ OU の下に CI/CD のアカウントを作成します。
- 移行: これは、既存のアカウントとワークロードを組織の標準エリアに移動する前の、一時的な保持エリアとして使用されます。これは、アカウントが取得の一部であり、以前はサードパーティーによって管理されていたか、古い組織構造のレガシーアカウントが原因である可能性があります。

次の図は、サンドボックス、ワークロード、ポリシーステージング、一時停止、個々のビジネスユーザー、例外、デプロイ、移行アカウントの追加の OU を示しています。

結論

優れた設計のマルチアカウント戦略は、セキュリティとスケーラビリティのニーズを満たすと同時に AWS、 のイノベーションに役立ちます。このトピックで説明するフレームワークは、 AWS ジャーニーの開始点として使用する必要がある AWS ベストプラクティスを示しています。

次の図は、推奨される基本 OU と追加の OU を示しています。

を使用したルートおよび組織単位 (OU) 階層のナビゲーション AWS Organizations

アカウントの移動またはポリシーのアタッチの際に、別の OU またはルートに移動するには、デフォルトの「ツリー」ビューを使用します。

AWS Management Console

「ツリー」ビューで組織内を移動するには

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. AWS アカウントページの [Organization] (組織) セクションの上部で [List] (リスト) ではなく、[Hierarchy] (階層) を選択します。
3. 初期状態のツリーにはルートと、階層の最初の子 OU および アカウントのみが表示されます。ツリーを展開してより深い階層を表示するには、親エンティティの横にある展開アイコン ( ) を選択します。表示をシンプルにするためにツリーのブランチを折りたたむには、展開された親エンティティの横にある折りたたみアイコン ( ) を選択します。
4. 詳細の確認や、特定の操作を行うには、OU またはルートの名前を選択します。または、名前の横にあるラジオボタンを選択し、[Actions] (アクション) メニューからエンティティに対する特定の操作を行うこともできます。

組織内のアカウントのみの一覧を表形式ビューで表示することもでき、特定のアカウントを見つけるために逐一 OU に移動する必要はありません。このビューでは、OU の表示や、OU にアタッチされたポリシーの操作はできません。

AWS Management Console

アカウントのフラットリストとして階層なしで組織を表示するには

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. AWS アカウント ページの組織セクションの上部で、表示 AWS アカウント のみの切り替えアイコンを選択してオンにします。
3. アカウントの一覧が階層なしで表示されます。

を使用した組織単位 (OU) の詳細の表示 AWS Organizations

AWS Organizations コンソールで組織の管理アカウントにサインインすると、組織の OU の詳細を表示できます。

最小アクセス許可

組織単位 (OU) の詳細を表示するには、次のアクセス権限が必要です。

- `organizations:DescribeOrganizationalUnit`
- `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要
- `organizations:ListOrganizationsUnitsForParent` - Organizations コンソールを使用する場合にのみ必要
- `organizations:ListRoots` - Organizations コンソールを使用する場合にのみ必要

AWS Management Console

OU の詳細を表示するには

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. AWS アカウント ページで、調べたい OU の名前 (ラジオボタンではなく) を選択します。目的の OU が別の OU の子 OU である場合は、親 OU の横にある三角形のアイコンを選択して展開すると、次の階層に子 OU が表示されます。目的の OU が表示されるまで繰り返します。

   [Organizational unit details] (組織単位の詳細) ボックスに、OU に関する情報が表示されます。

AWS CLI & AWS SDKs

OU の詳細を表示するには

次のいずれかのコマンドを使用して、OU の詳細を表示できます。

- AWS CLI、 AWS SDKs:
  - list-roots
  - list-children
  - describe-organizational-unit

  次の例は、 AWS CLIを使用して OU の ID を見つける方法を示しています。OU ID を見つけるには、階層をトラバースします。はじめに `list-roots` コマンドを実行します。次に、`list-children` をまずルートで実行し、その後は子 OU で、目的の OU ID が見つかるまで繰り返し実行します。

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": []
```

```
        }
    ]
}
$ aws organizations list-children --parent-id r-a1b2 --child-type
 ORGANIZATIONAL_UNIT
{
    "Children": [
        {
            "Id": "ou-a1b2-f6g7h111",
            "Type": "ORGANIZATIONAL_UNIT"
        }
    ]
}
```

次の例は、OU の ID を見つけた後に、OU の詳細を取得する方法を示しています。

```
$ aws organizations describe-organizational-unit --organizational-unit-id ou-a1b2-
f6g7h111
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h111",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
        "Name": "Production-Apps"
    }
}
```

- AWS SDKs:
  - ListRoots
  - ListChildren
  - DescribeOrganizationalUnit

を使用した組織単位 (OU) の作成 AWS Organizations

組織の管理アカウントにサインインすると、組織のルートに OU を作成できます。OU は、最大 5 レベルの深さまでネストできます。OU を作成するには、次のステップを完了します。

> **Important**
>
> この組織が で管理されている場合は AWS Control Tower、 AWS Control Tower コンソールまたは APIs を使用して OUs を作成します。Organizations で OU を作成すると、その OU は に登録されません AWS Control Tower。詳細については、AWS Control Tower ユーザーガイドの AWS Control Tower外のリソースを参照するを参照してください。

> **最小アクセス許可**
>
> 組織のルート内に OU を作成するには、次のアクセス権限が必要です。
>
> - `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要
> - `organizations:CreateOrganizationalUnit`

AWS Management Console

OU を作成するには

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. AWS アカウント ページに移動します。

   ルート OU とその内容がコンソールに表示されます。初めてルートにアクセスするときは、コンソールの最上位のビューにすべての AWS アカウント が表示されます。以前に OU を作成してその OU にアカウントを移動している場合、コンソールには最上位の OU と、OU に移動していないアカウントのみ表示されます。
3. (オプション) 既存の OU 内に OU を作成する場合は、子 OU に移動します。移動するには、子 OU の名前 (チェックボックスではなく) を選択するか、ツリービューで OU の横の

   を選択して目的の OU が表示されるまで展開し、目的の子 OU の名前を選択します。
4. 階層内の正しい親 OU を選択したら、[Actions] (アクション) メニューの [Organizational Unit] (組織単位) で [Create new] (新規作成) を選択します。

5. [Create organizational unit] (組織単位の作成) ダイアログボックスで、作成する OU の名前を入力します。
6. (オプション) [Add tag] (タグの追加) を選択してキーとオプションの値を入力し、1 つ以上のタグを追加します。値を空白のままにすると、空の文字列が設定され、null にはなりません。1 つの OU に最大 50 個のタグをアタッチできます。
7. 最後に、[Create organizational unit] (組織単位の作成) を選択します。

親 OU 内に新しい OU が作成されます。これで、この OU にアカウントを移動する、またはポリシーをアタッチすることができるようになりました。

AWS CLI & AWS SDKs

OU を作成するには

以下のコード例は、`CreateOrganizationalUnit` の使用方法を示しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new organizational unit in AWS Organizations.
/// </summary>
public class CreateOrganizationalUnit
{
    /// <summary>
    /// Initializes an Organizations client object and then uses it to call
    /// the CreateOrganizationalUnit method. If the call succeeds, it
    /// displays information about the new organizational unit.
```

```
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var orgUnitName = "ProductDevelopmentUnit";

            var request = new CreateOrganizationalUnitRequest
            {
                Name = orgUnitName,
                ParentId = "r-0000",
            };

            var response = await client.CreateOrganizationalUnitAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully created organizational unit:
{orgUnitName}.");
                Console.WriteLine($"Organizational unit {orgUnitName} Details");
                Console.WriteLine($"ARN: {response.OrganizationalUnit.Arn} Id:
{response.OrganizationalUnit.Id}");
            }
            else
            {
                Console.WriteLine("Could not create new organizational unit.");
            }
        }
    }
```

- API の詳細については、AWS SDK for .NET API リファレンスの「CreateOrganizationalUnit」を参照してください。

CLI

AWS CLI

ルート OU または親 OU に OU を作成するには

次の例は、AccountingOU という名前の OU を作成する方法を示しています。

```
aws organizations create-organizational-unit --parent-id r-examplerootid111 --
name AccountingOU
```

出力には、新しい OU に関する詳細を含む organizationalUnit オブジェクトが含まれます。

```
{
        "OrganizationalUnit": {
                "Id": "ou-examplerootid111-exampleouid111",
                "Arn": "arn:aws:organizations::111111111111:ou/o-exampleorgid/ou-
examplerootid111-exampleouid111",
                "Name": "AccountingOU"
        }
}
```

- API の詳細については、AWS CLI コマンドリファレンスの「CreateOrganizationalUnit」を参照してください。

を使用した組織単位 (OU) の名前変更 AWS Organizations

組織の管理アカウントにサインインすると、OU の名前を変更することができます。そのためには、以下の手順を完了します。

> 最小アクセス許可
>
> 組織のルート内にある OU の名前を変更するには、次のアクセス権限が必要です。
>
> - `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要
> - `organizations:UpdateOrganizationalUnit`

AWS Management Console

OU の名前を変更するには

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. AWS アカウントページで、名前を変更する OU に移動し、次のいずれかのステップを実施します。

   - 名前を変更する OU の横にあるラジオボタン

     を選択します。次に、[Actions] (アクション) メニューの [Organizational Unit] (組織単位) で、[Rename] (名前の変更) を選択します。
   - OU の名前を選択し、OU の詳細ページにアクセスします。ページの上部で、[Rename] (名前の変更) を選択します。

3. [Rename organizational unit] (組織単位名の変更) ダイアログボックスで新しい名前を入力し、[Save changes] (変更の保存) を選択します。

AWS CLI & AWS SDKs

OU の名前を変更するには

OU の名前を変更するには、次のいずれかのコマンドを使用します。

- AWS CLI: update-organizational-unit

  次の例は、OU の名前を変更する方法を示しています。

```
$ aws organizations update-organizational-unit \
    --organizational-unit-id ou-a1b2-f6g7h222 \
    --name "Renamed-OU"
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "Renamed-OU"
    }
}
```

- AWS SDKs: UpdateOrganizationalUnit

を使用した組織単位 (OU) のタグ付け AWS Organizations

組織の管理アカウントにサインインすると、OU にアタッチされるタグを追加または削除できます。そのためには、以下の手順を完了します。

> **最小アクセス許可**
>
> 組織のルート内にある OU にアタッチされたタグを編集するには、次のアクセス許可が必要です。
>
> - `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要
> - `organizations:DescribeOrganizationalUnit` - Organizations コンソールを使用する場合にのみ必要
> - `organizations:TagResource`
> - `organizations:UntagResource`

AWS Management Console

OU にアタッチされたタグを編集するには

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. AWS アカウント ページで、編集する OU に移動して名前を選択します。
3. OU の詳細ページで、[Tags] (タグ) タブを選択し、[Manage tags] (タグ管理) を選択します。
4. このタブでは次のアクションが実行可能です。
   - 古い値に上書きして新しい値を入力し、任意のタグの値を編集します。タグキーは変更できません。キーを変更するには、古いキーを持つタグを削除し、新しいキーを持つタグを追加する必要があります。
   - 削除するタグの横にある [Remove] (削除) を選択し、既存のタグを削除します。
   - 新しいタグのキーと値のペアを追加します。[Add tag] (タグの追加) を選択し、表示されたボックスに新しいキー名とオプションの値を入力します。[Value] (値) ボックスを空白のままにすると、値は空の文字列に設定され、`null` にはなりません。
5. 必要な追加、削除、編集をすべて終えたら、[Save changes] (変更の保存) を選択します。

AWS CLI & AWS SDKs

OU にアタッチされたタグを編集するには

OU にアタッチされたタグを変更するには、次のいずれかのコマンドを使用します。

- AWS CLI: tag-resource および untag-resource

  次の例では、タグ "Department"="12345" を OU にアタッチしています。Key と Value では大文字と小文字が区別されます。

```
$ aws organizations tag-resource \
    --resource-id ou-a1b2-f6g7h222 \
    --tags Key=Department,Value=12345
```

  このコマンドが成功した場合、出力は生成されません。

  次の例では、Department タグを OU から削除しています。

```
$ aws organizations untag-resource \
    --resource-id ou-a1b2-f6g7h222 \
    --tag-keys Department
```

  このコマンドが成功した場合、出力は生成されません。

- AWS SDKs: TagResource と UntagResource

を使用して組織単位 (OU) またはルートと OUsする AWS Organizations

組織の管理アカウントにサインインすると、ルートと OU の間、または OU どうしの間で組織のアカウントを移動させることができます。OU 内にアカウントを配置すると、親 OU、およびその OU からルートまでの間にあるすべての OU にアタッチされているポリシーが適用されます。OU に属していないアカウントには、ルート、およびそのアカウントに直接アタッチされているポリシーのみが適用されます。アカウントを移動させるには、次のステップを実施します。

> **最小アクセス許可**
>
> OU 階層の新しい場所にアカウントを移動させるには、次のアクセス許可が必要です。

- `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要
- `organizations:MoveAccount`

AWS Management Console

アカウントを OU に移動させるには

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. AWS アカウント ページで、移動させるアカウントを見つけます。OU の階層を移動するか、[View AWS アカウント only] (AWS アカウント だけを表示する) を有効にして OU 構造のないフラットリストでアカウントを表示します。アカウントが多い場合、削除対象をすべて見つけるにはリスト下部の [Load more accounts in 'ou-name'] ('ou-name' のアカウントをさらに読み込む) を選択する必要がある場合があります。
3. 移動させるアカウントの名前の横にあるチェックボックス

   を選択します。
4. [Actions] (アクション) メニューの [AWS アカウント] で、[Move] (移動) を選択します。
5. [Move AWS アカウント] (AWS アカウントの移動) ダイアログボックスで、アカウントの移動先の OU またはルートを見つけて選択し、[Move AWS アカウント] (AWS アカウントの移動) を選択します。

AWS CLI & AWS SDKs

アカウントを OU に移動させるには

アカウントを移動するには、次のいずれかのコマンドを使用します。

- AWS CLI: move-account

  次の例では、 をルート AWS アカウント から OU に移動します。ソースコンテナと宛先コンテナの両方の ID を指定する必要があります。

```
$ aws organizations move-account \
```

```
    --account-id 111122223333 \
    --source-parent-id r-a1b2 \
    --destination-parent-id ou-a1b2-f6g7h111
```

このコマンドが成功した場合、出力は生成されません。

- AWS SDKs: MoveAccount

を使用したルートの詳細の表示 AWS Organizations

AWS Organizations コンソールで組織の管理アカウントにサインインすると、管理ルートの詳細を表示できます。

> **最小アクセス許可**
>
> ルートの詳細を表示するには、次のアクセス許可が必要です。
>
> - `organizations:DescribeOrganization` (コンソールのみ)
> - `organizations:ListRoots`

ルートは、組織単位 (OU) の階層の最上位コンテナであり、通常は OU として動作します。ただし、階層の最上部にあるコンテナとして、ルートへの変更は、他のすべての OU と組織 AWS アカウント内のすべての に影響します。

AWS Management Console

ルートの詳細を表示するには

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. AWS アカウント ページに移動し、ルート OU (ラジオボタンではなくその名前) を選択します。
3. ルートの詳細ページが表示され、ルートの詳細を確認できます。

AWS CLI & AWS SDKs

ルートの詳細を表示するには

ルートの詳細を表示するには、次のいずれかのコマンドを使用します。

- AWS CLI: list-roots

  次の例は、組織で現在どのポリシータイプが有効になっているかなど、ルートの詳細情報を取得する方法を示しています。

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": [
                {
                    "Type": "BACKUP_POLICY",
                    "Status": "ENABLED"
                }
            ]
        }
    ]
}
```

- AWS SDKs: ListRoots

を使用した組織単位 (OU) の削除 AWS Organizations

組織の管理アカウントにサインインすると、不要になった OU を削除できます。

子 OU を削除するには、まず OU とその子 OU 内のアカウントをすべて移動させる必要があります。

> **最小アクセス許可**
>
> OU を削除するには、次のアクセス権限が必要です。
>
> - `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要
> - `organizations:DeleteOrganizationalUnit`

AWS Management Console

OU を削除するには

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. AWS アカウント ページで、削除する OU を探し、その OU 名の横にあるチェックボックス

   をオンにします。
3. [Actions] (アクション) を選択し、[Organizational unit] (組織単位) で [Delete] (削除) を選択します。
4. その OU の削除を確定するには、OU の名前 (削除対象が 1 つだけの場合) または「delete」という文字列 (削除対象が複数ある場合) を入力してから、[Delete] (削除) を選択します。

   AWS Organizations は OUsし、リストからそれらを削除します。

AWS CLI & AWS SDKs

OU を削除するには

以下のコード例は、`DeleteOrganizationalUnit` の使用方法を示しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;
```

```
    /// <summary>
    /// Shows how to delete an existing AWS Organizations organizational unit.
    /// </summary>
    public class DeleteOrganizationalUnit
    {
        /// <summary>
        /// Initializes the Organizations client object and calls
        /// DeleteOrganizationalUnitAsync to delete the organizational unit
        /// with the selected ID.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var orgUnitId = "ou-0000-00000000";

            var request = new DeleteOrganizationalUnitRequest
            {
                OrganizationalUnitId = orgUnitId,
            };

            var response = await client.DeleteOrganizationalUnitAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully deleted the organizational unit
with ID: {orgUnitId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete the organizational unit with
ID: {orgUnitId}.");
            }
        }
    }
```

- API の詳細については、AWS SDK for .NET API リファレンスの「DeleteOrganizationalUnit」を参照してください。

CLI

AWS CLI

OU を削除するには

次の例は、OU を削除する方法を示しています。この例では、OU からすべてのアカウントと他の OU を削除済みであることを前提としています。

```
aws organizations delete-organizational-unit --organizational-unit-id ou-examplerootid111-exampleouid111
```

- API の詳細については、AWS CLI コマンドリファレンスの「DeleteOrganizationalUnit」を参照してください。

を使用した組織ポリシーの管理 AWS Organizations

のポリシー AWS Organizations を使用すると、組織 AWS アカウント 内の に追加の管理タイプを適用できます。組織ですべての機能が有効にされている場合、ポリシーを使用できます。

AWS Organizations コンソールには、各ポリシータイプの有効または無効のステータスが表示されます。[Organize accounts (アカウントの整理)] タブの左側のナビゲーションペインで、Root を選択します。画面の右側の詳細ペインには、使用可能なすべてのポリシータイプが表示されます。リストには、その組織ルートで有効になっているものと、無効になっているものが示されます。タイプを [Enable (有効)] にするオプションが存在する場合、そのタイプは現在無効であることを意味します。タイプを [Disable (無効)] にするオプションが存在する場合、そのタイプは現在有効であることを意味します。

トピック

- ポリシータイプ
- の承認ポリシー AWS Organizations
- の管理ポリシー AWS Organizations
- の委任管理者 AWS Organizations
- ポリシータイプの有効化
- ポリシータイプの無効化
- を使用した組織ポリシーの作成 AWS Organizations
- を使用した組織ポリシーの更新 AWS Organizations
- AWS Organizationsを使用して組織ポリシーにアタッチされたタグを編集する
- での組織ポリシーのアタッチ AWS Organizations
- を使用した組織ポリシーのデタッチ AWS Organizations
- 組織のポリシーに関する情報の取得
- を使用した組織ポリシーの削除 AWS Organizations

ポリシータイプ

Organizations のポリシータイプは、次の 2 つのカテゴリに大別されます。

承認ポリシー

承認ポリシーは、組織全体の AWS アカウント のセキュリティを一元管理するのに役立ちます。

- サービスコントロールポリシー (SCPs) は、組織内の IAM ユーザーと IAM ロールが利用できるアクセス許可の最大数を一元的に制御します。
- リソースコントロールポリシー (RCPsは、組織内のリソースに対して使用可能なアクセス許可の最大数を一元的に制御します。

管理ポリシー

管理ポリシーは、組織全体で AWS のサービス とその機能を一元的に設定および管理するのに役立ちます。

- 宣言型ポリシーを使用すると、組織全体 AWS のサービス で特定の に必要な設定を一元的に宣言して適用できます。一度接続すると、サービスに新しい機能や API が追加されても、設定は常に維持されます。
- バックアップポリシーを使用すると、バックアッププランを一元管理し、組織のアカウント全体の AWS リソースに適用できます。
- タグポリシーを使用すると、組織のアカウントの AWS リソースにアタッチされたタグを標準化できます。
- チャットアプリケーションポリシーを使用すると、Slack や Microsoft Teams などのチャットアプリケーションから組織のアカウントへのアクセスを制御できます。
- AI サービスのオプトアウトポリシーを使用すると、組織内のすべてのアカウントの AWS AI サービスのデータ収集を制御できます。
- Security Hub ポリシーを使用すると、組織のセキュリティ要件に沿ったセキュリティカバレッジギャップに対処し、組織全体に一元的に適用できます。

次の表は、各ポリシータイプの主な特性をまとめたものです。これらのポリシータイプのその他の特徴については、のクォータとサービス制限 AWS Organizations を参照してください。

ポリシータイプ	ポリシーカテゴリ	管理アカウントに影響するか	アタッチの最大数 (ルート、OU、アカウントの合計)	最大サイズ	OU またはアカウントの有効なポリシーを表示可能か
SCP	Authorization	 いいえ	5	5120 文字	 いいえ
RCP	Authorization	 いいえ	5	5120 文字	 いいえ
宣言ポリシー	管理	 はい	10	10,000 文字	 はい
バックアップポリシー	管理	 はい	10	10,000 文字	 はい
タグポリシー	管理	 はい	10	10,000 文字	 はい
チャットアプリケーションポリシー	管理	 はい	5	10,000 文字	 はい

ポリシータイプ	ポリシーカテゴリ	管理アカウントに影響するか	アタッチの最大数 (ルート、OU、アカウントの合計)	最大サイズ	OU またはアカウントの有効なポリシーを表示可能か
AI サービスのオプトアウトポリシー	管理	 はい	5	2500 文字	 はい
Security Hub ポリシー	管理	 はい	10	10,000 文字	 はい

の承認ポリシー AWS Organizations

の承認ポリシー AWS Organizations により、メンバーアカウントのプリンシパルとリソースのアクセスを一元的に設定および管理できます。これらのポリシーが組織単位 (OUs) とアカウントにどのように影響するかは、適用する承認ポリシーのタイプによって異なります。

には、 AWS Organizationsサービスコントロールポリシー (SCPs) とリソースコントロールポリシー (RCPs。

トピック

- SCPs と RCPsの違い
- SCPs と RCPs
- サービスコントロールポリシー (SCP)
- リソースコントロールポリシー (RCPs)

SCPs と RCPsの違い

SCPsはプリンシパル中心のコントロールです。SCPs は、メンバーアカウントのプリンシパルが利用できるアクセス許可の上限に対して、アクセス許可ガードレールを作成するか、制限を設定しま

す。SCP は、組織内のプリンシパルに一貫したアクセスコントロールを一元的に適用する場合に使用できます。これには、IAM ユーザーと IAM ロールがアクセスできるサービス、アクセスできるリソース、またはリクエストを実行できる条件 (特定のリージョンやネットワークなど) の指定が含まれます。

RCPsコントロールです。RCPs は、メンバーアカウントのリソースで使用できるアクセス許可の上限に対して、アクセス許可ガードレールを作成するか、制限を設定します。RCP は、組織内のリソース間で一貫したアクセスコントロールを一元的に適用する場合に使用できます。これにより、リソースへのアクセスが制限され、組織に属する ID のみがアクセスできるようにしたり、組織外部の ID がリソースにアクセスできる条件を指定したりできます。

一部のコントロールは、SCPs と RCPs を通じて同様の方法で適用できます。例えば、暗号化されていないオブジェクトをユーザーが S3 にアップロードできないようにして、プリンシパルが S3 バケットに対して実行できるアクションを SCP として記述できます。このコントロールは、プリンシパルが S3 バケットにオブジェクトをアップロードするたびに暗号化を要求する RCP として記述することもできます。2 番目のオプションは、バケットがサードパーティーベンダーなどの組織外のプリンシパルに S3 バケットへのオブジェクトのアップロードを許可している場合に推奨されます。ただし、一部のコントロールは RCP でのみ実装でき、一部のコントロールは SCP でのみ実装できます。詳細については、「SCPs一般的なユースケース RCPs」を参照してください。

SCPs と RCPs

SCPsと RCPsは独立したコントロールです。SCPs または RCPs のみを有効にするか、両方のポリシータイプを一緒に使用することを選択できます。SCPs と RCPs の両方を使用することで、ID とリソースの周囲にデータ境界を作成できます。

SCPsは、ID がアクセスできるリソースを制御する機能を提供します。例えば、ID に AWS 組織内のリソースへのアクセスを許可できます。ただし、ID が組織外のリソースにアクセスできないようにしたい場合があります。SCPs を使用してこのコントロールを適用できます。

RCPsでは、どの ID がリソースにアクセスできるかを制御できます。例えば、組織内の ID が組織内のリソースにアクセスできるようにしたい場合があります。ただし、組織外部の ID が リソースにアクセスできないようにすることもできます。RCPs を使用してこのコントロールを適用できます。RCPsは、 リソースにアクセスしている組織外のプリンシパルの有効なアクセス許可に影響を与える機能を提供します。SCPsは、 AWS 組織内のプリンシパルの有効なアクセス許可にのみ影響します。

SCPs一般的なユースケース RCPs

次の表は、SCP と RCPs。

ユースケース	ポリシータイプ	影響 ID	外部 ID	リソース	外部リソース (リクエストのターゲット)
Restrict which services or actions your identities can use	SCP	X		X	X
Restrict which resources your identities can access	SCP	X		X	X
Enforce requirements on how your identities can access resources	SCP	X		X	X
Restrict which identities can access your resources	RCP	X	X	X	
Protect sensitive resources in your organization	RCP	X	X	X	
Enforce requirements	RCP	X	X	X	

	影響
on how your resources can be accessed	

サービスコントロールポリシー (SCP)

サービスコントロールポリシー (SCP) は、組織のアクセス許可の管理に使用できる組織ポリシーの一種です。SCP では、組織の IAM ユーザーと IAM ロールで使用可能な最大アクセス許可を一元的に制御できます。SCP は、アカウントが組織のアクセスコントロールガイドラインに従っていることを確認するのに役立ちます。SCP は、すべての機能が有効になっている 組織でのみ使用できます。組織が一括請求機能のみを有効にしている場合、SCP は使用できません。SCP を有効にする方法については、「ポリシータイプの有効化」を参照してください。

SCP は、組織内の IAM ユーザーと IAM ロールにアクセス許可を付与しません。SCP によってアクセス許可を付与することはできません。SCP は、組織内の IAM ユーザーと IAM ロールが実行できるアクションに対するアクセス許可ガードレールを定義するか、制限を設定します。アクセス許可を付与するには、管理者は、IAM ユーザーと IAM ロールにアタッチされたアイデンティティベースのポリシーや、アカウントのリソースにアタッチされたリソースベースのポリシーなど、アクセスを制御するポリシーをアタッチする必要があります。詳細については、「IAM ユーザーガイド」の「アイデンティティベースおよびリソースベースのポリシー」を参照してください。

有効なアクセス許可は、SCP とリソースコントロールポリシー (RCPs) で許可されているものと、アイデンティティベースおよびリソースベースのポリシーで許可されているものとの間の論理的な共通部分です。

> ⚠ SCPs管理アカウントのユーザーまたはロールには影響しません
>
> SCP は、管理アカウントのユーザーやロールには影響を与えません。SCP は、組織内のメンバーアカウントにのみ影響を与えます。つまり、SCPsは委任管理者として指定されたメンバーアカウントにも適用されます。

このページのトピック

- SCP の効果をテストする

- SCP の上限サイズ
- SCP を組織内のさまざまなレベルにアタッチする
- アクセス許可における SCP 効果
- アクセスデータを使用して SCP を改善する
- SCP によって制限されないタスクおよびエンティティ
- SCP 評価
- SCP 構文
- サービスコントロールポリシーの例
- を使用したサービスコントロールポリシー (SCPsトラブルシューティング AWS Organizations

SCP の効果をテストする

AWS では、ポリシーがアカウントに与える影響を徹底的にテストすることなく、SCPs を組織のルートにアタッチしないことを強くお勧めします。代わりに、お客様のアカウントを一度に 1 つずつ、または少なくとも少人数ずつ移動できる OU を作成し、誤って主要なサービスからユーザーを締め出すことのないようにします。アカウントでサービスが使用されているかどうかを判断する方法の 1 つは、IAM のサービスの最終アクセス時間データを調べることです。もう 1 つの方法は、 AWS CloudTrail を使用して API レベルでサービス使用状況を ログに記録することです。

> **Note**
>
> [FullAWSAccess] ポリシーを変更するか、許可されたアクションを含む別のポリシーに置き換えない限り、FullAWSAccess ポリシーを削除しないでください。そうしないと、メンバーアカウントからのすべての AWS アクションが失敗します。

SCP の上限サイズ

SCP 内のすべての文字は、その上限サイズに対してカウントされます。このガイドの例では、読みやすさを向上させるため、空白文字を追加してフォーマットされた SCP を示します。ただし、ポリシーサイズが上限サイズに近づいている場合は、スペースを節約するために、引用符の外側にあるすべての空白文字 (スペースや改行など) を削除できます。

> **Tip**
>
> ビジュアルエディタを使用して SCP を構築します。これによって、よけいな空白が自動的に削除されます。

SCP を組織内のさまざまなレベルにアタッチする

SCP の動作の詳細な説明については、「SCP 評価」を参照してください。

アクセス許可における SCP 効果

SCPsはアクセス AWS Identity and Access Management 許可ポリシーに似ており、ほぼ同じ構文を使用します。ただし、SCP がアクセス権限を付与することはありません。代わりに、SCPsは、組織内の IAM ユーザーと IAM ロールで使用できるアクセス許可の最大数を指定するアクセスコントロールです。詳細については、IAM ユーザーガイドのポリシーの評価論理を参照してください。

- SCP は、組織の一部であるアカウントが管理する IAM ユーザーとロールのみに影響します。SCP はリソースベースのポリシーには直接影響しません。また、組織外のアカウントに属するユーザーやロールにも影響しません。組織内のアカウント A が所有する Amazon S3 バケットについて考えてみます。このバケットポリシー (リソースベースのポリシー) は、組織外のアカウント B に属するユーザーにアクセスを許可します。アカウント A には SCP がアタッチされています。この SCP はアカウント B の外部ユーザーには適用されません。SCP は組織内のアカウント A が管理するユーザーにのみ適用されます。
- SCP は、メンバーアカウントのルートユーザーを含む、メンバーアカウントの IAM ユーザーとロールのアクセス許可を制限します。すべてのアカウントには、その上位のすべての親で許可されている権限のみがあります。アクセス許可が、暗黙的に (`Allow` ポリシーステートメントに含まれない)、または明示的に (`Deny` ポリシーステートメントに含まれる)、アカウントのレベルでブロックされている場合、影響を受けるアカウントのユーザーまたはロールは、アカウント管理者が `*/*` アクセス許可を持つ `AdministratorAccess` IAM ポリシーをユーザーにアタッチしても、そのアクセス許可を使用することはできません。
- SCP は、組織内のメンバーアカウントのみに影響します。管理アカウントのユーザーやロールには影響しません。つまり、SCPsは委任管理者として指定されたメンバーアカウントにも適用されます。詳細については、「管理アカウントのベストプラクティス」を参照してください。
- ユーザーとロールには、適切な IAM アクセス許可ポリシーを使用してアクセス許可を付与する必要があります。IAM アクセス許可ポリシーがアタッチされていないユーザーは、たとえ適用され

る SCP によりすべてのサービスとアクションが許可されても、いずれのサービスもアクセスも許可されません。

- アクションへのアクセスを付与する IAM アクセス許可ポリシーがユーザーまたはロールに付与されており、そのアクションが適用可能な SCP によって許可されている場合、ユーザーまたはロールはそのアクションを実行できます。
- アクションへのアクセスを許可する IAM アクセス許可ポリシーがユーザーまたはロールに付与されており、そのアクションが適用可能な SCP によって許可されていないか、または明示的に拒否されている場合、ユーザーまたはロールがそのアクションを実行することはできません。
- SCP は、アタッチされたアカウントのすべてのユーザーやロール (ルートユーザーを含む) に影響します。唯一の例外は、「SCP によって制限されないタスクおよびエンティティ」で説明されているものです。
- SCP はサービスにリンクされたロールに影響しません。サービスにリンクされたロールにより AWS のサービス 、他の は と統合 AWS Organizations でき、SCPs によって制限することはできません。
- ルートで SCP ポリシータイプを無効にすると、そのルート内のすべての AWS Organizations エンティティからすべての SCPs が自動的にデタッチされます。 AWS Organizations エンティティには、組織単位、組織、アカウントが含まれます。そのルートの SCP を再度有効にすると、そのルートはすべてのエンティティに自動的にアタッチされたデフォルトの `FullAWSAccess` ポリシーに戻ります。SCP の無効化の前に AWS Organizations にアタッチされていたすべての SCP は失われ、自動的には復旧されません。ただし、手動で再度アタッチできます。
- アクセス許可の境界 (高度な IAM 機能) と SCP が両方存在する場合は、アクセス許可の境界、SCP、およびアイデンティティのポリシーによって、すべてのアクションが許可されます。

アクセスデータを使用して SCP を改善する

管理アカウントの認証情報を使用してサインインすると、IAM コンソールの AWS Organizationsセクションで AWS Organizations エンティティまたはポリシーのサービスの最終アクセス時間データを表示できます。IAM で AWS Command Line Interface （ AWS CLI) または AWS API を使用して、サービスの最終アクセス時間データを取得することもできます。このデータには、 AWS Organizations アカウントの IAM ユーザーとロールが最後にアクセスを試みた許可されたサービスとその日時に関する情報が含まれます。この情報を使用して不要なアクセス許可を識別し、最小権限の原則により良く準拠するように SCP を改良できます。

例えば、3 つの AWS のサービスへのアクセスを禁止する拒否リスト SCP があるとします。SCP の `Deny` ステートメントにリストされていないすべてのサービスが許可されます。IAM のサービスの最

終アクセス時間データでは、SCP で AWS のサービス 許可されているが、使用されていないデータが に指示されます。この情報により、SCP を更新して、必要でないサービスへのアクセスを拒否できます。

詳細については、IAM ユーザーガイドにある下記のトピックを参照してください。

- 組織の組織サービスの最終アクセス データの表示
- データを使用した組織単位のアクセス権限の調整

SCP によって制限されないタスクおよびエンティティ

SCP を使用して次のタスクを制限することはできません。

- 管理アカウントによって実行されるすべてのアクション
- サービスにリンクされたロールにアタッチされたアクセス許可を使用して実行されるすべてのアクション。
- root ユーザーとして Enterprise サポートプランに登録する
- 信頼された署名者に CloudFront プライベートコンテンツの機能を提供する
- Amazon Lightsail メールサーバーおよび Amazon EC2 インスタンスの逆引き DNS をルートユーザーとして設定する
- 一部の AWS関連サービスのタスク：
  - Alexa Top Sites
  - Alexa Web Information Service
  - Amazon Mechanical Turk
  - Amazon Product Marketing API

SCP 評価

> **Note**
>
> このセクションの情報は、バックアップポリシー、タグポリシー、チャットアプリケーションポリシー、AI サービスのオプトアウトポリシーなどの管理ポリシータイプには適用されません。詳細については、「管理ポリシーの継承を理解する」を参照してください。

AWS Organizationsではさまざまなレベルで複数のサービスコントロールポリシー (SCP) を関連付けることができるため、SCP の評価方法を理解しておくと、正しい結果をもたらす SCP を作成するのに役立ちます。

トピック

- SCP と Allow の連携の仕組み
- SCP と Deny の連携の仕組み
- SCP の使用戦略

SCP と Allow の連携の仕組み

特定のアカウントに対してアクセス許可を許可するには、アカウント (ターゲット アカウント自体を含む) への直接パスのルートから各 OU までのすべてのレベルで明示的な **`Allow`** ステートメントが必要です。そのため、SCPs を有効にすると、 は FullAWSAccess という名前の AWS マネージド SCP ポリシーを AWS Organizations アタッチし、すべてのサービスとアクションを許可します。このポリシーが組織のどのレベルでも削除され、置き換えられない場合、そのレベルのすべての OU とアカウントはいかなるアクションも実行できなくなります。

例えば、図 1 と図 2 のシナリオを見ていきましょう。アカウント B でアクセス権限またはサービスを許可するには、そのアクセス権限またはサービスを許可する SCP を Production OU であるルート、およびアカウント B 自体にアタッチする必要があります。

SCP の評価はデフォルトで拒否されるモデルに従います。つまり、SCP で明示的に許可されていないアクセス権限はすべて拒否されます。ルート、Production OU、アカウント B などのどのレベルでも SCP に許可ステートメントが存在しない場合、アクセスは拒否されます。

> **メモ**
>
> - SCP 内の `Allow` ステートメントにより、`Resource` 要素に "*" エントリのみを含めることが許可されます。
> - SCP 内の `Allow` ステートメントには、`Condition` 要素を含めることは一切できません。

図 1: ルート、Production OU、アカウント B に `Allow` ステートメントがアタッチされた組織構造の例

図 2: Production OU で Allow ステートメントが欠落している組織構造の例と、アカウント B への影響

SCP と Deny の連携の仕組み

特定のアカウントに対するアクセス許可が拒否される場合、ルートからアカウント (ターゲット アカウント自体を含む) への直接パス内の各 OU を経由するすべての SCPがそのアクセス許可を拒否できます。

例えば、Production OU にアタッチされている SCP に、特定のサービスに対して明示的な Deny ステートメントが指定されているとします。また、図 3 に示すように、同じサービスへのアクセスを明示的に許可する別の SCP がルートとアカウント B にアタッチされている場合もあります。その結果、組織内のどのレベルにも適用された拒否ポリシーが、その下にあるすべての OU とメンバーアカウントに対して評価されるため、アカウント A とアカウント B の両方がサービスへのアクセスを拒否されます。

図 3: Production OU で Deny ステートメントがアタッチされた組織構造の例と、アカウント B への影響

SCP の使用戦略

SCP を作成する際、Allow と Deny ステートメントを組み合わせて使用することで、組織内で意図したアクションやサービスを実現できます。Deny ステートメントは、ルートレベルまたは OU レベルで適用されると、その下にあるすべてのアカウントに影響するため、組織や OU のより広い範囲に適用すべき制限を実装する強力な方法です。

例えば、Deny ステートメントを使用して メンバーアカウントが組織を離れるのを禁止する にルートレベルでポリシーを実装すると、組織内のすべてのアカウントに有効になります。Deny ステートメントは、例外の作成に役立つ条件要素もサポートしています。

> **Tip**
>
> IAM でサービスの最終アクセス時間データを使用して SCP を更新し、必要な AWS のサービス のみへのアクセスを制限できます。詳細については、IAM ユーザーガイドの「組織の Organizations サービスの最終アクセス時間データを表示する」を参照してください。

AWS Organizations は、作成時にすべてのルート、OU、アカウントに FullAWSAccess という名前の AWS マネージド SCP をアタッチします。このポリシーはすべてのサービスとアクションを許可します。FullAWSAccess を一連のサービスのみを許可するポリシーに置き換えて、SCPs を更新することで明示的に許可されない限り、新しい AWS のサービス は許可されません。例えば、組織内で一部のサービスの使用のみを許可したい場合は、`Allow` ステートメントを使用して特定のサービスのみを許可できます。

JSON

```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        }
    ]
}
```

この 2 つのステートメントを組み合わせたポリシーは、次の例のようになります。このポリシーでは、メンバーアカウントが組織から退出することを防ぎ、必要な AWS サービスの使用を許可します。組織の管理者は、[FullAWSAccess] ポリシーをデタッチして、これを代わりにアタッチできます。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
```

```
                "organizations:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action":"organizations:LeaveOrganization",
            "Resource": "*"
        }
    ]
}
```

次に、以下のサンプル組織構造を検討して、組織内のさまざまなレベルで複数の SCP を適用する方法を理解してください。

次の表は、サンドボックス OU で有効なポリシーを示しています。

シナリオ	[ルート] における SCP	[サンドボックス] OU における SCP	[アカウント A] における SCP	[アカウント A] における適用されるポリシー	[アカウント B] と [アカウント C] における適用されるポリシー
1	フル AWS アクセス	フル AWS アクセス + S3 アクセス拒否	フル AWS アクセス + EC2 アクセス拒否	S3 も EC2 もアクセスなし	S3 アクセスなし
2	フル AWS アクセス	EC2 アクセスを許可する	EC2 アクセスを許可する	EC2 アクセスを許可する	EC2 アクセスを許可する
3	S3 アクセスを拒否する	S3 アクセスを許可する	フル AWS アクセス	サービスへのアクセスなし	サービスへのアクセスなし

次の表は、ワークロード OU で有効なポリシーを示しています。

シナリオ	[ルート] における SCP	[ワークロード] OU における SCP	[テスト] OU における SCP	[アカウント D] における適用されるポリシー	[Production] OU、[アカウント E]、[アカウント F] における適用されるポリシー
1	フル AWS アクセス	フル AWS アクセス	フル AWS アクセス + EC2 アクセス拒否	EC2 アクセスなし	フル AWS アクセス
2	フル AWS アクセス	フル AWS アクセス	EC2 アクセスを許可する	EC2 アクセスを許可する	フル AWS アクセス
3	S3 アクセスを拒否する	フル AWS アクセス	S3 アクセスを許可する	サービスへのアクセスなし	S3 アクセスなし

SCP 構文

サービスコントロールポリシー (SCPs、 AWS Identity and Access Management (IAM) アクセス許可ポリシーおよびリソースベースのポリシー (Amazon S3 バケットポリシーなど) で使用される構文と同様の構文を使用します。IAM ポリシーの詳細とその構文については、IAM ユーザーガイドの「IAM ポリシーの概要」を参照してください。

SCP は、JSON のルールに従って構造化されたプレーンテキストファイルです。このトピックで説明されている要素を使用します。

> **Note**
>
> SCP 内のすべての文字は、その上限サイズに対してカウントされます。このガイドの例では、読みやすさを向上させるため、空白文字を追加してフォーマットされた SCP を示します。ただし、ポリシーサイズが上限サイズに近づいている場合は、スペースを節約するために、引用符の外側にあるすべての空白文字 (スペースや改行など) を削除できます。

SCP に関する一般情報については、「サービスコントロールポリシー (SCP)」を参照してください。

要素の概要

次の表には、SCP で使用できるポリシー要素を要約しています。一部のポリシー要素はアクションを拒否する SCP のみで使用できます。[Supported Effects] (サポートされる効果) の列には、SCP の各ポリシー要素で使用できる効果のタイプが一覧表示されています。

要素	目的	サポートされる効果
アクション	SCP が許可または拒否する AWS サービスとアクションを指定します。	`Allow`, `Deny`
[Effect] (効果)	SCP ステートメントがプリンシパルおよびアカウント内の IAM ユーザーとロールへのアクセスを許可するか拒否するかを定義します。	`Allow`, `Deny`

要素	目的	サポートされる効果
Statement	ポリシー要素のコンテナとして機能します。SCP には複数のステートメントを含めることができます。	Allow, Deny
Statement ID (Sid)	(オプション) ステートメントにわかりやすい名前を付けます。	Allow, Deny
Version	ポリシーの処理に使用する言語構文ルールを指定します。	Allow, Deny

要素	目的	サポートされる効果
条件	ステートメントを実行するタイミングの条件を指定します。	Deny
NotAction	SCP から除外される AWS サービスとアクションを指定します。Actior 要素の代わりに使用します。	Deny
[リソース]	SCP が適用される AWS リソースを指定します。	Deny

次のセクションでは、SCP でポリシー要素がどのように使用されるかについての詳細および例を提供しています。

トピック

- Action および NotAction 要素
- Condition 要素

- Effect 要素
- Resource 要素
- Statement 要素
- ステートメント ID (Sid) 要素
- Version 要素
- サポートされていない要素

Action および **NotAction** 要素

各ステートメントには、次のいずれかが含まれている必要があります。

- 許可あるいは拒否ステートメントの `Action` 要素。
- 拒否ステートメントのみ (`Effect` 要素の値が `Deny` の場合) では、`Action` または `NotAction` 要素。

`Action` または `NotAction`要素の値は、ステートメントによって許可または拒否される AWS サービスとアクションを識別する文字列のリスト (JSON 配列) です。

各文字列は、サービスの略称 (「s3」、「ec2」、「iam」、「organizations」など) で構成されており、すべて小文字で、コロンと、その後にサービスのアクションが続きます。アクションと表記では、大文字と小文字は区別されません。一般的に、すべて大文字と小文字で始まる各単語で入力されます。例: `"s3:ListAllMyBuckets"`。

SCP でアスタリスク (*) や疑問符 (?) などのワイルドカード文字を使用することもできます。

- 名前の一部を共有する複数のアクションを検索するには、アスタリスクをワイルドカードとして使用します。値 `"s3:*"` は、Amazon S3 サービス内のすべてのアクションを意味します。値 `"ec2:Describe*"` は「Describe」で始まる EC2 アクションのみに一致します。
- 単一の文字を検索する場合は疑問符 (?) を使用します。

> **Note**
>
> SCP では、`Action` または `NotAction` 要素のワイルドカード文字 (* および ?) は、要素自身、または文字列の末尾にのみ使用できます。文字列の先頭または中間には表示されませ

ん。そのため、"servicename:action*" は有効ですが、"servicename:*action" と "servicename:some*action" はいずれも、SCP で無効です。

AWS Organizations SCPs と IAM アクセス許可ポリシーの両方でサポートされるすべてのサービスとアクションのリストについては、IAM ユーザーガイドの「AWS サービスのアクション、リソース、および条件キー」を参照してください。

詳細については、IAM ユーザーガイドの「IAM JSON ポリシー要素: Action」および「IAM JSON ポリシー要素: NotAction」を参照してください。

Action 要素の例

次の例では、アカウント管理者に、アカウント内の EC2 インスタンスの許可を記述、開始、停止、終了する権限を委譲することを許可するステートメントを持つ SCP を示しています。これは、許可リストの例であり、デフォルトではアクセス許可を暗黙的に拒否するためにデフォルトの Allow * ポリシーがアタッチされていない場合に便利です。デフォルトの Allow * ポリシーがルート、OU、次のポリシーがアタッチされるアカウントに引き続きアタッチされている場合は、ポリシーの効果はありません。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
          "ec2:DescribeInstances", "ec2:DescribeImages", "ec2:DescribeKeyPairs",
          "ec2:DescribeSecurityGroups", "ec2:DescribeAvailabilityZones",
 "ec2:RunInstances",
          "ec2:TerminateInstances", "ec2:StopInstances", "ec2:StartInstances"
        ],
        "Resource": "*"
    }
}
```

次の例では、アタッチされたアカウントで使用されたくないサービスへのアクセスを拒否する方法を示しています。デフォルトの "Allow *" SCP がすべての OU および root にまだアタッチされていることを前提としています。このポリシーの例では、アタッチされたアカウントのアカウント管理者

は、IAM、Amazon EC2、Amazon RDS サービスにアクセス許可を移譲することはできません。他のサービスからのあらゆるアクションは、移譲を拒否する他のポリシーがアタッチされていない限り移譲できます。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": [ "iam:*", "ec2:*", "rds:*" ],
        "Resource": "*"
    }
}
```

NotAction 要素の例

次の例は、 NotAction要素を使用して、ポリシーの影響から AWS サービスを除外する方法を示しています。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LimitActionsInRegion",
      "Effect": "Deny",
      "NotAction": "iam:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-west-1"
        }
       }
     }
   ]
}
```

このステートメントでは、IAM アクションを使用する場合を除き AWS リージョン、影響を受けるアカウントは指定された でアクションを実行することに限定されます。

Condition 要素

SCP の拒否ステートメントに Condition 要素を指定することができます。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "cloudfront:*",
                "iam:*",
                "route53:*",
                "support:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

この SCP は、リストされたサービスを除く、eu-central-1 および eu-west-1 リージョンの外部のすべてのオペレーションへのアクセスを拒否します。

詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素: 条件」を参照してください。

Effect 要素

各ステートメントには必ず Effect を 1 つ含める必要があります。この値は Allow または Deny となります。これは、同じステートメントにリストされたアクションが影響を受けます。

詳細については、IAM ユーザーガイドの「IAM JSON ポリシーの要素: Effect」を参照してください。

"Effect": "Allow"

次の例では、Allow の値を持つ Effect 要素を含むステートメントを持つ SCP を示しています。これにより、アカウントユーザーが Amazon S3 サービスのアクションを実行できるようになります。この例は、許可リスト戦略を使用する組織で役立ちます (デフォルトの FullAWSAccess ポリシーがすべてデタッチされているため、デフォルトでアクセス許可は暗黙的に拒否されます)。その結果、このステートメントでは、アタッチされているすべてのアカウントに対する Amazon S3 のアクセスが許可されます。

```
{
    "Statement": {
        "Effect": "Allow",
        "Action": "s3:*",
        "Resource": "*"
    }
}
```

このステートメントは IAM アクセス許可ポリシーに同じ Allow 値を使用しますが、SCP では実際に何かを実行するためのアクセス許可をユーザーに付与しません。代わりに、SCPは、組織、組織単位 (OU)、またはアカウントに対するアクセス許可の上限を指定するフィルターとして機能します。前述の例では、アカウント内のユーザーで AdministratorAccess 管理ポリシーがアタッチされている場合でも、SCP は影響を受けるアカウントのすべてのユーザーによるアクションを Amazon S3 アクションのみに制限します。

"Effect": "Deny"

また、Effect 要素に Deny の値があるステートメントでは、SCP の有効時に特定のリソースへのアクセスを制限したり、条件を定義することもできます。

次の例は、拒否ステートメントで条件キーを使用する方法の例を示しています。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "ec2:RunInstances",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:InstanceType": "t2.micro"
            }
        }
    }
}
```

SCP のこのステートメントは、影響が及ぶアカウント (SCP がアカウント自体にアタッチされているか、アカウントがある組織ルートあるいは OU にアタッチされている場合) が、Amazon EC2 インスタンスが `t2.micro` に設定されていないときに Amazon EC2 インスタンスを起動しないようにするガードレールを設定します。このアクションを許可する IAM ポリシーがアカウントにアタッチされている場合でも、SCP によって作成されたガードレールはこれを許可しません。

`Resource` 要素

`Effect` 要素に `Allow` の値があるステートメントでは、SCP の `Resource` 要素の「`*`」のみを指定することができます。個々のリソースの Amazon リソースネーム (ARN) を指定することはできません。

リソース要素でアスタリスク (*) や疑問符 (?) などのワイルドカード文字を使用することもできます。

- 名前の一部を共有する複数のアクションを検索するには、アスタリスクをワイルドカードとして使用します。
- 単一の文字を検索する場合は疑問符 (?) を使用します。

`Effect` 要素に `Deny` の値があるステートメントでは、次の例に示すように、個々の ARN を指定することができます。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToAdminRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/role-to-deny"
      ]
    }
  ]
}
```

この SCP は、影響を受けるアカウントの IAM ユーザーとロールが、組織内のすべてのアカウントに作成された共通の管理 IAM ロールに変更を加えることを制限します。

詳細については、IAM ユーザーガイドの「IAM JSON ポリシー要素: Resource」を参照してください。

Statement 要素

SCP は、1 つ以上の Statement 要素で構成されます。ポリシーには Statement キーワードを 1 つだけ含めることができますが、値は、ステートメントの JSON 配列 ([ ] の文字で囲まれる) もあります。

以下の例は、単一の Effect 要素、Action 要素、Resource 要素で構成される単一のステートメントを示しています。

```
    "Statement": {
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
```

次の例では、1 つの Statement 要素内に、配列リストとして 2 つのステートメントが含まれています。最初のステートメントではすべてのアクションが許可されますが、2 つ目のステートメントではすべての EC2 アクションが拒否されます。結果的に、アカウントの管理者は、Amazon Elastic Compute Cloud (Amazon EC2) 以外のアクセス許可をすべて委譲できます。

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*"
        }
    ]
```

詳細については、IAM ユーザーガイドの「IAM JSON ポリシー要素: Statement」を参照してください。

ステートメント ID (**Sid**) 要素

Sid は、ポリシーステートメントに提供するオプションの識別子です。Sid 値は、ステートメント配列内の各ステートメントに割り当てることができます。次の SCP の例は、Sid ステートメントのサンプルを示しています。

```
{
    "Statement": {
        "Sid": "AllowsAllActions",
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
}
```

詳細については、IAM ユーザーガイドの「IAM JSON ポリシー要素: ID」を参照してください。

`Version` 要素

すべての SCP には、`Version`値を持つ要素`"2012-10-17"`が含まれる必要があります。これは、IAM アクセス許可ポリシーの最新バージョンと同じバージョンの値です。

```
    "Version": "2012-10-17",
```

詳細については、IAM ユーザーガイドの「IAM JSON ポリシー要素: Version」を参照してください。

サポートされていない要素

以下の要素は SCP ではサポートされていません。

- `Principal`
- `NotPrincipal`
- `NotResource`

サービスコントロールポリシーの例

このトピックで表示されているサービスコントロールポリシー (SCP) の例は、情報提供のみを目的としています。

> **これらの例を使用する前に**
>
> 組織内でこれらの SCP の例を使用する前に、以下のことを実行します。
>
> - お客様の固有要件に応じて SCP を慎重にレビューし、カスタマイズします。
> - AWS のサービス 使用する を使用して、環境内の SCPs を徹底的にテストします。
>
> このセクションのポリシーの例では、SCP の実装と使用について説明します。これらの例は、公式な AWS 推奨事項やベストプラクティスとして解釈されることを意図したものではありません。拒否ベースのポリシーが、お客様の環境のビジネス要件を解決するために適切であるかどうかを慎重にテストする責任はお客様にあります。拒否ベースのサービスコントロールポリシーは、ポリシーに必要な例外を追加 AWS のサービス しない限り、 の使用を意図せずに制限またはブロックする可能性があります。このような例外の例については、不要な へのアクセスをブロックするルールからグローバルサービスを免除する最初の例を参照してください AWS リージョン。

- SCP は、ルートユーザーを含む、それが関連付けられているすべてのアカウントのすべてのユーザーとロールに影響することに注意してください。
- SCP はサービスにリンクされたロールには影響しないことに注意してください。サービスにリンクされたロールにより AWS のサービス 、他の は と統合 AWS Organizations でき、SCPs によって制限することはできません。

> **Tip**
>
> IAM でサービスの最終アクセス時間データを使用して SCP を更新し、必要な AWS のサービス のみへのアクセスを制限できます。詳細については、IAM ユーザーガイドの「組織の Organizations サービスの最終アクセス時間データを表示する」を参照してください。

次の各種ポリシーは、「拒否リストポリシー」戦略の例です。拒否リストポリシーは、影響を受けるアカウントの承認済みアクションを許可する他のポリシーと合わせてアタッチする必要があります。例えば、デフォルトの `FullAWSAccess` ポリシーは、アカウントによるすべてのサービスの使用を許可します。このポリシーは、デフォルトによって、ルート、すべての組織単位 (OU)、およびすべてのアカウントにアタッチされます。実際、アクセス許可は付与されません。付与する SCP がないためです。代わりに、そのアカウントの管理者は、アカウントのユーザー、ロール、またはグループに標準 AWS Identity and Access Management (IAM) アクセス許可ポリシーをアタッチして、これらのアクションへのアクセスを委任できます。これらの各拒否リストポリシーによって、指定されたサービスまたはアクションへのアクセスがブロックされ、ポリシーはすべて上書きされます。

例

- 一般的な例
  - リクエスト AWS された に基づいて へのアクセスを拒否する AWS リージョン
  - IAM ユーザーとロールによる特定の変更を禁止する
  - 指定された管理者ロール以外の IAM ユーザーとロールが特定の変更を行うことを禁止する
  - API オペレーションの実行に MFA を要求する
  - ルートユーザーによるサービスへのアクセスをブロックする
  - メンバーアカウントが組織を離れるのを禁止する
- チャットアプリケーションにおける Amazon Q Developer SCPs の例
  - すべての IAM オペレーションを拒否する
  - 指定された Slack チャネルからの S3 バケットの PUT リクエストを拒否する

- Amazon CloudWatch の SCP の例
  - ユーザーによる CloudWatch の無効化または設定の変更を禁止する
- AWS Configの SCP の例
  - ユーザーがルールを無効化 AWS Config または変更できないようにする
- Amazon Elastic Compute Cloud (Amazon EC2) の SCP の例
  - 指定するタイプを使用するよう Amazon EC2 インスタンスに要求する
  - IMDSv2 なしで EC2 インスタンスが起動することを禁止する
  - デフォルトの Amazon EBS 暗号化の無効化を禁止する
  - gp3 以外のボリュームの作成とアタッチを禁止する
- Amazon GuardDuty の SCP の例
  - ユーザーによる GuardDuty の無効化または設定の変更を禁止する
- SCPs の例 AWS Resource Access Manager
  - 外部共有の禁止
  - 特定のアカウントが、指定したリソースタイプのみを共有できるようにする
  - 組織または組織単位 (OU) との共有を禁止する
  - 指定した IAM ユーザーおよびロールのみとの共有を許可する
- Amazon Application Recovery Controller (ARC) の SCP 例
  - ユーザーが ARC ルーティング制御状態を更新できないようにする
- Amazon S3 の SCP の例
  - Amazon S3 の暗号化されていないオブジェクトのアップロードを禁止する
- リソースのタグ付けの SCP の例
  - 作成される特定のリソースにタグを要求する
  - 許可されたプリンシパル以外のタグが変更されないようにする
- Amazon Virtual Private Cloud (Amazon VPC) の SCP の例
  - ユーザーによる VPC フローログの削除を禁止する
  - インターネットアクセスに接続されていない VPC を使用した取得を禁止する

一般的な例

リクエスト AWS された に基づいて へのアクセスを拒否する AWS リージョン

この SCP は、指定されたリージョン外でのオペレーションへのアクセスを拒否します。eu-central-1 と AWS リージョン を、使用する eu-west-1に置き換えます。これにより、承認されたグローバルサービスでオペレーションが除外されます。この例では、指定した 2 つの管理者ロールのいずれかによるリクエストを除外する方法についても説明します。

> **Note**
>
> でリージョン拒否 SCP を使用するには AWS Control Tower、「 AWS Control Tower コントロールリファレンスガイド」の「リクエスト AWS された に基づいて へのアクセスを拒否する AWS リージョン」を参照してください。

このポリシーは、Deny 効果を使用して、承認された 2 つのリージョン (eu-central-1 および eu-west-1) のいずれかをターゲットとしないオペレーションに対するリクエストへのアクセスを拒否します。NotAction 要素を使用すると、すべてのオペレーション (または個別のオペレーション) がこの制限から除外されるサービスのリストを指定できます。グローバルサービスには us-east-1 リージョンによって物理的にホストされるエンドポイントがあるため、この方法で除外する必要があります。このように構成された SCP では、リクエストされたサービスが NotAction 要素に含まれている場合、us-east-1 リージョン内のグローバルサービスに対するリクエストが許可されます。us-east-1 リージョン内のサービスに対するその他のリクエストは、このポリシー例によって拒否されます。

> **Note**
>
> この例では、最新のグローバルオペレーション AWS のサービス または オペレーションの一部が含まれていない場合があります。サービスとオペレーションのリストを、組織内のアカウントによって使用されるグローバルサービスで置換えてください。
>
> > **ヒント**
> >
> > IAM コンソールでサービスの最終アクセスデータを表示すると、組織が使用しているグローバルサービスを確認できます。IAM ユーザー、グループ、またはロールの

詳細ページの [Access Advisor] (アクセスアドバイザー) タブには、そのエンティティによって使用された AWS のサービスが最新のアクセス順に表示されます。

考慮事項

- AWS KMS と はリージョンエンドポイント AWS Certificate Manager をサポートします。ただし、Amazon CloudFront などのグローバルサービスでそれらを使用する場合は、次の SCP の例のグローバルサービス除外リストに含める必要があります。Amazon CloudFront などのグローバルサービスでは、通常、同じリージョンの AWS KMS と ACM にアクセスする必要があります。グローバルサービスの場合、 は米国東部 (バージニア北部) リージョン () ですus-east-1。
- デフォルトでは、 AWS STS はグローバルサービスであり、グローバルサービス除外リストに含める必要があります。ただし、 を有効に AWS STS して、単一のグローバルエンドポイントの代わりにリージョンエンドポイントを使用できます。これを行うと、次の SCP の例にあるグローバルサービスの免除リストから STS を削除できます。詳細については、AWS STS 「 での の管理 AWS リージョン」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "chime:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
```

```
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeVpnGateways",
                "fms:*",
                "globalaccelerator:*",
                "health:*",
                "iam:*",
                "importexport:*",
                "kms:*",
                "mobileanalytics:*",
                "networkmanager:*",
                "organizations:*",
                "pricing:*",
                "route53:*",
                "route53domains:*",
                "route53-recovery-cluster:*",
                "route53-recovery-control-config:*",
                "route53-recovery-readiness:*",
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints",
                "s3:PutAccountPublic*",
                "shield:*",
                "sts:*",
                "support:*",
                "trustedadvisor:*",
                "waf-regional:*",
                "waf:*",
                "wafv2:*",
                "wellarchitected:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
```

```
                }
            }
        }
    ]
}
```

IAM ユーザーとロールによる特定の変更を禁止する

この SCP は、IAM ユーザーとロールが、組織内のすべてのアカウントで作成した特定の IAM ロールに変更を加えることを制限します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToASpecificRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ]
    }
  ]
}
```

指定された管理者ロール以外の IAM ユーザーとロールが特定の変更を行うことを禁止する

この SCP は、前述の例において、管理者の例外を追加します。これにより、影響を受けるアカウントの IAM ユーザーやロールが、指定されたロールを使用する、組織内の管理者以外のすべてのアカウントで作成された共通の管理用 IAM ロールに変更を加えられないようにします。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessWithException",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ],
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalARN":"arn:aws:iam::*:role/name-of-admin-role-to-allow"
        }
      }
    }
  ]
}
```

API オペレーションの実行に MFA を要求する

以下のような SCP を使用して、IAM ユーザーまたはロールがアクションを実行する前に多要素認証 (MFA) を要求するようにします。この例では、アクションは Amazon EC2 インスタンスを停止することです。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
      "Effect": "Deny",
      "Action": [
        "ec2:StopInstances",
```

```
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": false}}
    }
  ]
}
```

ルートユーザーによるサービスへのアクセスをブロックする

以下のポリシーでは、メンバーアカウントのルートユーザーに対して、指定したアクションへのすべてのアクセスを制限します。アカウントで特定の方法のルート認証情報を使用できないようにするには、このポリシーに独自のアクションを追加します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictEC2ForRoot",
      "Effect": "Deny",
      "Action": [
        "ec2:*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:root"
          ]
        }
      }
    }
  ]
}
```

メンバーアカウントが組織を離れるのを禁止する

次のポリシーでは、LeaveOrganization API オペレーションを使用して、メンバーアカウントの管理者が組織からアカウントを削除できないようにします。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "organizations:LeaveOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

チャットアプリケーションにおける Amazon Q Developer SCPs の例

このカテゴリの例

- すべての IAM オペレーションを拒否する
- 指定された Slack チャネルからの S3 バケットの PUT リクエストを拒否する

すべての IAM オペレーションを拒否する

次の SCP は、チャットアプリケーション設定のすべての Amazon Q Developer を通じて呼び出されたすべての IAM オペレーションを拒否します。

```
{
    "Effect": "Deny",
    "Action": "iam:*",
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:ChatbotSourceArn": "arn:aws:chatbot::*:*"
        }
    }
}
```

指定された Slack チャネルからの S3 バケットの PUT リクエストを拒否する

次のポリシーは、Slack チャネルから発信されるすべてのリクエストに対して、指定されたバケットへの S3 の PUT リクエストをすべて拒否します。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ExampleS3Deny",
            "Effect": "Deny",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "ArnLike": {
                      "aws:ChatbotSourceArn": "arn:aws:chatbot::*:chat-
configuration/slack-channel/*"
                }
            }
        }
    ]
}
```

Amazon CloudWatch の SCP の例

このカテゴリの例

- ユーザーによる CloudWatch の無効化または設定の変更を禁止する

ユーザーによる CloudWatch の無効化または設定の変更を禁止する

CloudWatch の下位レベルのオペレーターについては、ダッシュボードとアラームをモニタリングする必要があります。ただし、オペレーターが、上級者が設置したダッシュボードやアラームを削除または変更できないようにする必要があります。この SCP では、影響を受けるアカウントのユーザーまたはロールは、ダッシュボードまたはアラームを削除または変更する可能性のある CloudWatch コマンドを実行できなくなります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
```

```
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DeleteDashboards",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:PutDashboard",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:SetAlarmState"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Configの SCP の例

このカテゴリの例

- ユーザーがルールを無効化 AWS Config または変更できないようにする

ユーザーがルールを無効化 AWS Config または変更できないようにする

この SCP は、影響を受けるアカウントのユーザーまたはロールが、そのルール AWS Config またはトリガーを無効化または変更する可能性のある AWS Config オペレーションを実行できないようにします。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "config:DeleteConfigRule",
        "config:DeleteConfigurationRecorder",
        "config:DeleteDeliveryChannel",
        "config:StopConfigurationRecorder"
      ],
      "Resource": "*"
    }
  ]
}
```

Amazon Elastic Compute Cloud (Amazon EC2) の SCP の例

このカテゴリの例

- 指定するタイプを使用するよう Amazon EC2 インスタンスに要求する
- IMDSv2 なしで EC2 インスタンスが起動することを禁止する
- デフォルトの Amazon EBS 暗号化の無効化を禁止する
- gp3 以外のボリュームの作成とアタッチを禁止する

指定するタイプを使用するよう Amazon EC2 インスタンスに要求する

この SCP を使用すると、`t2.micro` インスタンスタイプを使用していないすべてのインスタンスの起動は拒否されます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireMicroInstanceType",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ec2:InstanceType": "t2.micro"
        }
      }
    }
  ]
}
```

IMDSv2 なしで EC2 インスタンスが起動することを禁止する

以下のポリシーは、すべてのユーザーが IMDSv2 なしで EC2 インスタンスを起動することを制限します。

```
[
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "StringNotEquals":{
```

```
            "ec2:MetadataHttpTokens":"required"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "NumericGreaterThan":{
            "ec2:MetadataHttpPutResponseHopLimit":"2"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"*",
      "Resource":"*",
      "Condition":{
         "NumericLessThan":{
            "ec2:RoleDelivery":"2.0"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:ModifyInstanceMetadataOptions",
      "Resource":"*"
   }
]
```

以下のポリシーは、すべてのユーザーが IMDSv2 なしで EC2 インスタンスを起動することを制限しますが、特定の IAM ID がインスタンスのメタデータオプションを変更することを許可します。

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
```

```
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "NumericGreaterThan": {
        "ec2:MetadataHttpPutResponseHopLimit": "2"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*",
    "Condition": {
      "ArnNotLike": {
        "aws:PrincipalARN": [
          "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
        ]
      }
    }
  }
]
```

デフォルトの Amazon EBS 暗号化の無効化を禁止する

以下のポリシーは、すべてのユーザーがデフォルトの Amazon EBS 暗号化を無効にすることを制限します。

```
{
  "Effect": "Deny",
```

```
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

gp3 以外のボリュームの作成とアタッチを禁止する

次のポリシーは、すべてのユーザーが gp3 ボリュームタイプではない Amazon EBS ボリュームを作成またはアタッチすることを制限します。詳細については、「Amazon EBS ボリュームのタイプ」を参照してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCreationAndAttachmentOfNonGP3Volumes",
      "Effect": "Deny",
      "Action": [
        "ec2:AttachVolume",
        "ec2:CreateVolume",
        "ec2:RunInstances"
      ],
      "Resource": "arn:aws:ec2:*:*:volume/*",
      "Condition": {
        "StringNotEquals": {
          "ec2:VolumeType": "gp3"
        }
      }
    }
  ]
}
```

これにより、組織全体で標準化されたボリューム設定を適用できます。

> **ボリュームタイプの変更は妨げられません**
>
> SCPs を使用して、既存の gp3 ボリュームを別のタイプの Amazon EBS ボリュームに変更するアクションを制限することはできません。例えば、この SCP では、既存の gp3 ボリュームを gp2 ボリュームに変更することはできません。これは、 条件キーがボリュームタイプを変更する前に`ec2:VolumeType`チェックするためです。

Amazon GuardDuty の SCP の例

このカテゴリの例

- ユーザーによる GuardDuty の無効化または設定の変更を禁止する

ユーザーによる GuardDuty の無効化または設定の変更を禁止する

この SCP は、影響を受けるアカウントのユーザーまたはロールが、コマンドとして直接、またはコンソールから GuardDuty を無効にしたり、設定を変更したりするのを防ぎます。これにより、GuardDuty の情報とリソースへの読み取り専用アクセスを効果的に実現できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "guardduty:AcceptInvitation",
                "guardduty:ArchiveFindings",
                "guardduty:CreateDetector",
                "guardduty:CreateFilter",
                "guardduty:CreateIPSet",
                "guardduty:CreateMembers",
                "guardduty:CreatePublishingDestination",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeclineInvitations",
                "guardduty:DeleteDetector",
                "guardduty:DeleteFilter",
                "guardduty:DeleteInvitations",
                "guardduty:DeleteIPSet",
                "guardduty:DeleteMembers",
                "guardduty:DeletePublishingDestination",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:DisassociateMembers",
                "guardduty:InviteMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:TagResource",
                "guardduty:UnarchiveFindings",
                "guardduty:UntagResource",
```

```
                "guardduty:UpdateDetector",
                "guardduty:UpdateFilter",
                "guardduty:UpdateFindingsFeedback",
                "guardduty:UpdateIPSet",
                "guardduty:UpdatePublishingDestination",
                "guardduty:UpdateThreatIntelSet"
            ],
            "Resource": "*"
        }
    ]
}
```

SCPs の例 AWS Resource Access Manager

このカテゴリの例

- 外部共有の禁止
- 特定のアカウントが、指定したリソースタイプのみを共有できるようにする
- 組織または組織単位 (OU) との共有を禁止する
- 指定した IAM ユーザーおよびロールのみとの共有を許可する

外部共有の禁止

以下の SCP の例では、組織の一部ではない IAM ユーザーおよびロールとの共有を許可するリソース共有を、ユーザーが作成できないようにします。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:UpdateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "ram:RequestedAllowsExternalPrincipals": "true"
                }
            }
```

```
        }
    ]
}
```

特定のアカウントが、指定したリソースタイプのみを共有できるようにする

以下の SCP では、アカウント 111111111111 と 222222222222 が、プレフィックスリストを共有するリソース共有を作成し、プレフィックスリストを既存のリソース共有に関連付けることができます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OnlyNamedAccountsCanSharePrefixLists",
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalAccount": [
                        "111111111111",
                        "222222222222"
                    ]
                },
                "StringEquals": {
                    "ram:RequestedResourceType": "ec2:PrefixList"
                }
            }
        }
    ]
}
```

組織または組織単位 (OU) との共有を禁止する

次の SCP は、ユーザーが組織または OU とリソースを共有するリソース共有を作成することを防ぎます。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "ram:Principal": [
                        "arn:aws:organizations::*:organization/*",
                        "arn:aws:organizations::*:ou/*"
                    ]
                }
            }
        }
    ]
}
```

指定した IAM ユーザーおよびロールのみとの共有を許可する

以下の SCP の例では、ユーザーは組織 o-12345abcdef、組織単位 ou-98765fedcba、およびアカウント 111111111111 のみとリソースを共有できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "ram:Principal": [
                        "arn:aws:organizations::123456789012:organization/
o-12345abcdef",
                        "arn:aws:organizations::123456789012:ou/o-12345abcdef/
ou-98765fedcba",
```

```
                    "111111111111"
                ]
            }
        }
    }
]
}
```

Amazon Application Recovery Controller (ARC) の SCP 例

このカテゴリの例

- ユーザーが ARC ルーティング制御状態を更新できないようにする

ユーザーが ARC ルーティング制御状態を更新できないようにする

下位レベルの ARC オペレーターは、ダッシュボードをモニタリングして ARC 情報を確認する必要があります。ただし、上級オペレーターが許可されている可能性があるため AWS リージョン 、オペレーターはルーティングコントロールを更新して、アプリケーションをフェイルオーバーすることはできません。この SCP は、影響されたアカウントのユーザーまたはロールが、ARC ルーティング制御を更新する ARC 操作の実行を防止します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAll",
            "Effect": "Deny",
            "Action": [
                "route53-recovery-cluster:UpdateRoutingControlState",
                "route53-recovery-cluster:UpdateRoutingControlStates"
            ],
            "Resource": "*",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
```

```
    ]
}
```

Amazon S3 の SCP の例

> **Note**
>
> Amazon Simple Storage Service (Amazon S3) は、別の暗号化オプションを指定しない限り、新しいオブジェクトごとにサーバー側の暗号化 (SSE-S3) を自動的に適用します。詳細については、「Amazon S3 ユーザーガイド」の「Amazon S3 ですべての新しいオブジェクトが自動的に暗号化」を参照してください。

このカテゴリの例

- Amazon S3 の暗号化されていないオブジェクトのアップロードを禁止する

Amazon S3 の暗号化されていないオブジェクトのアップロードを禁止する

次のポリシーは、すべてのユーザーに対して、暗号化されていないオブジェクトを S3 バケットへのアップロードを制限します。

```
{
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "*",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption": "true"
    }
  }
}
```

次のポリシーは、すべてのユーザーに対して、暗号化されていないオブジェクトを S3 バケットにアップロードすることを制限し、バケットへのオブジェクトのアップロードに指定された暗号化タイプ (AES256 または aws:kms) を適用します。

```
[
  {
    "Effect": "Deny",
```

```
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "Null": {
        "s3:x-amz-server-side-encryption": "true"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": "AES256"
      }
    }
  }
]
```

リソースのタグ付けの SCP の例

このカテゴリの例

- 作成される特定のリソースにタグを要求する
- 許可されたプリンシパル以外のタグが変更されないようにする

作成される特定のリソースにタグを要求する

次の SCP では、リクエストに指定されたタグが含まれていない場合、影響を受けるアカウントの IAM ユーザーとロールが特定のリソースタイプを作成できないようにします。

> **Important**
>
> お客様の環境で使用するサービスを使用して、拒否ベースのポリシーを必ずテストしてください。以下の例は、タグ付けされていないシークレットを作成したり、タグ付けされていない Amazon EC2 インスタンスを実行したりする単純なブロックであり、例外は含まれていません。
>
> 次のポリシー例では、シークレットを作成し、2 つの個別のステップとしてタグ付けするため、記述 AWS CloudFormation されているように と互換性がありません。このポリシー例では、このようなアクションは、短時間でも、必要に応じてタグ付けされていないシークレッ

トに発生するため、スタックの一部としてシークレット AWS CloudFormation を作成することを実質的にブロックします。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCreateSecretWithNoProjectTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoProjectTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyCreateSecretWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    },
    {
```

```
      "Sid": "DenyRunInstanceWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    }
  ]
}
```

AWS Organizations SCPs「 のアクション、リソース、および条件キー AWS のサービス」を参照してください。

許可されたプリンシパル以外のタグが変更されないようにする

次の SCP では、ポリシーによって、許可されたプリンシパルのみがリソースにアタッチされたタグを変更できるようにする方法を示します。これは、 AWS クラウドセキュリティ戦略の一環として属性ベースのアクセスコントロール (ABAC) を使用する上で重要な部分です。このポリシーでは、発信者は、認可タグ (この例では access-project)がリクエストを行ったユーザーまたはロールに付けられた認可タグと完全に一致するリソースのみでタグを修正することができます。また、このポリシーでは、許可されたユーザーが、認可に使用されるタグの値を変更することを防ぎます。呼び出し元のプリンシパルが変更を行うには、認可タグが必要になります。

このポリシーは、権限のないユーザーによるタグの変更のみをブロックします。このポリシーでブロックされずに認可されたユーザーには、関連する API のタグ付けの際に Allow アクセス許可を明示的に付与する別の IAM ポリシーが必要です。例えば、ユーザーが管理者ポリシーで Allow */* (すべてのサービスとすべてのオペレーションを許可) を設定している場合、この組み合わせによって、管理者ユーザーは、ユーザーのプリンシパルにアタッチされた認可タグと一致する認可タグの値を含むタグのみの変更が許可されることになります。これは、このポリシーの明示的な Deny が、管理者ポリシーの明示的な Allow よりも優先されるためです。

> **Important**
>
> これはポリシーによる完全な解決策ではないため、ここで説明したとおりに使用することはできません。この例は、ABAC 戦略の一部を説明することを目的としているため、本番環境向けにカスタマイズし、テストする必要があります。

その仕組みの詳細な分析を含む完全なポリシーについては、「AWS Organizationsのサービスコントロールポリシーを使用して、認可に使用されるリソースのタグを保護する」を参照してください。
お客様の環境で使用するサービスを使用して、拒否ベースのポリシーを必ずテストしてください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "ec2:ResourceTag/access-project": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
```

```
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "access-project"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "aws:PrincipalTag/access-project": true
                }
            }
        }
    ]
}
```

Amazon Virtual Private Cloud (Amazon VPC) の SCP の例

このカテゴリの例

- ユーザーによる VPC フローログの削除を禁止する
- インターネットアクセスに接続されていない VPC を使用した取得を禁止する

ユーザーによる VPC フローログの削除を禁止する

この SCP では、影響を受けるアカウントのユーザーまたはロールは Amazon Elastic Compute Cloud (Amazon EC2) フローログ、CloudWatch ロググループまたはログストリームを削除できなくなります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteFlowLogs",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": "*"
    }
  ]
 }
```

インターネットアクセスに接続されていない VPC を使用した取得を禁止する

この SCP では、影響を受けるアカウントのユーザーまたはロールは、Amazon EC2 仮想プライベートクラウド (VPC) の設定を変更して、インターネットへの直接アクセスを許可しないようにします。既存の直接アクセスや、オンプレミスネットワーク環境を経由するアクセスはブロックされません。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:AttachInternetGateway",
        "ec2:CreateInternetGateway",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateVpcPeeringConnection",
        "ec2:AcceptVpcPeeringConnection",
        "globalaccelerator:Create*",
        "globalaccelerator:Update*"
      ],
```

```
      "Resource": "*"
    }
  ]
}
```

を使用したサービスコントロールポリシー (SCPsトラブルシューティング AWS Organizations

サービスコントロールポリシー (SCP) で検出された共通のエラーを診断して変更するために、この情報を使用します。

のサービスコントロールポリシー (SCPs) AWS Organizations は IAM ポリシーと似ており、共通の構文を共有します。この構文は、JavaScript Object Notation(JSON) のルールで始まります。JSON では、オブジェクトおよびオブジェクトを構成する名前と値のペアを指定します。IAM ポリシーの文法は、アクセス許可を付与するためにポリシーを使用する AWS のサービス に対して名前と値がどのような意味を持ち、どのように解釈されるかを定義するものです。

AWS Organizations は、IAM 構文と文法のサブセットを使用します。詳細については、「SCP 構文」を参照してください。

一般的なポリシーエラー

- 複数のポリシーオブジェクト
- 複数の Statement 要素
- ポリシードキュメントが最大サイズを超えています

複数のポリシーオブジェクト

SCP は、1 つの JSON オブジェクトのみで構成する必要があります。オブジェクトは括弧 ({ }) で囲んで示します。外側の { } のペア内に追加の { } を埋め込むことによって JSON オブジェクト内で他のオブジェクトをネストすることができますが、ポリシーに含めることができるのは一番外側の { } のペアのみです。次の例は、最上位に 2 つのオブジェクト (#で示した箇所) が含まれているため、誤りです。

JSON

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

```
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

ただし、正しいポリシーの文法を使用して、前述の例の目的を果たすことができます。それぞれに独自の Statement 要素を含む 2 つのポリシーオブジェクトを含める代わりに、1 つの Statement 要素に 2 つのブロックを組み合わせて使用することができます。Statement 要素には、次の例に示すように 2 つのオブジェクトの配列を値として指定します。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

この例では、2 つの要素による効果は異なるため、1 つの要素を含む Statement に圧縮することはできません。構文は、各構文の Effect や、Resource 要素が同一の場合にのみ、組み合わせることができます。

複数の Statement 要素

このエラーは、一見、前のセクションのエラーのバリエーションのように見えますが、構文上はエラーの種類が異なります。次の例では、最上位の 1 ペアの { } で示された 1 つのポリシーオブジェクトのみが存在します。そのオブジェクト内に 2 つの Statement 要素が含まれています。

SCP には、名前 (Statement) の後にコロン、その後に値という形式で構成される 1 つの Statement 要素のみを指定する必要があります。Statement 要素の値は、{} で示され、1 つの Effect 要素、1 つの Action 要素、および 1 つの Resource 要素を含むオブジェクトである必要があります。次の例は、ポリシーオブジェクトに 2 つの Statement 要素が含まれているため、誤りです。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

値オブジェクトは複数の値オブジェクトの配列にすることができるため、次の例に示すように、2 つの Statement 要素を組み合わせて 1 つの要素にすることで、この問題を解決できます。

JSON

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

```
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":"*"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

Statement 要素の値はオブジェクト配列です。例の配列は 2 つのオブジェクトで構成され、各オブジェクトに Statement 要素の正しい値が指定されています。配列内の各オブジェクトはカンマで区切ります。

ポリシードキュメントが最大サイズを超えています

SCP ドキュメントの最大サイズは 5,120 文字です。この最大サイズには、空白を含むすべての文字が含まれます。SCP のサイズを減らすには、引用符の外側にあるすべての空白文字 (スペースや改行など) を削除できます。

> **Note**
>
> を使用してポリシーを保存すると AWS Management Console、JSON 要素と引用符の外側の間の余分な空白は削除され、カウントされません。SDK オペレーションまたは を使用してポリシーを保存すると AWS CLI、指定したとおりにポリシーが保存され、文字の自動削除は行われません。

リソースコントロールポリシー (RCPs)

> **Note**
>
> サービスコントロールポリシー (SCPsとリソースコントロールポリシー (RCPs)
> 組織のメンバーアカウント内の IAM プリンシパルのアクセス許可を制限する必要がある場合は、SCP を使用します。
> 組織のメンバーアカウント内のリソースへのアクセスをリクエストする組織アカウントの外部にある IAM プリンシパルを制限する必要がある場合は、RCP を使用します。

詳細については、SCPs と RCPs」を参照してください。

リソースコントロールポリシー (RCPsは、組織内のアクセス許可を管理するために使用できる組織ポリシーの一種です。RCP では、組織のすべてのリソースで使用可能な最大アクセス許可を一元的に制御できます。RCPs、アカウントのリソースが組織のアクセスコントロールガイドラインの範囲内に収まるようにするのに役立ちます。RCPsは、すべての機能が有効になっている組織でのみ使用できます。組織が一括請求機能のみを有効にしている場合、RCPs は使用できません。RCPs「」を参照してくださいポリシータイプの有効化。

RCPsだけでは、組織内のリソースにアクセス許可を付与するには不十分です。RCP によってアクセス許可は付与されません。RCP は、ID が組織内のリソースに対して実行できるアクションに対するアクセス許可ガードレールを定義するか、制限を設定します。管理者は、実際にアクセス許可を付与するために、IAM ユーザーまたはロールにアイデンティティベースのポリシーをアタッチするか、アカウント内のリソースにリソースベースのポリシーをアタッチする必要があります。詳細については、「IAM ユーザーガイド」の「アイデンティティベースおよびリソースベースのポリシー」を参照してください。

有効なアクセス許可は、RCPs とサービスコントロールポリシー (SCPs) で許可されているものと、アイデンティティベースおよびリソースベースのポリシーで許可されているものとの間の論理的な共通部分です。

⚠ RCPs管理アカウントのリソースには影響しません

RCPs管理アカウントのリソースには影響しません。これらは、組織内のメンバーアカウント内のリソースにのみ影響します。つまり、RCPsは委任管理者として指定されたメンバーアカウントにも適用されます。

このページのトピック

- RCPs AWS のサービス をサポートする のリスト
- RCPs の効果のテスト
- RCPs の最大サイズ
- 組織内のさまざまなレベルに RCPs をアタッチする
- アクセス許可に対する RCP の影響
- RCPs によって制限されていないリソースとエンティティ

- RCP 評価
- RCP 構文
- リソースコントロールポリシーの例

RCPs AWS のサービス をサポートする のリスト

RCPs、以下のアクションに適用されます AWS のサービス。

- Amazon S3
- AWS Security Token Service
- AWS Key Management Service
- Amazon SQS
- AWS Secrets Manager
- Amazon Elastic Container Registry
- Amazon OpenSearch Serverless

RCPs の効果のテスト

AWS では、ポリシーがアカウントのリソースに与える影響を徹底的にテストすることなく、RCPs を組織のルートにアタッチしないことを強くお勧めします。まず、個々のテストアカウントに RCPs をアタッチし、階層の下位の OUs に移動してから、必要に応じて組織構造を進めます。影響を判断する 1 つの方法は、アクセス拒否エラーの AWS CloudTrail ログを確認することです。

RCPs の最大サイズ

RCP 内のすべての文字は、その最大サイズに対してカウントされます。このガイドの例では、読みやすさを向上させるために余分な空白でフォーマットされた RCPs を示しています。ただし、ポリシーサイズが上限サイズに近づいている場合は、スペースを節約するために、引用符の外側にあるすべての空白文字 (スペースや改行など) を削除できます。

> **Tip**
>
> ビジュアルエディタを使用して RCP を構築します。これによって、よけいな空白が自動的に削除されます。

組織内のさまざまなレベルに RCPs をアタッチする

RCPs、個々のアカウント、OUs、または組織のルートに直接アタッチできます。RCPs「」を参照してくださいRCP 評価。

アクセス許可に対する RCP の影響

RCPsは AWS Identity and Access Management (IAM) ポリシーの一種です。これらは、リソースベースのポリシーと最も密接に関連しています。ただし、RCP がアクセス許可を付与することはありません。代わりに、RCPsは、組織内のリソースに対して使用可能なアクセス許可の最大数を指定するアクセスコントロールです。詳細については、「 IAM ユーザーガイド」の「ポリシーの評価論理」を参照してください。

- RCPs、 のサブセットのリソースに適用されます AWS のサービス。詳細については、「RCPs AWS のサービス をサポートする のリスト」を参照してください。
- RCP は、RCP をアタッチした組織の一部であるアカウントによって管理されるリソースにのみ影響します。 RCPs これらは、組織外のアカウントのリソースには影響しません。たとえば、組織内のアカウント A が所有する Amazon S3 バケットを考えてみましょう。バケットポリシー (リソースベースのポリシー) は、組織外のアカウント B のユーザーにアクセス権を付与します。アカウント A には RCP がアタッチされています。この RCP は、アカウント B のユーザーがアクセスした場合でも、アカウント A の S3 バケットに適用されます。ただし、アカウント A のユーザーがアクセスしたアカウント B のリソースには適用されません。
- RCP は、メンバーアカウントのリソースのアクセス許可を制限します。アカウントのリソースには、その上のすべての親が許可するアクセス許可のみがあります。アクセス許可がアカウントの上の任意のレベルでブロックされている場合、リソース所有者が任意のユーザーにフルアクセスを許可するリソースベースのポリシーをアタッチしても、影響を受けるアカウントのリソースにはそのアクセス許可がありません。
- RCPsは、オペレーションリクエストの一部として承認されたリソースに適用されます。これらのリソースは、サービス認可リファレンスのアクションテーブルの「リソースタイプ」列にあります。リソースが「リソースタイプRCPs が適用されます。たとえば、 はオブジェクトリソース`s3:GetObject`を承認します。`GetObject` リクエストが行われるたびに、該当する RCP を適用して、リクエスト元のプリンシパルが`GetObject`オペレーションを呼び出すことができるかどうかを判断します。該当する RCP は、アカウント、組織単位 (OU)、またはアクセスされるリソースを所有する組織のルートにアタッチされた RCP です。
- RCPs、組織のメンバーアカウント内のリソースにのみ影響します。管理アカウントのリソースには影響しません。つまり、RCPsは委任管理者として指定されたメンバーアカウントにも適用されます。詳細については、「管理アカウントのベストプラクティス」を参照してください。

- プリンシパルが RCP がアタッチされたアカウント内のリソース (該当する RCP を持つリソース) へのアクセスをリクエストすると、RCP はポリシー評価ロジックに含まれ、プリンシパルがアクセスを許可または拒否されているかどうかを判断します。
- RCPsは、プリンシパルが同じ組織に属しているかどうかにかかわらず、該当する RCP を持つメンバーアカウントのリソースにアクセスしようとするプリンシパルの有効なアクセス許可に影響します。これにはルートユーザーが含まれます。例外は、プリンシパルがサービスにリンクされたロールである場合です。これはRCPs がサービスにリンクされたロールによって行われた呼び出しに適用されないためです。サービスにリンクされたロールにより AWS のサービス 、 はユーザーに代わって必要なアクションを実行でき、RCPs によって制限することはできません。
- ユーザーとロールには、アイデンティティベースのポリシーやリソースベースのポリシーなど、適切な IAM アクセス許可ポリシーを持つアクセス許可が付与されている必要があります。IAM アクセス許可ポリシーのないユーザーまたはロールは、該当する RCP がすべてのサービス、すべてのアクション、およびすべてのリソースを許可している場合でも、アクセスできません。

RCPs によって制限されていないリソースとエンティティ

RCPs を使用して以下を制限することはできません。

- 管理アカウントのリソースに対するアクション。
- RCPs、サービスにリンクされたロールの有効なアクセス許可には影響しません。サービスにリンクされたロールは、 AWS サービスに直接リンクされた一意のタイプの IAM ロールであり、サービスがユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれます。サービスにリンクされたロールのアクセス許可を RCPs で制限することはできません。RCP は AWS 、サービスにリンクされたロールを引き受けるサービスの能力にも影響しません。つまり、サービスにリンクされたロールの信頼ポリシーも RCPsの影響を受けません。
- RCPsは AWS マネージドキー for AWS Key Management Serviceには適用されません。 AWS マネージドキー はユーザーに代わって によって作成、管理、使用されます AWS のサービス。アクセス許可を変更または管理することはできません。
- RCPs次のアクセス許可には影響しません。

サービス	API	RCPs によって承認されていないリソース
AWS Key Management Service	`kms:RetireGrant`	RCPsアクセス`kms:RetireGrant` 許可には影響しません。へのアクセス許

サービス	API	RCPs によって承認されていないリソース
		可kms:RetireGrant の決定方法の詳細については、「 デベロッパーガイド」の「許可の廃止と取り消し」を参照してください。 AWS KMS

RCP 評価

> **Note**
>
> このセクションの情報は、バックアップポリシー、タグポリシー、チャットアプリケーションポリシー、AI サービスのオプトアウトポリシーなどの管理ポリシータイプには適用されません。詳細については、「管理ポリシーの継承を理解する」を参照してください。

のさまざまなレベルで複数のリソースコントロールポリシー (RCPs) をアタッチできるため AWS Organizations、RCPs の評価方法を理解することで、適切な結果をもたらす RCPs。

RCPsを使用するための戦略

RCPFullAWSAccess ポリシーは AWS マネージドポリシーです。リソースコントロールポリシー (RCPs。このポリシーをデタッチすることはできません。このデフォルトの RCP では、すべてのプリンシパルとアクションのアクセスが RCP 評価を通過できます。つまり、RCPs の作成とアタッチを開始するまで、既存のすべての IAM アクセス許可はそのまま動作し続けます。この AWS 管理ポリシーはアクセスを許可しません。

Deny ステートメントを使用して、組織内のリソースへのアクセスをブロックできます。特定のアカウントのリソースに対するアクセス許可を拒否するには、ルートからアカウント (ターゲットアカウント自体を含む) への直接パス内の各 OU までの RCP がそのアクセス許可を拒否できます。

Deny ステートメントは、組織のより広範な部分に対して適用される制限を実装する強力な方法です。たとえば、組織外の ID がリソースルートレベルにアクセスできないようにポリシーをアタッチできます。これは、組織内のすべてのアカウントに対して有効です。 では、ポリシーがアカウント

のリソースに与える影響を徹底的にテストすることなくRCPs を組織のルートにアタッチしないことを AWS 強くお勧めします。詳細については、「RCPs の効果のテスト」を参照してください。

図 1 では、特定のサービスに明示的なDenyステートメントが指定されている RCP が本番稼働用 OU にアタッチされています。その結果、組織内のどのレベルにも適用された拒否ポリシーが、その下にあるすべての OU とメンバーアカウントに対して評価されるため、アカウント A とアカウント B の両方がサービスへのアクセスを拒否されます。

図 1: Production OU にアタッチされた*Deny*ステートメントと、アカウント A とアカウント B への影響を含む組織構造の例

RCP 構文

リソースコントロールポリシー (RCPs、リソースベースのポリシーで使用される構文と同様の構文を使用します。IAM ポリシーの詳細とその構文については、IAM ユーザーガイドの「IAM ポリシーの概要」を参照してください。

RCP は JSON のルールに従って構造化されます。このトピックで説明されている要素を使用します。

> **Note**
>
> RCP 内のすべての文字は、その最大サイズに対してカウントされます。このガイドの例では、読みやすさを向上させるために余分な空白でフォーマットされた RCPs を示しています。ただし、ポリシーサイズが上限サイズに近づいている場合は、スペースを節約するために、引用符の外側にあるすべての空白文字 (スペースや改行など) を削除できます。

RCPs「」を参照してくださいリソースコントロールポリシー (RCPs)。

要素の概要

次の表は、RCPs。

> **Note**
>
> の効果**Allow**は、 **RCPFullAWSAccess**ポリシーでのみサポートされます。
> の効果Allowは、 RCPFullAWSAccessポリシーでのみサポートされています。このポリシーは、リソースコントロールポリシー (RCPs。このポリシーをデタッチすることはできません。このデフォルトの RCP では、すべてのプリンシパルとアクションのアクセスが RCP

評価を通過できます。つまり、RCPs の作成とアタッチを開始するまで、既存の IAM アクセス許可はすべてそのまま動作し続けます。これにより、アクセスは許可されません。

要素	目的	
Version	ポリシーの処理に使用する言語構文ルールを指定します。	
Statement	ポリシー要素のコンテナとして機能します。RCPs には複数のステートメントを含めることができます。	
Statement ID (Sid)	(オプション) ステートメントにわかりやすい名前を付けます。	
[Effect] (効果)	RCP ステートメントがアカウントのリソースへのアクセスを拒否するかどうかを定義します。	
プリンシパル	アカウントのリソースへのアクセスを許可または拒否するプリンシパルを指定します。	
アクション	RCP が許可または拒否する AWS	

要素	目的
	サービスとアクションを指定します。
[リソース]	RCP が適用される AWS リソースを指定します。
NotResource	RCP から除外される AWS リソースを指定します。Resource 要素の代わりに使用します。
条件	ステートメントを実行するタイミングの条件を指定します。

トピック

- Version 要素
- Statement 要素
- ステートメント ID (Sid) 要素
- Effect 要素
- Principal 要素
- Action 要素
- Resource および NotResource 要素
- Condition 要素
- サポートされていない要素

Version 要素

すべての RCP には、値 を持つ Version要素を含める必要があります"2012-10-17"。これは、IAM アクセス許可ポリシーの最新バージョンと同じバージョンの値です。

```
    "Version": "2012-10-17",
```

詳細については、IAM ユーザーガイドの「IAM JSON ポリシー要素: Version」を参照してください。

Statement 要素

RCP は 1 つ以上のStatement要素で構成されます。ポリシーには Statement キーワードを 1 つだけ含めることができますが、値は、ステートメントの JSON 配列 ([ ] の文字で囲まれる) もあります。

次の例は、単一の 、Effect、Principal、Actionおよび Resource要素で構成される単一のステートメントを示しています。

```
 {
    "Statement": {
        "Effect": "Deny",
        "Principal": "*",
        "Action": "*",
        "Resource": "*"
    }
}
```

詳細については、IAM ユーザーガイドの「IAM JSON ポリシー要素: Statement」を参照してください。

ステートメント ID (**Sid**) 要素

Sid は、ポリシーステートメントに提供するオプションの識別子です。Sid 値は、ステートメント配列内の各ステートメントに割り当てることができます。次の RCP の例は、サンプルSidステートメントを示しています。

```
{
    "Statement": {
        "Sid": "DenyAllActions",
        "Effect": "Deny",
        "Principal": "*",
```

```
        "Action": "*",
        "Resource": "*"
    }
}
```

詳細については、IAM ユーザーガイドの「IAM JSON ポリシーエレメント: Sid」を参照してください。

`Effect` 要素

各ステートメントには必ず `Effect` を 1 つ含める必要があります。`Effect` 要素`Deny`で の値を使用すると、特定のリソースへのアクセスを制限したりRCPs が有効になるタイミングの条件を定義したりできます。作成する RCPs の場合、値は である必要がありますDeny。詳細については、「IAM ユーザーガイド」のRCP 評価「」および「IAM JSON ポリシーエレメント: 効果」を参照してください。 https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_effect.html

`Principal` 要素

各ステートメントには `Principal`要素が含まれている必要があります。RCP の `Principal`要素でのみ`*`「」を指定できます。`Conditions` 要素を使用して、特定のプリンシパルを制限します。

詳細については、IAM ユーザーガイドの「IAM JSON ポリシーエレメント: プリンシパル」を参照してください。

`Action` 要素

各ステートメントには `Action`要素が含まれている必要があります。

`Action` 要素の値は、ステートメントによって許可または拒否される AWS サービスとアクションを識別する文字列の文字列またはリスト (JSON 配列) です。

各文字列は、すべての小文字のサービスの略語 (「s3」、「sqs」、「sts」など) で構成され、その後にコロンが続き、そのサービスのアクションが続きます。通常、すべて大文字と小文字で始まる各単語で入力されます。例: `"s3:ListAllMyBuckets"`。

RCP では、アスタリスク (*) や疑問符 (?) などのワイルドカード文字を使用することもできます。

- 名前の一部を共有する複数のアクションを検索するには、アスタリスクをワイルドカードとして使用します。値 `"s3:*"` は、Amazon S3 サービス内のすべてのアクションを意味します。値は、「Get」で始まる AWS STS アクションのみ`"sts:Get*"`に一致します。
- 単一の文字を検索する場合は疑問符 (?) を使用します。

> **Note**
>
> ワイルドカード (*) と疑問符 (?) は、アクション名の任意の場所で使用できます。
> SCPs とは異なり、アクション名の任意の場所でアスタリスク (*) や疑問符 (?) などのワイルドカード文字を使用できます。

RCPs「」を参照してくださいRCPs AWS のサービス をサポートする のリスト。が AWS のサービス サポートするアクションのリストについては、「サービス認可リファレンス」のAWS 「 サービスのアクション、リソース、および条件キー」を参照してください。

詳細については、IAM ユーザーガイドの「IAM JSON ポリシーの要素: Action」を参照してください。

`Resource` および `NotResource` 要素

各ステートメントには、 `Resource`または `NotResource`要素が含まれている必要があります。

リソース要素では、アスタリスク (*) や疑問符 (?) などのワイルドカード文字を使用できます。

- 名前の一部を共有する複数のリソースを照合するには、ワイルドカードとしてアスタリスク (*) を使用します。
- 単一の文字を検索する場合は疑問符 (?) を使用します。

詳細については、IAM ユーザーガイドの「IAM JSON ポリシーエレメント: リソース」および「IAM JSON ポリシーエレメント: NotResource」を参照してください。

`Condition` 要素

RCP の拒否ステートメントで`Condition`要素を指定できます。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
```

```
            "Action": "s3:*",
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

この RCP は、リクエストが安全なトランスポート経由で発生した (リクエストが TLS 経由で送信された) 場合を除き、Amazon S3 オペレーションとリソースへのアクセスを拒否します。

詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素: 条件」を参照してください。

サポートされていない要素

RCPs では、次の要素はサポートされていません。

- `NotPrincipal`
- `NotAction`

リソースコントロールポリシーの例

このトピックに表示されるリソースコントロールポリシー (RCPs) の例は、情報提供のみを目的としています。データ境界の例については、GitHub のデータ境界ポリシーの例を参照してください。

> **これらの例を使用する前に**
>
> 組織でこれらの RCPsの例を使用する前に、次の操作を行います。
>
> - RCPs を慎重に確認し、固有の要件に合わせてカスタマイズします。
> - 使用する AWS サービスを使用して、環境内の RCPs を徹底的にテストします。
>
> このセクションのポリシー例は、RCPs の実装と使用を示しています。これらの例は、公式な AWS 推奨事項やベストプラクティスとして解釈されることを意図したものではありません。環境のビジネス要件を解決するために、ポリシーの適合性を慎重にテストするのはお客

様の責任です。拒否ベースのリソースコントロールポリシーは、ポリシーに必要な例外を追加しない限り、 AWS サービスの使用を意図せずに制限またはブロックする可能性があります。

一般的な例

トピック

- RCPFullAWSAccess
- サービス間の混乱した代理保護
- リソースへの HTTPS 接続のみへのアクセスを制限する
- Amazon S3 バケットポリシーの一貫したコントロール

RCPFullAWSAccess

次のポリシーは AWS マネージドポリシーであり、リソースコントロールポリシー (RCPs。このポリシーをデタッチすることはできません。このデフォルトの RCP では、すべてのプリンシパルとアクションが リソースにアクセスできます。つまり、RCPs の作成とアタッチを開始するまで、既存の IAM アクセス許可はすべてそのまま動作し続けます。このポリシーの効果をテストする必要はありません。既存の認可動作を リソースで継続できるためです。

JSON

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

サービス間の混乱した代理保護

一部の AWS のサービス（呼び出しサービス) は、プリン AWS のサービス シパルを使用して他の AWS のサービス（呼び出しサービス) から AWS リソースにアクセスします。アクターが AWS リソースへのアクセスを意図していない場合、プリン AWS のサービス シパルの信頼を使用して、アクセスを意図していないリソースとやり取りしようとすると、サービス間の混乱した代理問題と呼ばれます。詳細については、IAM ユーザーガイドの「混乱した代理問題」を参照してください。

次のポリシーでは、リソースにアクセスする AWS のサービス プリンシパルは、組織からのリクエストに代わってのみアクセスする必要があります。このポリシーは、 aws:SourceAccountが存在するリクエストにのみコントロールを適用し、 の使用を必要としないサービス統合aws:SourceAccountが影響を受けないようにします。aws:SourceAccount がリクエストコンテキストに存在する場合、Null条件は に評価されtrue、aws:SourceOrgIDキーが適用されます。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceConfusedDeputyProtection",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "s3:*",
                "sqs:*",
                "kms:*",
                "secretsmanager:*",
                "sts:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceOrgID": "my-org-id",
                    "aws:SourceAccount": [
                        "third-party-account-a",
                        "third-party-account-b"
                    ]
                },
                "Bool": {
```

```
                    "aws:PrincipalIsAWSService": "true"
                },
                 "Null": {
                    "aws:SourceArn": "false"
                }
            }
        }
    ]
}
```

リソースへの HTTPS 接続のみへのアクセスを制限する

次のポリシーでは、HTTPS (TLS) 経由の暗号化された接続でのみリソースにアクセスする必要があります。これにより、潜在的な攻撃者がネットワークトラフィックを操作するのを防ぐことができます。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceSecureTransport",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "sts:*",
                "s3:*",
                "sqs:*",
                "secretsmanager:*",
                "kms:*"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

Amazon S3 バケットポリシーの一貫したコントロール

次の RCP には、組織内の Amazon S3 バケットに一貫したアクセスコントロールを適用するための複数のステートメントが含まれています。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceS3TlsVersion",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition": {
                "NumericLessThan": {
                    "s3:TlsVersion": [
                        "1.2"
                    ]
                }
            }
        },
        {
            "Sid": "EnforceKMSEncryption",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "s3:x-amz-server-side-encryption-aws-kms-key-id": "true"
                }
            }
        }
    ]
}
```

- ステートメント ID `EnforceS3TlsVersion` – S3 バケットにアクセスするには、TLS バージョン 1.2 以上が必要です。

- ステートメント ID `EnforceKMSEncryption` – オブジェクトは KMS キーでサーバー側で暗号化する必要があります。

の管理ポリシー AWS Organizations

管理ポリシーを使用すると、 AWS のサービス とその機能を一元的に設定および管理できます。ポリシーが OU とそれを継承するアカウントに与える影響は、 AWS Organizationsに適用した管理ポリシーの種類によって異なります。管理ポリシーに関連する用語や概念を理解するには、このセクションのトピックを確認してください。

トピック

- の管理ポリシーの前提条件とアクセス許可 AWS Organizations
- 管理ポリシーの継承を理解する
- 効果的な管理ポリシーの表示
- 無効な有効なポリシーアラートについて
- 宣言ポリシー
- バックアップポリシー
- タグポリシー
- チャットアプリケーションポリシー
- AI サービスのオプトアウトポリシー
- Security Hub ポリシー

の管理ポリシーの前提条件とアクセス許可 AWS Organizations

このページでは、 AWS Organizationsのポリシーを管理するための前提条件と必要なアクセス許可について説明します。

トピック

- 管理ポリシーの前提条件
- 管理ポリシーのアクセス許可

管理ポリシーの前提条件

組織内のポリシーを管理するには、次のことが必要です。

- 組織で、すべての機能が有効になっている必要があります。
- 組織の管理アカウントにサインインしているか、委任された管理者である必要があります。
- （ AWS Identity and Access Management IAM) ユーザーまたはロールには、次のセクションに記載されているアクセス許可が必要です。

管理ポリシーのアクセス許可

次のサンプル IAM ポリシーは、組織内の管理ポリシーを全面的に使用するためのアクセス許可を提供します。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OrganizationPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeAccount",
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:DetachPolicy",
                "organizations:DisableAWSServiceAccess",
                "organizations:DisablePolicyType",
                "organizations:EnableAWSServiceAccess",
                "organizations:EnablePolicyType",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListCreateAccountStatus",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
```

```
                "organizations:ListRoots",
                "organizations:ListTargetsForPolicy",
                "organizations:UpdatePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

IAM ポリシーおよび許可の詳細については、IAM ユーザーガイドを参照してください。

管理ポリシーの継承を理解する

> **Important**
>
> このセクションの情報は、サービスコントロールポリシー (SCPs) とリソースコントロールポリシー (RCPs認可ポリシーには適用されません。SCPsRCPs「」を参照してくださいRCP 評価。 AWS Organizations SCP 評価

組織内の組織エンティティ (組織ルート、組織単位 (OU)、またはアカウント) に管理ポリシーをアタッチできます。

- 管理ポリシーを組織ルートにアタッチすると、組織内のすべての OU およびアカウントがそのポリシーを継承します。
- 特定の OU に管理ポリシーをアタッチすると、その OU または子 OU の直下にあるアカウントがポリシーを継承します。
- 特定のアカウントに管理ポリシーをアタッチすると、そのアカウントにのみ影響します。

組織内の複数のレベルに管理ポリシーをアタッチできるため、アカウントは複数のポリシーを継承できます。

次のトピックでは、親ポリシーと子ポリシーがアカウントの有効なポリシーにどのように処理されるかを説明します。

トピック

- 継承用語
- 管理ポリシータイプのポリシー構文と継承

- 継承演算子
- 継承の例

継承用語

このトピックでは、管理ポリシーの継承について説明するときに、次の用語を使用します。

ポリシーの継承

組織の最上位ルートから、組織単位 (OU) 階層、個々のアカウントへと移行する、組織のさまざまなレベルでのポリシーの相互作用です。

ポリシーは、組織ルート、OU、個々のアカウント、およびこれらの組織エンティティの任意の組み合わせにアタッチできます。ポリシーの継承とは、組織ルートまたは OU にアタッチされた管理ポリシーを指します。管理ポリシーがアタッチされている組織ルートまたは OU のメンバーであるすべてのアカウントは、そのポリシーを継承します。

例えば、管理ポリシーを組織ルートにアタッチすると、組織内のすべてのアカウントがそのポリシーを継承します。これは、組織内のすべてのアカウントが常に組織ルートの下にあるためです。特定の OU にポリシーをアタッチすると、その OU または子 OU の直下にあるアカウントがそのポリシーを継承します。組織内の複数のレベルにポリシーをアタッチできるため、アカウントは 1 つのポリシータイプに対して複数のポリシードキュメントを継承する場合があります。

親ポリシー

組織ツリーで下位のエンティティにアタッチされているポリシーよりも上位にアタッチされているポリシー。

例えば、管理ポリシー A を組織ルートにアタッチすると、それは単なるポリシーです。ここでポリシー B を そのルートの下にある OU にアタッチすると、ポリシー A はポリシー B の親ポリシーとなり、ポリシー B はポリシー A の子ポリシーとなります。ポリシー A とポリシー B がマージされ、OU のアカウントの有効なタグポリシーになります。

子ポリシー

組織ツリーで親ポリシーよりも下位レベルでアタッチされているポリシー。

有効なポリシー

アカウントに適用されるルールを指定する、最終的な 1 つのポリシードキュメント。有効なポリシーは、アカウントが継承するすべてのポリシーと、アカウントに直接アタッチされたポリシー

が集約されたものです。詳細については、「効果的な管理ポリシーの表示」を参照してください。

継承演算子

継承されたポリシーを 1 つの有効なポリシーにマージする方法を制御する演算子。これらの演算子は、アドバンスト機能とみなされます。経験豊富なポリシー作成者は、ポリシーを使用して、子ポリシーがどのような変更を行うことができるか、ポリシーの設定がどのようにマージされるかを制限できます。詳細については、「継承演算子」を参照してください。

管理ポリシータイプのポリシー構文と継承

ポリシーが OU とそれを継承するアカウントに与える影響は、選択した管理ポリシーの種類によって異なります。管理ポリシーには、次のタイプがあります。

- 宣言ポリシー
- バックアップポリシー
- タグポリシー
- チャットアプリケーションポリシー
- AI サービスのオプトアウトポリシー

この管理ポリシータイプの構文には、継承演算子 が含まれています。継承演算子を使用すると、適用する親ポリシーの要素や、子 OU とアカウントが継承する際に上書きまたは変更できる要素を細かく指定できます。

有効なポリシーは、組織ルートと OU から継承されるルールのセットと、アカウントに直接アタッチされたルールのセットです。有効なポリシーは、アカウントに適用される最終的なルールセットを指定します。適用されたポリシー内のすべての継承演算子の効果を含む、アカウントの有効なポリシーを表示できます。詳細については、「効果的な管理ポリシーの表示」を参照してください。

継承演算子

継承演算子は、アカウントの有効なポリシーが作成される際に、継承されたポリシーとアカウントポリシーがどのようにマージされるかを制御します。これらの演算子には、値設定演算子と子制御演算子が含まれます。

AWS Organizations コンソールでビジュアルエディタを使用する場合は、 `@@assign`演算子のみを使用できます。他の演算子は、アドバンスト機能とみなされます。他の演算子を使用するには、JSON ポリシーを手動で作成する必要があります。経験豊富なポリシーの作成者は、継承演算子

を使用して、有効なポリシーに適用するタグ値を制御し、子ポリシーがどのような変更を行うことができるかを制限できます。

組織でのポリシー継承の仕組みについては、「」を参照してください継承の例。

値設定演算子

次の値設定演算子を使用して、ポリシーと親ポリシーとの相互作用を制御できます。

- `@@assign` - 継承されたポリシー設定を指定した設定で上書きします。指定した設定が継承されていない場合、この演算子はその設定を有効なポリシーに追加します。この演算子は、任意のタイプのポリシー設定に適用できます。
  - 単一値の設定の場合、この演算子は、継承された値を指定された値に置き換えます。
  - 複数値設定 (JSON 配列) の場合、この演算子は、継承された値をすべて削除し、このポリシーで指定された値に置き換えます。
- `@@append` - 継承された設定に、指定した設定を (一切削除せずに) 追加します。指定した設定が継承されていない場合、この演算子はその設定を有効なポリシーに追加します。この演算子は、複数値の設定でのみ使用できます。
  - この演算子は、指定された値を継承された配列内の任意の値に追加します。
- `@@remove` - 継承された指定の設定を有効なポリシーから削除します (存在する場合)。この演算子は、複数値の設定でのみ使用できます。
  - この演算子は、親ポリシーから継承された値の配列から、指定された値のみを削除します。他の値は配列内に引き続き存在することができ、子ポリシーによって継承できます。

子制御演算子

制御演算子の使用はオプションです。`@@operators_allowed_for_child_policies` 演算子を使用して、子ポリシーで使用できる値設定演算子を制御できます。すべての演算子、一部の演算子を許可するか、または演算子を一切許可しないという選択肢があります。デフォルトでは、すべての演算子 (`@@all`) が許可されます。

- `"@@operators_allowed_for_child_policies": ["@@all"]` - 子 OU とアカウントは、ポリシーの任意の演算子を使用できます。デフォルトでは、子ポリシーですべての演算子が許可されます。
- `"@@operators_allowed_for_child_policies": ["@@assign", "@@append", "@@remove"]` - 子 OU とアカウントは、子ポリシーで指定された演算子のみを使用できます。この子制御演算子では、1 つ以上の値設定演算子を指定できます。

- `"@@operators_allowed_for_child_policies": ["@@none"]` - 子 OU とアカウントは、ポリシーの演算子を使用できません。この演算子を使用して、子ポリシーがこれらの値を追加、付加、または削除できないように、親ポリシーで定義されている値で効果的にロックできます。

> **Note**
>
> 継承された子制御演算子によって演算子の使用が制限されている場合、子ポリシーでそのルールを元に戻すことはできません。親ポリシーに子制御演算子を含めると、すべての子ポリシーの値設定演算子が制限されます。

継承の例

これらの例は、親タグポリシーと子タグポリシーがマージされてアカウントの有効なタグポリシーになるのを示すことにより、ポリシーの継承がどのように機能するかを示しています。

この例では、次の図に示す組織構造があることを前提としています。

例

- 例 1: 子ポリシーによるタグ値のみの上書きを許可する
- 例 2: 継承されたタグに新しい値を追加する
- 例 3: 継承されたタグから値を削除する
- 例 4: 子ポリシーへの変更を制限する
- 例 5: 子制御演算子との競合
- 例 6: 同じ階層レベルで値を追加した場合の競合

例 1: 子ポリシーによるタグ値のみの上書きを許可する

次のタグポリシーは、`CostCenter` タグキーと 2 つの許容値 (`Development` および `Support`) を定義します。組織ルートにアタッチすると、タグポリシーは組織内のすべてのアカウントで有効になります。

ポリシー A - 組織ルートのタグポリシー

```
{
```

```
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

OU1 のユーザーにキーに別のタグ値を使用してもらい、特定のリソースタイプに対してタグポリシーを適用するようにしたいとします。ポリシー A では、許可される子制御演算子が指定されていないため、すべての演算子が許可されます。@@assign 演算子を使用して、次のようなタグポリシーを作成し、OU1 にアタッチできます。

ポリシー B - OU1 タグポリシー

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Sandbox"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

タグの @@assign 演算子を指定すると、ポリシー A とポリシー B が統合されてアカウントの有効なタグポリシーが形成された場合に、以下のようになります。

- ポリシー B は、親ポリシーであるポリシー A で指定された 2 つのタグ値を上書きします。その結果、Sandbox は、CostCenter タグキーの準拠値のみとなります。
- enforced_for を追加することで、すべての Amazon Redshift リソースと Amazon DynamoDB テーブルで、指定されたタグ値として CostCenter タグを使用する必要があることが指定されます。

図に示すように、OU1 には 2 つのアカウント (111111111111 と 222222222222) が含まれています。

アカウント 111111111111 および 222222222222 に対して有効な、結果として生じるタグポリシー

> **Note**
>
> 表示された有効なポリシーの内容を、新しいポリシーの内容として直接使用することはできません。構文には、他の子ポリシーと親ポリシーのマージを制御するために必要な演算子は含まれていません。有効なポリシーの表示は、マージの結果を把握することのみを目的としています。

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Sandbox"
            ],
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

例 2: 継承されたタグに新しい値を追加する

組織内のすべてのアカウントで、許容値の短いリストでタグキーを指定する必要がある場合が考えられます。1 つの OU のアカウントでは、リソースの作成時にそれらのアカウントのみが指定できる追加の値を許可することをおすすめします。この例では、@@append 演算子を使用してその方法を指定します。@@append 演算子はアドバンスト機能です。

例 1 と同様、この例も組織ルートのタグポリシーのポリシー A から始まります。

ポリシー A - 組織ルートのタグポリシー

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

この例では、ポリシー C を OU2 にアタッチします。この例の違いは、ポリシー C で @@append 演算子を使用すると、許容可能な値のリストと enforced_for ルールが上書きされるのではなく、追加されることです。

ポリシー C - 値を追加するための OU2 タグポリシー

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@append": [
                    "Marketing"
                ]
```

```
            },
            "enforced_for": {
                "@@append": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

ポリシー C を OU2 にアタッチすると、ポリシー A とポリシー C がマージしてアカウントの有効なタグポリシーを形成した時点で次のような効果があります。

- ポリシー C には @@append 演算子が含まれているため、ポリシー A で指定されている許容タグ値のリストを上書きするのではなく、追加できます。
- ポリシー B では、enforced_for を追加することにより、すべての Amazon Redshift リソースと Amazon DynamoDB テーブルで、指定されたタグ値として CostCenter タグを使用する必要があることが指定されます。上書き (@@assign) と追加 (@@append) は、子ポリシーが指定できるものを制限する子制御演算子が親ポリシーに含まれていない場合、同じ効果があります。

図に示すように、OU2 には 1 つのアカウント (999999999999) が含まれています。ポリシー A とポリシー C をマージして、アカウント 999999999999 に対する有効なタグポリシーを作成します。

アカウント 999999999999 に対する有効なタグポリシー

> **Note**
>
> 表示された有効なポリシーの内容を、新しいポリシーの内容として直接使用することはできません。構文には、他の子ポリシーと親ポリシーのマージを制御するために必要な演算子は含まれていません。有効なポリシーの表示は、マージの結果を把握することのみを目的としています。

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Development",
```

```
                "Support",
                "Marketing"
            ],
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

例 3: 継承されたタグから値を削除する

組織にアタッチされたタグポリシーで、アカウントで使用するよりも多くのタグ値が定義されている場合があります。この例では、@@remove 演算子を使用してタグポリシーを変更する方法について説明します。@@remove はアドバンスト機能です。

他の例と同様、この例は組織ルートのタグポリシーのポリシー A から始まります。

ポリシー A - 組織ルートのタグポリシー

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

この例では、ポリシー D をアカウント 999999999999 にアタッチします。

ポリシー D - 値を削除するためのアカウント 999999999999 のタグポリシー

```
{
    "tags": {
```

```
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@remove": [
                    "Development",
                    "Marketing"
                ],
                "enforced_for": {
                    "@@remove": [
                        "redshift:*",
                        "dynamodb:table"
                    ]
                }
            }
        }
    }
}
```

ポリシー D をアカウント 999999999999 にアタッチすると、ポリシー A、ポリシー C、およびポリシー D をマージして有効なタグポリシーを形成した時点で、次の効果があります。

- 前述の例をすべて実行した場合、ポリシー B、C、および C は A の子ポリシーになっています。ポリシー B は OU1 にのみアタッチされるため、アカウント 9999999999999 には影響しません。
- アカウント 9999999999999 の場合、CostCenter タグキーの許容値は Support のみです。
- CostCenter タグキーに対してコンプライアンスは強制されません。

アカウント 999999999999 の新しい有効なタグポリシー

> **Note**
>
> 表示された有効なポリシーの内容を、新しいポリシーの内容として直接使用することはできません。構文には、他の子ポリシーと親ポリシーのマージを制御するために必要な演算子は含まれていません。有効なポリシーの表示は、マージの結果を把握することのみを目的としています。

```
{
    "tags": {
```

```
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Support"
            ]
        }
    }
}
```

後で OU2 にアカウントを追加すると、追加したアカウントの有効なタグポリシーはアカウント 999999999999 とは異なるものになります。これは、より制限の厳しいポリシー D がアカウントレベルでのみアタッチされ、OU にはアタッチされていないためです。

例 4: 子ポリシーへの変更を制限する

子ポリシーの変更を制限する必要がある場合があります。この例では、子制御演算子を使用してそれを行う方法について説明します。

この例では、新しい組織ルートタグポリシーから開始し、タグポリシーがまだ組織エンティティにアタッチされていないことを前提としています。

ポリシー E – 子ポリシーの変更を制限する組織ルートのタグポリシー

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "Project"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance",
                    "Escalations"
                ]
            }
        }
    }
}
```

ポリシー E を組織ルートにアタッチすると、子ポリシーが Project タグキーを変更できなくなります。ただし、子ポリシーはタグ値を上書きまたは追加できます。

その後、次のポリシー F を OU にアタッチすると仮定します。

ポリシー F - OU のタグポリシー

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": [
                    "Escalations - research"
                ]
            }
        }
    }
}
```

ポリシー E とポリシー F をマージした時点で、OU のアカウントに次のような影響があります。

- ポリシー F は、ポリシー E の子ポリシーです。
- ポリシー F は大文字と小文字の取り扱いを変更しようとしますが、できません。これは、ポリシー E にタグキーの `"@@operators_allowed_for_child_policies": ["@@none"]` 演算子が含まれているためです。
- ただし、ポリシー F はキーのタグ値を追加できます。これは、ポリシー E にタグ値の `"@@operators_allowed_for_child_policies": ["@@append"]` が含まれているためです。

OU のアカウントに対する有効なポリシー

> **Note**
>
> 表示された有効なポリシーの内容を、新しいポリシーの内容として直接使用することはできません。構文には、他の子ポリシーと親ポリシーのマージを制御するために必要な演算子は含まれていません。有効なポリシーの表示は、マージの結果を把握することのみを目的としています。

```
{
    "tags": {
        "project": {
            "tag_key": "Project",
            "tag_value": [
                "Maintenance",
                "Escalations",
                "Escalations - research"
            ]
        }
    }
}
```

例 5: 子制御演算子との競合

子制御演算子は、組織階層の同じレベルでアタッチされたタグポリシー内に存在することができます。この場合、ポリシーがマージされてアカウントの有効なポリシーを形成するときに、許可された演算子の共通部分が使用されます。

ポリシー G とポリシー H が組織ルートにアタッチされていると仮定します。

ポリシー G - 組織ルートのタグポリシー 1

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance"
                ]
            }
        }
    }
}
```

ポリシー H - 組織ルートのタグポリシー 2

```
{
    "tags": {
        "project": {
            "tag_value": {
```

```
                "@@operators_allowed_for_child_policies": ["@@append", "@@remove"]
            }
        }
    }
}
```

この例では、組織ルートの 1 つのポリシーで、タグキーの値のみを追加できるということが定義されています。組織ルートにアタッチされたもう 1 つのポリシーは、子ポリシーが値の追加と削除の両方を行うことを許可します。これら 2 つのアクセス許可の共通部分が子ポリシーに使用されます。その結果、子ポリシーは値を追加できますが、値は削除できません。したがって、子ポリシーはタグ値のリストに値を追加できますが、Maintenance の値を削除することはできません。

例 6: 同じ階層レベルで値を追加した場合の競合

各組織エンティティに複数のタグポリシーをアタッチできます。これを行うと、同じ組織エンティティにアタッチされているタグポリシーに競合する情報が含まれる場合があります。ポリシーは、組織エンティティにアタッチされた順序に基づいて評価されます。最初に評価されるポリシーを変更するには、ポリシーをデタッチしてから再度アタッチします。

ポリシー J が最初に組織ルートにアタッチされ、その次にポリシー K が組織ルートにアタッチされると仮定します。

ポリシー J - 組織ルートにアタッチされた最初のタグポリシー

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": ["Maintenance"]
            }
        }
    }
}
```

ポリシー K - 組織ルートにアタッチされた 2 番目のタグポリシー

```
{
    "tags": {
        "project": {
```

```
            "tag_key": {
                "@@assign": "project"
            }
        }
    }
}
```

この例では、PROJECT タグキーを定義したポリシーが最初に組織ルートにアタッチされたため、このタグキーが有効なタグポリシーで使用されます。

ポリシー JK - アカウントの有効なタグポリシー

アカウントの有効なポリシーは次のようになります。

> **Note**
>
> 表示された有効なポリシーの内容を、新しいポリシーの内容として直接使用することはできません。構文には、他の子ポリシーと親ポリシーのマージを制御するために必要な演算子は含まれていません。有効なポリシーの表示は、マージの結果を把握することのみを目的としています。

```
{
    "tags": {
        "project": {
            "tag_key": "PROJECT",
            "tag_value": [
                "Maintenance"
            ]
        }
    }
}
```

効果的な管理ポリシーの表示

組織内のアカウントの有効な管理ポリシーを決定します。

有効な管理ポリシーとは

有効なポリシーは、管理ポリシータイプの AWS アカウント に適用される最終ルールを指定します。これは、アカウントが継承する管理ポリシーと、アカウントに直接アタッチされている管理ポリ

シータイプのすべてのポリシーの集約です。組織ルートに管理ポリシーをアタッチすると、組織内のすべてのアカウントに適用されます。組織単位 (OU) に管理ポリシーをアタッチすると、OU に属するすべてのアカウントと OU に適用されます。管理ポリシーをアカウントに直接アタッチすると、そのポリシーにのみ適用されます AWS アカウント。

複数のポリシーが集約され、最終的に有効なポリシーが構成される仕組みについては、管理ポリシーの継承を理解する を参照してください。

バックアップポリシーの例

組織のルートにアタッチされたバックアップポリシーでは、組織内のすべてのアカウントが、デフォルトのバックアップ頻度 (週に 1 回) ですべての Amazon DynamoDB テーブルをバックアップするように指定できます。テーブル内の重要な情報を持つ 1 つのメンバーアカウントに直接アタッチされた個別のバックアップポリシーは、1 日に 1 回の値で頻度を上書きできます。これらのバックアップポリシーの組み合わせは、有効なバックアップポリシーで構成されます。有効なバックアップポリシーは、組織内のアカウントごとに個別に決定されます。この例では、例外的に毎日テーブルをバックアップする 1 つのアカウントを除き、組織内のすべてのアカウントが 1 週間に 1 回ずつ DynamoDB テーブルをバックアップします。

タグポリシーの例

組織ルートにアタッチされたタグポリシーで、4 つの準拠値を持つ `CostCenter` タグを定義するとします。この場合、アカウントにアタッチされた別のタグポリシーで、 `CostCenter` キーを 4 つの準拠値のうち 2 つだけに制限できます。これらのタグポリシーを組み合わせることにより、有効なタグポリシーが構成されます。その結果、組織ルートのタグポリシーで定義されている 4 つの準拠タグ値のうち 2 つだけがアカウントで準拠することになります。

チャットアプリケーションポリシーの例

チャットアプリケーションの Amazon Q Developer は、チャットアプリケーション設定で以前に作成された Amazon Q Developer を有効なチャットアプリケーションポリシーと照らし合わせて再評価し、有効なポリシーで許可された設定とガードレールと一致している場合、以前に許可されたアクションを拒否します。メンバーアカウントの有効なポリシーは、許可された設定とガードレールを定義します。たとえば、パブリック Slack チャネルへのアクセスを拒否するチャットアプリケーションポリシーがメンバーアカウントに適用されている場合、メンバーアカウントのパブリック Slack チャネルのチャットアプリケーション設定の既存の Amazon Q Developer は無効になります。チャットアプリケーションの Amazon Q Developer は通知を配信せず、チャネルメンバーはブロックされたチャネルでタスクを実行できません。チャットアプリケーションの Amazon Q Developer コンソールでは、影響を受けるチャネルが無効としてマークされ、その横に適切なエラーメッセージが表示されます。

AI サービスのオプトアウトの例

組織のルートにアタッチされた AI サービスのオプトアウトポリシーでは、組織内のすべてのアカウントがすべての AWS 機械学習サービスによるコンテンツ使用をオプトアウトするように指定できます。一方、あるメンバーアカウントに直接アタッチされた別の AI サービスのオプトアウトポリシーでは、Amazon Rekognition によるコンテンツの使用だけはオプトインするよう指定されています。これらの AI サービスのオプトアウトポリシーが組み合わされ、有効な AI サービスのオプトアウトポリシーが構成されます。その結果、組織内のすべてのアカウントは、Amazon Rekognition にオプトインする 1 つのアカウントを除き AWS のサービス、すべてオプトアウトされます。

有効な管理ポリシーの表示方法

アカウントの管理ポリシータイプの有効なポリシーは AWS Management Console、、 AWS API、または から表示できます AWS Command Line Interface。

> **最小アクセス許可**
>
> アカウントの管理ポリシータイプの有効なポリシーを表示するには、以下のアクションを実行する権限が必要です。
>
> - `organizations:DescribeEffectivePolicy`
> - `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要

AWS Management Console

アカウントの管理ポリシータイプの有効なポリシーを表示するには

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 (非推奨) としてサインインする必要があります。
2. AWS アカウントページで、有効なタグポリシーを表示するアカウントの名前を選択します。場合によっては、目的のアカウントを見つけるには OU を展開
   (
   を選択) する必要があります。
3. ポリシー タブで、有効なポリシーを表示する管理ポリシータイプを選択します。
4. [この AWS アカウントの有効なポリシーの表示] を選択します。

指定したアカウントに適用されている有効なポリシーがコンソールに表示されます。

> **Note**
>
> 有効なポリシーをコピーして貼り付けて、大きな変更を加えずに別のポリシーの JSON として使用することはできません。ポリシードキュメントには、各設定を最終的な有効なポリシーにマージする方法を指定する継承演算子を含める必要があります。

AWS CLI & AWS SDKs

アカウントの管理ポリシータイプの有効なポリシーを表示するには

次のいずれかの方法を使用して、有効なポリシーを表示できます。

- AWS CLI: describe-effective-policy

  次の例は、アカウントの有効な AI サービスのオプトアウトポリシーを示しています。

```
$ aws organizations describe-effective-policy \
    --policy-type AISERVICES_OPT_OUT_POLICY \
    --target-id 123456789012
{
    "EffectivePolicy": {
        "PolicyContent": "{\"services\":{\"comprehend\":{\"opt_out_policy\":
\"optOut\"},   ....TRUNCATED FOR BREVITY....   "opt_out_policy\":\"optIn\"}}}",
        "LastUpdatedTimestamp": "2020-12-09T12:58:53.548000-08:00",
        "TargetId": "123456789012",
        "PolicyType": "AISERVICES_OPT_OUT_POLICY"
    }
}
```

- AWS SDKs: DescribeEffectivePolicy

有効なポリシーが無効になる可能性がある状況の詳細については、「無効なポリシーアラートの表示」を参照してください。

無効な有効なポリシーアラートについて

無効なポリシーアラートは、無効な有効なポリシーについて知らせ、無効なポリシーを持つアカウントを識別するメカニズム (APIs) を提供します。いずれかのアカウントに無効な有効なポリシーがある場合、 は非同期的に AWS Organizations 通知します。通知は AWS Organizations コンソールページにバナーとして表示され、イベントとして AWS CloudTrail 記録されます。

組織内の無効な有効な管理ポリシーを検出する

組織内の無効な有効な管理ポリシーを表示するには、 AWS マネジメントコンソール、 AWS API、AWS コマンドラインインターフェイス (CLI)、または AWS CloudTrail イベントとして、いくつかの方法があります。

最小アクセス許可

組織内の管理ポリシータイプの無効な有効なポリシーに関連する情報を検索するには、次のアクションを実行するアクセス許可が必要です。

- `organizations:ListAccountsWithInvalidEffectivePolicy`
- `organizations:ListEffectivePolicyValidationErrors`
- `organizations:ListRoots` - Organizations コンソールを使用する場合にのみ必要です

AWS Management Console

コンソールから無効な有効な管理ポリシーを表示するには

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 (非推奨) としてサインインする必要があります。
2. AWS アカウント ページでは、組織に無効な有効なポリシーがある場合、ページの上部に警告バナーが表示されます。
3. バナーで、検出された問題を表示をクリックして、無効な有効なポリシーを持つ組織内のすべてのアカウントのリストを表示します。
4. リスト内の各アカウントについて、「問題の表示」を選択して、このページの「有効なポリシーの問題」セクションに示されている各アカウントのエラーに関する詳細情報を取得します。

AWS CLI & AWS SDKs

アカウントの管理ポリシータイプの有効なポリシーを表示するには

次のコマンドは、無効な有効なポリシーを持つアカウントを表示するのに役立ちます。

- AWS CLI: list-accounts-with-invalid-effective-policy
- AWS SDKs: ListAccountsWithInvalidEffectivePolicy

次のコマンドは、アカウントで有効なポリシーエラーを表示するのに役立ちます。

- AWS CLI: list-effective-policy-validation-errors
- AWS SDKs: ListEffectivePolicyValidationErrors

AWS CloudTrail

AWS CloudTrail イベントを使用して、組織内のアカウントに無効な有効な管理ポリシーがあるかどうか、およびポリシーが修正されたかどうかをモニタリングできます。詳細については、AWS Organizations 「ログファイルエントリを理解する」の「有効なポリシーの例」を参照してください。

無効な有効なポリシー通知を受け取った場合は、 AWS Organizations コンソールを操作するか、管理アカウントまたは委任管理者アカウントからこれらの APIs を呼び出して、特定のアカウントとポリシーのステータスに関する詳細を確認できます。

- `ListAccountsWithInvalidEffectivePolicy` – 指定されたタイプの無効な有効なポリシーを持つ組織内のアカウントのリストを返します。
- `ListEffectivePolicyValidationErrors` – 指定されたアカウントと管理ポリシータイプの検証エラーのリストを返します。検証エラーには、エラーコード、エラーの説明、有効なポリシーを無効にした寄与ポリシーなどの詳細が含まれます。

有効な管理ポリシーが無効と見なされる可能性がある場合

アカウントの有効なポリシーは、特定のポリシータイプに定義されている制約に違反すると無効になる可能性があります。たとえば、ポリシーが最終的な有効なポリシーで必須パラメータを欠落しているか、ポリシータイプに定義されている特定のクォータを超えている可能性があります。

バックアップポリシーの例

9 つのバックアップルールを使用してバックアップポリシーを作成し、組織のルートにアタッチするとします。後で、同じバックアッププランに 2 つのルールを追加して別のバックアップポリシーを作成し、組織内の任意のアカウントにアタッチします。この場合、アカウントには無効な有効なポリシーがあります。2 つのポリシーの集約は、バックアッププランの 11 個のルールを定義するため、無効です。プラン内のバックアップルールの上限は 10 です。

> **Warning**
>
> 組織内のいずれかのアカウントに無効な有効なポリシーがある場合、そのアカウントは特定のポリシータイプの有効なポリシー更新を受信しません。すべてのエラーが修正されない限り、アカウントに対して最後に適用された有効な有効なポリシーが続きます。

有効なポリシーで発生する可能性のあるエラーの例

- `ELEMENTS_TOO_MANY` – 有効なポリシー内の特定の属性が、バックアッププランに 10 を超えるルールが指定されているなど、許可された制限を超えた場合に発生します。
- `ELEMENTS_TOO_FEW` – バックアッププランにリージョンが定義されていない場合など、有効なポリシー内の特定の属性が最小制限を満たさない場合に発生します。
- `KEY_REQUIRED` – バックアッププランにバックアップルールがない場合など、有効なポリシーに必要な設定がない場合に発生します。

AWS Organizations は、有効なポリシーを検証してから、組織内のアカウントに適用します。この監査プロセスは、組織構造が大きく、組織のポリシーが複数のチームによって管理されている場合に特に役立ちます。

宣言ポリシー

宣言型ポリシーを使用すると、組織全体 AWS のサービス で特定の に必要な設定を一元的に宣言して適用できます。一度接続すると、サービスに新しい機能や API が追加されても、設定は常に維持されます。宣言ポリシーを使用して、非準拠のアクションを防止します。たとえば、組織全体の Amazon VPC リソースへのパブリックインターネットアクセスをブロックできます。

宣言ポリシーを使用する主な利点は次のとおりです。

- 使いやすさ: AWS Organizations AWS Control Tower とコンソールでいくつかの選択 AWS のサービス を行うか、 AWS CLI & AWS SDKs を使用していくつかのコマンドを使用して、 のベースライン設定を適用できます。

- Set once and forget: サービスが新機能や API を導入しても、 のベースライン設定 AWS のサービス は常に維持されます。 APIs ベースライン設定は、新しいアカウントが組織に追加された場合や、新しいプリンシパルとリソースが作成された場合でも維持されます。
- 透明性: アカウントステータスレポートでは、対象範囲内のアカウントの宣言ポリシーでサポートされているすべての属性の現在のステータスを確認できます。カスタマイズ可能なエラーメッセージを作成することもできます。これにより、管理者はエンドユーザーを内部 Wiki ページにリダイレクトしたり、エンドユーザーがアクションが失敗した理由を理解するのに役立つ説明メッセージを提供したりできます。

サポートされている AWS のサービス および 属性の完全なリストについては、「」を参照してくださいサポートされている AWS のサービス および 属性。

トピック

- 宣言ポリシーの仕組み
- 宣言ポリシーのカスタムエラーメッセージ
- 宣言ポリシーのアカウントステータスレポート
- サポートされている AWS のサービス および 属性
- 宣言ポリシーの開始方法
- 宣言ポリシーを使用するためのベストプラクティス
- 宣言ポリシーのアカウントステータスレポートの生成
- 宣言型ポリシーの構文と例

宣言ポリシーの仕組み

宣言型ポリシーは、サービスのコントロールプレーンで適用されます。これは、サービスコントロールポリシー (SCPs) やリソースコントロールポリシー (RCPs) などの認可ポリシーとの重要な違いです。認可ポリシーは APIs へのアクセスを規制しますが、宣言ポリシーはサービスレベルで直接適用され、永続的なインテントが適用されます。これにより、サービスによって新機能や APIs が導入された場合でも、ベースライン設定が常に適用されます。

次の表は、この区別を説明し、いくつかのユースケースを示しています。

	サービスコントロールポリシー	リソースコントロールポリシー	宣言ポリシー		
目的	大規模なプリンシパル (IAM ユーザーや IAM ロールなど) に対して一貫したアクセスコントロールを一元的に定義して適用します。	大規模なリソースに対して一貫したアクセスコントロールを一元的に定義して適用するには	大規模な AWS サービスのベースライン設定を一元的に定義して適用します。		
その方法は?	API レベルでプリンシパルの利用可能なアクセス許可の最大数を制御する。	API レベルでリソースに対して使用可能なアクセス許可の最大数を制御する。	API アクションを使用 AWS のサービス せずにの必要な設定を適用します。		
サービスにリンクされたロールを管理しますか？	なし	なし	あり		
フィードバックメカニズム	カスタマイズ不可能なアクセスが SCP エラーを拒否しました。	カスタマイズ不可能なアクセスが RCP エラーを拒否しました。	カスタマイズ可能なエラーメッセージ。詳細については、「宣言ポリシーのカスタムエラーメッセージ」		

	サービスコントロールポリシー	リソースコントロールポリシー	宣言ポリシー		
			を参照してください。		
ポリシーの例	リクエストが AWS されたに基づいてへのアクセスを拒否する AWS リージョン	リソースへの HTTPS 接続のみへのアクセスを制限する	許可されたイメージの設定		

宣言ポリシーを作成してアタッチすると、組織全体に適用および適用されます。宣言ポリシーは、組織全体、組織単位 (OUs)、またはアカウントに適用できます。組織に参加するアカウントは、組織内の宣言ポリシーを自動的に継承します。詳細については、「管理ポリシーの継承を理解する」を参照してください。

有効なポリシーは、組織ルートと OU から継承されるルールのセットと、アカウントに直接アタッチされたルールのセットです。有効なポリシーは、アカウントに適用される最終的なルールセットを指定します。詳細については、「効果的な管理ポリシーの表示」を参照してください。

宣言ポリシーがデタッチされると、属性の状態は宣言ポリシーがアタッチされる前の状態にロールバックされます。

宣言ポリシーのカスタムエラーメッセージ

宣言ポリシーを使用すると、カスタムエラーメッセージを作成できます。たとえば、宣言ポリシーが原因で API オペレーションが失敗した場合、エラーメッセージを設定するか、内部 Wiki へのリンクや失敗を説明するメッセージへのリンクなどのカスタム URL を指定できます。カスタムエラーメッセージを指定しない場合、 はデフォルトのエラーメッセージ AWS Organizations を提供しますExample: `This action is denied due to an organizational policy in effect`。

また、宣言ポリシーの作成、宣言ポリシーの更新、宣言ポリシーの削除のプロセスも監査できます AWS CloudTrail。CloudTrail は、宣言ポリシーによる API オペレーションの失敗にフラグを付けることができます。詳細については、「ログ記録とモニタリング」を参照してください。

> **Important**
>
> カスタムエラーメッセージには、個人を特定できる情報 (PII) やその他の機密情報を含めないでください。PII には、個人を特定または特定するために使用できる一般的な情報が含まれています。財務、医療、教育、雇用などの記録を対象としています。PII の例には、住所、銀行口座番号、電話番号などがあります。

宣言ポリシーのアカウントステータスレポート

アカウントステータスレポートを使用すると、対象範囲内のアカウントの宣言ポリシーでサポートされているすべての属性の現在のステータスを確認できます。レポートスコープに含めるアカウントと組織単位 (OUs) を選択するか、ルートを選択して組織全体を選択できます。

このレポートは、リージョンの内訳を提供し、属性の現在の状態がアカウント間で統一されている (経由`numberOfMatchedAccounts`) か、一貫性がない (経由) かを評価することで、準備状況を評価するのに役立ちます`numberOfUnmatchedAccounts`。また、最も頻繁な値を表示することもできます。これは、 属性で最も頻繁に観測される設定値です。

図 1 では、生成されたアカウントステータスレポートがあり、VPC ブロックパブリックアクセスとイメージブロックパブリックアクセスの属性のアカウント間の統一性を示しています。つまり、各属性について、スコープ内のすべてのアカウントがその属性に対して同じ設定を持つことになります。

生成されたアカウントステータスレポートには、許可されたイメージ設定、インスタンスメタデータのデフォルト、シリアルコンソールアクセス、スナップショットブロックパブリックアクセスの属性について、一貫性のないアカウントが表示されます。この例では、一貫性のないアカウントを持つ各属性は、異なる設定値を持つアカウントが 1 つあることが原因です。

最も頻繁な値がある場合、その値はそれぞれの列に表示されます。各属性が制御する機能の詳細については、「宣言型ポリシー構文」と「ポリシーの例」を参照してください。

属性を展開して、リージョンの内訳を表示することもできます。この例では、Image Block Public Access が展開され、各リージョンでアカウント間で統一されていることがわかります。

ベースライン設定を適用するための宣言ポリシーをアタッチする選択は、特定のユースケースによって異なります。アカウントステータスレポートは、宣言ポリシーをアタッチする前に準備状況を評価するのに役立ちます。

詳細については、「アカウントステータスレポートの生成」を参照してください。

図 1: VPC ブロックパブリックアクセスとイメージブロックパブリックアクセスのアカウント間で統一されたアカウントステータスレポートの例。

サポートされている AWS のサービス および 属性

EC2 の宣言ポリシーでサポートされている属性

次の表は、Amazon EC2 関連サービスでサポートされている属性を示しています。

EC2 の宣言ポリシー

AWS サービス	属性	ポリシー効果	ポリシーの内容	詳細情報
Amazon VPC	VPC ブロックパブリックアクセス	Amazon VPCs とサブネットのリソースがインターネットゲートウェイ (IGWs) を介してインターネットに到達できるかどうかを制御します。	ポリシーを表示	詳細については、VPCs ユーザーガイド」の「VPC とサブネットへのパブリックアクセスをブロックする」を参照してください。
Amazon EC2	シリアルコンソールアクセス	EC2 シリアルコンソールにアクセスできるかどうかを制御します。	ポリシーを表示	詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」のEC2 シリアルコンソールへのアクセスを設定する」を参照してください。
	イメージブロックのパブリックアクセス	Amazon マシンイメージ (AMIs) がパブリックに共有可能かど	ポリシーを表示	詳細については、「Amazon Elastic Compute Cloud ユーザー

AWS サービス	属性	ポリシー効果	ポリシーの内容	詳細情報
		うかを制御します。		ガイド」のAMIs のパブリックアクセスブロックを理解する」を参照してください。
	許可されたイメージの設定	許可された AMI を使用した Amazon EC2 での Amazon マシンイメージ (AMIs。	ポリシーを表示	詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」の AMIs)」を参照してください。
	インスタンスメタデータのデフォルト	すべての新しい EC2 インスタンスの起動の IMDS のデフォルトを制御します。	ポリシーを表示	詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」の「新しいインスタンスのインスタンスメタデータオプションを設定する」を参照してください。

AWS サービス	属性	ポリシー効果	ポリシーの内容	詳細情報
Amazon EBS	スナップショットブロックパブリックアクセス	Amazon EBS スナップショットがパブリックにアクセス可能かどうかを制御します。	ポリシーを表示	詳細については、「Amazon Elastic Block Store ユーザーガイド」の「Amazon EBS スナップショットのパブリックアクセスのブロック」を参照してください。

宣言ポリシーの開始方法

宣言ポリシーの使用を開始するには、次の手順に従います。

1. 宣言ポリシータスクを実行するために必要なアクセス許可について説明します。
2. 組織の宣言ポリシーを有効にします。

> **Note**
>
> 信頼アクセスを有効にする必要があります
> 宣言ポリシーがベースライン設定を適用する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。これにより、組織全体のアカウントの既存の設定に関するアカウントステータスレポートを生成するために使用される読み取り専用のサービスにリンクされたロールが作成されます。
> コンソールの使用
> Organizations コンソールを使用する場合、このステップは宣言ポリシーを有効にするプロセスの一部です。
> の使用 AWS CLI
> を使用する場合 AWS CLI、2 つの異なる APIsがあります。
>
> - EnablePolicyType。宣言ポリシーを有効にするために使用されます。
> - EnableAWSServiceAccess。信頼されたアクセスを有効にするために使用されます。

で特定のサービスの信頼されたアクセスを有効にする方法の詳細については、AWS のサービスAWS Organizations AWS CLI「」を参照してください。

3. アカウントステータスレポートを実行します。
4. 宣言ポリシーを作成します。
5. 宣言ポリシーを組織のルート、OU、またはアカウントにアタッチします。
6. アカウントに適用される有効な宣言ポリシーの組み合わせを表示します。

これらすべてのステップでは、組織の管理アカウントの 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 (推奨されません) としてサインインします。

その他の情報

- 宣言型ポリシー構文とポリシーの例について説明します。

宣言ポリシーを使用するためのベストプラクティス

AWS では、宣言ポリシーを使用するための以下のベストプラクティスを推奨しています。

準備状況評価を活用する

宣言ポリシーアカウントステータスレポートを使用して、対象範囲内のアカウントの宣言ポリシーでサポートされているすべての属性の現在のステータスを評価します。レポートスコープに含めるアカウントと組織単位 (OUs) を選択するか、ルートを選択して組織全体を選択できます。

このレポートは、リージョンの内訳を提供し、属性の現在の状態がアカウント間で統一されている (経由numberOfMatchedAccounts) か、一貫性がない (経由) かを評価することで、準備状況を評価するのに役立ちますnumberOfUnmatchedAccounts。また、最も頻繁な値を表示することもできます。これは、 属性に対して最も頻繁に観測される設定値です。

ベースライン設定を適用するための宣言ポリシーをアタッチする選択は、特定のユースケースによって異なります。

詳細と例については、「」を参照してください宣言ポリシーのアカウントステータスレポート。

小規模から始めてスケールする

デバッグを簡素化するには、テストポリシーから始めます。次の変更を行う前に、各変更の動作と影響を検証します。このアプローチにより、エラーや予期しない結果が発生したときに考慮する必要がある変数の数が減少します。

たとえば、重要でないテスト環境の単一のアカウントにアタッチされたテストポリシーから開始できます。仕様どおりに動作することを確認したら、ポリシーを組織構造の上に段階的に移動して、より多くのアカウントとより多くの組織単位 (OUsできます。

レビュープロセスを確立する

新しい宣言属性をモニタリングし、ポリシーの例外を評価し、組織のセキュリティと運用要件との整合性を維持するために調整するプロセスを実装します。

を使用して変更を検証する **`DescribeEffectivePolicy`**

宣言ポリシーを変更したら、変更を行ったレベル以下の代表的なアカウントの有効なポリシーを確認します。有効なポリシーを表示するには、 を使用する AWS Management Consoleか、DescribeEffectivePolicy API オペレーション、またはそのいずれかの AWS CLI または AWS SDK バリアントを使用します。加えた変更が、有効なポリシーに意図した影響を与えていることを確認します。

コミュニケーションとトレーニング

組織が宣言ポリシーの目的と影響を理解していることを確認します。期待される動作と、ポリシーの適用による障害に対処する方法について、明確なガイダンスを提供します。

宣言ポリシーのアカウントステータスレポートの生成

アカウントステータスレポートでは、対象範囲内のアカウントの宣言ポリシーでサポートされているすべての属性の現在のステータスを確認できます。レポートスコープに含めるアカウントと組織単位 (OUs) を選択するか、ルートを選択して組織全体を選択できます。

このレポートは、リージョンの内訳を提供し、属性の現在の状態がアカウント間で統一されている (経由`numberOfMatchedAccounts`) か、一貫性がない (経由) かを評価することで、準備状況を評価するのに役立ちます`numberOfUnmatchedAccounts`。また、最も頻繁な値を表示することもできます。これは、 属性に対して最も頻繁に観測される設定値です。

ベースライン設定を適用するための宣言ポリシーをアタッチする選択は、特定のユースケースによって異なります。

詳細と例については、「」を参照してください宣言ポリシーのアカウントステータスレポート。

前提条件

アカウントステータスレポートを生成する前に、次の手順を実行する必要があります。

1. StartDeclarativePoliciesReport API を呼び出すことができるのは、組織の管理アカウントまたは委任された管理者のみです。
2. レポートを生成する前に (新しいバケットを作成するか、既存のバケットを使用する) S3 バケットが必要です。S3 バケットは、リクエストが行われたリージョンと同じリージョンにあり、適切な S3 バケットポリシーを持っている必要があります。サンプル S3 ポリシーについては、「Amazon EC2 API リファレンス」の「例」の「サンプル Amazon S3 ポリシー」を参照してください。 https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_StartDeclarativePoliciesReport.html#API_StartDeclarativePoliciesReport_Examples Amazon EC2
3. 宣言ポリシーがベースライン設定を適用する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。これにより、組織全体のアカウントの既存の設定に関するアカウントステータスレポートを生成するために使用される読み取り専用のサービスにリンクされたロールが作成されます。

   コンソールの使用

   Organizations コンソールの場合、このステップは宣言ポリシーを有効にするプロセスの一部です。

   の使用 AWS CLI

   には AWS CLI、EnableAWSServiceAccess API を使用します。

   で特定のサービスの信頼されたアクセスを有効にする方法の詳細については、AWS のサービス AWS Organizations AWS CLI 「」を参照してください。
4. 一度に生成できるレポートは、組織ごとに 1 つだけです。別の の進行中にレポートを生成しようとすると、エラーが発生します。

コンプライアンスステータスレポートにアクセスする

最小アクセス許可

コンプライアンスステータスレポートを生成するには、次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。

- ec2:StartDeclarativePoliciesReport
- ec2:DescribeDeclarativePoliciesReports
- ec2:GetDeclarativePoliciesReportSummary

- ec2:CancelDeclarativePoliciesReport
- organizations:DescribeAccount
- organizations:DescribeOrganization
- organizations:DescribeOrganizationalUnit
- organizations:ListAccounts
- organizations:ListDelegatedAdministrators
- organizations:ListAWSServiceAccessForOrganization
- s3:PutObject

> **Note**
>
> Amazon S3 バケットが SSE-KMS 暗号化を使用している場合は、ポリシーに アクセスkms:GenerateDataKey許可も含める必要があります。

AWS Management Console

アカウントステータスレポートを生成するには、次の手順に従います。

アカウントステータスレポートを生成するには

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 (非推奨) としてサインインする必要があります。
2. ポリシーページで、EC2 の宣言ポリシーを選択します。
3. EC2 の宣言ポリシーページで、アクションドロップダウンメニューからアカウントステータスレポートの表示を選択します。
4. アカウントステータスレポートの表示ページで、ステータスレポートの生成を選択します。
5. 組織構造ウィジェットで、レポートに含める組織単位 (OUs) を指定します。
6. [Submit] を選択してください。

AWS CLI & AWS SDKs

アカウントステータスレポートを生成するには

次のオペレーションを使用して、コンプライアンスステータスレポートを生成し、そのステータスをチェックして、レポートを表示します。

- `ec2:start-declarative-policies-report`: アカウントステータスレポートを生成します。レポートは非同期的に生成され、完了までに数時間かかる場合があります。詳細については、Amazon EC2 API リファレンス」のStartDeclarativePoliciesReport」を参照してください。
- `ec2:describe-declarative-policies-report`: レポートの状態など、アカウントステータスレポートのメタデータを記述します。詳細については、Amazon EC2 API リファレンス」の「DescribeDeclarativePoliciesReports」を参照してください。
- `ec2:get-declarative-policies-report-summary`: アカウントステータスレポートの概要を取得します。詳細については、Amazon EC2 API リファレンス」のGetDeclarativePoliciesReportSummary」を参照してください。
- `ec2:cancel-declarative-policies-report`: アカウントステータスレポートの生成をキャンセルします。詳細については、Amazon EC2 API リファレンス」の「CancelDeclarativePoliciesReport」を参照してください。

レポートを生成する前に、レポートが保存される Amazon S3 バケットへのアクセス権を EC2 宣言ポリシープリンシパルに付与します。これを行うには、次のポリシーをバケットにアタッチします。`amzn-s3-demo-bucket` を実際の Amazon S3 バケット名に置き換え、 を `StartDeclarativePoliciesReport` API の呼び出しに使用される IAM ID `identity_ARN` に置き換えます。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DeclarativePoliciesReportDelivery",
            "Effect": "Allow",
            "Principal": {
                "AWS": "identity_ARN"
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "organizations.amazonaws.com"
                }
            }
        }
    ]
}
```

宣言型ポリシーの構文と例

このページでは、宣言ポリシー構文について説明し、例を示します。

考慮事項

- 宣言ポリシーを使用してサービス属性を設定すると、複数の APIs に影響する可能性があります。非準拠のアクションは失敗します。
- アカウント管理者は、個々のアカウントレベルでサービス属性の値を変更することはできません。

宣言ポリシーの構文

宣言ポリシーは、JSON のルールに従って構造化されたプレーンテキストファイルです。宣言ポリシーの構文は、すべての管理ポリシータイプの構文に従います。この構文の詳細については、「ポリシー構文と管理ポリシータイプの継承」を参照してください。このトピックでは、宣言ポリシータイプの特定の要件にその一般的な構文を適用することに重点を置いています。

次の例は、基本的な宣言ポリシー構文を示しています。

```
{
    "ec2_attributes": {
        "exception_message": {
            "@@assign": "Your custom error message.https://myURL"
        },

        ...

        [Insert supported service attributes]

        ...
    }
```

```
}
```

- ec2_attributes フィールドキーの名前。宣言ポリシーは、常に指定された固定キー名で始まります AWS のサービス。上記のポリシーの例では一番上の行です。現在、宣言ポリシーは Amazon EC2 関連サービスのみをサポートしていました。
- でec2_attributes、 exception_messageを使用してカスタムエラーメッセージを設定できます。詳細については、「宣言ポリシーのカスタムエラーメッセージ」を参照してください。
- ではec2_attributes、サポートされている宣言ポリシーを 1 つ以上挿入できます。これらのスキーマについては、「」を参照してくださいサポートされている宣言ポリシー。

サポートされている宣言ポリシー

以下は、宣言ポリシーがサポートする AWS のサービス および 属性です。以下の例の一部では、スペースを節約するために JSON の空白書式が圧縮される場合があります。

- VPC ブロックパブリックアクセス
- シリアルコンソールアクセス
- イメージブロックのパブリックアクセス
- 許可されたイメージの設定
- インスタンスメタデータのデフォルト
- スナップショットブロックパブリックアクセス

VPC Block Public Access

ポリシー効果

Amazon VPCsとサブネットのリソースがインターネットゲートウェイ (IGWs) を介してインターネットに到達できるかどうかを制御します。詳細については、Amazon Virtual Private Cloud ユーザーガイドの「インターネットアクセスの設定」を参照してください。

ポリシーの内容

```
"vpc_block_public_access": {
    "internet_gateway_block": { // (optional)
        "mode": { // (required)
            "@@assign": "block_ingress" // off | block_ingress | block_bidirectional
        },
        "exclusions_allowed": { // (required)
```

```
            "@@assign": "enabled" // enabled | disabled
        }
    }
}
```

この属性で使用できるフィールドは次のとおりです。

- "internet_gateway":
  - "mode":
    - "off": VPC BPA が有効になっていません。
    - "block_ingress": VPCs へのすべてのインターネットトラフィック (除外されている VPCs またはサブネットを除く) がブロックされます。NAT ゲートウェイとエグレスのみのインターネットゲートウェイとの間のトラフィックのみが許可されます。なぜなら、これらのゲートウェイはアウトバウンド接続の確立のみを許可するからです。
    - "block_bidirectional": インターネットゲートウェイと Egress-Only インターネットゲートウェイとの間のすべてのトラフィック (除外された VPCsとサブネットを除く) がブロックされます。
- "exclusions_allowed": 除外は、アカウントの VPC BPA モードから除外し、双方向または出力のみのアクセスを許可する単一の VPC またはサブネットに適用できるモードです。
  - "enabled": 除外はアカウントで作成できます。
  - "disabled": アカウントで除外を作成することはできません。

> **Note**
>
> 属性を使用して除外が許可されているかどうかを設定できますが、この属性自体で除外を作成することはできません。除外を作成するには、VPC を所有するアカウントで除外を作成する必要があります。VPC BPA 除外の作成の詳細については、「Amazon VPC ユーザーガイド」の「除外の作成と削除」を参照してください。

考慮事項

宣言ポリシーでこの属性を使用する場合、次のオペレーションを使用して、対象範囲内のアカウントの強制設定を変更することはできません。このリストは網羅的なものではありません。

- ModifyVpcBlockPublicAccessOptions
- CreateVpcBlockPublicAccessExclusion

- `ModifyVpcBlockPublicAccessExclusion`

Serial Console Access

ポリシー効果

EC2 シリアルコンソールにアクセスできるかどうかを制御します。EC2 シリアルコンソールの詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」のEC2 シリアルコンソール」を参照してください。

ポリシーの内容

```
"serial_console_access": {
    "status": { // (required)
        "@@assign": "enabled" // enabled | disabled
    }
}
```

この属性で使用できるフィールドは次のとおりです。

- `"status"`:
  - `"enabled"`: EC2 シリアルコンソールへのアクセスが許可されます。
  - `"disabled"`: EC2 シリアルコンソールへのアクセスがブロックされます。

考慮事項

宣言ポリシーでこの属性を使用する場合、次のオペレーションを使用して、対象範囲内のアカウントの強制設定を変更することはできません。このリストは網羅的なものではありません。

- `EnableSerialConsoleAccess`
- `DisableSerialConsoleAccess`

Image Block Public Access

ポリシー効果

Amazon マシンイメージ (AMIs) がパブリックに共有可能かどうかを制御します。AMI の詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」の「Amazon マシンイメージ (AMIs」を参照してください。

ポリシーの内容

```
"image_block_public_access": {
    "state": { // (required)
        "@@assign": "block_new_sharing" // unblocked | block_new_sharing
    }
}
```

この属性で使用できるフィールドは次のとおりです。

- "state":
  - "unblocked": AMIs。
  - "block_new_sharing": AMIs。既にパブリックに共有されていた AMIs は、引き続きパブリックに利用できます。

考慮事項

宣言ポリシーでこの属性を使用する場合、次のオペレーションを使用して、対象範囲内のアカウントの強制設定を変更することはできません。このリストは網羅的なものではありません。

- EnableImageBlockPublicAccess
- DisableImageBlockPublicAccess

Allowed Images Settings

ポリシー効果

許可された AMI を使用した Amazon EC2 での Amazon マシンイメージ (AMIs.. AMI の詳細については、「Amazon Elastic Compute Cloud ユーザーガイドAMIs)」を参照してください。

ポリシーの内容

この属性で使用できるフィールドは次のとおりです。

```
"allowed_images_settings": {
    "state": { // (required)
        "@@assign": "enabled" // enabled | disabled | audit_mode
    },
    "image_criteria": { // (optional)
        "criteria_1": {
```

```
            "allowed_image_providers": { // limit 200
                "@@append": [
                    "amazon" // amazon | aws_marketplace | aws_backup_vault | 12
 digit account ID
                ]
            }
        }
    }
}
```

- "state":
  - "enabled": 属性はアクティブで強制されます。
  - "disabled": 属性は非アクティブであり、強制されません。
  - "audit_mode": 属性は監査モードです。つまり、非準拠のイメージは識別されますが、その使用はブロックされません。
- "image_criteria": 許可された AMI ソースを定義するallowed_image_providersオブジェクトのリスト。
  - "allowed_image_providers": プロバイダー名またはアカウント IDs のカンマ区切りリスト。

考慮事項

宣言ポリシーでこの属性を使用する場合、次のオペレーションを使用して、対象範囲内のアカウントの強制設定を変更することはできません。このリストは網羅的なものではありません。

- EnableAllowedImagesSettings
- ReplaceImageCriteriaInAllowedImagesSettings
- DisableAllowedImagesSettings

Instance Metadata Defaults

ポリシー効果

すべての新しい EC2 インスタンス起動の IMDS のデフォルトを制御します。この設定ではデフォルトのみが設定され、IMDS バージョン設定は強制されないことに注意してください。IMDS のデフォルトの詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」の「IMDS」を参照してください。

ポリシーの内容

この属性で使用できるフィールドは次のとおりです。

```
"instance_metadata_defaults": {
    "http_tokens": { // (required)
        "@@assign": "required" // no_preference | required | optional
    },
    "http_put_response_hop_limit": { // (required)
        "@@assign": "4" // -1 | 1 -> 64
    },
    "http_endpoint": { // (required)
        "@@assign": "enabled" // no_preference | enabled | disabled
    },
    "instance_metadata_tags": { // (required)
        "@@assign": "enabled" // no_preference | enabled | disabled
    }
}
```

- "http_tokens":
  - "no_preference": その他のデフォルトが適用されます。たとえば、該当する場合、AMI はデフォルトで設定されます。
  - "required": IMDSv2 を使用する必要があります。IMDSv1 は許可されていません。
  - "optional": IMDSv1 と IMDSv2 の両方が許可されます。

> **Note**
>
> メタデータバージョン
> http_tokens を に設定する前に required (IMDSv2 を使用する必要があります) 、どのインスタンスも IMDSv1 呼び出しを行っていないことを確認してください。

- "http_put_response_hop_limit":
  - "*Integer*": -1 ~ 64 の整数値。メタデータトークンが移動できるホップの最大数を表します。設定を指定しない場合は、-1 を指定します。

> **Note**
>
> ホップ制限

http_tokens が に設定されている場合required、 を最低 2 http_put_response_hop_limitに設定することをお勧めします。詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」の「インスタンスメタデータのアクセスに関する考慮事項」を参照してください。

- "http_endpoint":
  - "no_preference": その他のデフォルトが適用されます。たとえば、該当する場合、AMI はデフォルトで設定されます。
  - "enabled": インスタンスメタデータサービスエンドポイントにアクセスできます。
  - "disabled": インスタンスメタデータサービスエンドポイントにアクセスできません。
- "instance_metadata_tags":
  - "no_preference": その他のデフォルトが適用されます。たとえば、該当する場合、AMI はデフォルトで設定されます。
  - "enabled": インスタンスタグには、インスタンスメタデータからアクセスできます。
  - "disabled": インスタンスタグにはインスタンスメタデータからアクセスできません。

Snapshot Block Public Access

ポリシー効果

Amazon EBS スナップショットがパブリックにアクセス可能かどうかを制御します。EBS スナップショットの詳細については、「Amazon Elastic Block Store ユーザーガイド」の「Amazon EBS スナップショット」を参照してください。

ポリシーの内容

```
"snapshot_block_public_access": {
    "state": { // (required)
        "@@assign": "block_new_sharing" // unblocked | block_new_sharing |
 block_all_sharing
    }
}
```

この属性で使用できるフィールドは次のとおりです。

- "state":

- "block_all_sharing": スナップショットのすべてのパブリック共有をブロックします。既にパブリックに共有されていたスナップショットはプライベートとして扱われ、公開されなくなります。
- "block_new_sharing": スナップショットの新しいパブリック共有をブロックします。既にパブリックに共有されていたスナップショットは、公開されたままです。
- "unblocked": スナップショットのパブリック共有に制限はありません。

考慮事項

宣言ポリシーでこの属性を使用する場合、次のオペレーションを使用して、範囲内のアカウントの強制設定を変更することはできません。このリストは網羅的なものではありません。

- EnableSnapshotBlockPublicAccess
- DisableSnapshotBlockPublicAccess

バックアップポリシー

バックアップポリシーを使用すると、バックアッププランを一元管理し、組織のアカウント全体の AWS リソースに適用できます。

AWS Backup では、 AWS リソースのバックアップ方法を定義するバックアッププランを作成できます。プランのルールには、バックアップの頻度、バックアップが発生する時間枠、バックアップするリソース AWS リージョン を含む 、バックアップを保存するボールトなど、さまざまな設定が含まれます。その後、タグを使用して識別された AWS リソースのグループにバックアッププランを適用できます。また、ユーザーに代わってバックアップオペレーションを実行するアクセス許可を付与 AWS Backup する AWS Identity and Access Management (IAM) ロールも指定する必要があります。

のバックアップポリシー AWS Organizations は、これらのすべての要素を JSON テキストドキュメントに結合します。バックアップポリシーは、ルート、組織単位 (OU)、個々のアカウントなど、組織構造の任意の要素にアタッチできます。Organizations は継承ルールに基づき、組織のルート、親 OU、アカウントにアタッチされたポリシーを集約します。これにより、各アカウントに対して 有効なバックアップポリシー が生成されます。この有効なポリシーは、 リソースを自動的にバックアップ AWS Backup する方法を に指示します AWS 。

バックアップポリシーの仕組み

バックアップポリシーを使用すると、組織が必要とするあらゆるレベルでリソースのバックアップをきめ細かく制御できます。例えば、組織のルートにアタッチされたポリシーで、すべての Amazon

DynamoDB テーブルをバックアップするよう指定できます。このポリシーには、デフォルトのバックアップ頻度を含めることができます。その後、各 OU の要件に従ってバックアップ頻度を上書きするバックアップポリシーを OU にアタッチできます。例えば、`Developers` OU ではバックアップ頻度を週に 1 回指定し、`Production` OU では 1 日に 1 回指定することができます。

リソースを正常にバックアップするために必要な情報の一部だけを個別に含む部分的なバックアップポリシーを作成できます。これらのポリシーを下位レベルの OU とアカウントによって継承されることを意図して、ルートや親 OU などの組織ツリーのさまざまな部分にアタッチできます。Organizations の継承ルールに基づき、アカウントのすべてのポリシーを組み合わせて構成される有効なポリシーは、必要な要素をすべて備えている必要があります。それ以外の場合、 はポリシーが無効である AWS Backup と見なし、影響を受けるリソースをバックアップしません。

> **Important**
>
> AWS Backup は、必要なすべての要素を含む完全な有効なポリシーによって呼び出された場合にのみ、成功したバックアップを実行できます。
> 前述の部分ポリシー戦略は機能しますが、アカウントの有効なポリシーが不完全な場合は、エラーになるか、リソースが正常にバックアップされなくなります。代替戦略として、すべてのバックアップポリシーが単独で完全かつ有効であることが必要であることを検討してください。階層の上位にアタッチされたポリシーによって提供される デフォルト値を使用し、継承子制御演算子を含めることによって、子ポリシーで必要に応じてオーバーライドします。

組織 AWS アカウント 内の各 の有効なバックアッププランは、そのアカウントのイミュータブルなプランとしてコンソールに表示されます AWS Backup 。表示することはできますが、変更することはできません。ただし、TagResource および UntagResource APIs を使用してバックアッププランタグを追加または削除することはできます。

がポリシーによって作成されたバックアッププランに基づいてバックアップ AWS Backup を開始すると、 AWS Backup コンソールにバックアップジョブのステータスが表示されます。メンバーアカウントのユーザーは、そのメンバーアカウントのバックアップジョブのステータスとエラーを確認できます。で信頼されたサービスアクセスも有効にすると AWS Backup、組織の管理アカウントのユーザーは、組織内のすべてのバックアップジョブのステータスとエラーを確認できます。詳細については、AWS Backup デベロッパーガイドのクロスアカウント管理の有効化を参照してください。

バックアップポリシーの使用開始

バックアップポリシーの使用を開始するには、次のステップを実行します。

1. バックアップポリシータスクの実行に必要なアクセス許可について説明します
2. バックアップポリシーを使用する際に推奨されるベストプラクティスについて説明します。
3. 組織のバックアップポリシーを有効にします。
4. バックアップポリシーを作成します。
5. バックアップポリシーを組織のルート、OU、またはアカウントにアタッチします。
6. アカウントに適用される有効なバックアップポリシーを組み合わせて表示します。

これらすべてのステップでは、組織の管理アカウントの 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 (推奨されません) としてサインインします。

その他の情報

- バックアップポリシーの構文について説明し、ポリシーの例を参照します

バックアップポリシーを使用する場合のベストプラクティス

AWS では、バックアップポリシーを使用する際に以下のベストプラクティスを推奨しています。

バックアップポリシー戦略を決定する

継承およびマージされた不完全な部分でバックアップポリシーを作成し、各メンバーアカウントの完全なポリシーを作成できます。これを行う場合、あるレベルで、そのレベルより低いすべてのアカウントに対する変更の影響を慎重に考慮せずに変更を加えると、不完全な効果的なポリシーになる危険性があります。これを回避するために、すべてのレベルで実装するバックアップポリシーが単独で完全であるようにすることをお勧めします。親ポリシーは、子ポリシーで指定された設定によってオーバーライドできるデフォルトポリシーとして扱います。これにより、子ポリシーが存在しない場合でも、継承されたポリシーは完全であり、デフォルト値が使用されます。子制御継承演算子を使用して、子ポリシーで追加、変更、または削除できる設定を制御できます。

`GetEffectivePolicy` を使用してバックアップポリシーの変更を検証する

バックアップポリシーを変更した後、変更を行ったレベルより低い代表アカウントの有効なポリシーを確認します。有効なポリシーを表示するには、 を使用する AWS Management Consoleか、GetEffectivePolicy API オペレーション、その AWS CLI または AWS SDK バリアントのいずれかを使用します。加えた変更が、有効なポリシーに意図した影響を与えていることを確認します。

単純なものから始めて、小さな変更を加える

デバッグを簡素化するには、単純なポリシーから開始し、一度に 1 つの項目を変更します。次の変更を行う前に、各変更の動作と影響を検証します。こうすることで、エラーや予期しない結果が発生した場合に考慮する必要がある変数が減ります。

バックアップのコピーを組織内の他の AWS リージョン およびアカウントに保存する

バックアップのコピーを保存しておくと、災害対策の強化につながります。

- 別のリージョン – バックアップのコピーを追加で保存すると AWS リージョン、元のリージョンで誤って破損したり削除されたりしないようにバックアップを保護できます。ポリシーの `copy_actions` セクションを使用し、バックアッププランが実行されるアカウントの 1 つ以上のリージョンにボールトを指定します。これを行うには、バックアップのコピーを保存するバックアップボールトの ARN を指定する際に `$account` 変数を使用し、アカウントを特定します。`$account` 変数は、バックアップポリシーが実行されているアカウント ID に、実行時に自動的に置き換えられます。
- 別のアカウント – バックアップのコピーを追加で保存する場合は AWS アカウント、いずれかのアカウントを侵害する悪意のある攻撃者から保護するのに役立つセキュリティ障壁を追加します。ポリシーの `copy_actions` セクションを使用し、組織内の 1 つ以上のアカウントにボールトを指定します。バックアッププランを実行するアカウントとは別にする必要があります。これを行うには、バックアップのコピーを保存するバックアップボールトの ARN を指定する際に実際のアカウント ID 番号を使用し、アカウントを特定します。

ポリシーごとのプラン数を制限する

複数のプランを含むポリシーは、すべてを検証する必要がある多数の出力のため、トラブルシューティングが複雑になります。デバッグとトラブルシューティングを簡素化するために、各ポリシーにはバックアッププランを 1 つだけ含めるようにします。その後、他の要件を満たすために、他のプランにポリシーを追加できます。こうすることで、プランに関する問題が 1 つのポリシーに分離され、他のポリシーとそのプランに関する問題のトラブルシューティングが複雑になるのを防ぐことができます。

スタックセットを使用して必要なバックアップボールトと IAM ロールを作成する

Organizations と AWS CloudFormation スタックセットの統合を使用して、組織内の各メンバーアカウントに、必要なバックアップボールトと AWS Identity and Access Management (IAM) ロールを自動的に作成します。組織 AWS アカウント 内のすべての で自動的に利用できるリソースを含むスタックセットを作成できます。こうすることで、依存関係がすでに満たされていることが保証され

た状態でバックアッププランを実行できます。詳細については、AWS CloudFormation ユーザーガイドのセルフマネージド型のアクセス許可を持つスタックセットの作成を参照してください。

各アカウントで作成された最初のバックアップを確認して、結果をチェックします。

ポリシーを変更するときは、その変更後に作成された次のバックアップをチェックして、変更が目的の影響を与えたことを確認します。このステップでは、有効なポリシーを確認するだけでなく、AWS Backup がポリシーを解釈し、バックアッププランを意図したとおりに実装します。

AWS CloudTrail イベントを使用した組織内のバックアップポリシーのモニタリング

AWS CloudTrail イベントを使用して、バックアップポリシーが組織内の任意のアカウントから作成、更新、または削除されたとき、または無効な組織バックアッププランがあるときをモニタリングできます。詳細については、「AWS Backup デベロッパーガイド」の「クロスアカウント管理イベントのログ」を参照してください。

バックアップポリシーの構文と例

このページでは、バックアップポリシーの構文について説明し、例を示します。

バックアップポリシーの構文

バックアップポリシーは、JSON のルールに従って構造化されたプレーンテキストファイルです。バックアップポリシーの構文は、すべての管理ポリシータイプの構文に従います。詳細については、「管理ポリシータイプのポリシー構文と継承」を参照してください。このトピックでは、一般的な構文をバックアップポリシータイプの特定の要件に適用することを重点的に扱っています。

AWS Backup プランの詳細については、CreateBackupPlan」を参照してください。 AWS Backup

考慮事項

ポリシー構文

重複するキー名は JSON で拒否されます。

ポリシーでは、バックアップする AWS リージョン および リソースを指定する必要があります。

ポリシーでは、 が AWS Backup 引き受ける IAM ロールを指定する必要があります。

同じレベルで @@assign演算子を使用すると、既存の設定が上書きされる可能性があります。詳細については、「子ポリシーが親ポリシーの設定を上書きする」を参照してください。

継承演算子は、アカウントの有効なポリシーが作成される際に、継承されたポリシーとアカウントポリシーがどのようにマージされるかを制御します。これらの演算子には、値設定演算子と子制御演算子が含まれます。

詳細については、「継承演算子」および「バックアップポリシーの例」を参照してください。

IAM ロール

IAM ロールは、バックアッププランを初めて作成するときに存在する必要があります。

IAM ロールには、タグクエリで識別されるリソースにアクセスするためのアクセス許可が必要です。

IAM ロールには、バックアップを実行するアクセス許可が必要です。

バックアップボールト

ボールトは、バックアッププランを実行する AWS リージョン 前に、指定された各 に存在する必要があります。

ボールトは、有効なポリシーを受け取る AWS アカウントごとに存在する必要があります。詳細については、「 AWS Backup デベロッパーガイド」の「バックアップボールトの作成と削除」を参照してください。

AWS CloudFormation スタックセットとその Organizations との統合を使用して、組織内の各メンバーアカウントのバックアップボールトと IAM ロールを自動的に作成および設定することをお勧めします。詳細については、AWS CloudFormation ユーザーガイドのセルフマネージド型のアクセス許可を持つスタックセットの作成を参照してください。

クォータ

クォータのリストについては、「 AWS Backup デベロッパーガイド」のAWS Backup 「クォータ」を参照してください。

バックアップ構文: 概要

バックアップポリシー構文には、次のコンポーネントが含まれます。

```
{
    "plans": {
```

```
        "PlanName": {
            "rules": { ... },
            "regions": { ... },
            "selections": { ... },
            "advanced_backup_settings": { ... },
            "backup_plan_tags": { ... }
        }
    }
}
```

バックアップポリシーの要素

要素	説明	必須
ルール	バックアップルールのリスト。各ルールは、および selections 要素で指定されたリソースのバックアップの開始時期regionsと実行ウィンドウを定義します。	はい
リージョン	バックアップポリシー AWS リージョン がリソースを保護できる のリスト。	はい
選択	バックアップがrules保護regionsする指定された 内の 1 つ以上のリソースタイプ。	はい
advanced_backup_settings	特定のバックアップシナリオの設定オプション。 現在サポートされている高度なバックアップ設定は、Amazon EC2 インスタンスで実行されている Windows または SQL Server の Microsoft Volume Shadow Copy Service (VSS) バックアップを有効にすることです。	いいえ
backup_plan_tags	バックアッププランに関連付けるタグ。各タグは、ユーザー定義のキーと値で構成されるラベルです。 タグは、バックアッププランの管理、識別、整理、検索、フィルタリングに役立ちます。	いいえ

バックアップ構文: ルール

rules ポリシーキーは、選択したリソースで が AWS Backup 実行するスケジュールされたバックアップタスクを指定します。

バックアップルールの要素

要素	説明	必須
schedule_expression	がバックアップジョブ AWS Backup を開始するタイミングを指定する UTC の Cron 式。 cron 式の詳細については、「Amazon EventBridge ユーザーガイド」の「cron 式と rate 式を使用してルールをスケジュールする」を参照してください。	はい
target_backup_vault_name	バックアップが保存されるバックアップボールト。 バックアップボールトは、それらを作成するために使用されるアカウントと、それらが作成される AWS リージョン に固有の名前で識別されます。	はい
start_backup_window_minutes	バックアップジョブが正常に開始されない場合、バックアップジョブをキャンセルするまで待機する分数。 この値を含める場合、エラーを避けるために少なくとも 60 分必要です。	いいえ
complete_backup_window_minutes	N バックアップジョブが正常に開始されてから完了するまでの分数。完了しないと、 によってキャンセルされます AWS Backup。	いいえ
enable_continuous_backup	が継続的バックアップ AWS Backup を作成するかどうかを指定します。 True は、 AWS Backup がpoint-in-time復元 (PITR) が可能な継続的バックアップを作成	いいえ

要素	説明	必須
	します。 `False` (または指定なし) は、 AWS Backup がスナップショットバックアップを作成します。 連続バックアップの詳細については、AWS Backup デベロッパーガイドのポイントインタイムリカバリを参照してください。 注： PITR 対応バックアップの最大保持期間は 35 日です。	

要素	説明	必須
lifecycle	がバックアップをコールドストレージ AWS Backup に移行するタイミングと有効期限を指定します。 コールドストレージに移行できるリソースタイプは、「 AWS Backup デベロッパーガイド」の「リソース別の機能の可用性」表「リソース別の機能の可用性」に記載されています。 各ライフサイクルには、次の要素が含まれます。 • move_to_cold_storage_after_days ：が復旧ポイントをコールドストレージ AWS Backup に移動するまでのバックアップ発生からの日数。 • delete_after_days ：が復旧ポイント AWS Backup を削除するまでにバックアップが発生してからの日数。 • opt_in_to_archive_for_supported_resources ：この値が として割り当てられている場合true、バックアッププランは、ライフサイクル設定に従って、サポートされているリソースをアーカイブ (コールド) ストレージ階層に移行します。 注: コールドストレージに移行するバックアップは、最低 90 日間コールドストレージに保存する必要があります。 つまり、 は より 90 日長くdelete_after_days する必要がありますmove_to_cold_storage_after_days 。	いいえ

要素	説明	必須

copy_actions	がバックアップを 1 つ以上の追加の場所 AWS Backup にコピーするかどうかを指定します。
	
	各コピーアクションには、次の要素が含まれます。
	
	• target_backup_vault_arn : が AWS Backup バックアップの追加のコピーを保存するボールト。
	  • 同じアカウントのコピー$accountに を使用する
	  • クロスアカウントコピーに実際のアカウント ID を使用する
	• lifecycle : がバックアップをコールドストレージ AWS Backup に移行するタイミングと有効期限を指定します。
	
	  各ライフサイクルには、次の要素が含まれます。
	  • move_to_cold_storage_after_days : が復旧ポイントをコールドストレージに移動するまでの AWS Backup バックアップ発生からの日数。
	  • delete_after_days : が復旧ポイント AWS Backup を削除するまでに のバックアップが発生してからの日数。
	
	注: コールドストレージに移行したバックアップは、最低 90 日間コールドストレージに保存する必要があります。
	
	つまり、 は より 90 日長くdelete_after_days する必要がありますmove_to_cold_storage_after_days 。
		いいえ

要素	説明	必須
recovery_point_tags	バックアップから復元されたリソースに割り当てるタグ。 各タグには、次の要素が含まれています。 • tag_key: タグ名 (大文字と小文字を区別) • tag_value ：タグ値 (大文字と小文字を区別)	いいえ
index_actions	が Amazon EBS スナップショットおよび/または Amazon S3 バックアップのバックアップインデックス AWS Backup を作成するかどうかを指定します。バックアップインデックスは、バックアップのメタデータを検索するために作成されます。バックアップインデックスの作成とバックアップ検索の詳細については、「バックアップ検索」を参照してください。 注： Amazon EBS スナップショットバックアップインデックスを作成するには、追加の IAM ロールのアクセス許可が必要です。 各インデックスアクションには次の要素が含まれます。インデックス作成でサポートされているresource_types リソースタイプは Amazon EBS と Amazon S3 です。このパラメータは、インデックス作成にオプトインするリソースタイプを指定します。	いいえ

バックアップ構文: リージョン

regions ポリシーキーは、 AWS リージョン がselectionsキーの条件に一致するリソースを見つけるためにどの AWS Backup を検索するかを指定します。

バックアップリージョンの要素

要素	説明	必須
regions	AWS リージョン コードを指定します。例: ["us-east-1", "eu-north-1"] 。	はい

バックアップ構文: 選択

selections ポリシーキーは、バックアップポリシーのルールによってバックアップされるリソースを指定します。

相互に排他的な要素は tagsと の 2 つですresources。有効なポリシーを有効にするには、タグresourcesとして または haveを選択する必要があります。

タグ条件とリソース条件の両方を含む選択が必要な場合は、 resourcesキーを使用します。

バックアップ選択要素: タグ

要素	説明	必須
iam_role_arn	が、指定されたリージョン全体のリソースをクエリ、検出、バックアップすることを AWS Backup 引き受ける IAM ロール。 ロールには、タグ条件に基づいてリソースをクエリし、一致するリソースに対してバックアップオペレーションを実行するための十分なアクセス許可が必要です。	はい
tag_key	検索するタグキー名。	はい
tag_value	一致する tag_key に関連付ける必要がある値。 AWS Backup には、tag_key と tag_value の両方が一致する (大文字と小文字が区別される) 場合にのみ、 リソースが含まれます。	はい
conditions	含めるか除外するタグキーと値	いいえ

要素	説明	必須
	string_equals または string_not_equals を使用して、完全に一致するタグを含めるか除外します。 string_like と string_not_like を使用して、特定の文字を含むタグまたは含まないタグを含めるか除外する 注： 選択ごとに 30 の条件に制限されています。	

バックアップ選択要素: リソース

要素	説明	必須
`iam_role_arn`	が、指定されたリージョン全体のリソースをクエリ、検出、バックアップすることを AWS Backup 引き受ける IAM ロール。 ロールには、タグ条件に基づいてリソースをクエリし、一致するリソースに対してバックアップオペレーションを実行するための十分なアクセス許可が必要です。 注： では AWS GovCloud (US) Regions、パーティションの名前を ARN に追加する必要があります。 たとえば、`arn:aws:ec2:*:*:volume/*`「」は`arn:aws-us-gov:ec2:*:*:volume/*` 「」である必要があります。	はい
`resource_types`	バックアッププランに含めるリソースタイプ。	はい
`not_resource_types`	バックアッププランから除外するリソースタイプ。	いいえ

要素	説明	必須
conditions	含めるか除外するタグキーと値 string_equals または string_not_equals を使用して、完全に一致するタグを含めるか除外します。 string_like と string_not_like を使用して、特定の文字を含むタグまたは含まないタグを含めるか除外する 注： 選択ごとに 30 の条件に制限されています。	いいえ

サポートされているリソースタイプ

Organizations は、 要素resource_typesと not_resource_types要素に対して次のリソースタイプをサポートしています。

- AWS Backup gateway 仮想マシン: "arn:aws:backup-gateway:*:*:vm/*"
- AWS CloudFormation スタック: "arn:aws:cloudformation:*:*:stack/*"
- Amazon DynamoDB テーブル: "arn:aws:dynamodb:*:*:table/*"
- Amazon EC2 インスタンス: "arn:aws:ec2:*:*:instance/*"
- Amazon EBS ボリューム: "arn:aws:ec2:*:*:volume/*"
- Amazon EFS ファイルシステム: "arn:aws:elasticfilesystem:*:*:file-system/*"
- Amazon Aurora/Amazon DocumentDB/Amazon Neptune クラスター: "arn:aws:rds:*:*:cluster:*"
- Amazon RDS データベース: "arn:aws:rds:*:*:db:*"
- Amazon Redshift クラスター: "arn:aws:redshift:*:*:cluster:*"
- Amazon S3: "arn:aws:s3:::*"
- AWS Systems Manager for SAP HANA データベース: "arn:aws:ssm-sap:*:*:HANA/*"
- AWS Storage Gateway ゲートウェイ: "arn:aws:storagegateway:*:*:gateway/*"
- Amazon Timestream データベース: "arn:aws:timestream:*:*:database/*"
- Amazon FSx ファイルシステム: "arn:aws:fsx:*:*:file-system/*"

- Amazon FSx ボリューム: `"arn:aws:fsx:*:*:volume/*"`

コード例

詳細については、「タグブロックを使用したリソースの指定」および「リソースブロックを使用したリソースの指定」を参照してください。

バックアップ構文: 高度なバックアップ設定

`advanced_backup_settings` キーは、特定のバックアップシナリオの設定オプションを指定します。各設定には、次の要素が含まれます。

高度なバックアップ設定の要素

要素	説明	必須
`advanced_backup_settings`	特定のバックアップシナリオの設定を指定します。このキーには 1 つ以上の設定が含まれます。各設定は、次の要素を持つ JSON オブジェクト文字列です。 現在サポートされている高度なバックアップ設定は、Amazon EC2 インスタンスで実行されている Windows または SQL Server の Microsoft Volume Shadow Copy Service (VSS) バックアップを有効にすることです。 各高度なバックアップでは、次の要素が設定されます。 • `Object key name`: 次の詳細設定が適用されるリソースのタイプを指定する文字列。	いいえ

要素	説明	必須
	キー名は"ec2"リソースタイプである必要があります • Object value: 関連付けられたリソースタイプに固有の 1 つ以上のバックアップ設定を含む Dtring。 値は、Amazon EC2 インスタンスで実行されるバックアップdisabledのサポート"windows_vss" が enabledまたは であることを指定します。	

例:

```
"advanced_backup_settings": {
    "ec2": {
        "windows_vss": {
            "@@assign": "enabled"
        }
    }
},
```

バックアップ構文: バックアッププランタグ

backup_plan_tags ポリシーキーは、バックアッププラン自体にアタッチされるタグを指定します。これは、 rulesまたは に指定されたタグには影響しませんselections。

バックアッププランのタグ要素

要素	説明	必須
backup_plan_tags	各タグは、ユーザー定義のキーと値で構成されるラベルです。	いいえ

要素	説明	必須
	• tag_key: 検索するキー名にタグを付けます。 値では、大文字と小文字が区別されます。 • tag_value : バックアッププランにアタッチされ、 に関連付けられている値tag_key。 値では、大文字と小文字が区別されます。	

バックアップポリシーの例

次のサンプルバックアップポリシーは、情報提供のみを目的としています。以下の例の一部では、スペースを節約するために JSON の空白書式が圧縮される場合があります。

- 例 1: 親ノードに割り当てられたポリシー
- 例 2: 親ポリシーが子ポリシーとマージされる
- 例 3: 親ポリシーが子ポリシーによる変更を禁止する
- 例 4: 親ポリシーは、子ポリシーによる 1 つのバックアッププランへの変更を禁止する
- 例 5: 子ポリシーが親ポリシーの設定を上書きする
- 例 6: タグブロックを使用したリソースの指定
- 例 7: リソースブロックを使用したリソースの指定

例 1: 親ノードに割り当てられたポリシー

次の例は、アカウントの親ノードの 1 つに割り当てられているバックアップポリシーを示しています。

親ポリシー - このポリシーは、組織のルート、またはすべての対象アカウントの親である任意の OU にアタッチできます。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "ap-northeast-2",
```

```
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {
                        "@@assign": "cron(0 5/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@assign": "480"
                    },
                    "complete_backup_window_minutes": {
                        "@@assign": "10080"
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {
                            "@@assign": "180"
                        },
                        "delete_after_days": {
                            "@@assign": "270"
                        },
                        "opt_in_to_archive_for_supported_resources": {
                            "@@assign": "false"
                        }
                    },
                    "target_backup_vault_name": {
                        "@@assign": "FortKnox"
                    },
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
```

```
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
                                },
                                "opt_in_to_archive_for_supported_resources": {
                                    "@@assign": "false"
                                }
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:backup-vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
                                },
                                "opt_in_to_archive_for_supported_resources": {
                                    "@@assign": "false"
                                }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {
                            "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                        },
                        "tag_key": {
                            "@@assign": "dataType"
                        },
                        "tag_value": {
                            "@@assign": [
```

```
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": {
                        "@@assign": "enabled"
                    }
                }
            }
        }
    }
}
```

他のポリシーがアカウントに継承またはアタッチされていない場合、該当する各 でレンダリングされる有効なポリシーは次の例の AWS アカウント ようになります。CRON 式を使用すると、バックアップは毎正時に実行されます。アカウント ID 123456789012 は、各アカウントの実際のアカウント ID になります。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
```

```
                    },
                    "lifecycle": {
                        "delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180",
                        "opt_in_to_archive_for_supported_resources": "false"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180",
                                "opt_in_to_archive_for_supported_resources": "false"
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:backup-vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180",
                                "opt_in_to_archive_for_supported_resources": "false"
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "datatype": {
                            "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                            "tag_key": "dataType",
                            "tag_value": [
                                "PII",
                                "RED"
                            ]
                        }
```

```
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": "enabled"
                }
            }
        }
    }
}
```

例 2: 親ポリシーが子ポリシーとマージされる

次の例では、継承された親ポリシーと子ポリシーを継承するか、 AWS アカウント マージに直接アタッチして有効なポリシーを形成します。

親ポリシー - このポリシーは、組織のルートまたは任意の親 OU にアタッチできます。

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": { "@@append":[ "us-east-1", "ap-northeast-3", "eu-north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 0/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "60" },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "28" },
                        "delete_after_days": { "@@assign": "180" },
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault" : {
```

```
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "28" },
                                "delete_after_days": { "@@assign": "180" },
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII", "RED" ] }
                    }
                }
            }
        }
    }
}
```

子ポリシー - このポリシーは、アカウントに直接アタッチすることも、親ポリシーがアタッチされているより低いレベルの OU にアタッチすることもできます。

```
{
    "plans": {
       "Monthly_Backup_Plan": {
            "regions": {
                "@@append":[ "us-east-1", "eu-central-1" ] },
            "rules": {
                "Monthly": {
                    "schedule_expression": { "@@assign": "cron(0 5 1 * ? *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "target_backup_vault_name": { "@@assign": "Default" },
                    "lifecycle": {
```

```
                        "move_to_cold_storage_after_days": { "@@assign": "30" },
                        "delete_after_days": { "@@assign": "365" },
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:Default" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "30" },
                                "delete_after_days": { "@@assign": "365" },
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "MonthlyDatatype": {
                            "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyMonthlyBackupIamRole" },
                            "tag_key": { "@@assign": "BackupType" },
                            "tag_value": { "@@assign": [ "MONTHLY", "RED" ] }
                        }
                    }
                }
            }
        }
}
```

最終的に適用される有効なポリシー - アカウントに適用される有効なポリシーには、2 つのプランがあり、それぞれに独自のルールのセットとルールを適用するリソースのセットがあります。

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": [ "us-east-1", "ap-northeast-3", "eu-north-1" ],
```

```
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180",
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "delete_after_days": "180",
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [ "PII", "RED" ]
                    }
                }
```

```
            }
        },
        "Monthly_Backup_Plan": {
            "regions": [ "us-east-1", "eu-central-1" ],
            "rules": {
                "monthly": {
                    "schedule_expression": "cron(0 5 1 * ? *)",
                    "start_backup_window_minutes": "480",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30",
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:Default" : {
                            "target_backup_vault_arn": {
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "30",
                                "delete_after_days": "365",
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "monthlydatatype": {
                        "iam_role_arn": "arn:aws:iam::&ExampleAWSAccountNo3;:role/
MyMonthlyBackupIamRole",
                        "tag_key": "BackupType",
                        "tag_value": [ "MONTHLY", "RED" ]
                    }
                }
            }
        }
    }
```

```
}
```

例 3: 親ポリシーが子ポリシーによる変更を防止する

次の例では、継承された親ポリシーが子制御演算子を使用してすべての設定を強制し、子ポリシーによって変更またはオーバーライドされないようにします。

親ポリシー - このポリシーは、組織のルートまたは任意の親 OU にアタッチできます。ポリシーのすべてのノードに "@@operators_allowed_for_child_policies": ["@@none"] が存在するということは、子ポリシーがどのような変更もプランに加えられないことを意味します。また、子ポリシーにより有効なポリシーにプランを追加することもできません。このポリシーは、関連付けられている OU の下にあるすべての OU およびアカウントに対して有効なポリシーになります。

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@none"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "Hourly": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "schedule_expression": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "cron(0 0/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "60"
                    },
                    "target_backup_vault_name": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "FortKnox"
                    },
                    "index_actions": {
```

```
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                    },
                    "lifecycle": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "move_to_cold_storage_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "28"
                        },
                        "delete_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "180"
                        },
                        "opt_in_to_archive_for_supported_resources": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "false"
                        }
                    },
                    "copy_actions": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault",
                                "@@operators_allowed_for_child_policies": ["@@none"]
                            },
                            "lifecycle": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "delete_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "28"
                                },
                                "move_to_cold_storage_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "180"
```

```
                                },
                                 "opt_in_to_archive_for_supported_resources": {
                                    "@@operators_allowed_for_child_policies":
["@@none"],
                                    "@@assign": "false"
                                }
                            }
                        }
                    }
                },
                "selections": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "tags": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "datatype": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "iam_role_arn": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                            },
                            "tag_key": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "@@assign": "dataType"
                            },
                            "tag_value": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "@@assign": [
                                    "PII",
                                    "RED"
                                ]
                            }
                        }
                    }
                },
                "advanced_backup_settings": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "ec2": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "windows_vss": {
                            "@@assign": "enabled",
                            "@@operators_allowed_for_child_policies": ["@@none"]
                        }
                    }
```

```
            }
        }
    }
}
```

最終的に適用される有効なポリシー - 子バックアップポリシーが存在する場合、それらは無視され、親ポリシーが有効なポリシーになります。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180",
                        "opt_in_to_archive_for_supported_resources": "false"
                    },
                    "copy_actions": {
                        "target_backup_vault_arn": "arn:aws:backup:us-
east-1:123456789012:backup-vault:secondary_vault",
                        "lifecycle": {
                            "move_to_cold_storage_after_days": "28",
                            "delete_after_days": "180",
                            "opt_in_to_archive_for_supported_resources": "false"
                        }
                    }
```

```
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {"windows_vss": "enabled"}
            }
        }
    }
}
```

例 4: 親ポリシーが、子ポリシーによる 1 つのバックアッププランへの変更を防止する

次の例では、継承された親ポリシーが子制御演算子を使用して単一のプランの設定を強制し、子ポリシーによって変更またはオーバーライドされないようにします。子ポリシーがプランを追加することはできます。

親ポリシー - このポリシーは、組織のルートまたは任意の親 OU にアタッチできます。この例は、plans 最上位レベルを除き、すべての子継承演算子がブロックされた前の例に似ています。このレベルでの @@append の設定により、子ポリシーが、有効なポリシーのコレクションに他の計画を追加できます。継承されたプランに対する変更は引き続きブロックされます。

プラン内のセクションは、わかりやすくするために切り捨てられています。

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@append"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
```

```
        }
    }
}
```

子ポリシー - このポリシーは、アカウントに直接アタッチすることも、親ポリシーがアタッチされているより低いレベルの OU にアタッチすることもできます。この子ポリシーは、新しいプランを定義します。

プラン内のセクションは、わかりやすくするために切り捨てられています。

```
{
    "plans": {
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

最終的に適用される有効なポリシー - 有効なポリシーには、両方のプランが含まれます。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        },
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

例 5: 子ポリシーが親ポリシーの設定をオーバーライドする

次の例では、子ポリシーが値設定演算子を使用して、親ポリシーから継承された設定の一部をオーバーライドしています。

親ポリシー - このポリシーは、組織のルートまたは任意の親 OU にアタッチできます。どの設定も子ポリシーによりオーバーライドできます。これは、デフォルトの動作を禁止する子制御演算子がない場合は、子ポリシーに @@assign、@@append、または@@remove が許可されるためです。親ポリシーには、有効なバックアッププランに必要なすべての要素が含まれているため、そのまま継承されていればリソースが正常にバックアップされます。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/1 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "target_backup_vault_name": {"@@assign": "FortKnox"},
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "delete_after_days": {"@@assign": "2"},
                        "move_to_cold_storage_after_days": {"@@assign": "180"},
                        "opt_in_to_archive_for_supported_resources": {"@@assign":
 false}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:t2": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:backup-vault:t2"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "28"},
                                "delete_after_days": {"@@assign": "180"},
```

```
                                "opt_in_to_archive_for_supported_resources":
 {"@@assign": false}
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            }
        }
    }
}
```

子ポリシー - 子ポリシーには、継承された親ポリシーとは異なる必要がある設定のみが含まれます。有効なポリシーにマージするときは、その他の必須設定を提供する、継承された親ポリシーが必要です。それがないと、有効なバックアップポリシーには無効なバックアッププランが格納され、期待どおりにリソースがバックアップされません。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "us-west-2",
                    "eu-central-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/2 ? * * *)"},
```

```
                    "start_backup_window_minutes": {"@@assign": "80"},
                    "target_backup_vault_name": {"@@assign": "Default"},
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "30"},
                        "delete_after_days": {"@@assign": "365"},
                        "opt_in_to_archive_for_supported_resources": {"@@assign":
 false}
                    }
                }
            }
        }
    }
}
```

最終的に適用される有効なポリシー - 有効なポリシーには両方のポリシーの設定が含まれます。子ポリシーによって提供される設定が、親ポリシーから継承された設定をオーバーライドします。この例では、以下の変更が発生します。

- リージョンのリストは、まったく別のリストに置き換えられます。継承リストにリージョンを追加する場合、子ポリシーで @@assign の代わりに @@append を使用します。
- AWS Backup は、時間単位ではなく 2 時間ごとに実行します。
- AWS Backup では、60 分ではなく 80 分でバックアップを開始できます。
- AWS Backup はDefault、 の代わりにボールトを使用しますFortKnox。
- ライフサイクルは、コールドストレージへの転送とバックアップの最終的な削除の両方について延長されます。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-west-2",
                "eu-central-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/2 ? * * *)",
                    "start_backup_window_minutes": "80",
                    "target_backup_vault_name": "Default",
                     "index_actions": {
                        "resource_types": {
```

```
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30",
                        "opt_in_to_archive_for_supported_resources": "false"

                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:backup-vault:secondary_vault"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "delete_after_days": "180",
                                "opt_in_to_archive_for_supported_resources": "false"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            }
        }
    }
}
```

例 6: **tags**ブロックを使用したリソースの指定

次の例には、 tag_key = “env”および = および tag_value "prod" を持つすべてのリソースが含まれています"gamma"。この例では、 tag_key = "backup"および = tag_value のリソースを除外します"false"。

```
...
"selections":{
    "tags":{
        "selection_name":{
            "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/IAMRole"},
            "tag_key":{"@@assign": "env"},
            "tag_value":{"@@assign": ["prod", "gamma"]},
            "conditions":{
                "string_not_equals":{
                    "condition_name1":{
                        "condition_key": { "@@assign": "aws:ResourceTag/backup"  },
                        "condition_value": {  "@@assign": "false" }
                    }
                }
            }
        }
    }
},
...
```

例 7: **resources**ブロックを使用したリソースの指定

以下は、 resourcesブロックを使用してリソースを指定する例です。

Example: Select all resources in my account

ブールロジックは、IAM ポリシーで使用するものと似ています。"resource_types" ブロックはブール値ANDを使用してリソースタイプを組み合わせます。

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
```

```
            ]
        }
    }
},
...
```

Example: Select all resources in my account, but exclude Amazon EBS volumes

ブールロジックは、IAM ポリシーで使用するものと似ています。ブロック"resource_types"と "not_resource_types"ブロックは、ブール値ANDを使用してリソースタイプを組み合わせます。

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
            ]
        },
        "not_resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*"
            ]
        }
    }
},
...
```

Example: Select all resources tagged with "backup" : "true", but exclude Amazon EBS volumes

ブールロジックは、IAM ポリシーで使用するものと似ています。ブロック"resource_types"と "not_resource_types"ブロックは、ブール値ANDを使用してリソースタイプを組み合わせます。"conditions" ブロックはブール型 を使用しますAND。

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
```

```
                "*"
            ]
        },
        "not_resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*"
            ]
        },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key": { "@@assign":"aws:ResourceTag/backup"},
                    "condition_value": {  "@@assign":"true" }
                }
            }
        }
    }
},
...
```

Example: Select all Amazon EBS volumes and Amazon RDS DB instances tagged with both "backup" : "true" and "stage" : "prod"

ブールロジックは、IAM ポリシーで使用するものと似ています。"resource_types" ブロックはブール値ANDを使用してリソースタイプを組み合わせます。"conditions" ブロックはブール値を使用してANDリソースタイプとタグ条件を組み合わせます。

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:rds:*:*:db:*"
            ]
        },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/backup"},
                    "condition_value":{"@@assign":"true"}
                },
```

```
                "condition_name2":{
                    "condition_key":{"@@assign":"aws:ResourceTag/stage"},
                    "condition_value":{"@@assign":"prod"}
                }
            }
        }
    }
},
...
```

Example: Select all Amazon EBS volumes and Amazon RDS instances tagged with "backup" : "true" but not "stage" : "test"

ブールロジックは、IAM ポリシーで使用するものと似ています。"resource_types" ブロックはブール値ANDを使用してリソースタイプを組み合わせます。"conditions" ブロックはブール値を使用してANDリソースタイプとタグ条件を組み合わせます。

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:rds:*:*:db:*"
            ]
        },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/backup"},
                    "condition_value":{"@@assign":"true"}
                  }
            },
            "string_not_equals":{
                "condition_name2":{
                    "condition_key":{"@@assign":"aws:ResourceTag/stage"},
                    "condition_value":{"@@assign":"test"}
                }
            }
        }
    }
},
```

```
...
```

Example: Select all resources tagged with "key1" and a value which begins with "include" but not with "key2" and value that contains the word "exclude"

ブールロジックは、IAM ポリシーで使用するものと似ています。"resource_types" ブロックはブール値ANDを使用してリソースタイプを組み合わせます。"conditions" ブロックはブール値を使用してANDリソースタイプとタグ条件を組み合わせます。

この例では、、include*、*exclude*および (*)でワイルドカード文字を使用することに注意してくださいarn:aws:rds:*:*:db:*。ワイルドカード文字は、文字列の先頭、末尾、中間(*)で使用できます。

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
            ]
        },
        "conditions":{
            "string_like":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/key1"},
                    "condition_value":{"@@assign":"include*"}
                }
            },
            "string_not_like":{
                "condition_name2":{
                    "condition_key":{"@@assign":"aws:ResourceTag/key2"},
                    "condition_value":{"@@assign":"*exclude*"}
                }
            }
        }
    }
},
...
```

Example: Select all resources tagged with "backup" : "true" except Amazon FSx file systems and Amazon RDS resources

ブールロジックは、IAM ポリシーで使用するものと似ています。ブロック"resource_types"と "not_resource_types"ブロックは、ブール値ANDを使用してリソースタイプを組み合わせます。"conditions" ブロックはブール値を使用してANDリソースタイプとタグ条件を組み合わせます。

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
            "resource_types":{
                "@@assign": [
                    "*"
               ]
            },
            "not_resource_types":{
                "@@assign":[
                    "arn:aws:fsx:*:*:file-system/*",
                    "arn:aws:rds:*:*:db:*"
                ]
            },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/backup"},
                    "condition_value":{"@@assign":"true"}
                }
            }
        }
    }
},
...
```

タグポリシー

タグポリシーを使用すると、組織のアカウントの AWS リソースにアタッチされたタグを標準化できます。

タグポリシーを使用して、タグキーおよびタグ値の大文字と小文字の処理方法の設定など、一貫したタグを維持できます。

タグとは

タグは、ユーザーが割り当てるか、 が AWS AWS リソースに割り当てるカスタム属性ラベルです。各タグは 2 つの部分で構成されます。

- タグキー (例： `CostCenter`、`Environment`、または `Project`)。タグキーでは、大文字と小文字が区別されます。
- タグ値として知られるオプションのフィールド (例： `111122223333` または `Production`)。タグ値を省略すると、空の文字列を使用した場合と同じになります。タグキーと同様に、タグ値では大文字と小文字が区別されます。

このページの残りの部分では、タグポリシーについて説明します。タグの詳細については、次のソースを参照してください。

- 命名規則や使用規則など、タグ付けに関する一般的な情報については、AWS 「 リソースのタグ付けユーザーガイド」を参照してください。
- タグの使用をサポートするサービスのリストについては、「リResource Groups のタグ付け API リファレンス」を参照してください。
- タグを使用してリソースを分類する方法については、「Best Practices for Tagging AWS Resources Whitepaper」を参照してください。
- Organizations リソースのタグ付けについては、「AWS Organizations リソースのタグ付け」を参照してください。
- 他の のリソースのタグ付けについては AWS のサービス、そのサービスのドキュメントを参照してください。

タグポリシーとは

タグポリシーはポリシーの一種で、組織のアカウント内のリソース間でタグを標準化するのに役立ちます。タグポリシーでは、リソースのタグ付けの際に適用されるタグ付けルールを指定します。

例えば、タグポリシーでは、`CostCenter` タグがリソースにアタッチされる際に、タグポリシーで定義されている大文字小文字の処理とタグ値を使用する必要があることを指定できます。タグポリシーは、指定したリソースタイプで非準拠のタグ付け操作を強制するように指定することもできま

す。つまり、指定されたリソースタイプで非準拠のタグ付けリクエストは完了できません。タグなしリソースまたはタグポリシーで定義されていないタグは、タグポリシーに準拠しているかどうか評価されません。

タグポリシーを使用するには、複数の を使用する必要があります AWS のサービス。

- AWS Organizations を使用してタグポリシーを管理します。組織の管理アカウントにサインインする場合、Organizations を使用してタグポリシー機能を有効にします。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。次に、タグポリシーを作成して組織エンティティにアタッチし、タグ付けルールを有効にすることができます。
- AWS Resource Groups を使用して、タグポリシーへの準拠を管理します。組織のアカウントにサインインする場合は、Resource Groups を使用してアカウント内のリソースで非準拠のタグを検索します。リソースを作成した AWS サービスで非準拠のタグを修正できます。タグエディタと Resource Groups Tagging API を使用して、複数の サービスからリソースにタグ付けおよびタグ解除することもできます。

  組織の管理アカウントにサインインすると、組織のすべてのアカウントのコンプライアンス情報を表示できます。

タグポリシーは、すべての機能が有効になっている組織でのみ使用できます。タグポリシーを使用するための詳しい要件については、「の管理ポリシーの前提条件とアクセス許可 AWS Organizations」を参照してください。

> **Important**
>
> タグポリシーの使用を開始するには、 では、より高度なタグポリシーに進むタグポリシーの開始方法前に、「」で説明されているワークフロー例に従うことを AWS 強くお勧めします。OU または組織全体にタグポリシーを展開する前に、単純なタグポリシーを単一のアカウントにアタッチした場合の影響を理解しておくことをお勧めします。タグポリシーへの準拠を強制する前に、タグポリシーの影響を理解することは特に重要です。タグポリシーの開始方法 ページの表には、より高度なポリシー関連タスクの手順へのリンクも記載されています。

タグポリシー使用のベストプラクティス

AWS では、タグポリシーを使用する際に以下のベストプラクティスを推奨しています。

タグの大文字小文字に関する方針を決定する

タグを大文字小文字どちらにするかを決め、その方針をすべてのリソースタイプに一貫して実装します。例えば、Costcenter、costcenter、CostCenter のいずれを使用するかを決定し、すべてのタグに同じ規則を使用します。コンプライアンスレポートの結果に一貫性を持たせるには、大文字と小文字が異なる類似タグを使用しないでください。この方針は、組織のタグポリシーを定義するのに役立ちます。

推奨されるワークフローを使用する

単純なタグポリシーを作成して、小規模なものから始めます。次に、テスト目的で使用できるメンバーアカウントにアタッチします。「タグポリシーの開始方法」で説明されているワークフローを使用します。

タグ付けルールを決定する

これは、組織のニーズによって異なります。たとえば、CostCenterタグを AWS Secrets Manager シークレットにアタッチするときに、指定された大文字と小文字の処理を使用するように指定できます。準拠タグを定義するタグポリシーを作成し、タグ付けルールを有効にする組織エンティティにアタッチします。

アカウント管理者を教育する

タグポリシーの使用範囲を広げる準備ができたら、アカウント管理者を次のように教育します。

- タグ付け方針を伝えます。
- 管理者は特定のリソースタイプでタグを使用する必要があることを強調します。

  タグなしリソースは、コンプライアンス結果で非準拠と表示されないため、これが重要となります。
- タグポリシーへの準拠を確認するためのガイダンスを提供します。「 リソースのタグ付けユーザーガイド」の「 アカウントのコンプライアンスの評価」で説明されている手順を使用して、 アカウントのリソースの非準拠タグを検索して修正するように管理者に指示します。 AWS コンプライアンスをチェックする頻度を知らせます。

コンプライアンスの強制には注意が必要です。

コンプライアンスの強制によって、組織のアカウントのユーザーが必要なリソースにタグ付けできなくなる可能性があります。「強制について」の情報を確認します。「タグポリシーの開始方法」で説明されているワークフローも参照してください。

リソース作成リクエストにガードレールを設定するための SCP の作成を検討する

タグが付けられたことがないリソースは、レポートで非準拠として表示されません。アカウント管理者は、それでもタグなしリソースを作成できます。場合によっては、サービスコントロールポリシー (SCP) を使用して、リソース作成リクエストの周囲にガードレールを設定できます。SCP の例については、「 作成される特定のリソースにタグを要求する」を参照してください。

AWS サービスがタグを使用したアクセスの制御をサポートしているかどうかを確認するには、AWS のサービス「IAM ユーザーガイド」の「IAM と連携する 」を参照してください。 ABAC (タグに基づく認可) 列に「はい」があるサービスを探します。サービスの名前を選択すると、そのサービスの認可とアクセスコントロールに関するドキュメントが表示されます。

タグポリシーの開始方法

タグポリシーを使用するには、複数の を使用する必要があります AWS のサービス。開始するには、次のページを参照してください。次に、このページのワークフローに従って、タグポリシーとその影響について理解を深めます。

- の管理ポリシーの前提条件とアクセス許可 AWS Organizations
- タグポリシー使用のベストプラクティス

初めてのタグポリシーの使用

タグポリシーを初めて使用するには、次の手順に従います。

タスク	サインインするアカウント	AWS 使用する サービスコンソール
ステップ 1: 組織のタグポリシーを有効にします。	組織の管理アカウント[1]	AWS Organizations
ステップ 2: タグポリシーを作成します。 最初のタグポリシーはシンプルにするよう心がけます。使用する大文字小文字の処理に 1 つのタグキーを入力し、そ	組織の管理アカウント[1]	AWS Organizations

タスク	サインインするアカウント	AWS 使用する サービスコンソール
の他のオプションはすべてデフォルトのままにします。		
ステップ 3: テストに使用できる単一のメンバーアカウントにタグポリシーをアタッチします。 次のステップでは、このアカウントにサインインする必要があります。	組織の管理アカウント[1]	AWS Organizations
ステップ 4: 準拠タグを持つリソースと、非準拠タグを持つリソースを作成します。	テスト目的で使用するメンバーアカウント。	使い慣れた AWS サービス。例えば、AWS Secrets Manager を使って「基本的なシークレットを作成する」の手順に従い、準拠したシークレットと非準拠のシークレットを持つシークレットを作成できます。
ステップ 5: 有効なタグポリシーを表示し、アカウントのコンプライアンス状況を評価します。	テスト目的で使用するメンバーアカウント。	Resource Groups とリソースが作成された AWS サービス。 準拠タグと非準拠タグを使用してリソースを作成した場合、結果に非準拠タグが表示されます。
ステップ 6: テストアカウントのリソースがタグポリシーに準拠するまで、コンプライアンスの問題を検出して修正するプロセスを繰り返します。	テスト目的で使用するメンバーアカウント。	Resource Groups とリソースが作成された AWS サービス。

タスク	サインインするアカウント	AWS 使用する サービスコンソール
いつでも、組織全体のコンプライアンスを評価できます。	組織の管理アカウント[1]	リソースグループ

[1] 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。

タグポリシーの使用の拡大

次のタスクを任意の順序で実行すると、タグポリシーの使用を拡張できます。

高度なタスク	サインインするアカウント	AWS 使用する サービスコンソール
より高度なタグポリシーを作成します。 初回ユーザーと同じプロセスを実行しますが、他のタスクを試します。例えば、追加のキーや値を定義したり、タグキーに対して異なる大文字小文字の処理を指定したりします。 「管理ポリシーの継承を理解する」および「タグポリシー構文」の情報を使用して、より詳細なタグポリシーを作成できます。	組織の管理アカウント[1]	AWS Organizations
タグポリシーを追加のアカウントまたは OU にアタッチします。	組織の管理アカウント[1]	AWS Organizations

高度なタスク	サインインするアカウント	AWS 使用する サービスコンソール
アカウントまたはアカウントがメンバーである OU にさらにポリシーをアタッチした後、そのアカウントの有効なタグポリシーを確認します。		
新しいリソースが作成されたら、タグをリクエストする SCP を作成します。例については、 作成される特定のリソースにタグを要求するを参照してください。	組織の管理アカウント[1]	AWS Organizations
有効なタグポリシーが変更されるたびに、アカウントのコンプライアンスステータスが引き続き評価します。非準拠タグを修正します。	有効なタグポリシーを持つメンバーアカウント。	Resource Groups とリソースが作成された AWS サービス。
組織全体のコンプライアンスを評価します。	組織の管理アカウント[1]	リソースグループ

[1] 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。

初めてのタグポリシーの強制

初めてタグポリシーを強制するには、タグポリシーを初めて使用する場合と同じワークフローに従い、テストアカウントを使用します。

> **Warning**
>
> コンプライアンスの強制には注意が必要です。タグポリシーを使用した場合の影響を理解し、推奨されるワークフローに従ってください。テストアカウントで強制の仕組みをテストしてから、他のアカウントに展開します。そうしないと、組織のアカウントのユーザーが

必要なリソースにタグ付けできなくなる可能性があります。詳細については、「強制について」を参照してください。

強制タスク	サインインするアカウント	AWS 使用する サービスコンソール
ステップ 1: タグポリシーを作成します。 最初に強制するタグポリシーはシンプルにするよう心がけます。使用する大文字小文字の処理にタグキーを 1 つ入力し、[Prevent noncompliant operations for this tag (このタグに対する非準拠操作を防止する)] オプションを選択します。次に、適用するリソースタイプを 1 つ指定します。前述の例の続きとして、Secrets Manager シークレットに強制するよう選択します。	組織の管理アカウント[1]	AWS Organizations
ステップ 2: タグポリシーを単一のテストアカウントにアタッチします。	組織の管理アカウント[1]	AWS Organizations
ステップ 3: 準拠タグを持つリソースと、非準拠タグを持つリソースを作成してみます。タグポリシーで指定されたタイプのリソースに、非準拠のタグを作成することはできません。	テスト目的で使用するメンバーアカウント。	使い慣れた AWS サービス。例えば、AWS Secrets Manager を使って「基本的なシークレットを作成する」の手順に従い、準拠したシークレットと非準拠のシークレットを持つシークレットを作成できます。

強制タスク	サインインするアカウント	AWS 使用する サービスコンソール
手順 4: 有効なタグポリシーに対してアカウントのコンプライアンスステータスを評価し、非準拠タグを修正します。	テスト目的で使用するメンバーアカウント。	Resource Groups とリソースが作成された AWS サービス。
ステップ 5: テストアカウントのリソースがタグポリシーに準拠するまで、コンプライアンスの問題を検出して修正するプロセスを繰り返します。	テスト目的で使用するメンバーアカウント。	Resource Groups とリソースが作成された AWS サービス。
いつでも、組織全体のコンプライアンスを評価できます。	組織の管理アカウント[1]	リソースグループ

[1] 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。

Amazon EventBridge を使用した非準拠タグのモニタリング

Amazon EventBridge (旧 Amazon CloudWatch Events) を使用すると、非準拠タグが導入された場合にモニタリングできます。次のイベント例では、`tag-policy-compliant` の `"false"` 値が、新しいタグが有効なタグポリシーに準拠していないことを示します。

```
{
  "detail-type": "Tag Change on Resource",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "a-new-key"
    ],
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
    "tag-policy-compliant": "false",
```

```
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added"
    }
  }
}
```

イベントにサブスクライブし、監視する文字列またはパターンを指定できます。EventBridge の詳細は、「Amazon EventBridge ユーザーガイド」を参照してください。

強制について

タグポリシーは、指定したリソースタイプで非準拠のタグ付けオペレーションを強制するように指定できます。つまり、指定されたリソースタイプで非準拠のタグ付けリクエストは完了できません。

> **Important**
>
> 強制は、タグなしで作成されたリソースには影響しません。

タグポリシーへのコンプライアンスを強制するには、タグポリシーを作成するときに、次のいずれかの操作を行います。

- [Visual editor (ビジュアルエディタ)] タブで、[Prevent noncompliant operations for this tag (このタグに対する非準拠のオペレーションを禁止する)] を選択します。
- [JSON] タブで、`enforced_for` フィールドを使用します。タグポリシーの構文については、「タグポリシーの構文と例」を参照してください。

タグポリシーへの準拠を強制するには、次のベストプラクティスに従います。

- コンプライアンスの強制には注意が必要です - タグポリシーを使用した場合の影響を理解し、「タグポリシーの開始方法」で説明されている推奨ワークフローに従ってください。テストアカウントで強制の仕組みをテストしてから、他のアカウントに展開します。そうしないと、組織のアカウントのユーザーが必要なリソースにタグ付けできなくなる可能性があります。
- 強制できるリソースタイプに注意する - サポートされているリソースタイプに対してのみ、タグポリシーへの準拠を強制できます。コンプライアンスの強制をサポートするリソースタイプは、ビジュアルエディタを使用してタグポリシーを構築するときに一覧表示されます。
- 一部の サービスとのやり取りを理解する – 一部の AWS のサービス には、リソースを自動的に作成するコンテナのようなリソースのグループがあり、タグは 1 つのサービスのリソースから別

のサービスに伝播できます。例えば、Amazon EC2 Auto Scaling グループと Amazon EMR クラスターのタグは、それら含む Amazon EC2 インスタンスに自動的に伝播します。Auto Scaling グループまたは EMR クラスターよりも厳しい Amazon EC2 のタグポリシーがある場合があります。強制を有効にすると、タグポリシーによってリソースにタグ付けできなくなり、動的なスケーリングおよびプロビジョニングがブロックされる可能性があります。

次のセクションでは、非準拠のリソースを見つけ、準拠するものに修正する方法を説明します。

トピック

- でアカウントの非準拠リソースを検索する AWS Organizations
- を使用した リソースの非準拠タグの修正 AWS Organizations
- を使用した組織全体のコンプライアンスレポートの生成 AWS Organizations
- 強制をサポートするサービスとリソースタイプ

でアカウントの非準拠リソースを検索する AWS Organizations

各アカウントについて、非準拠のリソースに関する情報を取得できます。このコマンドは、アカウントにリソースがあるすべてのリージョンから実行する必要があります。

タグポリシーを使用するアカウントの非準拠のリソースを見つけるには、次のコマンドを実行し、結果をファイルに保存します。

```
$ aws resourcegroupstaggingapi get-resources  --region us-east-1 \
    --include-compliance-details \
    --exclude-compliant-resources > outputfile.txt
```

を使用した リソースの非準拠タグの修正 AWS Organizations

非準拠タグを見つけたら、以下のいずれかの方法を使用して修正します。非準拠タグの付いたリソースがあるアカウントにサインインする必要があります。

- 非準拠リソースを作成した AWS サービスのコンソールまたはタグ付け API オペレーションを使用します。
- 有効なポリシーに準拠するタグを追加したり、非準拠のタグを削除したりするには、 AWS Resource Groups TagResources および UntagResources オペレーションを使用します。

を使用した組織全体のコンプライアンスレポートの生成 AWS Organizations

組織全体の 内のタグ付けされたリソースをすべて一覧表示するレポートは、いつでも生成 AWS アカウント できます。レポートには、各リソースが有効なタグポリシーに準拠しているかどうかが表示されます。タグポリシーまたはリソースに加えた変更が組織全体のコンプライアンスレポートに反映されるまで、最大で 48 時間かかる可能性があります。例えば、リソースタイプに対して新しい標準化されたタグを定義するタグポリシーがあるとします。レポートでは、このタイプでこのタグを持たないリソースが最大 48 時間にわたって準拠していると表示されます。

us-east-1 リージョンの組織の管理アカウントが Amazon S3 バケットにアクセスできる場合、このアカウントからレポートを生成できます。「Amazon S3 Bucket Policy for Storing Report」に示されているように、バケットにはバケットポリシーがアタッチされている必要があります。レポートを生成するには、次のコマンドを実行します。

```
$ aws resourcegroupstaggingapi start-report-creation --region us-east-1
```

一度に生成できるレポートは 1 つです。

このレポートは完了までに時間がかかる場合があります。ステータスを確認するには、次のコマンドを実行します。

```
$ aws resourcegroupstaggingapi describe-report-creation --region us-east-1
{
    "Status": "SUCCEEDED"
}
```

上記のコマンドが SUCCEEDED を返したら、Amazon S3 バケットのレポートを開くことができます。

強制をサポートするサービスとリソースタイプ

タグポリシーへのコンプライアンスをサポートするサービスとリソースタイプは以下のとおりです。

サービス	リソースタイプ	JSON 構文名
Amazon API Gateway	• すべて • API キー • ドメイン名 • REST API オペレーション • ステージ	• "apigateway:ALL_SUPPORTED" • "apigateway:apikeys" • "apigateway:domainnames" • "apigateway:restapis" • "apigateway:restapis/stages"
AWS Amplify	• すべて • コンポーネント	• "amplifyuibuilder:ALL_SUPPORTED" • "amplifyuibuilder:app/

JSON 構文名

サブタイプ

envir
onment/
co
mponents"

- Theme (テーマ)
- "amplifyuibuilder:app/environment/themes"

JSON構文

- AWS AppConfig: "appconfig:application"
- AWS AppConfig 設定プロファイル: "appconfig:application/configurationprofile"
- AWS AppConfig デプロイ環境: "appconfig:application/environment/deployment"
- AWS AppConfig デプロイ戦略: "appconfig:deploymentstrategy"
- AWS AppConfig 環境: "appconfig:application/environment"

サービス	リソースタイプ	JSON 構文名
AWS App Mesh	すべて	"appmesh:ALL_SUPPORTED"
	ゲートウェイルート	"appmesh:mesh/virtualGateway/gatewayRoute"
	[Mesh] (メッシュ)	"appmesh:mesh"
	ルート	"appmesh:mesh/virtualRouter/route"
	仮想ゲートウェイ	"appmesh:mesh/virtualGateway"
	仮想ノード	"appmesh:mesh/virtualNode"
	仮想ルーター	

サービス	JSON 構文名	タイプ
仮想サービス	"appmesh:mesh/virtualRouter" "appmesh:mesh/virtualService"	
Amazon Athena	"athena:ATHENA_SUPPORTED"	Workgroup
	"athena:workgroup"	

JSON
構文
文
名
イプ

AWS Audit Manager Managed

- 評価
- auditmanager:assessment "
- auditmanager:assessmentFramework "
- auditmanager:control "

JSON
構一
文
名
イ
プ

AWS Backup:A
BackupSUPPOR
TED"

- バ backup:b
ackup-
プ plan
ラ
ン
- ボ backup:b
ackup-
ル vau
t"
- backup-
g
- ゲ ateway:ga
ト teway"
ウ "backup-
イ g
- ハ ateway:hy
イ pervisor"
パ
バ "backup-
イ g
ザ ateway:vm
- VM

JSON
構一
文
名
イ
プ

- AWS Batch:ALL_SUPPORTED"
- "batch:job"
- "batch:job-definition"
- "batch:job-queue"

- AWS Bugbust:ALL_SUPPORTED"
- "bugbust:event"

JSON
構文
文
名
イプ

- AWS Certificate Manager
  - "acm:ALL_SUPPORTED"
  - "acm:certificate"
  - "acm-pca:certificate-authority"

JSON
構
文
名
イ
プ

Amazon Chime
- "chime:AL
LOCATED
_TO"
- "chime:ap
p-
instanc
e"
- "chime:ap
p-
instanc
e/
channel
"
- "chime:me
dia-
pipel
ine"
- "chime:me
eting"
- "chime:sm
a"
- "chime:ap
p-
instanc
e/
user"
- "chime:vc
"

JSON
構
ー
文
名
イ
プ

- SIP
  メ
  デ
  ィ
  ア
  ア
  プ
  リ
  ケ
  ー
  シ
  ョ
  ン
- ユー
  ザー
  ア
  プ
  リ
  ケ
  ー
  シ
  ョ
  ン
  イ
  ン
  ス
  タ
  ン
  ス
- Voice
  Connect

JSON
構文
文字
名前
タイプ

AWS Clean Rooms
"cleanrooms:ALL_SUPPORTED"

- "cleanrooms:collaboration"
- "cleanrooms:configuredtable"
- "cleanrooms:membership"
- "cleanrooms:membership/configuredtablelassociation"
- 設定済みのテーブル

JSON構文名前タイプ

関連付け

- AWSCloud9:AwsCloud9SupportEnabled
- cloud9:environment

- AmazonCloudFront:AmazonCloudFrontSupported
- cloudfront:distribution

リビジョン

- AWSCloudTrail:AwsCloudTrailSupported
- cloudtrail:trail

JSON
構文
文字
名前
タイプ

Amazon CloudWatch

"cloudwatch:PutMetricData"

- "cloudwatch:DescribeAlarms"
- "cloudwatch:DescribeInsightRules"
- "cloudwatch:PutMetricStream"

Amazon CloudWatch Internet Monitor

"internet-monitor:*"

JSON構文

- Amazon CloudWatch Logs
  - ディスティネーション
  - ロググループ
- Amazon CloudWatch Observability Access Manager
  - シンク
- AWS CodeBuild
  - プロジェクト

```
"Amazon:destination"
"logs:log-group"
"oam:sink"
"codebuild:project"
```

JSON
構一
文
名
イ
プ

- Amazon CodeCatalyst: "codecatalyst:SUPPORTED"
- Connectio
- "codecatalyst:connections"

- AWS CodeComm t: "codecommit:SUPPORTED"
- "codecommit:repository"

サービス	JSON 構文名	タイプ
AWS CodePipeline	• "codepipeline:ALL_SUPPORTED" • "codepipeline:actiontype" • "codepipeline:pipeline" • "codepipeline:webhook"	• サービス • アクションタイプ • パイプライン • ウェブフック
Amazon Cognito ID	• "cognito-identity:ALL_SUPPORTED" • "cognito-identity:identitypool"	• サービス • ID プール

JSON構文名前タイプ

- Amazon Cognito ユーザープール: "cognito-idp:userpool"
- Amazon Comprehend ADL_SUPPORTED": "comprehend:AdlSupported"
- ドキュメント分類子: "comprehend:documentclassifier"
- エンティティ認識機能: "comprehend:entityrecognizer"

JSON構文
名前
タイプ

- AWS Config
  - "config:SUPPORTED"
- 集計の承認
  - "config:aggregation-authorization"
- Configアグリゲーター
  - "config:configAggregator"
- Configルール
  - "config:configRule"
- Amazon CodeGuru Reviewer
  - "codeguru-reviewer:ALL_SUPPORTED"
- 関連付け
  - "codeguru-reviewer:association"

JSON
構
文
名
イ
プ

Amazon CodeGuru Security
- "codeguru-security:ALL_SUPPORTED"
- "codeguru-security:scans"

CodeConnections
- "codestar-connections:ALL_SUPPORTED"
- "codestar-connections:connection"
- "codestar-connections:host"

JSON
構文
文
名
イプ

Amazon Connect: "ALL_SUPPORTED"

- 問い合わせフロー "connect:instance/contact-flow"
- 統合アソシエーション "connect:instance/integration-association"
- キュー "connect:instance/queue"
- クイック接続 "connect:instance/transfer-destination"
- ルーティングプロファイル "connect:instance/routing-profile"

JSON
構
ー
文
名
イ
プ

- プ connect:
  ロ Instance/
  フ *
  ァ
  イ
  ル
- ユー
  ザー

JSON
構
文
名
イ
プ

Amazon Connect Wisdom
"wisdom:A
ll_SUPPOR
TED_
ACTIONS"

- Assistant
- 関連付けは
- コンテンツ
- ナレッジベース
- セッション

JSON
構文
文
名
イプ

- AWS Database Migration Service
  - "dms:ALL_SUPPORTED"
  - "dms:endpoint"
  - "dms:es"
  - "dms:rep"
  - "dms:subgrp"
  - "dms:task"
- Amazon Data Lifecycle Manager
  - "dlm:ALL_SUPPORTED"
  - "dlm:policy"

JSON
構
文
名
イ
プ

- AWS Direct Connect
  - "directconnect:ALLOCATEDXCON"
  - "directconnect:DXCON"
  - "directconnect:DXLAG"
  - "directconnect:DXVIF"
  - "directconnect:DXLAG"
  - "directconnect:DXVIF"
- Amazon DynamoDB
  - "dynamodb:ENABLEKMS"
  - "dynamodb:TAGRESOURCE"
  - [リソースタイプ:] "dynamodb:table"

JSON
構
文
名
イ
プ

Amazon EC2: ALL_SUPPORTED

- "ec2:capacity-reservation"
- "ec2:capacity-reservation-fleet"
- "ec2:carrier-gateway"
- "ec2:client-vpn-endpoint"
- "ec2:coip-pool"
- "ec2:customer-

JSON
構文
文
名
イプ

ゲートウェイ
- "ec2:dedicated-hostVPN エンドポイント
- "ec2:dhcp-optionsCoIP プール
- "ec2:egress-only-internet-gatewayカスタマーゲートウェイ
- "ec2:elastic-ipサブネット
- "ec2:instance-event-windowホスト
- "ec2:export-image-task"

JSON
構
ー
文
名
イ
プ

- DHCP
- Egress
- Elastic
- "ec2:expo
rt-
instan
ce-
task"
- "ec2:fleet"
- "ec2:fpga
image"
- "ec2:host
reservat
ion"
- "ec2:imag
e"
- "ec2:impo
rt-
image-
task"
- "ec2:impo
rt-
snapsh
ot-
task"
- "ec2:inst
ance"

JSON
構文
文
名
イプ

- "ec2:instance-connect-endpoint"
- "ec2:internet-gateway"
- "ec2:ipam-external-resource-verification-token"
- "ec2:ipam-pool"
- "ec2:ipam-resource"

JSON
構
文
名
イ
プ

- FPGA
- discover
- "ec2:ipam
- ホ
- resource
- ト
- discover
- 約
- associa
- tion"
- ジ
- ec2:ipam
- イ
- scope"
- ジ
- ec2:ipv4
- の
- pool-
- ec2"
- ン
- ポ
- "ec2:key-
- ト
- pair"
- タ
- "ec2:laun
- ス
- ch-
- ク
- templa
- te"
- ナッ
- "ec2:loca
- プ
- l-
- ジョッ
- gateway
- ト
- の

JSON
構一
文
名
イ
プ

route-
ta
ble"
- "ec2:loca
タ
-
gateway
ク
-
イ
- route-
ta
ble-
タ
virtu
al-
interf
ace
- instance
Group
connect
エ
associat
ion"
ト
- ポ "ec2:loca
-
gateway
ト
- route-
ta
ble-
vpc-
ト
sociatio
n"

JSON
構
文
名
イ
プ

- "ec2:natgateway"
- "ec2:networkinsights-access-scope-analysis"
- "ec2:networkinsights-analysis"
- "ec2:networkinsights-path"
- "ec2:networkinsights-access-scope"
- "ec2:networkinsights-access-scope-analysis"
- "ec2:networkinsights-analysis"
- "ec2:networkinsights-path"

JSON 構文名

- analysis"
- "ec2:network-insights-path"
- "ec2:placement-group"
- "ec2:prefix-list"
- "ec2:replace-root-volume-task"
- "ec2:reserved-instances"
- "ec2:route-table"

- IP Address Manager リソース検出
- IP Address Manager リソース検出の関連付け
- IP アドレス管理者

JSON
構文
文
名
イ
プ

- 範ec2:secu
囲rity-
- IPv4
グ
ル
- ec2:snap
- shot"
- ペec2:spot
ア
- 起fleet-
動
gu
- ンec2:spot
プ
ト
- Req
カ
ル
- ec2:subn
ゲ
ト
- "ec2:subn
ウェ
et-
イ
cidr-
ルー
r
ト
eservatio
テー
n"
ブ
- "ec2:traf
ル
fic-
- ロー
mirro
カ

JSON 構文名 / タイプ	
ルールグループ / フィルター / トラフィック…	filter"
ルートテーブル / 仮想インターフェイスグループの関連付け / ローカルゲートウェイ…	• "ec2:traffic-mirror-session" • "ec2:traffic-mirror-target" • "ec2:transit-gateway" • "ec2:transit-gateway-attachment" • "ec2:transit-gateway-

JSON
構文
文字
名前
タイプ

connec
ピア
peer"
ルー
• "ec2:tran
トラ
sit-
ンジ
gatew
ット
ay-
ゲー
multic
ast-
domai
n"
• "ec2:tran
sit-
gatew
ay-
policy
table"
• "ec2:tran
sit-
gatew
ay-
route-
table"
• "ec2:tran
sit-
gatew
ay-
route-
ネット
ワーク
ACL
ネット
ワーク
インス

JSON
構文
文
名
イプ

table-
ann
ouncement
ワェ
イ
ec2:veri
fied-
Network
acce
ss-
endpoi
nt"
セ
ec2:veri
fied-
範
acce
囲
ss-
Network
group"
Insights
ア
ec2:veri
ク
fied-
セ
acce
ス
ss-
範
instan
囲
ce"
分
"ec2:veri
析
fied-
Network
acce
Insights
ss-
分
trust-
析

JSON
構文
文
名
イプ

- Network Insights パス: "ec2:network-insights-path"
- 配置グループ: "ec2:placement-group"
- ルートテーブル: "ec2:route-table"
- セキュリティグループ: "ec2:security-group"
- スナップショット: "ec2:snapshot"
- サブネット: "ec2:subnet"
- タグ: "ec2:tag"
- ボリューム: "ec2:volume"
- 配置フローログ: "ec2:vpc-flow-log"
- VPC: "ec2:vpc"
- プレフィックスリスト: "ec2:vpc-endpoint"
- VPC エンドポイントサービス: "ec2:vpc-endpoint-service"
- VPC ピアリング接続: "ec2:vpc-peering-connection"
- VPN 接続: "ec2:vpn-connection"
- VPN ゲートウェイを置き換え: "ec2:vpn-gateway"

JSON構文
一文字
名前
イプ

える

- 予約インスタンス
- ルートテーブル
- セキュリティグループ
- Snapshot
- スポットフリート

JSON構文

一文字

名前

タイプ

のリクエスト

- スポットインスタンスリクエスト
- サブネット
- サブネットCIDR

JSON構文
ー
文
名
イ
プ
の
予
約

- Traffic mirror フィルター
- Traffic mirror セッション
- Traffic mirror ターゲット
- Transit Gateway
- Transit Gateway アタッチメント

JSON
構
ー
文
名
イ
プ

- Transit Gateway 接続ピア
- Transit Gateway のマルチキャストドメイン
- Transit Gateway ポリシーテーブル
- トラ

JSON構文
ー
文
名
イ
プ

ン
ジッ
ト
ゲー
ト
ウェ
イ
ルー
ト
テー
ブ
ル

- Transit Gateway ルートテーブルアナウンス
- Verified Access エンド

JSON構文エラー

ポイント

- Verified Access グループ
- Verified Access インスタンス
- Verified Access 信頼プロバイダー
- ボリューム

JSON
構
ー
文
名
イ
プ

- VPC フローログ
- VPC
- VPC エンドポイント
- VPC エンドポイントサービス
- VPC ピア

JSON
構
ー
文
名
イ
プ

接
続

- VPN
接
続
- VPN
ゲー
ト
ウェ
イ

Am
EC2
の
ご
み
箱

JSON構文名前タイプ

AWS Elastic Beanstalk

- "elasticbeanstalk:ENABLED"
- "elasticbeanstalk:application"
- "elasticbeanstalk:applicationversion"
- "elasticbeanstalk:configurationtemplate"
- "elasticbeanstalk:platform"

JSON構文名前タイプ

フォーム

- Amazon Elastic Container Registry: "ecr:repository"

サービス	JSON 構文名	タイプ
Amazon Elastic Container Service	• "ecs:ALL_SUPPORTED" • "ecs:capacity-provider" • "ecs:cluster" • "ecs:service" • "ecs:task-definition" • "ecs:task-set"	• すべて • キャパシティープロバイダー • クラスター • サービス • タスク定義 • タスク

JSON 構文名タイプ		セット
Amazon Elastic File System	• すべて • ファイルシステム	• "elasticfilesystem:ALL_SUPPORTED" • "elasticfilesystem:file-system"
Amazon Elastic Kubernetes Service	• すべて • クラスター	• "eks:ALL_SUPPORTED" • "eks:cluster"
Amazon Elastic Search	• すべて • ドメイン	• "es:ALL_SUPPORTED" • "es:domain"

JSON
構文
文
名
イプ

- Amazon EMR
  - "elasticmapreduce:ALL_SUPPORTED"
  - "elasticmapreduce:cluster"
  - "elasticmapreduce:editor" (エディタ)
- Amazon EMR Serverless
  - "emr-serverless:application" (アプリケーション)

JSON構文

- AWSエンティティ解決
  - マッチングワークフロー
  - スキーママッピング
- Amazon ElastiCache
  - クラスター

JSON構文名前タイプ

- Amazon EventBridge: "events:EVENT_BUS_SUPPORTED"
- イベントバス: "events:event-bus"
- ルール: "events:rule"

- Amazon EventBridge Pipes: "pipes:ALL" または "pipes:PIPE_SUPPORTED"
- パイプ: "pipes:pipe"

- Amazon EventBridge スケジューラ: "scheduler:SCHEDULE_GROUP_SUPPORTED"
- スケジューラグループ: "scheduler:schedule-group"

JSON
構文
文
名
イ
プ

Amazon Fraud Detector:ALL_SUPPORTED_ENTITY_TYPES
- "frauddetector:detector"
- "frauddetector:detector-version"
- "frauddetector:model"
- "frauddetector:rule"
- "frauddetector:variable"

JSON
構文
文字
名前
タイプ

- Amazon Global Accelerator
  "globalaccelerator"
  グローバルアクセラレーター
- Elastic Load Balancing リスナー
  "elasticloadbalancing:listener"
- Elastic Load Balancing ルール
  "elasticloadbalancing:listener-rule"
- Elastic Load Balancing ロードバランサー
  "elasticloadbalancing:loadbalancer"
- Elastic Load Balancing ターゲットグループ
  "elasticloadbalancing:targetgroup"

JSON
構一
文
名
イ
プ

Amazon FSx
て

- バックアップ
- ファイルシステム

サービス	リソースタイプ	JSON 構文名
Amazon GuardDuty	• ディテクター • ディテクターフィルター • IP セット • 脅威インテリジェンスセット	• "guardduty:detector" • "guardduty:detector/filter" • "guardduty:detector/ipset" • "guardduty:detector/threatintelset"

サービス	JSON 構文名 タイプ
AWS HealthLake	• サービス "healthlake:ALL_SUPPORTED" • データストア "healthlake:datastore"

サービス	リソースタイプ	JSON 構文名
AWS Omics	• すべて • アノテーションストア • アノテーションストアのバージョン • リファレンスストア	• "omics:ALL_SUPPORTED" • "omics:annotationStore" • "omics:annotationStore/version" • "omics:referenceStore" • "omics:referenceStore/reference" • "omics:run" • "omics:runGroup" • "omics:sequenceStore" • "omics:sequenceSto

JSON
構ー
文
名
イ
プ

re/
eadSe
- t"
- omics:va
liantStor
e"
- omics:wo
- rkflow"
行
- 実
行
グ
ル
ー
プ
- シ
ー
ケ
ン
ス
ト
ア
- リ
ー
ド
セ
ッ
ト
- バ
リ
ア
ン

JSON
構文
文字
名前
イプ

トストア

- ワークフロー

- Amazon Inspector: "inspector2:ListCoverage" または "inspector2:ListCoverageStatistics"
- ワイルドカード: "inspector2:filter" フィルター

サービス	タイプ	JSON 構文名
AWS Identity and Access Management	• すべて • インスタンスプロファイル • MFA • OIDC プロバイダー • ポリシー • SAML プロ	• "iam:ALL_SUPPORTED • "iam:instance-profile" • "iam:mfa" • "iam:oidc-provider" • "iam:policy" • "iam:saml-provider" • "iam:server-certificate"

JSON
構
ー
文
名
イ
プ

バ
イ
ダー

- サー
バー
証
明
書

- AWS IoT Analytics: "iotanalytics:ALL_RESOURCES"
- Channel: "iotanalytics:channel"
- データセット: "iotanalytics:dataset"
- データストア: "iotanalytics:datastore"
- パイプライン: "iotanalytics:pipeline"

サービス	リソースタイプ	JSON 構文名
AWS IoT Events	• すべてのリソース • 検出器モデル • Input	• "iotevents:ALL_SUPPORTED" • "iotevents:detectorModel" • "iotevents:input"
AWS IoT Fleet Hub	• すべてのリソース • フリートハブアプリケーション	• "iotfleethub:ALL_SUPPORTED" • "iotfleethub:application"

JSON
構
文
名
イ
プ

AWS
lo
Si

- ア
- セ
- ア
- セ
  モ
  デ
  ル

JSON
構文
文
名
イプ

AWS IoT Greengrass

- "greengrass:ALL_SUPPORTED"
- "greengrass:bulk"
- "greengrass:connectorsDefinition"
- "greengrass:coresDefinition"
- "greengrass:deviceDefinition"
- "greengrass:functionsDefinition"
- "greengrass:loggerDefinition"
- "greengrass:resour

サービスタイプ	JSON 構文名
- 関数の定義 - ロガー定義 - リソースの定義 - サブスクリプションの定義	…esDefinition" "greengrass:subscriptionsDefinition"

JSON
構文
文
名
イ
プ

AWS
Key
Management
Service

Amazon
Kinesis
Data
Analytics

Amazon
Data
Firehose

"kms:ALL_SUPPORTED"
"kms:key"

"kinesisanalytics:ALL_SUPPORTED"
"kinesisanalytics:application"

"firehose:ALL_SUPPORTED"
"firehose:deliverystream"

サービス	リソースタイプ	JSON 構文
AWS Lambda	すべて	"lambda:ALL_SUPPORTED"
	関数	"lambda:function"
Amazon Macie	すべて	"macie2:ALL_SUPPORTED"
	カスタムデータ識別子	"macie2:custom-data-identifier"
Amazon MediaStore	すべて	"mediastore:ALL_SUPPORTED"
	コンテナ	"mediastore:container"

JSON
構
文
名
イ
プ

Amazon MQ
て

- ブ
ロー
カー
- 設
定

JSON
構
文
名
イ
プ

Amazon Network Firewall
- "network-firewall:FirewallSUPPORTED"
- "network-firewall:firewall"
- "network-firewall:firewall-policy"
- "network-firewall:statefulrulegroup
- "network-firewall:statelessrulegroup"
- ス
テー
ト

JSON
構文
文
名
イ
プ

レ
ス
ルー
ル
グ
ルー
プ

Amazon OpenSearch Serverless

- "aoss:ALL_OPERATIONS"
- "aoss:CreateCollection"

JSON
構
文
名
イ
プ

AWS Organizations: ALL_SUPPORTED

- "organizations:account"
- "organizations:ou"
- "organizations:policy"
- "organizations:root"

サービス	リソースタイプ	JSON 構文名
Amazon Pinpoint SMS Voice V2	• すべて • 設定セット • オプトアウトリスト • 電話番号 • プール • 送信者 ID	• "sms-voice:ALL_SUPPORTED" • "sms-voice:configuration-set" • "sms-voice:opt-out-list" • "sms-voice:phone-number" • "sms-voice:pool" • "sms-voice:sender-id"

JSON構文名前タイプ

Amazon RDS

- "arn:aws:rds:*:*:cluster-pg"
- "arn:aws:rds:*:*:cluster-endpoint"
- "arn:aws:rds:*:*:es"
- "arn:aws:rds:*:*:og"
- "arn:aws:rds:*:*:pg"
- "arn:aws:rds:*:*:db-proxy"
- "arn:aws:rds:*:*:db-proxy-endpoint"
- "arn:aws:rds:*:*:ri"
- "arn:aws:rds:*:*:secgrp"
- "arn:aws:rds:*:*:subgrp"
- "arn:aws:rds:*:*:target-group"

JSON構文エラー
名前タイプ
サブスクリプション
- DBオプショングループ
- DBパラメータグループ
- DBプロキシ

JSON構文

- RDSプロキシエンドポイント
- リザーブドDBインスタンス
- DBセキュリティグ

JSON構文名前タイプ

ループ

- DBサブネットグループ
- ターゲットグループ

JSON
構
ー
文
名
イ
プ

Amazon Redshift
- "redshift:SUPPORTED"
- ウ
ラ
ス
タ
ー
- "redshift:cluster"
- イ
ベ
ン
ト
サ
ブ
ス
ク
リ
プ
シ
ョ
ン
- "redshift:eventsubscription"
- "redshift:hsmclientcertificate"
- "redshift:hsmconfiguration"
- HSM
グ
ル
ー
プ
- "redshift:parametergroup"
- "redshift:snapshot"
- "redshift:snapshotcopygrant"
証
明
書

JSON
構
ー
文
名
イ
プ

- HSM
- Redshift
- パラメータグループ
- Snapshot
- スナップショットコピー権限
- スナップショットスケ

JSON
構
文
名
イ
プ

ジュー
ル

- サ
ブ
ネッ
ト
グ
ル
ー
プ

Amazon
Redshift
Serverless

- "redshift
-
serverle
ss:ALL_SU
PPORTED"
- redshift
-
serverle
ss:namesp
ace"
- "redshift
-
serverle
ss:workgr
oup"

サービス	リソースタイプ	JSON 構文名
AWS Resource Access Manager	• すべて • リソースの共有	• ram:ALL_SUPPORTED • "ram:resource-share"
AWS Resource Groups	• すべて • リソースグループ	• resource-groups:ALL_SUPPORTED" • "resource-groups:group"
Amazon Route 53	• すべて • ホストゾーン	• route53:ALL_SUPPORTED" • "route53:hostedzone"

JSON
構文
文
名
イプ

Amazon Route 53 Resolver:AssociateResolverRule

- "route53resolver:AssociateResolverEndpoint"
- "route53resolver:AssociateResolverRule"

JSON
構一
文
名
イ
プ

Amazon
S3"
て

- バ s3:bucke
ケ"ッ
ト
- " s3:stora
- Storage
Lens"
- ス s3:stora
ge-
Lens-
ジ
Loup"
ン
ズ
グ
ル
ー
プ

サービス	リソースタイプ	JSON 構文名
Amazon SageMaker AI	• アプリケーションイメージ構成 • アーティファクト • Context • トレーニングジョブ • ジョブの処	• "sagemaker:app-image-config" • "sagemaker:artifact" • "sagemaker:context" • "sagemaker:training-job" • "sagemaker:processing-job" • "sagemaker:model-package-group"

JSON
構
ー
文
名
イ
プ

- 理 sagemake
中: human-
- パ task-
ラ ui"
- ヴ sagemake
ル r:model-
プ package"
- モ sagemake
デ r:action"
ル
- ヒュー sagemake
マ r:pipelin
ン e"
- タ "sagemake
ス r:experim
ク ent"
UI
- "sagemake
- モ r:flow-
デ de
ル finition"
パッ
ケー
- ジ sagemake
r:project
- ア "
ク
シ
ョ
ン

サービス	タイプ	JSON構文名
	• パイプライン • 実験 • フロー定義 • プロジェクト	
AWS Secrets Manager	• すべて • シークレット	• "secretsmanager:ALL_SUPPORTED" • "secretsmanager:secret"

JSON
構文
文
名
イ
プ

AWS Security Lake
- AWS Security Lake:ALL_SUPPORTED
- データ
- security lake:data lake"
- security lake:subscriber"

サービス	リソースタイプ	JSON 構文名
AWS Service Catalog	• すべてのリソースタイプ • アプリケーション • 属性グループ • ポートフォリオ • 製品	• "servicecatalog:ALL_SUPPORTED" • "servicecatalog:application" • "servicecatalog:attribute-groups " • "catalog:portfolio " • "catalog:product "
「Amazon Simple Notification Service (SNS)」	• すべてのリソースタイプ • トピック	• sns:ALL_SUPPORTED • sns:topic

JSON
構
文
名
イ
プ

- "Amazon Simple Queue Service (SQS)"
  - "sqs:ALL_SUPPORTED"
  - "sqs:queue"
- "AWS Step Functions"
  - "states:ALL_SUPPORTED"
  - "states:activity"
  - "states:stateMachine"
- [State Machine] (ステートマシン)
- "AWS Step Functions"
  - "states:activity"

JSON
構文
文
名
イ
プ

AWS Storage Gateway

- "storageg
- ateway:sh
  are"
- "storageg
  ateway:ta
- ge"
- "storageg
  ateway:ga
  teway/
  vol
  ume"

JSON
構
ー
文
名
イ
プ

AWS
System
Manager

"ssm:ALL_
SUPPORTED
"

- "ssm:asso
ciation"
- "ssm:auto
mation-
execution"
- "ssm:docu
ment"
- "ssm:main
tenancewi
ndow"
- "ssm:mana
ged-
insta
nce"
- "ssm:opsi
tem"
- "ssm:patc
hbaseline
"
- "ssm-
cont
acts:cont
act"

JSON構文エラー
名前タイプ

- マネージドインスタンス
- Opsitem
- パッチベースライン
- 問い合わせ

JSON
構文
文
名
イ
プ

Amazon Textract
- "textract:adapters:SUPPORTED"
- アダプター
- "textract:adapters:versions"
- バージョン

AWS Transfer Family
- "transfer:Server"（サーバー）
- "transfer:User"（ユーザー）
- "transfer:Workflow"（ワークフロー）

JSON
構
ー
文
名
イ
プ

- Amazon Well-Architected:ARCHITECTED"
- ワークロード wellarchitected:workload"
- AWS Wickr:ALLOWED"
- ネットワーク wickr:network"

JSON
構文
文
名
イプ

Amazon WorkSpaces SUPPORTED"

- workspaces:connectionalias
- "workspaces:directory"
- "workspaces:workspace"
- "workspaces:workspacebundle"
- WorkSpaces
- "workspaces:workspaceimage"
- "workspaces:workspaceipgroup"

メージ

JSON
構ー
文
名
イ
プ

- WorkSpace
  s
  IP
  グ
  ルー
  プ

タグポリシーの構文と例

このページでは、タグポリシーの構文について説明し、例を示します。

タグポリシー構文

タグポリシーは、JSON のルールに従って構造化されたプレーンテキストファイルです。タグポリシーの構文は、すべての管理ポリシータイプの構文に従います。この構文の詳しい説明については、「管理ポリシーの継承を理解する」を参照してください。このトピックは、一般的な構文をタグアップポリシータイプの特定の要件に適用することに焦点を当てています。

次のタグポリシーは、基本的なタグポリシーの構文を示しています。

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "100",
                    "200",
                    "300*"
                ]
            },
```

```
            "enforced_for": {
                "@@assign": [
                    "secretsmanager:ALL_SUPPORTED"
                ]
            }
        }
    }
}
```

タグポリシー構文には、次の要素が含まれます。

- tags フィールドキーの名前。タグポリシーは、常にこの固定キー名で始まります。上記のポリシーの例では一番上の行です。
- ポリシーステートメントを一意に識別するポリシーキー。大文字小文字の処理を除き、タグキーの値と一致する必要があります。ポリシー値は大文字と小文字が区別されます。

  この例では、costcenter がポリシーキーです。
- リソースを準拠させる大文字小文字表記を持つ許容タグキーを指定するタグキーを 1 つ以上指定します。大文字小文字の処理が定義されていない場合、タグキーのデフォルトは小文字です。タグキーの値は、ポリシーキーの値と一致する必要があります。ただし、ポリシーのキーバリューでは大文字と小文字が区別されないため、大文字と小文字が異なる可能性があります。

  この例では、CostCenter がタグキーです。これは、タグポリシーに準拠するために必要な大文字と小文字の処理です。このタグキーに対して大文字と小文字の処理が異なるリソースは、タグポリシーに準拠していません。

  タグポリシーでは、複数のタグキーを定義できます。
- (オプション) タグキーに対して受け入れ可能な 1 つ以上のタグ値のリスト。タグポリシーがタグキーのタグ値を指定しない場合、すべての値 (値なしの場合を含む) が準拠していると見なされます。

  この例では、CostCenterタグキーの許容値は 100、200、および です300*。
- (オプション) 指定されたサービスおよびリソースに対する非準拠のタグ付け操作を防止するかどうかを示す enforced_for オプション。コンソールでは、タグポリシーを作成するためのビジュアルエディタの [Prevent noncompliant operations for this tag (このタグに対する非準拠操作を防止する)] オプションです。このオプションのデフォルト設定は null です。

  タグポリシーの例では、すべての AWS Secrets Manager リソースに渡されるCostCenterタグがこのポリシーに準拠する必要があることを指定します。

> **Warning**
>
> タグポリシーの使用経験がある場合にのみ、このオプションをデフォルトから変更してください。そうしないと、組織のアカウントのユーザーが必要なリソースを作成できなくなる可能性があります。

- タグポリシーを組織ツリーの他のタグポリシーとマージして、アカウントの有効なタグポリシーを作成する方法を指定する演算子。この例では、@@assign を使用して、tag_key、tag_value、および enforced_for に文字列を割り当てます。演算子についての詳細は、「継承演算子」を参照してください。
- タグ値で*ワイルドカードを使用できます。
  - タグ値ごとに、ワイルドカードを 1 つのみ使用できます。例えば、*@example.com は許可されますが、*@*.com は許可されません。
  - 一部のサービスで enforced_forフィールドのALL_SUPPORTEDワイルドカードを使用して、そのサービスのすべてのリソースを適用できます。enforced_for がサポートするサービスとリソースタイプのリストについては、「強制をサポートするサービスとリソースタイプ」を参照してください。
  - ワイルドカードを使用してすべてのサービスを指定したり、すべてのサービスのリソースを指定したりすることはできません。

タグポリシーの例

次のタグポリシーの例は、情報提供のみを目的としています。

> **Note**
>
> 組織でこれらのタグポリシーの例を使用する前に、次の点に注意してください。
>
> - タグポリシーの使用を開始するための推奨ワークフローを実行したことを確認します。
> - 固有の要件に合わせて、これらのタグポリシーを慎重に確認し、カスタマイズする必要があります。
> - タグポリシーのすべての文字には、上限サイズが適用されます。このガイドの例では、読みやすさを向上させるため、空白文字を追加してフォーマットされたタグポリシーを示しています。ただし、ポリシーのサイズが上限サイズに近づいたら、スペースを節約するために空白を削除できます。空白の例としては、空白文字や引用符の外側の改行などがあります。

- タグ付けされていないリソースは、結果で非準拠と表示されません。

例 1: 組織全体のタグキーの大文字小文字取り扱いの定義

次の例は、組織内のアカウントに標準化させる 2 つのタグキーと大文字小文字のみを定義するタグポリシーを示しています。

ポリシー A - 組織ルートのタグポリシー

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        },
        "Project": {
            "tag_key": {
                "@@assign": "Project",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

このタグポリシーは、CostCenter と Project という 2 つのタグキーを定義します。このタグポリシーを組織のルートにアタッチすると、次の効果があります。

- 組織内のすべてのアカウントは、このタグポリシーを継承します。
- 組織内のすべてのアカウントは、準拠のために、定義された大文字と小文字の処理を使用する必要があります。CostCenter タグと Project とタグの付いたリソースは準拠しています。タグキーに対して大文字小文字の処理が異なるリソース (costcenter、Costcenter、COSTCENTER など) は準拠していません。
- @@operators_allowed_for_child_policies": ["@@none"] 行はタグキーをロックダウンします。組織ツリーの下位にアタッチされたタグポリシー (子ポリシー) は、大文字と小文字の処理を含め、値設定演算子を使用してタグキーを変更することはできません。
- すべてのタグポリシーと同じように、タグなしリソースまたはタグポリシーで定義されていないタグは、タグポリシーに準拠しているかどうか評価されません。

AWS では、使用するタグキーの同様のタグポリシーを作成する際のガイドとして、この例を使用することをお勧めします。組織のルートにアタッチします。次に、下の例のようなタグポリシーを作成します。この例では、定義されたタグキーの許容値のみを定義します。

次のステップ: 値の定義

組織ルートに先ほどのタグポリシーをアタッチしたと仮定します。次に、次のようなタグポリシーを作成し、アカウントにアタッチできます。このポリシーは、CostCenter および Project タグキーの許容値を定義します。

ポリシー B - アカウントのタグポリシー

```
{
    "tags": {
        "CostCenter": {
            "tag_value": {
                "@@assign": [
                    "Production",
                    "Test"
                ]
            }
        },
        "Project": {
            "tag_value": {
                "@@assign": [
                    "A",
                    "B"
                ]
            }
        }
    }
}
```

ポリシー A を組織ルートにアタッチし、ポリシー B をアカウントにアタッチすると、ポリシーが結合され、次の有効なタグポリシーがアカウントに対して作成されます。

ポリシー A + ポリシー B = アカウントの有効なタグポリシー

```
{
    "tags": {
        "Project": {
            "tag_value": [
                "A",
```

```
                "B"
            ],
            "tag_key": "Project"
        },
        "CostCenter": {
            "tag_value": [
                "Production",
                "Test"
            ],
            "tag_key": "CostCenter"
        }
    }
}
```

継承演算子の動作例や有効なタグポリシーの例など、ポリシー継承に関する詳細については、「管理ポリシーの継承を理解する」を参照してください。

例 2: タグキーの使用を禁止する

タグキーの使用を禁止するには、次のようなタグポリシーを組織エンティティにアタッチします。

このサンプルポリシーは、Color タグキーに対して使用できる値がないことを指定します。また、子タグポリシーで演算子を使用できないことも指定します。したがって、影響を受けるアカウントのリソース上の Color タグは、非準拠と見なされます。ただし enforced_for オプションは、実際には、影響を受けるアカウントが Color タグを使用して Amazon DynamoDB テーブルのみにタグ付けできないようにします。

```
{
    "tags": {
        "Color": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": "Color"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": []
            },
            "enforced_for": {
```

```
                "@@assign": [
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

例 3: 特定の AWS サービスのサポートされているすべてのリソースタイプにタグポリシーを指定する

特定の AWS サービスのサポートされているすべてのリソースタイプにタグポリシーを指定するには、ALL_SUPPORTEDワイルドカードを使用します。

このポリシーは、ALL_SUPPORTEDワイルドカードを使用して、タグキーを持つすべての Amazon EC2 インスタンスが Prodまたは のタグ値のみを持つEnvironmentことができるように指定しますNon-prod。このワイルドカードは、各 Amazon EC2 インスタンスを個別に一覧表示する効果的な単一行の代替手段を提供します。ALL_SUPPORTED ワイルドカードをサポートするサービスとリソースタイプのリストについては、「」を参照してください強制をサポートするサービスとリソースタイプ。

```
{
    "tags": {
        "Environment": {
            "tag_key": {
                "@@assign": "Environment",
                "@@operators_allowed_for_child_policies": ["@@none"]
            },
            "tag_value": {
                "@@assign": [
                    "Prod",
                    "Non-prod"
                ],
                "@@operators_allowed_for_child_policies": ["@@none"]
            },
            "enforced_for": {
                "@@assign": [
                    "ec2:ALL_SUPPORTED"
                ]
            }
        }
    }
```

```
}
```

サポートされるリージョン

タグポリシー機能は、次のリージョンで使用できます。

リージョン名	リージョンパラメータ
米国東部 (バージニア北部) リージョン[1]	**us-east-1**
米国東部 (オハイオ) リージョン	us-east-2
米国西部 (北カリフォルニア) リージョン	us-west-1
米国西部 (オレゴン) リージョン	us-west-2
アフリカ (ケープタウン) リージョン[2]	af-south-1
アジアパシフィック (香港) リージョン[2]	ap-east-1
アジアパシフィック (ムンバイ) リージョン	ap-south-1
アジアパシフィック (ハイデラバード)[2]	ap-south-2
アジアパシフィック (東京) リージョン	ap-northeast-1
アジアパシフィック (ソウル) リージョン	ap-northeast-2
アジアパシフィック (大阪) リージョン	ap-northeast-3
アジアパシフィック (シンガポール) リージョン	ap-southeast-1
アジアパシフィック (シドニー) リージョン	ap-southeast-2
アジアパシフィック (ジャカルタ) リージョン[2]	ap-southeast-3
アジアパシフィック (マレーシア) リージョン	ap-southeast-5
アジアパシフィック (メルボルン)2	ap-southeast-4
アジアパシフィック (タイ)	ap-southeast-7

リージョン名	リージョンパラメータ
カナダ (中部) リージョン	ca-central-1
カナダ西部 (カルガリー)[2]	ca-west-1
中国 (北京) リージョン	cn-north-1
中国 (寧夏) リージョン	cn-northwest-1
欧州 (フランクフルト) リージョン	eu-central-1
欧州 (チューリッヒ) リージョン[2]	eu-central-2
欧州 (ミラノ) リージョン[2]	eu-south-1
欧州 (スペイン)[2]	eu-south-2
欧州 (アイルランド) リージョン	eu-west-1
欧州 (ロンドン) リージョン	eu-west-2
欧州 (パリ) リージョン	eu-west-3
欧州 (ストックホルム) リージョン	eu-north-1
メキシコ (中部) リージョン	mx-central-1
中東 (バーレーン) リージョン[2]	me-south-1
南米 (サンパウロ) リージョン	sa-east-1
イスラエル (テルアビブ)2	il-central-1
AWS GovCloud (米国東部) リージョン	us-gov-east-1
AWS GovCloud (米国西部) リージョン	us-gov-west-1

[1]次の Organizations オペレーションを呼び出す場合は、**us-east-1** リージョンを指定する必要があります。

- DeletePolicy
- DisablePolicyType
- EnablePolicyType
- 組織ルート上のその他の操作 (ListRoots など)。

タグポリシー機能の一部である次のリソースグループタグ付け API 操作を呼び出す場合も、**us-east-1** リージョンを指定する必要があります。

- DescribeReportCreation
- GetComplianceSummary
- StartReportCreation

> **Note**
>
> 組織全体でのタグポリシーへの準拠を評価するには、レポートを保存するため、米国東部 (バージニア北部) リージョンの Amazon S3 バケットにもアクセスできる必要があります。詳細については、「 リソースのタグ付けユーザーガイド」の「レポートストレージ用の Amazon S3 バケットポリシー」を参照してください。 AWS

[2]これらのリージョンは、手動で有効にする必要があります。 AWS リージョンを有効および無効にする方法については、「AWS Account Management リファレンスガイド」の「Specify which AWS リージョン your account can use」を参照してください。Resource Groups コンソールは、これらのリージョンでは利用できません。

チャットアプリケーションポリシー

のチャットアプリケーションポリシー AWS Organizations を使用すると、Slack や Microsoft Teams などのチャットアプリケーションから組織のアカウントへのアクセスを制御できます。

チャットアプリケーションの Amazon Q Developer は、 AWS DevOps およびソフトウェア開発チームがメッセージングプログラムチャットルームを使用して、 の運用イベントをモニタリングして対応できるようにする サービスです AWS クラウド。チャットアプリケーションの Amazon Q Developer は、Amazon Simple Notification Service (Amazon SNS) からの AWS のサービス 通知を処理し、チャットルームに転送します。これにより、チームは場所に関係なく、チャットルームをすぐに分析して対応できます。

チャットアプリケーションポリシーの仕組み

チャットアプリケーションポリシーを使用すると、組織の管理アカウントまたは委任管理者は、組織全体で次のことを実行できます。

- サポートされているチャットアプリケーション (Amazon Chime、Microsoft Teams、および Slack) を使用できます。
- チャットクライアントへのアクセスを特定のワークスペース (Slack) とチーム (Microsoft Teams) に制限します。
- Slack チャネルの可視性をパブリックチャネルまたはプライベートチャネルに制限します。
- 特定のロール設定を設定して適用します。

チャットアプリケーションポリシーは、ロール設定やチャネルガードレールポリシーなどのアカウントレベルの設定を制限し、優先します。チャットアプリケーションまたは Organizations コンソールで、Amazon Q Developer からチャットアプリケーションポリシーにアクセスして変更できます。

ポリシーがアカウントと組織単位 (OU) にアタッチされると、対象範囲内のアカウントのチャットアプリケーション設定で現在および将来の Amazon Q Developer は、ガバナンスとアクセス許可の設定に自動的に準拠します。詳細については、「Understanding management policy inheritance」を参照してください。

チャットアプリケーションポリシーによって制限されたアクションを実行しようとすると、チャットアプリケーションポリシーが原因でアクションが許可されていないことを知らせるエラーメッセージが表示され、組織の管理アカウントまたは委任された管理者に連絡することをお勧めします。

> **Note**
>
> チャットアプリケーションポリシーは実行時に検証されます。つまり、既存のリソースがコンプライアンスを継続的にチェックされます。チャットアプリケーションで通知を送信したり Amazon Q Developer とやり取りしたりするためのランタイムベースの IAM アクセス許可は現在サポートされていないため、既存の IAM アクセス許可と重複することはありません。

チャットアプリケーションポリシーの開始方法

チャットアプリケーションポリシーの使用を開始するには、次の手順に従います。

1. チャットアプリケーションポリシータスクを実行するために必要なアクセス許可について説明します。
2. 組織のチャットアプリケーションポリシーを有効にします。
3. チャットアプリケーションポリシーを作成します。
4. チャットアプリケーションポリシーを組織のルート、OU、またはアカウントにアタッチします。
5. アカウントに適用される効果的なチャットアプリケーションポリシーの組み合わせを表示します。

これらすべてのステップでは、組織の管理アカウントの 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 (推奨されません) としてサインインします。

その他の情報

- チャットアプリケーションポリシーの構文とポリシーの例について説明します。

チャットアプリケーションポリシーの構文と例

このトピックでは、チャットアプリケーションポリシーの構文と例について説明します。

チャットアプリケーションポリシーの構文

チャットアプリケーションポリシーは、JSON のルールに従って構造化されたプレーンテキストファイルです。チャットアプリケーションポリシーの構文は、管理ポリシータイプの構文に従います。この構文の詳しい説明については、「管理ポリシーの継承を理解する」を参照してください。このトピックでは、チャットアプリケーションポリシータイプの特定の要件にその一般的な構文を適用することに重点を置いています。

次の例は、チャットアプリケーションポリシーの基本的な構文を示しています。

```
{
    "chatbot":{
       "platforms":{
          "slack":{
             "client":{
                "@@assign":"enabled" // enabled | disabled
             },
             "workspaces": { // limit 255
                   "@@assign":[
                      "Slack-Workspace-Id"
```

```
                ]
            },
            "default":{
               "supported_channel_types":{
                  "@@assign":[
                     "private" // public | private
                  ]
               },
               "supported_role_settings":{
                  "@@assign":[
                     "user_role" // user_role | channel_role
                  ]
               }
            },
            "overrides":{ // limit 255
               "Slack-Workspace-Id":{
                  "supported_channel_types":{
                     "@@assign":[
                        "public" // public | private
                     ]
                  },
                  "supported_role_settings":{
                     "@@assign":[
                        "user_role" // user_role | channel_role
                     ]
                  }
               }
            }
         },
         "microsoft_teams":{
            "client":{
               "@@assign":"enabled"
            },
            "tenants":{ // limit 36
               "Microsoft-Teams-Tenant-Id":{ // limit 36
                  "@@assign":[
                     "Microsoft-Teams-Team-Id"
                  ]
               }
            },
            "default":{
               "supported_role_settings":{
                  "@@assign":[
                     "user_role" // user_role | channel_role
```

```
                ]
             }
          },
          "overrides":{ // limit 36
             "Microsoft-Teams-Tenant-Id":{ // limit 36
                "Microsoft-Teams-Team-Id":{
                   "supported_role_settings":{
                      "@@assign":[
                         "user_role" // user_role | channel_role
                      ]
                   }
                }
             }
          }
       },
       "chime":{
         "client":{
            "@@assign":"disabled" // enabled | disabled
         }
       }
    },
    "default":{
       "client":{
          "@@assign":"disabled" // enabled | disabled
       }
    }
 }
}
```

このチャットアプリケーションポリシーには、次の要素が含まれています。

- chatbot フィールドキーの名前。チャットアプリケーションポリシーは、常にこの固定キー名で始まります。このポリシー例では一番上の行です。
- chatbot の下には、サポートされているさまざまなチャットアプリケーション Slack、Microsoft Teams、Amazon Chime の設定を含む platforms ブロックがあります。
  - Slack では、以下のフィールドが利用できます。
    - "client":
      - "enabled": Slack クライアントが有効になっています。Slack 統合は許可されています。
      - "disabled": Slack クライアントは無効になっています。Slack 統合は許可されていません。

- "workspaces": 許可された Slack ワークスペースのカンマ区切りリスト。この例では、許可された Slack ワークスペースは *Slack-Workspace-Id1* と *Slack-Workspace-Id2* です。
- "default": Slack ワークスペースのデフォルト設定。
  - "supported_channel_types":
    - "public": 範囲内の Slack ワークスペースでは、デフォルトでパブリック Slack チャネルが許可されます。
    - "private": 範囲内の Slack ワークスペースでは、デフォルトでプライベート Slack チャネルが許可されます。
  - supported_role_settings:
    - "user_role": 範囲内の Slack ワークスペースでは、デフォルトでユーザーレベルの IAM ロールが許可されます。
    - "channel_role": 範囲内の Slack ワークスペースでは、デフォルトでチャネルレベルの IAM ロールが許可されます。
- "overrides": Slack ワークスペースのオーバーライド設定。
  - *Slack-Workspace-Id2*: オーバーライド設定が適用される Slack ワークスペースのカンマ区切りリスト。この例では、Slack ワークスペースは *Slack-Workspace-Id2* です。
    - "supported_channel_types":
      - "public": 範囲内の Slack ワークスペースでは、パブリック Slack チャネルを許可するかどうかの設定が上書きされます。
      - "private": 範囲内の Slack ワークスペースでは、プライベート Slack チャネルを許可するかどうかの設定が上書きされます。
    - supported_role_settings:
      - "user_role": 範囲内の Slack ワークスペースでは、ユーザーレベルの IAM ロールを許可するかどうかの設定が上書きされます。
      - "channel_role": 範囲内の Slack ワークスペースでは、チャネルレベルの IAM ロールを許可するかどうかの設定が上書きされます。
- Microsoft Teams では、次のフィールドを使用できます。
  - "client":
    - "enabled": Microsoft Teams クライアントが有効になっています。Microsoft Teams の統合は許可されています。
    - "disabled": Microsoft Teams クライアントは無効になっています。Microsoft Teams の統合は許可されていません。

- "tenants": 許可された Microsoft Teams テナントのカンマ区切りリスト。この例では、許可されたテナントは *Microsoft-Teams-Tenant-Id* です。
  - *Microsoft-Teams-Tenant-Id*: テナント内で許可されているチームのカンマ区切りリスト。この例では、許可されるチームは *Microsoft-Teams-Team-Id* です。
- "default": テナント内のチームのデフォルト設定。
  - supported_role_settings:
    - "user_role": 範囲内のチームは、デフォルトでユーザーレベルの IAM ロールを許可します。
    - "channel_role": 範囲内のチームは、デフォルトでチャネルレベルの IAM ロールを許可します。
- "overrides": Microsoft Teams テナントのオーバーライド設定。
  - *Microsoft-Teams-Tenant-Id*: オーバーライド設定が適用されるテナントのカンマ区切りリスト。この例では、テナントは *Microsoft-Teams-Tenant-Id* です。
    - *Microsoft-Teams-Team-Id*: テナント内のチームのカンマ区切りリスト。この例では、許可されるチームは *Microsoft-Teams-Team-Id* です。
      - supported_role_settings:
        - "user_role": 範囲内のチームがユーザーレベルの IAM ロールを許可するかどうかの設定を上書きします。
        - "channel_role": 範囲内のチームがチャネルレベルの IAM ロールを許可するかどうかの設定を上書きします。
- Amazon Chime では、次のメトリックを使用できます。
  - "client":
    - "enabled": Amazon Chime クライアントが有効になっています。Amazon Chime の統合は許可されています。
    - "disabled": Amazon Chime クライアントは無効になっています。Amazon Chime の統合は許可されていません。
- の下にはchatbot、下位レベルで上書きされない限り、組織全体のチャットアプリケーションで Amazon Q Developer を無効にするdefaultブロックがあります。このデフォルトは、チャットアプリケーションの Amazon Q Developer がサポートする新しいチャットアプリケーションも無効にします。例えば、チャットアプリケーションの Amazon Q Developer が新しいチャットアプリケーションをサポートしている場合、このデフォルトは新しくサポートされたチャットアプリケーションも無効にします。

> **Note**
>
> チャネルレベルの IAM ロールとユーザーレベルの IAM ロールの詳細については、「Amazon Q Developer in chat applications 管理者ガイド」の「Understanding Amazon Q Developer in chat applications permissions」を参照してください。

チャットアプリケーションポリシーの例

次のポリシーの例は、情報提供のみを目的としています。

例 1: 特定のワークスペースでプライベート Slack チャネルのみを許可する、Microsoft Teams を無効にする、すべての認証モードをサポート

次のポリシーは、Slack と Microsoft Teams のチャットボット統合で許可される設定の制御に焦点を当てています。

```
{
   "chatbot": {
      "platforms": {
         "slack": {
            "client": {
               "@@assign": "enabled"
            },
            "workspaces": {
               "@@assign": [
                  "Slack-Workspace-Id"
               ]
            },
            "default": {
               "supported_channel_types": {
                  "@@assign": [
                     "private"
                  ]
               },
               "supported_role_settings": {
                  "@@assign": [
                     "channel_role",
                     "user_role"
                  ]
               }
            }
```

```
         },
         "microsoft_teams": {
            "client": {
               "@@assign": "disabled"
            }
         },
         "chime":{
            "client":{
               "@@assign":"disabled"
            }
         },
         "default":{
            "client":{
               "@@assign":"disabled"
            }
         }
      }
   }
}
```

Slack の場合

- Slack クライアントが有効になっています。
- 特定の Slack ワークスペース *Slack-Workspace-Id* のみが許可されます。
- デフォルト設定では、プライベート Slack チャネル、チャネルレベルの IAM ロール、およびユーザーレベルの IAM ロールのみを許可します。

Microsoft Teams の場合

- Microsoft Teams クライアントは無効になっています。

Amazon Chime の場合

- Amazon Chime クライアントは無効になっています。

その他の詳細

- 下部の `default`ブロックはクライアントを無効に設定します。これにより、下位レベルで上書きされない限り、組織全体のチャットアプリケーションで Amazon Q Developer が無効になります。このデフォルトは、チャットアプリケーションの Amazon Q Developer がサポートする新し

いチャットアプリケーションも無効にします。例えば、チャットアプリケーションの Amazon Q Developer が新しいチャットアプリケーションをサポートしている場合、このデフォルトは新しくサポートされたチャットアプリケーションも無効にします。

例 2: ユーザーレベルの IAM ロールとの Slack 統合のみを許可する

次のポリシーでは、Slack に対してより寛容なアプローチを取り、すべての Slack ワークスペースを許可しますが、認証モードはユーザーレベルの IAM ロールのみに制限します。

```
{
   "chatbot":{
      "platforms":{
         "slack":{
            "client":{
               "@@assign":"enabled"
            },
            "workspaces":
               {
                  "@@assign":[
                     "*"
                  ]
               },
            "default":{
               "supported_role_settings":{
                  "@@assign":[
                     "user_role"
                  ]
               }
            }
         },
         "microsoft_teams":{
            "client":{
               "@@assign":"disabled"
            }
         },
         "chime":{
            "client":{
               "@@assign":"disabled"
            }
         }
      },
      "default":{
```

```
         "client":{
            "@@assign":"disabled"
         }
      }
   }
}
```

Slack の場合

- Slack クライアントが有効になっています。
- ワイルドカード "*" を使用して特定の Slack ワークスペースが定義されないため、すべてのワークスペースが許可されます。
- デフォルト設定では、ユーザーレベルの IAM ロールのみを許可します。

Microsoft Teams の場合

- Microsoft Teams クライアントは無効になっています。

Amazon Chime の場合

- Amazon Chime クライアントは無効になっています。

その他の詳細

- 下部の `default`ブロックはクライアントを無効に設定します。これにより、下位レベルで上書きされない限り、組織全体のチャットアプリケーションで Amazon Q Developer が無効になります。このデフォルトは、チャットアプリケーションの Amazon Q Developer がサポートする新しいチャットアプリケーションも無効にします。例えば、チャットアプリケーションの Amazon Q Developer が新しいチャットアプリケーションをサポートしている場合、このデフォルトは新しくサポートされたチャットアプリケーションも無効にします。

例 3: 特定のテナントで Microsoft Teams 統合のみを許可する

次のポリシー例では、組織をロックダウンして、指定されたテナント内の Microsoft Teams チャットボット統合のみを許可し、Slack 統合を完全にブロックします。

```
{
   "chatbot":{
```

```
      "platforms":{
         "slack":{
            "client": {
               "@@assign": "disabled"
            },
         },
         "microsoft_teams":{
            "client": {
               "@@assign": "enabled"
            },
            "tenants":{
               "Microsoft-Teams-Tenant-Id":{
                  "@@assign":[
                     "*"
                  ]
               }
            }
         },
         "chime": {
            "client":{
               "@@assign": "disabled"
            }
         }
      }
   }
}
```

Slack の場合

- Slack クライアントは無効になっています。

Microsoft Teams の場合

- 特定のテナント *Microsoft-Teams-Tenant-Id* のみが許可され、ワイルドカードを使用してそのテナント内のすべてのチーム "*" を許可します。

Amazon Chime の場合

- Amazon Chime クライアントは無効になっています。

その他の詳細

- 下部の defaultブロックはクライアントを無効に設定します。これにより、下位レベルで上書きされない限り、組織全体のチャットアプリケーションで Amazon Q Developer が無効になります。このデフォルトは、チャットアプリケーションの Amazon Q Developer がサポートする新しいチャットアプリケーションも無効にします。例えば、チャットアプリケーションの Amazon Q Developer が新しいチャットアプリケーションをサポートしている場合、このデフォルトは新しくサポートされたチャットアプリケーションも無効にします。

例 4: Slack ワークスペースと Microsoft Teams テナントのチャットアプリケーションでの制限付き Amazon Q Developer アクセスを許可する

次のポリシーでは、選択した Slack ワークスペースと Microsoft Teams テナントのチャットアプリケーションへのアクセスが制限されています。

```
{
    "chatbot":{
       "platforms":{
          "slack":{
             "client":{
                "@@assign":"enabled"
             },
             "workspaces": {
                   "@@assign":[
                      "Slack-Workspace-Id1",
                      "Slack-Workspace-Id2"
                   ]
             },
             "default":{
                "supported_channel_types":{
                   "@@assign":[
                      "private"
                   ]
                },
                "supported_role_settings":{
                   "@@assign":[
                      "user_role"
                   ]
                }
             },
             "overrides":{
                "Slack-Workspace-Id2":{
                   "supported_channel_types":{
                      "@@assign":[
```

```
                        "public",
                        "private"
                    ]
                },
                "supported_role_settings":{
                    "@@assign":[
                        "channel_role",
                        "user_role"
                    ]
                }
            }
        }
    },
    "microsoft_teams":{
        "client":{
            "@@assign":"enabled"
        },
        "tenants":{
            "Microsoft-Teams-Tenant-Id":{
                "@@assign":[
                    "Microsoft-Teams-Team-Id"
                ]
            }
        },
        "default":{
            "supported_role_settings":{
                "@@assign":[
                    "user_role"
                ]
            }
        },
        "overrides":{
            "Microsoft-Teams-Tenant-Id":{
                "Microsoft-Teams-Team-Id":{
                    "supported_role_settings":{
                        "@@assign":[
                            "channel_role",
                            "user_role"
                        ]
                    }
                }
            }
        }
    }
```

```
        },
        "default":{
           "client":{
              "@@assign":"disabled"
           }
        }
     }
}
```

Slack の場合

- Slack クライアントが有効になっています。
- 許可された Slack ワークスペースは、*Slack-Workspace-Id1* と *Slack-Workspace-Id2* です。
- Slack のデフォルト設定では、プライベートチャネルとユーザーレベルの IAM ロールのみを許可します。
- ワークスペース *Slack-Workspace-Id2* には、パブリックチャネルとプライベートチャネルの両方、およびチャネルレベルの IAM ロールとユーザーレベルの IAM ロールの両方を許可するオーバーライドがあります。

Microsoft Teams の場合

- Microsoft Teams が有効になっています。
- 許可される Teams テナントは、チームの *Microsoft-Teams-Team-Id* を持つ *Microsoft-Teams-Tenant-Id* です。
- デフォルト設定では、ユーザーレベルの IAM ロールを許可のみします。
- テナントの *Microsoft-Teams-Tenant-Id* には、チームの *Microsoft-Teams-Team-Id* のチャネルレベルの IAM ロールとユーザーレベルの IAM ロールの両方を許可するオーバーライドがあります。

その他の詳細

- 下部の `default`ブロックはクライアントを無効に設定します。これにより、下位レベルで上書きされない限り、組織全体のチャットアプリケーションで Amazon Q Developer が無効になります。これは、この例では Amazon Chime が無効になっていることを意味します。このデフォルトは、チャットアプリケーションの Amazon Q Developer がサポートする新しいチャットアプリケーションも無効にします。例えば、チャットアプリケーションの Amazon Q Developer が新し

いチャットアプリケーションをサポートしている場合、このデフォルトは新しくサポートされたチャットアプリケーションも無効にします。

AI サービスのオプトアウトポリシー

AWS AI サービスは、運用上の問題の修正、サービスパフォーマンスの評価、デバッグ、モデルトレーニングなど、サービスの改善のためにお客様のコンテンツを使用および保存する場合があります。この目的のために、このようなコンテンツ AWS リージョン は、サービスを使用している の AWS リージョン 外部に保存される場合があります。オプトアウトポリシーを使用して、サービス改善のためのコンテンツの使用を AWS Organizations オプトアウトできます。

個々の AI サービス、または AI サービスのオプトアウトポリシーでサポートされているすべてのサービスのオプトアウトポリシーを作成できます。各アカウントに適用される有効なポリシーをクエリして、設定の選択の効果を確認することもできます。

詳細については、 AWS 「 サービス条件」のAWS Machine Learningと人工知能サービス」を参照してください。AI サービスのオプトアウトポリシーでサポートされているサービスのリストについては、「サポートされている AI サービスのリスト」を参照してください。

トピック

- AI サービスオプトアウトポリシーを使用する際の考慮事項
- AI サービスのオプトアウトポリシーの利用開始
- サポートされているすべての AWS AI サービスをオプトアウトする
- AI サービスのオプトアウトポリシーの構文と例

AI サービスオプトアウトポリシーを使用する際の考慮事項

オプトアウトすると、関連するすべての履歴コンテンツが削除されます

AWS AI サービスによるコンテンツの使用をオプトアウトすると、そのサービスは、オプションを設定する AWS 前に と共有された関連する履歴コンテンツをすべて削除します。この削除は、サービス機能を提供するために必要のない、保存されているコンテンツに限定されます。

例えば、オプトイン中にサービスを使用すると、そのサービスはサービス改善のためにコンテンツのコピーを保存する場合があります。オプトアウトすると、その目的のためにサービスによって保存されたコピーは削除されますが、サービスの提供に使用されるコンテンツは削除されません。

AI サービスのオプトアウトポリシーの利用開始

人工知能 (AI) サービスのオプトアウトポリシーの利用を開始するステップは以下のとおりです。

1. バックアップポリシータスクの実行に必要なアクセス許可について説明します
2. AI サービスのオプトアウトポリシーを組織で有効にする。
3. AI サービスのオプトアウトポリシーを作成する。
4. 組織ルート、OU、またはアカウントに AI サービスのオプトアウトポリシーをアタッチする。
5. アカウントに適用される集約された有効な AI サービスのオプトアウトポリシーを確認する。

これらのすべてのステップでは、組織の管理アカウントの AWS Identity and Access Management (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 (非推奨) としてサインインします。

その他の情報

- AI サービスのオプトアウトポリシーの構文と例を確認する

サポートされているすべての AWS AI サービスをオプトアウトする

このトピックの内容

- AWS Organizations コンソールで 1 つのボタンを選択してオプトアウトできます。
- オプトアウトするには、 AWS CLI & AWS SDKs。
- AI サービスのオプトアウトポリシーで AWS のサービス サポートされている のリストを表示できます。

サポートされているすべての AI サービスからオプトアウトする

AI サービスのオプトアウトポリシーを作成してアタッチすることで、サービスの改善に使用されるコンテンツから組織をオプトアウトできます。このポリシーは、現在および将来サポートされているすべての AWS AI サービスに適用されます。メンバーアカウントはポリシーを更新できません。

AWS Management Console

すべての AI サービスをオプトアウトするには

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 (非推奨) としてサインインする必要があります。
2. AI サービスのオプトアウトポリシーページで、[すべてのサービスからオプトアウト] を選択します。
3. [すべてのサービスからオプトアウト] の確認ページで、[すべてのサービスからオプトアウト] を選択します。

AWS CLI & AWS SDKs

すべての AI サービスをオプトアウトするには

1. AI サービスのオプトアウト例の「例 1: 組織内のすべてのアカウントで、すべての AI サービスをオプトアウトする」をコピーします。
2. 「AI サービスのオプトアウトのアタッチとデタッチ」の指示に従います。

> **Note**
>
> Amazon Monitron からオプトアウトするには、追加の手順が必要です。詳細については、「AWS サービス条件」を参照してください。

AI サービスのオプトアウトポリシーでサポートされているサービスのリスト

AI サービスのオプトアウトポリシーで AWS のサービス サポートされている のリストを次に示します。

- Amazon API オペレーション
- Amazon Chime SDK 音声分析
- Amazon CloudWatch
- Amazon CodeGuru Profiler
- Amazon CodeWhisperer (現在は Amazon Q Developer の一部)

- Amazon Comprehend
- Amazon Connect
- Amazon Connect 最適化
- Amazon Connect Contact Lens
- AWS データベース移行サービス
- Amazon DataZone
- AWS Entity Resolution
- Amazon Fraud Detector
- AWS Glue
- Amazon GuardDuty
- Amazon Lex
- Amazon Polly
- Amazon Q
- Amazon QuickSight
- Amazon Rekognition
- Amazon Security Lake
- AWS Supply Chain
- Amazon Textract
- Amazon Transcribe
- AWS [Transform] (変換)
- Amazon Translate

AI サービスのオプトアウトポリシーの構文と例

このトピックでは、人工知能 (AI) サービスのオプトアウトポリシーの構文を例を挙げて説明します。

AI サービスのオプトアウトポリシーの構文

AI サービスのオプトアウトポリシーは、JSON のルールに従って構造化されたプレーンテキストファイルです。AI サービスのオプトアウトポリシーの構文は、管理ポリシータイプの構文に従います。この構文の詳しい説明については、「管理ポリシーの継承を理解する」を参照してください。こ

のトピックでは、一般的な構文を AI サービスのオプトアウトポリシータイプの特定の要件に適用することを重点的に扱っています。

> **Important**
>
> このセクションでは、値の大文字と小文字の区別が重要な点として取り上げられます。トピックで説明されたとおりに大文字と小文字を区別し、値を入力するようにしてください。大文字と小文字の区別が不適切だと、ポリシーは機能しません。

次のポリシーは、AI サービスのオプトアウトポリシーの基本構文を示しています。この例がアカウントに直接アタッチされている場合、そのアカウントは、あるサービスで明示的にオプトアウトされ、もう 1 つのサービスではオプトインされます。他のサービスのオプトインとオプトアウトに関しては、より高いレベル (OU またはルートのポリシー) から継承したポリシーに依存します。

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

組織のルートに次のサンプルポリシーポリシーがアタッチされていると仮定します。これにより、組織はデフォルトですべての AI サービスをオプトアウトするよう設定されています。明示的に除外されない限りすべての AI サービスが自動的にこの対象になります。これには、 AWS によって将来デプロイされる AI サービスも例外なく含まれます。子ポリシーを OU、または直接アカウントにアタッチすることで、Amazon Comprehend 以外のすべての AI サービスに関し、この設定を上書きできます。次の例の 2 番目のエントリでは、`@@operators_allowed_for_child_policies` を none に設定して使用し、オーバーライドされないようにする必要があります。例の 3 番目のエントリでは、Amazon Rekognition の除外を組織全体に設定しています。そのサービスに対して組織全体がオプトインされますが、このポリシーでは、子ポリシーによる適切な上書きを許可しています。

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

AI サービスのオプトアウトポリシーの構文には、次の要素が含まれます。

- services 要素。AI サービスのオプトアウトポリシーは、この固定名により、JSON を含む最も外側の要素として識別されます。

  AI サービスのオプトアウトポリシーには、services 要素の下に 1 つ以上のステートメントを含めることができます。各ステートメントには以下の要素が含まれます。

  - AWS AI サービスを識別するサービス名キー。次のキー名は、このフィールドにおいて有効な値です。
    - **default** - 現在利用可能なすべての AI サービスを表します。将来追加される AI サービスも、暗黙的かつ自動的に含まれます。
    - aiops
    - awssupplychain
    - chimesdkvoiceanalytics
    - cloudwatch
    - codeguruprofiler
    - codewhisperer

- comprehend
- connectamd
- connectoptimization
- contactlens
- datazone
- dms
- entityresolution
- frauddetector
- glue
- guardduty
- lex
- polly
- q
- quicksightq
- rekognition
- securitylake
- textract
- transcribe
- transform
- translate

サービス名キーによって識別される各ポリシーステートメントには、次の要素を含めることができます。

- opt_out_policy キー。このキーは必須の要素です。サービス名キーの下に配置できる唯一のキーです。

  opt_out_policy キーには、次のいずれかの値の @@assign 演算子だけを含めることが可能です。

  - optOut - 指定した AI サービスによるコンテンツの使用のオプトアウトを選択します。
  - optIn - 指定した AI サービスによるコンテンツの使用のオプトインを選択します。

> **メモ**
>
> - @@append および @@remove 継承演算子は AI サービスのオプトアウトポリシーに使用できません。
> - @@enforced_for 演算子は AI サービスのオプトアウトポリシーに使用できません。

- どのレベルでも、@@operators_allowed_for_child_policies 演算子を使用し、親ポリシーによる設定を上書きして子ポリシーが設定できることをコントロールできます。次のいずれかの値を指定できます。
  - @@assign - このポリシーの子ポリシーは、@@assign 演算子を使用して継承された値を別の値で上書きします。
  - @@none - このポリシーの子ポリシーは値を変更できません。

  @@operators_allowed_for_child_policies がどのように動作するかは、配置される場所によって異なります。以下の場所を使用できます。
  - services キーの下 - 有効なポリシーのサービスリストの追加と変更を子ポリシーに許可するかどうかをコントロールします。
  - 特定の AI サービスのキーまたは default キーの下 - この特定のエントリの下にあるキーリストの追加と変更を子ポリシーに許可するかどうかをコントロールします。
  - 特定のサービスの opt_out_policies キーの下 - この特定のサービスの設定の変更を子ポリシーに許可するかどうかをコントロールします。

AI サービスのオプトアウトポリシーの例

次のポリシーの例は、情報提供のみを目的としています。

例 1: 組織内のすべてのアカウントで、すべての AI サービスをオプトアウトする

次の例は、組織内のアカウントで AI サービスをオプトアウトするよう、組織のルートにアタッチできるポリシーを示しています。

> **Tip**
>
> 例の右上隅にあるコピーボタンを使用して例をコピーした場合、行番号は除外され、そのまま貼り付けることができます。

```
    | {
    |     "services": {
[1] |         "@@operators_allowed_for_child_policies": ["@@none"],
    |         "default": {
[2] |             "@@operators_allowed_for_child_policies": ["@@none"],
    |             "opt_out_policy": {
[3] |                 "@@operators_allowed_for_child_policies": ["@@none"],
    |                 "@@assign": "optOut"
    |             }
    |         }
    |     }
    | }
```

- [1] - services の下の "@@operators_allowed_for_child_policies": ["@@none"] により、すべての子ポリシーに対し、個別のサービス用に新しいセクションを追加することを禁止しています。存在できるのは、すでにある default セクションだけです。Default は、「すべての AI サービス」を表すプレースホルダです。
- [2] - default の下の "@@operators_allowed_for_child_policies": ["@@none"] により、すべてのポリシーに対し、新しいセクションを追加することを禁止しています。存在できるのは、すでにある opt_out_policy セクションだけです。
- [3] - opt_out_policy の下の "@@operators_allowed_for_child_policies": ["@@none"] により、子ポリシーによる optOut 設定の値の変更、および設定の追加を禁止しています。

例 2: 組織のデフォルト設定をすべてのサービスに適用しつつ、子ポリシーによるサービスごとの設定の上書きを許可する

次のサンプルポリシーでは、すべての AI サービスを対象に、組織全体のデフォルトを設定しています。default の値により、子ポリシーによるサービス default (すべての AI サービスのプレースホルダ) の optOut 値の変更を禁止しています。このポリシーをルートまたは OU にアタッチして親ポリシーとして適用した場合、子ポリシーでは、2 つ目のポリシーに示すように、サービスごとにオプトアウト設定を変更できます。

- services キーの下に "@@operators_allowed_for_child_policies": ["@@none"] を配置していないため、個々のサービス用に新しいセクションを追加することを子ポリシーに許可しています。

- default の下の "@@operators_allowed_for_child_policies": ["@@none"] により、すべてのポリシーに対し、新しいセクションを追加することを禁止しています。存在できるのは、すでにある opt_out_policy セクションだけです。
- opt_out_policy の下の "@@operators_allowed_for_child_policies": ["@@none"] により、子ポリシーによる optOut 設定の値の変更、および設定の追加を禁止しています。

組織ルートのユーザー AI サービスのオプトアウト親ポリシー

```
{
    "services": {
        "default": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        }
    }
}
```

次のサンプルポリシーは、先に挙げたサンプルポリシーが組織ルートまたは親 OU にアタッチされており、その親ポリシーの影響を受けるアカウントに、このサンプルがアタッチされることを前提としています。デフォルトのオプトアウト設定を上書きし、Amazon Lex サービスのみに明示的にオプトインします。

AI サービスのオプトアウトポリシー (子)

```
{
    "services": {
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

の有効なポリシー AWS アカウント は、親ポリシーからオプトアウト設定が継承されているため、アカウントが Amazon Lex のみにオプトインし、他のすべての AWS AI サービスをdefaultオプトアウトすることです。

例 3: 単一のサービスに対して組織全体の AI サービスのオプトアウトポリシーを定義する

以下の例では、AI サービスのオプトアウトポリシーで単一の AI サービスに対する `optOut` 設定を定義しています。このポリシーが組織のルートにアタッチされている場合、すべての子ポリシーに対し、このサービスの `optOut` 設定の上書きが禁止されます。その他のサービスはこのポリシーの適用対象外ですが、他の OU またはアカウントの子ポリシーの影響を受ける可能性はあります。

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

Security Hub ポリシー

AWS Security Hub ポリシーは、セキュリティチーム全体でセキュリティ設定を管理するための一元的なアプローチを提供します AWS Organizations。これらのポリシーを活用することで、一元的な設定メカニズムを通じて一貫したセキュリティコントロールを確立および維持できます。この統合により、組織のセキュリティ要件に沿ったポリシーを作成し、アカウントと組織単位 (OUs) 全体に一元的に適用することで、セキュリティカバレッジのギャップに対処できます。

Security Hub ポリシーは と完全に統合されているため AWS Organizations、管理アカウントまたは委任された管理者がセキュリティ設定を定義して適用できます。アカウントが組織に参加すると、組織階層内の場所に基づいて、該当するポリシーが自動的に継承されます。これにより、組織の成長に合わせてセキュリティ標準が一貫して適用されます。このポリシーは、既存の組織構造を尊重し、重要なセキュリティ設定を一元的に制御しながら、セキュリティ設定の分散方法に柔軟性を提供します。

主な特徴と利点

Security Hub ポリシーは、 AWS 組織全体のセキュリティ設定を管理および適用するのに役立つ包括的な機能セットを提供します。これらの機能は、マルチアカウント環境を一貫して制御しながら、セキュリティ管理を合理化します。

- 組織内のアカウントとリージョン全体で Security Hub を一元的に有効にする

- アカウントと OUs
- 新しいアカウントが組織に参加するときに、セキュリティ設定を自動的に適用する
- 組織全体で一貫したセキュリティ設定を確保する
- メンバーアカウントが組織レベルのセキュリティ設定を変更できないようにする

Security Hub ポリシーとは

Security Hub ポリシーは、組織のアカウント全体のセキュリティ設定を一元的に制御する AWS Organizations ポリシーです。これらのポリシーは とシームレスに連携 AWS Organizations し、マルチアカウント環境全体で一貫したセキュリティ標準を確立して維持するのに役立ちます。

Security Hub ポリシーを実装すると、組織全体に自動的に伝達される特定のセキュリティ設定を定義できるようになります。これにより、新しく作成されたアカウントを含むすべてのアカウントが、組織のセキュリティ要件とベストプラクティスと一致します。

これらのポリシーは、一貫したセキュリティコントロールを適用し、個々のアカウントが組織レベルのセキュリティ設定を変更できないようにすることで、コンプライアンスを維持するのにも役立ちます。この一元化されたアプローチにより、大規模で複雑な AWS 環境全体でセキュリティ設定を管理するための管理オーバーヘッドが大幅に削減されます。

Security Hub ポリシーの仕組み

Security Hub ポリシーを組織または組織単位にアタッチすると、 AWS Organizations は自動的にポリシーを評価し、定義した範囲に基づいてポリシーを適用します。ポリシーの適用プロセスは、特定の競合解決ルールに従います。

有効リストと無効リストの両方にリージョンが表示される場合、無効設定が優先されます。例えば、リージョンが有効設定と無効設定の両方にリストされている場合、Security Hub はそのリージョンで無効になります。

を有効にするために `ALL_SUPPORTED`を指定すると、明示的に無効になっていない限り、Security Hub は現在および将来のすべてのリージョンで有効になります。これにより、 が新しいリージョンに AWS 拡大するにつれて、包括的なセキュリティカバレッジを維持できます。

子ポリシーは、継承演算子を使用して親ポリシー設定を変更できるため、さまざまな組織レベルで詳細に制御できます。この階層的アプローチにより、特定の組織単位がベースラインコントロールを維持しながらセキュリティ設定をカスタマイズできるようになります。

用語

このトピックでは、Security Hub ポリシーについて説明するときに、次の用語を使用します。

Security Hub ポリシーの用語

用語	定義
有効なポリシー	継承されたすべてのポリシーを結合した後にアカウントに適用される最後のポリシー。
ポリシーの継承	アカウントが親組織単位からポリシーを継承するプロセス。
委任管理者	組織に代わって Security Hub ポリシーを管理するために指定されたアカウント。
サービスリンクロール	Security Hub が他の AWS サービスとやり取りできるようにする IAM ロール。

Security Hub ポリシーのユースケース

Security Hub ポリシーは、マルチアカウント環境における一般的なセキュリティ管理の課題に対処します。次のユースケースは、組織が通常これらのポリシーを実装してセキュリティ体制を強化する方法を示しています。

ユースケースの例: リージョンのコンプライアンス要件

多国籍企業には、地理的リージョンごとに異なる Security Hub 設定が必要です。を使用してすべてのリージョンで Security Hub を有効にする親ポリシーを作成しALL_SUPPORTED、子ポリシーを使用して、異なるセキュリティコントロールが必要な特定のリージョンを無効にします。これにより、包括的なセキュリティカバレッジを確保しながら、リージョンの規制への準拠を維持できます。

ユースケースの例: 開発チームのセキュリティ標準

ソフトウェア開発組織は Security Hub ポリシーを実装し、開発リージョンを管理外に保ちながら、本番稼働用リージョンでのモニタリングを可能にします。セキュリティモニタリングカバレッジを正確に制御するのではなくALL_SUPPORTED、明示的なリージョンリストをポリシーで使用します。このアプローチにより、開発分野の柔軟性を維持しながら、本番環境でより厳格なセキュリティコントロールを適用できます。

ポリシーの継承と適用

組織全体で効果的なセキュリティ管理を行うには、ポリシーの継承方法と適用方法を理解することが不可欠です。継承モデルは階層に従い、予測可能で一貫したポリシーアプリケーションを確保します AWS Organizations 。

- ルートレベルでアタッチされたポリシーはすべてのアカウントに適用されます
- アカウントが親組織単位からポリシーを継承する
- 複数のポリシーを 1 つのアカウントに適用できます
- より具体的なポリシー (階層内のアカウントに近い) が優先されます

ポリシー検証

Security Hub ポリシーを作成すると、次の検証が行われます。

- リージョン名は有効な AWS リージョン識別子である必要があります
- リージョンは Security Hub でサポートされている必要があります
- ポリシー構造は AWS Organizations ポリシー構文ルールに従う必要があります
- リストenable_in_regionsと disable_in_regions リストの両方が存在する必要がありますが、空にすることもできます

リージョンに関する考慮事項とサポートされているリージョン

Security Hub ポリシーは複数のリージョンで動作するため、グローバルセキュリティ要件を慎重に検討する必要があります。リージョンの動作を理解することで、組織のグローバルフットプリント全体に効果的なセキュリティコントロールを実装できます。

- ポリシーの適用は各リージョンで個別に行われます
- ポリシーに含めるリージョンまたは除外するリージョンを指定できます。
- ALL_SUPPORTED オプションを使用すると、新しいリージョンが自動的に含まれます。
- ポリシーは、Security Hub が利用可能なリージョンにのみ適用されます。

次のステップ

Security Hub ポリシーの使用を開始するには：

1. Security Hub ポリシーの開始方法の前提条件を確認する
2. ベストプラクティスガイドを使用してポリシー戦略を計画する
3. ポリシー構文の詳細とポリシーの例を表示する

Security Hub ポリシーの開始方法

Security Hub ポリシーを設定する前に、前提条件と実装要件を理解していることを確認してください。このトピックでは、組織内でこれらのポリシーを設定および管理するためのプロセスについて説明します。

[開始する前に]

Security Hub ポリシーを実装する前に、次の要件を確認してください。

- アカウントは AWS Organizations 組織の一部である必要があります
- 次のいずれかとしてサインインする必要があります。
  - 組織の管理アカウント
  - Security Hub ポリシーを管理するアクセス許可を持つ委任管理者アカウント
- 組織内で Security Hub の信頼されたアクセスを有効にする必要があります
- 組織のルートで Security Hub ポリシータイプを有効にする必要があります

さらに、以下を確認します。

- Security Hub は、ポリシーを適用するリージョンでサポートされています
- 管理アカウントでAWSServiceRoleForSecurityHubV2サービスにリンクされたロールが設定されている。このロールが存在することを確認するには、 を実行しますaws iam get-role --role-name AWSServiceRoleForSecurityHubV2。このロールを作成する必要がある場合は、管理アカウントから任意のリージョンaws securityhub enable-security-hub-v2で を実行するか、 を実行して直接作成できますaws iam create-service-linked-role --aws-service-name securityhubv2.amazonaws.com。

実装手順

Security Hub ポリシーを効果的に実装するには、以下のステップを順番に実行します。各ステップにより、適切な設定が保証され、セットアップ中の一般的な問題を防ぐことができます。管理アカウン

トまたは委任管理者は、 AWS Organizations コンソール、 AWS コマンドラインインターフェイス (AWS CLI)、または AWS SDKs を使用してこれらのステップを実行できます。

1. Security Hub の信頼されたアクセスを有効にします。
2. 組織の Security Hub ポリシーを有効にします。
3. Security Hub ポリシーを作成します。
4. Security Hub ポリシーを組織のルート、OU、またはアカウントにアタッチします。
5. アカウントに適用される有効な Security Hub ポリシーの組み合わせを表示します。

これらのすべてのステップでは、組織の管理アカウントの AWS Identity and Access Management (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 (非推奨) としてサインインします。

その他の情報

- Security Hub ポリシーのポリシー構文とポリシーの例について説明します。

Security Hub ポリシーを使用するためのベストプラクティス

組織全体に Security Hub ポリシーを実装する場合、確立されたベストプラクティスに従うことで、セキュリティ設定のデプロイとメンテナンスを確実に成功させることができます。これらのガイドラインは、Security Hub ポリシーの管理と実施の固有の側面に特化しています AWS Organizations。

ポリシー設計の原則

Security Hub ポリシーを作成する前に、ポリシー構造の明確な原則を確立します。ポリシーはシンプルに保ち、最終的な結果を判断するのが難しい複雑な属性間ルールやネストされたルールは避けてください。組織のルートレベルで広範なポリシーから始め、必要に応じて子ポリシーを通じて絞り込みます。

空のリージョンリストを戦略的に使用することを検討してください。特定のリージョンで Security Hub を無効にするだけで済む場合は`enable_in_regions`空のままにすることも、リージョンをポリシーによって管理されないようにするために`disable_in_regions`空のままにすることもできます。この柔軟性により、セキュリティモニタリングカバレッジを正確に制御できます。

リージョン管理戦略

Security Hub ポリシーを使用してリージョンを管理する場合は、これらの実証済みのアプローチを検討してください。セキュリティカバレッジに将来のリージョンを自動的に含め`ALL_SUPPORTED`る場

合に使用します。より詳細な制御を行うには、特に異なるリージョンで異なるセキュリティ設定が必要な場合にALL_SUPPORTED、 に依存するのではなく、リージョンを明示的に一覧表示します。

リージョン固有の要件、特に以下の要件を文書化します。

- 特定の設定を必要とするコンプライアンスが必須のリージョン
- 開発環境と本番環境の違い
- 特別な考慮事項があるオプトインリージョン
- Security Hub を無効にしておく必要があるリージョン

ポリシー継承計画

ポリシー継承構造を慎重に計画し、必要な柔軟性を確保しながら、効果的なセキュリティコントロールを維持します。継承されたポリシーを変更できる組織単位と許可される変更を文書化します。厳格なセキュリティコントロールを適用する必要がある場合は、継承演算子 (@@assign、@@append、@@remove) を親レベルで制限することを検討してください。

モニタリングと検証

定期的なモニタリングプラクティスを実装して、ポリシーが引き続き有効であることを確認します。ポリシーの添付ファイルは、特に組織の変更後に定期的に確認します。リージョン設定が意図したセキュリティカバレッジと一致することを検証します。特に、 を使用する場合、ALL_SUPPORTEDまたは複数のリージョンリストを管理する場合です。

トラブルシューティング戦略

Security Hub ポリシーをトラブルシューティングするときは、まずポリシーの優先順位と継承に焦点を当てます。リージョンが両方のリストに表示される場合、無効化設定は有効化設定よりも優先されることに注意してください。ポリシー継承チェーンをチェックして、親ポリシーと子ポリシーを組み合わせて各アカウントの有効なポリシーを作成する方法を理解します。

Security Hub ポリシーの構文と例

Security Hub ポリシーは、組織全体で Security Hub を有効にして設定する方法を定義する標準化された JSON 構文に従います。ポリシー構造を理解すると、セキュリティ要件に対して効果的なポリシーを作成できます。

考慮事項

Security Hub ポリシーを作成する前に、ポリシー構文に関する以下の重要なポイントを理解してください。

- ポリシーでは enable_in_regionsと の両方disable_in_regionsのリストが必要ですが、空にすることもできます。
- 有効なポリシーを処理する場合、 disable_in_regionsが優先されます。enable_in_regions
- 子ポリシーは、明示的に制限されていない限り、継承演算子を使用して親ポリシーを変更できます
- ALL_SUPPORTED 指定には、現在および将来のリージョンの両方が含まれます。
- リージョン名は有効で、Security Hub で使用できる必要があります

基本的なポリシー構造

Security Hub ポリシーは、次の基本構造を使用します。

```
{
  "securityhub": {
    "enable_in_regions": {
      "@@append": ["ALL_SUPPORTED"],
      "@@operators_allowed_for_child_policies": ["@@all"]
    },
    "disable_in_regions": {
      "@@append": [],
      "@@operators_allowed_for_child_policies": ["@@all"]
    }
  }
}
```

ポリシーの構成要素

Security Hub ポリシーには、次の主要なコンポーネントが含まれています。

`securityhub`

ポリシー設定の最上位コンテナ

すべての Security Hub ポリシーに必須

`enable_in_regions`

Security Hub を有効にする必要があるリージョンのリスト

特定のリージョン名または を含めることができます `ALL_SUPPORTED`

必須フィールドですが、空にすることができます

を使用する場合`ALL_SUPPORTED`、 には将来のリージョンが含まれます。

`disable_in_regions`

Security Hub を無効にする必要があるリージョンのリスト

特定のリージョン名または を含めることができます `ALL_SUPPORTED`

必須フィールドですが、空にすることができます

両方のリストにリージョンが表示される`enable_in_regions`場合よりも優先されます

継承演算子

@@assign - 継承された値を上書きします

@@append - 既存の値に新しい値を追加します

@@remove - 継承された設定から特定の値を削除します

Security Hub ポリシーの例

次の例は、一般的な Security Hub ポリシー設定を示しています。

以下の例では、現在および将来のすべてのリージョンで Security Hub を有効にします。`enable_in_regions` リスト`ALL_SUPPORTED`で を使用し、`disable_in_regions`空のままにすることで、このポリシーは新しいリージョンが利用可能になったときに包括的なセキュリティカバレッジを確保します。

```
{
   "securityhub":{
      "enable_in_regions":{
         "@@assign":[
            "ALL_SUPPORTED"
         ]
      },
```

```
      "disable_in_regions":{
         "@@assign":[

         ]
      }
   }
}
```

この例では、disable_in_regionsリストが よりも優先されるため、将来のリージョンを含むすべてのリージョンで Security Hub を無効にしますenable_in_regions。

```
{
   "securityhub":{
      "enable_in_regions":{
         "@@assign":[
            "us-east-1",
            "us-west-2"
         ]
      },
      "disable_in_regions":{
         "@@assign":[
            "ALL_SUPPORTED"
         ]
      }
   }
}
```

次の例は、子ポリシーが継承演算子を使用して親ポリシー設定を変更する方法を示しています。このアプローチにより、ポリシー構造全体を維持しながらきめ細かな制御が可能になります。子ポリシーは、 に新しいリージョンを追加enable_in_regionsし、 からリージョンを削除しますdisable_in_regions。

```
{
   "securityhub":{
      "enable_in_regions":{
         "@@append":[
            "eu-central-1"
         ]
      },
      "disable_in_regions":{
         "@@remove":[
            "us-west-2"
```

```
         ]
      }
   }
}
```

この例では、 を使用せずに、複数の特定のリージョンで Security Hub を有効にする方法を示しますALL_SUPPORTED。これにより、Security Hub が有効になっているリージョンを正確に制御できますが、指定されていないリージョンはポリシーによって管理されません。

```
{
   "securityhub":{
      "enable_in_regions":{
         "@@assign":[
            "us-east-1",
            "us-west-2",
            "eu-west-1",
            "ap-southeast-1"
         ]
      },
      "disable_in_regions":{
         "@@assign":[

         ]
      }
   }
}
```

次の例は、ほとんどのリージョンで Security Hub を有効にし、特定の場所で明示的に無効にすることで、リージョンのコンプライアンス要件を処理する方法を示しています。disable_in_regions リストが優先されるため、他のポリシー設定に関係なく、これらのリージョンで Security Hub が無効のままになります。

```
{
   "securityhub":{
      "enable_in_regions":{
         "@@assign":[
            "ALL_SUPPORTED"
         ]
      },
      "disable_in_regions":{
         "@@assign":[
            "ap-east-1",
```

```
            "me-south-1"
         ]
      }
   }
}
```

の委任管理者 AWS Organizations

AWS Organizations 管理アカウントとそのユーザーとロールは、そのアカウントで実行する必要があるタスクにのみ使用することをお勧めします。また、すべての AWS リソースを組織内の他のメンバーアカウントに保存し、管理アカウントからは切り離すことをおすすめします。これは、Organizations のサービスコントロールポリシー (SCP) などのセキュリティ機能は、管理アカウントのユーザーやロールに制限を加えることができないためです。

組織の管理アカウントから、ポリシー管理を Organizations の指定のメンバーアカウントに委任して、デフォルトでは管理アカウントのみが使用できるポリシーアクションを実行できます。

リソースベースの委任ポリシーの例については、「のリソースベースのポリシーの例 AWS Organizations」を参照してください。

トピック

- を使用してリソースベースの委任ポリシーを作成する AWS Organizations
- でリソースベースの委任ポリシーを更新する AWS Organizations
- でリソースベースの委任ポリシーを表示する AWS Organizations
- を使用してリソースベースの委任ポリシーを削除する AWS Organizations

を使用してリソースベースの委任ポリシーを作成する AWS Organizations

管理アカウントから、組織のリソースベースの委任ポリシーを作成し、ポリシーに対してアクションを実行できるメンバーアカウントを指定するステートメントを追加します。ポリシーに複数のステートメントを追加して、メンバーアカウントにさまざまなアクセス許可を示すことができます。

> 最小アクセス許可
>
> リソースベースの委任ポリシーを作成するには、次のアクションを実行するアクセス許可が必要です。
>
> - `organizations:PutResourcePolicy`

- `organizations:DescribeResourcePolicy`

また、必要なアクションに対応する IAM アクセス許可を委任された管理者アカウントのロールとユーザーに付与する必要があります。IAM アクセス許可がない場合、呼び出し元のプリンシパルには AWS Organizations ポリシーを管理するために必要なアクセス許可がないと見なされます。

AWS Management Console

次のいずれかの方法を使用して、 AWS Management Console のリソースベースの委任ポリシーにステートメントを追加します。

- JSON ポリシー – リソースベースの委任ポリシーの例を貼り付けてカスタマイズしてアカウントで使用するか、JSON エディタでの独自の JSON ポリシードキュメントを入力します。
- ビジュアルエディタ — ビジュアルエディタで新しい委任ポリシーを作成します。これにより、JSON 構文を記述せずに委任ポリシーを作成できます。

JSON ポリシーエディタを使用して委任ポリシーを作成する

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. [設定] を選択します。
3. [AWS Organizations の委任管理者]セクションで、[委任] を選択して Organizations 委任ポリシーを作成します。
4. JSON ポリシードキュメントを入力します。IAM ポリシー言語の詳細については、「IAM JSON ポリシーリファレンス」を参照してください。
5. ポリシーの検証中に生成されたセキュリティ警告、エラー、または一般的な警告を解決し、[Create policy] (ポリシーの作成) を選択して作業を保存します。

ビジュアルエディタを使用して、委任ポリシーを作成する

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. [設定] を選択します。
3. [AWS Organizations の委任管理者]セクションで、[委任] を選択して Organizations 委任ポリシーを作成します。
4. [Create Delegation policy] (委任ポリシーの作成) ページで、[Add new statement] (新しいステートメントを追加)を選択します。
5. [Effect] (効果) を `Allow` に設定します。
6. `Principal` を追加して委任したいメンバーアカウントを定義します。
7. [Actions] (アクション) のリストから、委任するアクションを選択します。[Filter actions] (アクションのフィルタ)を使用して選択を絞り込むことができます。
8. 委任されたメンバーアカウントが組織ルートまたは組織単位 (OU) にポリシーをアタッチできるかどうかを指定するには、`Resources` を設定します。また、リソースタイプとして `policy` を選択する必要があります。リソースは次の方法で指定できます。

   - [Add a resource] (リソースの追加) を選択し、ダイアログボックスのプロンプトに従って Amazon リソースネーム (ARN) を作成します。
   - エディタでリソース ARN を手動で一覧表示します。ARN 構文の詳細については、「 AWS 全般のリファレンスガイド」の「Amazon リソースネーム (ARN)」を参照してください。ポリシーのリソース要素で ARN を使用する方法については、「IAM JSON ポリシー要素: Resource」を参照してください。
9. 委任するポリシータイプなど、他の条件を指定するには、[Add a condition] (条件の追加) を選択します。条件の [Condition key] (条件キー)、[Tag key] (タグキー)、[Qualifier] (修飾子)、[Operator] (演算子) を選択し、**`Value`** を入力します。完了したら、[Add condition] (条件の追加) を選択します。条件要素の詳細については、「IAM JSON ポリシーリファレンス」の「IAM JSON ポリシーの要素: 条件」を参照してください。
10. さらにアクセス許可ブロックを追加するには、[Add new statement] (新しいステートメントを追加) を選択します。各ブロックに対して、ステップ 5 から 9 を繰り返します。
11. ポリシーの検証で生成されたセキュリティ警告、エラー、または一般的な警告を解決し、[Create policy] (ポリシーの作成) を選択して作業を保存します。

AWS CLI & AWS SDKs

委任ポリシーを作成する

以下のコマンドを使用して委任ポリシーを作成できます。

- AWS CLI: put-resource-policy

以下は、委任ポリシーを作成する例です。

```
$ aws organizations put-resource-policy --content
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Fully_manage_backup_policies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "135791357913"
            },
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:CreatePolicy",
                "organizations:DescribePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy",
                "organizations:AttachPolicy",
                "organizations:DetachPolicy"
            ],
            "Resource": [
                "arn:aws:organizations::246802468024:root/o-abcdef/r-pqrstu",
                "arn:aws:organizations::246802468024:ou/o-abcdef/*",
                "arn:aws:organizations::246802468024:account/o-abcdef/*",
                "arn:aws:organizations::246802468024:organization/policy/
backup_policy/*",
            ],
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [
                        "BACKUP_POLICY"
                    ]
                }
            }
        }
    ]
}
```

- AWS SDK: PutResourcePolicy

サポート対象の委任ポリシーのアクション

委任ポリシーでは、次のアクションがサポートされています。

- AttachPolicy
- CreatePolicy
- DeletePolicy
- DescribeAccount
- DescribeCreateAccountStatus
- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization
- DescribeOrganizationalUnit
- DescribePolicy
- DescribeResourcePolicy
- DetachPolicy
- DisablePolicyType
- EnablePolicyType
- ListAccounts
- ListAccountsForParent
- ListAWSServiceAccessForOrganization
- ListChildren
- ListCreateAccountStatus
- ListDelegatedAdministrators
- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget

- `ListRoots`
- `ListTagsForResource`
- `ListTargetsForPolicy`
- `TagResource`
- `UntagResource`
- `UpdatePolicy`

サポートされている条件キー

委任ポリシーに使用できるのは AWS Organizations 、 でサポートされている条件キーのみです。詳細については、「Service Authorization Reference」の「Condition keys for AWS Organizations」を参照してください。

でリソースベースの委任ポリシーを更新する AWS Organizations

管理アカウントから、組織のリソースベースの委任ポリシーを更新し、ポリシーに対してアクションを実行できるメンバーアカウントを指定するステートメントを追加します。ポリシーに複数のステートメントを追加して、メンバーアカウントにさまざまなアクセス許可を示すことができます。

> **最小アクセス許可**
>
> リソースベースの委任ポリシーを更新するには、次のアクションを実行するアクセス許可が必要です。
>
> - `organizations:PutResourcePolicy`
> - `organizations:DescribeResourcePolicy`
>
> また、必要なアクションに対応する IAM アクセス許可を委任された管理者アカウントのロールとユーザーに付与する必要があります。IAM アクセス許可がない場合、呼び出し元のプリンシパルには AWS Organizations ポリシーを管理するために必要なアクセス許可がないと見なされます。

AWS Management Console

次のいずれかの方法を使用して、 AWS Management Console のリソースベースの委任ポリシーにステートメントを追加します。

- JSON ポリシー – リソースベースの委任ポリシーの例を貼り付けてカスタマイズしてアカウントで使用するか、JSON エディタでの独自の JSON ポリシードキュメントを入力します。
- ビジュアルエディタ — ビジュアルエディタで新しい委任ポリシーを作成します。これにより、JSON 構文を記述せずに委任ポリシーを作成できます。

JSON ポリシーエディタを使用して委任ポリシーを更新する

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. [設定] を選択します。
3. [AWS Organizationsの委任管理者] セクションで、[編集] を選択して Organizations 委任ポリシーを更新します。
4. JSON ポリシードキュメントを入力します。IAM ポリシー言語の詳細については、「IAM JSON ポリシーリファレンス」を参照してください。
5. ポリシーの検証中に生成されたセキュリティ警告、エラー、または一般的な警告を解決してから、[ポリシーの作成] を選択します。

ビジュアルエディタを使用して、委任ポリシーを更新します。

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. [設定] を選択します。
3. [AWS Organizationsの委任管理者] セクションで、[編集] を選択して Organizations 委任ポリシーを更新します。
4. [Create Delegation policy] (委任ポリシーの作成) ページで、[Add new statement] (新しいステートメントを追加)を選択します。
5. [Effect] (効果) を `Allow` に設定します。
6. `Principal` を追加して委任したいメンバーアカウントを定義します。
7. [Actions] (アクション) のリストから、委任するアクションを選択します。[Filter actions] (アクションのフィルタ)を使用して選択を絞り込むことができます。

8. 委任されたメンバーアカウントが組織ルートまたは組織単位 (OU) にポリシーをアタッチできるかどうかを指定するには、`Resources` を設定します。また、リソースタイプとして `policy` を選択する必要があります。リソースは次の方法で指定できます。

   - [Add a resource] (リソースの追加) を選択し、ダイアログボックスのプロンプトに従って Amazon リソースネーム (ARN) を作成します。
   - エディタでリソース ARN を手動で一覧表示します。ARN 構文の詳細については、「 AWS 全般のリファレンスガイド」の「Amazon リソースネーム (ARN)」を参照してください。ポリシーのリソース要素で ARN を使用する方法については、「IAM JSON ポリシー要素: Resource」を参照してください。
9. 委任するポリシータイプなど、他の条件を指定するには、[Add a condition] (条件の追加) を選択します。条件の [Condition key] (条件キー)、[Tag key] (タグキー)、[Qualifier] (修飾子)、[Operator] (演算子) を選択し、**`Value`** を入力します。完了したら、[Add condition] (条件の追加) を選択します。条件要素の詳細については、「IAM JSON ポリシーリファレンス」の「IAM JSON ポリシーの要素: 条件」を参照してください。
10. さらにアクセス許可ブロックを追加するには、[Add new statement] (新しいステートメントを追加) を選択します。各ブロックに対して、ステップ 5 から 9 を繰り返します。
11. ポリシーの検証中に生成されたセキュリティ警告、エラー、または一般的な警告を解決を選択してから、[ポリシーの保存] を選択します。

AWS CLI & AWS SDKs

委任ポリシーを作成または更新する

以下のコマンドを使用して委任ポリシーを作成または更新できます。

- AWS CLI: put-resource-policy

  以下は委任ポリシーを作成または更新する例です。

```
$ aws organizations put-resource-policy --content
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Fully_manage_backup_policies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "135791357913"
```

```
            },
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:CreatePolicy",
                "organizations:DescribePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy",
                "organizations:AttachPolicy",
                "organizations:DetachPolicy"
            ],
            "Resource": [
                "arn:aws:organizations::246802468024:root/o-abcdef/r-pqrstu",
                "arn:aws:organizations::246802468024:ou/o-abcdef/*",
                "arn:aws:organizations::246802468024:account/o-abcdef/*",
                "arn:aws:organizations::246802468024:organization/policy/
backup_policy/*",
            ],
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [
                        "BACKUP_POLICY"
                    ]
                }
            }
        }
    ]
}
```

- AWS SDK: PutResourcePolicy

サポート対象の委任ポリシーのアクション

委任ポリシーでは、次のアクションがサポートされています。

- `AttachPolicy`
- `CreatePolicy`
- `DeletePolicy`
- `DescribeAccount`
- `DescribeCreateAccountStatus`

- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization
- DescribeOrganizationalUnit
- DescribePolicy
- DescribeResourcePolicy
- DetachPolicy
- DisablePolicyType
- EnablePolicyType
- ListAccounts
- ListAccountsForParent
- ListAWSServiceAccessForOrganization
- ListChildren
- ListCreateAccountStatus
- ListDelegatedAdministrators
- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget
- ListRoots
- ListTagsForResource
- ListTargetsForPolicy
- TagResource
- UntagResource
- UpdatePolicy

サポートされている条件キー

委任ポリシーに使用できるのは AWS Organizations 、 でサポートされている条件キーのみです。詳細については、「Service Authorization Reference」の「Condition keys for AWS Organizations」を参照してください。

でリソースベースの委任ポリシーを表示する AWS Organizations

管理アカウントから、組織のリソースベースの委任ポリシーを表示して、どの委任管理者がどのポリシータイプを管理できるかを把握できます。

> **最小アクセス許可**
>
> リソースベースのデリゲーションポリシーを表示するには、`organizations:DescribeResourcePolicy` のアクションを実行するアクセス許可が必要です。

AWS Management Console

委任ポリシーを表示するには

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. [設定] を選択します。
3. [AWS Organizations の委任管理者]セクションをスクロールして、委任ポリシー全体を表示します。

AWS CLI & AWS SDKs

委任ポリシーを表示する

以下のコマンドを使用して委任ポリシーを表示できます。

- AWS CLI: describe-resource-policy

  以下はポリシーを取得する例です。

```
$ aws organizations describe-resource-policy
```

- AWS SDK: DescribeResourcePolicy

を使用してリソースベースの委任ポリシーを削除する AWS Organizations

組織内のポリシーの管理を委任する必要がなくなった場合、リソースベースの委任ポリシーを組織の管理アカウントから削除できます。

> **Important**
> リソースベースの委任ポリシーを削除した場合、回復できません。

> **最小アクセス許可**
> リソースベースのデリゲーションポリシーを削除するには、`organizations:DeleteResourcePolicy` のアクションを実行するアクセス許可が必要です。

AWS Management Console

委任ポリシーを削除するには

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. [設定] を選択します。
3. [AWS Organizations の委任管理者]セクションで、[削除]を選択します。
4. [Detach policy] (ポリシーの削除) のダイアログボックスで、 **`delete`** を入力します。[Delete policy] (ポリシーの削除) を選択します。

AWS CLI & AWS SDKs

委任ポリシーを削除する

以下のコマンドを使用して委任ポリシーを削除できます。

- AWS CLI: delete-resource-policy

以下はポリシーを削除する例です。

```
$ aws organizations delete-resource-policy
```

- AWS SDK: DeleteResourcePolicy

ポリシータイプの有効化

ポリシーを作成して組織にアタッチする前に、そのポリシータイプを有効にする必要があります。ポリシータイプの有効化は、組織ルートで行う 1 回限りのタスクです。ポリシータイプは、組織の管理アカウントまたは委任管理者として指定されたメンバーアカウントからのみ有効にできます。

> **最小アクセス許可**
>
> ポリシータイプを有効にするには、以下のアクションを実行するアクセス許可が必要です。
>
> - `organizations:EnablePolicyType`
> - `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要
> - `organizations:ListRoots` - Organizations コンソールを使用する場合にのみ必要

AWS Management Console

ポリシータイプを有効にするには

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. [Policies] (ポリシー) ページで、有効化するポリシータイプの名前を選択します。
3. ポリシータイプのページで [Enable ***policy type***] (ポリシータイプの有効化) を選択します。

   ページは、指定したタイプの使用可能なポリシーのリストに置き換えられます。

AWS CLI & AWS SDKs

ポリシータイプを有効にするには

次のいずれかのコマンドを使用して、ポリシータイプを有効にできます。

- AWS CLI: enable-policy-type

  次の例は、組織のバックアップポリシーを有効にする方法を示しています。組織のルートの ID を指定する必要があることに注意してください。

```
$ aws organizations enable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": [
            {
                "Type": "BACKUP_POLICY",
                "Status": "ENABLED"
            }
        ]
    }
}
```

  出力の PolicyTypes のリストには、指定したポリシータイプが ENABLED の Status で含まれるようになります。

- AWS SDKs: EnablePolicyType

ポリシータイプの無効化

組織内で特定のポリシータイプを使用しなくなった場合は、誤って使用されないように、そのタイプを無効にすることができます。ポリシータイプは、組織の管理アカウントまたは委任管理者として指定されたメンバーアカウントからのみ無効にできます。

考慮事項

無効ポリシーはすべてのエンティティからデタッチされますが、削除されません

ポリシータイプを無効にすると、指定されたされたタイプのすべてのポリシーは、組織ルート内のすべてのエンティティから自動的にデタッチされます。ポリシーの削除は行われません。

(サービスコントロールポリシータイプのみ) ルート内のすべてのエンティティは、最初にデフォルトの **FullAWSAccess** SCP にのみアタッチされます

(サービスコントロールポリシータイプのみ) 後で SCP ポリシータイプを再び有効にした場合、組織ルート内のすべてのエンティティはデフォルトの FullAWSAccess SCP にのみアタッチされた状態になります。組織で SCP が無効になった時点で、エンティティへの SCP のアタッチは解除されます。後から SCP を再度有効にした場合は、必要に応じて組織のルート、OU、アカウントにアタッチし直す必要があります。

ポリシータイプを無効にする

最小アクセス許可

SCP を無効にするには、以下のアクションを実行する権限が必要です。

- `organizations:DisablePolicyType`
- `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要
- `organizations:ListRoots` - Organizations コンソールを使用する場合にのみ必要

AWS Management Console

ポリシータイプを無効にするには

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. ポリシーページで、無効にするポリシータイプの名前を選択します。
3. ポリシータイプのページで [Disable ***policy type***] (ポリシータイプの無効化) を選択します。
4. 確認ダイアログボックスで、「**disable**」と入力してから、[Disable] (無効化する) を選択します。

   使用可能なポリシーの一覧に、指定したタイプが表示されなくなります。

AWS CLI & AWS SDKs

ポリシータイプを無効にするには

ポリシータイプを無効にするには、次のコマンドを使用します。

- AWS CLI: disable-policy-type

  次の例は、組織のバックアップポリシーを無効にする方法を示しています。組織のルートの ID を指定する必要があることに注意してください。

```
$ aws organizations disable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": []
    }
}
```

  出力の PolicyTypes のリストには、指定したポリシータイプが含まれなくなります。

- AWS SDKs: DisablePolicyType

を使用した組織ポリシーの作成 AWS Organizations

組織のポリシーを有効にすると、ポリシーを作成できます。

このトピックでは、 を使用してポリシーを作成する方法について説明します AWS Organizations。ポリシーは、グループに適用するコントロールを定義します AWS アカウント。

トピック

- サービスコントロールポリシー (SCP) を作成する
- リソースコントロールポリシー (RCP) を作成する
- 宣言ポリシーを作成する
- バックアップポリシーを作成する

- タグポリシーを作成する
- チャットアプリケーションポリシーを作成する
- AI サービスのオプトアウトポリシーを作成する
- Security Hub ポリシーを作成する

サービスコントロールポリシー (SCP) を作成する

> **最小アクセス許可**
>
> SCP を作成するには、以下のアクションを実行する権限が必要です。
>
> - `organizations:CreatePolicy`

AWS Management Console

サービスコントロールポリシーを作成するには

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 (非推奨) としてサインインする必要があります。
2. サービスコントロールポリシーページで、[Create policy] (ポリシーの作成) を選択します。
3. [Create new service control policy] (新しいサービスコントロールポリシーの作成) ページで、[Policy name] (ポリシー名) とオプションの [Policy description] (ポリシーの説明) に入力します。
4. (オプション) [Add tag] (タグの追加) を選択してキーとオプションの値を入力し、1 つ以上のタグを追加します。値を空白のままにすると、空の文字列が設定され、`null` にはなりません。1 つのポリシーに最大 50 個のタグをアタッチできます。詳細については、「AWS Organizations リソースのタグ付け」を参照してください。

> **Note**
>
> この後のほとんどのステップでは、JSON エディタの右側にあるコントロールを使用して、要素ごとにポリシーを構築する方法について説明します。また、ウィンドウの左側にある JSON エディタには、いつでもテキストを入力することもできます。直接入力することも、コピーアンドペーストを使用することもできます。

5. ポリシーを構築するための次のステップは、アクセスを拒否または許可するステートメントを追加するかどうかに応じて異なります。詳細については、「SCP 評価」を参照してください。Deny ステートメントを使用すると、特定のリソースへのアクセスを制限したり、SCP が有効になる条件を定義したり、NotAction 要素を使用したりできるため、さらなるコントロールが可能になります。構文の詳細については、「SCP 構文」を参照してください。

   アクセスを拒否するステートメントを追加するには

   a. エディタの右側の Edit ステートメントペインで、アクションの追加で AWS サービスを選択します。

      右側のオプションを選択すると、JSON エディタが更新され、左側に対応する JSON ポリシーが表示されます。

   b. サービスを選択すると、そのサービスで使用可能なアクションが記載されたリストが開きます。[All actions] (すべてのアクション) または、拒否する 1 つ以上の個別のアクションを選択します。

      左側の JSON が更新され、選択したアクションが表示されます。

      > **Note**
      >
      > 個別のアクションを選択したら、戻って [All actions] (すべてのアクション) を選択すると、予定される *servicename*:* のエントリが JSON に追加されますが、以前に選択した個別のアクションは JSON に残ったまま削除されません。

   c. 追加のサービスからアクションを追加したい場合は、[Statement] (ステートメント) ボックスの上部にある [All services] (すべてのサービス) を選択し、必要に応じて前の 2 つのステップを繰り返します。

   d. ステートメントに含めるリソースを指定します。

      - [リソースの追加] の横にある [追加] を選択します。
      - [Add a resource] (リソースの追加) ダイアログで、リソースを制御するサービスをリストから選択します。前のステップで選択したサービスからのみ選択できます。
      - [Resource type] (リソースタイプ) で、制御するリソースのタイプを選択します。
      - 最後に、[Resource ARN] (リソース ARN) で Amazon リソースネーム (ARN) を入力し、アクセスをコントロールするリソースを特定します。中括弧 {} で囲まれたすべてのプレースホルダーを置き換える必要があります。そのリソースタイプの ARN 構文で許可されているワイルドカード (*) を指定できます。ワイルドカードを使用でき

る場所については、特定のリソースタイプに関するドキュメントを参照してください。

- [Add a resource] (リソースの追加) を選択して、ポリシーへの追加を保存します。JSON の `Resource` 要素に、追加や変更が反映されます。[Resource] (リソース) 要素が必要です。

> **Tip**
>
> 選択したサービスのすべてのリソースを指定する場合は、リストの [All resource] (すべてのリソース) のオプションを選択するか、JSON で `Resource` ステートメントを直接編集して `"Resource":"*"` を読み取ります。

e. (オプション) ポリシーステートメントが有効なときに制限する条件を指定するには、[条件を追加] の横にある [追加] を選択します。

- 条件キー – リストから、すべての AWS サービスで使用できる任意の条件キー (など`aws:SourceIp`) 、またはこのステートメントで選択したサービスの 1 つのみのサービス固有のキーを選択できます。
- 修飾子 – (オプション) リクエストに複数値のコンテキストキーの値が複数ある場合、値に対してリクエストをテストするための修飾子を指定できます。詳細については、IAM ユーザーガイドの「単一値コンテキストキーと複数値コンテキストキー」を参照してください。リクエストに複数の値を含めることができるかどうかを確認するには、「サービス認可リファレンス」の「 のアクション、リソース、および条件キー AWS のサービス」を参照してください。
  - デフォルト値 — ポリシーの条件キーバリューに対する、リクエスト内の単一の値をテストします。リクエスト値がポリシーの値と一致する場合、条件は true を返します。ポリシーで複数の値を指定した場合、それらは「or」のテストとして扱われ、リクエスト値がポリシーの値のいずれかに一致すると、条件は true を返します。
  - リクエスト内の任意の値 — リクエストに複数の値を含めることができる場合、このオプションでは、リクエスト値の少なくとも 1 つが、ポリシーの少なくとも 1 つの条件キーバリューと一致するかどうかをテストします。リクエスト内のキーバリューのいずれかがポリシーの条件値のいずれかと一致する場合に true が返されます。一致するキーまたは空のデータセットがない場合、条件は false を返します。
  - リクエスト内のすべての値 - リクエストに複数の値を含めることができる場合、このオプションは、すべてのリクエスト値がポリシーの条件キーバリューと一致す

るかどうかをテストします。リクエストのすべてのキーバリューがポリシーの 1 つ以上の値と一致する場合、条件は true を返します。また、リクエストにキーがない場合、またはキーバリューが空の文字列などの null データセットに解決される場合は true を返します。

- 演算子 — 演算子は、比較するタイプを指定します。表示されるオプションは、条件キーのデータ型によって異なります。例えば、`aws:CurrentTime` グローバル条件キーを使用すると、任意の日付比較演算子または `Null` から選択でき、それを使用してリクエスト内に値が存在するかどうかをテストできます。

  `Null` テスト以外のすべての条件演算子については、IfExists オプションを選択できます。

- 値 — (オプション) リクエストをテストする 1 つ以上の値を指定します。

[条件を追加] を選択します。

条件キーの詳細については、IAM ユーザーガイドの「IAM JSON ポリシーの要素: Condition」を参照してください。

6. アクセスを許可するステートメントを追加するには

   a. 左側の JSON エディタで、行 `"Effect": "Deny"` を `"Effect": "Allow"` に変更します。

      右側のオプションを選択すると、JSON エディターが更新され、対応する JSON ポリシーが左側に表示されます。

   b. サービスを選択すると、そのサービスで使用可能なアクションが記載されたリストが開きます。[All actions] (すべてのアクション) または、許可する 1 つ以上のアクションを個別に選択できます。

      左側の JSON が更新され、選択したアクションが表示されます。

      > **Note**
      >
      > 個別のアクションを選択したら、戻って [All actions] (すべてのアクション) を選択すると、予定される *`servicename`*`:*` のエントリが JSON に追加されますが、以前に選択した個別のアクションは JSON に残ったまま削除されません。

c. 追加のサービスからアクションを追加したい場合は、[Statement] (ステートメント) ボックスの上部にある [All services] (すべてのサービス) を選択し、必要に応じて前の 2 つのステップを繰り返します。

7. (オプション) ポリシーに別のステートメントを追加するには、[Add statement] (ステートメントを追加) を選択し、ビジュアルエディタを使用して次のステートメントを構築します。
8. ステートメントの追加が終了したら、[ポリシーの作成] を選択して完了した SCP を保存します。

新しい SCP は組織のポリシーのリストに表示されます。SCP をルート、OU、またはアカウントにアタッチできるようになりました。

AWS CLI & AWS SDKs

サービスコントロールポリシーを作成するには

SCP を作成するには、次のいずれかのコマンドを使用します。

- AWS CLI: create-policy

次の例は、JSON ポリシーのテキストを含む Deny-IAM.json いう名前のファイルがあることを前提としたものです。このファイルを使用して、新しいサービスコントロールポリシーを作成します。

```
$ aws organizations create-policy \
    --content file://Deny-IAM.json \
    --description "Deny all IAM actions" \
    --name DenyIAMSCP \
    --type SERVICE_CONTROL_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "DenyIAMSCP",
            "Description": "Deny all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
```

```
    }
}
```

- AWS SDKs: CreatePolicy

> **Note**
>
> SCP は、管理アカウントやその他のいくつかの状況では有効になりません。詳細については、「SCP によって制限されないタスクおよびエンティティ」を参照してください。

リソースコントロールポリシー (RCP) を作成する

> **最小アクセス許可**
>
> RCPs を作成するには、次のアクションを実行するアクセス許可が必要です。
>
> - `organizations:CreatePolicy`

AWS Management Console

リソースコントロールポリシーを作成するには

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 (非推奨) としてサインインする必要があります。
2. リソースコントロールポリシーページで、ポリシーの作成を選択します。
3. 新しいリソースコントロールポリシーの作成ページで、ポリシー名とオプションのポリシーの説明を入力します。
4. (オプション) [Add tag] (タグの追加) を選択してキーとオプションの値を入力し、1 つ以上のタグを追加します。値を空白のままにすると、空の文字列が設定され、null にはなりません。1 つのポリシーに最大 50 個のタグをアタッチできます。詳細については、「AWS Organizations リソースのタグ付け」を参照してください。

> **Note**
>
> この後のほとんどのステップでは、JSON エディタの右側にあるコントロールを使用して、要素ごとにポリシーを構築する方法について説明します。また、ウィンドウの左側にある JSON エディタには、いつでもテキストを入力することもできます。直接入力することも、コピーアンドペーストを使用することもできます。

5. ステートメントを追加するには：

   a. エディタの右側のステートメントの編集ペインで、アクションの追加で AWS サービスを選択します。

      右側のオプションを選択すると、JSON エディタが更新され、左側に対応する JSON ポリシーが表示されます。

   b. サービスを選択すると、そのサービスで使用可能なアクションが記載されたリストが開きます。[All actions] (すべてのアクション) または、拒否する 1 つ以上の個別のアクションを選択します。

      左側の JSON が更新され、選択したアクションが表示されます。

      > **Note**
      >
      > 個別のアクションを選択したら、戻って [All actions] (すべてのアクション) を選択すると、予定される *servicename*:* のエントリが JSON に追加されますが、以前に選択した個別のアクションは JSON に残ったまま削除されません。

   c. 追加のサービスからアクションを追加したい場合は、[Statement] (ステートメント) ボックスの上部にある [All services] (すべてのサービス) を選択し、必要に応じて前の 2 つのステップを繰り返します。

   d. ステートメントに含めるリソースを指定します。

      - [リソースの追加] の横にある [追加] を選択します。
      - [Add a resource] (リソースの追加) ダイアログで、リソースを制御するサービスをリストから選択します。前のステップで選択したサービスからのみ選択できます。
      - [Resource type] (リソースタイプ) で、制御するリソースのタイプを選択します。
      - リソース ARN で Amazon リソースネーム (ARN) を入力して、アクセスを制御する特定のリソースを特定します。中括弧 {} で囲まれたすべてのプレースホルダーを置き

換える必要があります。そのリソースタイプの ARN 構文で許可されているワイルドカード (*) を指定できます。ワイルドカードが使用できる場所については、特定のリソースタイプのドキュメントを参照してください。

- [Add a resource] (リソースの追加) を選択して、ポリシーへの追加を保存します。JSON の `Resource` 要素に、追加や変更が反映されます。[Resource] (リソース) 要素が必要です。

> **Tip**
>
> 選択したサービスのすべてのリソースを指定する場合は、リストの [All resource] (すべてのリソース) のオプションを選択するか、JSON で `Resource` ステートメントを直接編集して `"Resource":"*"` を読み取ります。

e. (オプション) ポリシーステートメントが有効なときに制限する条件を指定するには、[条件を追加] の横にある [追加] を選択します。

- 条件キー – リストから、すべての AWS サービスで使用できる任意の条件キー (など`aws:SourceIp`) 、またはこのステートメントで選択したサービスの 1 つだけのサービス固有のキーを選択できます。
- 修飾子 – (オプション) リクエストに複数値のコンテキストキーの値が複数ある場合、値に対してリクエストをテストするための修飾子を指定できます。詳細については、IAM ユーザーガイドの「単一値コンテキストキーと複数値コンテキストキー」を参照してください。リクエストに複数の値を含めることができるかどうかを確認するには、「サービス認可リファレンス」の「 のアクション、リソース、および条件キー AWS のサービス」を参照してください。
  - デフォルト値 — ポリシーの条件キーバリューに対する、リクエスト内の単一の値をテストします。リクエスト値がポリシーの値と一致する場合、条件は true を返します。ポリシーで複数の値を指定した場合、それらは「or」のテストとして扱われ、リクエスト値がポリシーの値のいずれかに一致すると、条件は true を返します。
  - リクエスト内の任意の値 — リクエストに複数の値を含めることができる場合、このオプションでは、リクエスト値の少なくとも 1 つが、ポリシーの少なくとも 1 つの条件キーバリューと一致するかどうかをテストします。リクエスト内のキーバリューのいずれかがポリシーの条件値のいずれかと一致する場合に true が返されます。一致するキーまたは空のデータセットがない場合、条件は false を返します。

- リクエスト内のすべての値 - リクエストに複数の値を含めることができる場合、このオプションは、すべてのリクエスト値がポリシーの条件キーバリューと一致するかどうかをテストします。リクエストのすべてのキーバリューがポリシーの 1 つ以上の値と一致する場合、条件は true を返します。また、リクエストにキーがない場合、またはキーバリューが空の文字列などの null データセットに解決される場合は true を返します。

- 演算子 — 演算子は、比較するタイプを指定します。表示されるオプションは、条件キーのデータ型によって異なります。例えば、`aws:CurrentTime` グローバル条件キーを使用すると、任意の日付比較演算子または `Null` から選択でき、それを使用してリクエスト内に値が存在するかどうかをテストできます。

  `Null` テスト以外のすべての条件演算子については、IfExists オプションを選択できます。

- 値 — (オプション) リクエストをテストする 1 つ以上の値を指定します。

[条件を追加] を選択します。

条件キーの詳細については、IAM ユーザーガイドの「IAM JSON ポリシーの要素: Condition」を参照してください。

f. (オプション) `NotAction` 要素を使用して、指定したアクションを除くすべてのアクションへのアクセスを拒否するには、左側のペインにある `Action` を `NotAction` 要素の直後に表示される `"Effect": "Deny",` で置き換えます。詳細については、IAM ユーザーガイドの 「IAM JSON ポリシーの要素: NotAction」を参照してください。

6. (オプション) ポリシーに別のステートメントを追加するには、[Add statement] (ステートメントを追加) を選択し、ビジュアルエディタを使用して次のステートメントを構築します。

7. ステートメントの追加が完了したら、ポリシーの作成を選択して、完了した RCP を保存します。

新しい RCP が組織のポリシーのリストに表示されます。RCP をルート、OUs、またはアカウントにアタッチできるようになりました。

AWS CLI & AWS SDKs

リソースコントロールポリシーを作成するには

次のいずれかのコマンドを使用して RCP を作成できます。

- AWS CLI: create-policy

  次の例は、JSON ポリシーのテキストを含む Deny-IAM.json いう名前のファイルがあることを前提としたものです。このファイルを使用して、新しいリソースコントロールポリシーを作成します。

```
$ aws organizations create-policy \
    --content file://Deny-IAM.json \
    --description "Deny all IAM actions" \
    --name DenyIAMRCP \
    --type RESOURCE_CONTROL_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
resource_control_policy/p-i9j8k7l6m5",
            "Name": "DenyIAMRCP",
            "Description": "Deny all IAM actions",
            "Type": "RESOURCE_CONTROL_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

- AWS SDKs: CreatePolicy

> **Note**
>
> RCPs、管理アカウントや他のいくつかの状況では有効になりません。詳細については、「RCPs によって制限されていないリソースとエンティティ」を参照してください。

宣言ポリシーを作成する

> **最小アクセス許可**
>
> 宣言ポリシーを作成するには、次のアクションを実行するアクセス許可が必要です。

- `organizations:CreatePolicy`

AWS Management Console

宣言ポリシーを作成するには

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 (非推奨) としてサインインする必要があります。
2. 宣言ポリシーページで、ポリシーの作成を選択します。
3. EC2 の新しい宣言ポリシーの作成ページで、ポリシー名とオプションのポリシーの説明を入力します。
4. (オプション) [Add tag] (タグの追加) を選択してキーとオプションの値を入力することで、ポリシーに 1 つ以上のタグを追加できます。値を空白のままにすると、空の文字列が設定され、null にはなりません。1 つのポリシーに最大 50 個のタグをアタッチできます。詳細については、「AWS Organizations リソースのタグ付け」を参照してください。
5. この手順で説明するように、[ビジュアルエディタ] を使用してポリシーを構築できます。また、[JSON] タブにポリシーテキストを入力または貼り付けることもできます。宣言ポリシー構文の詳細については、「」を参照してください宣言型ポリシーの構文と例。

   ビジュアルエディタを使用する場合は、宣言ポリシーに含めるサービス属性を選択します。詳細については、「サポートされている AWS のサービス および 属性」を参照してください。
6. サービス属性を追加を選択し、仕様に合わせて属性を設定します。各効果の詳細については、「」を参照してください宣言型ポリシーの構文と例。
7. ポリシーの編集が完了したら、ページの右下隅の [Create policy] (ポリシーの作成) を選択します。

AWS CLI & AWS SDKs

宣言ポリシーを作成するには

宣言ポリシーを作成するには、次のいずれかを使用できます。

- AWS CLI: create-policy

1. 次のような宣言ポリシーを作成し、テキストファイルに保存します。

```
{
    "ec2_attributes": {
        "image_block_public_access": {
            "state": {
                "@@assign": "block_new_sharing"
            }
        }
    }
}
```

この宣言ポリシーでは、新しい Amazon マシンイメージ (AMIs) がパブリックに共有されないように、ポリシーの影響を受けるすべてのアカウントを設定する必要があります。宣言ポリシー構文の詳細については、「」を参照してください宣言型ポリシーの構文と例。

2. JSON ポリシーファイルをインポートして、組織内に新しいポリシーを作成します。この例では、先に扱った JSON ファイルは policy.json という名前になっています。

```
$ aws organizations create-policy \
    --type DECLARATIVE_POLICY_EC2 \
    --name "MyTestPolicy" \
    --description "My test policy" \
    --content file://policy.json
{
    "Policy": {
        "Content": "{"ec2_attributes":{"image_block_public_access":{"state":
{"@@assign":"block_new_sharing"}}}}".
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5"
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/
declarative_policy_ec2/p-i9j8k7l6m5",
            "Description": "My test policy",
            "Name": "MyTestPolicy",
            "Type": "DECLARATIVE_POLICY_EC2"
        }
    }
}
```

- AWS SDKs: CreatePolicy

次のステップ

宣言ポリシーを作成したら、アカウントステータスレポートを使用して準備状況を評価します。その後、ベースライン設定を適用できます。これを行うには、組織ルート、組織単位 (OU)、組織内の AWS アカウント 、またはこれらすべてにポリシーをアタッチします。

バックアップポリシーを作成する

> **最小アクセス許可**
>
> バックアップポリシーを作成するには、次のアクションを実行するアクセス許可が必要です。
>
> - `organizations:CreatePolicy`

AWS Management Console

バックアップポリシーは、次の 2 つの方法のいずれか AWS Management Console で で作成できます。

- オプションを選択し、JSON ポリシーテキストを生成できるビジュアルエディタ。
- JSON ポリシーテキストを直接作成できるテキストエディタ。

ビジュアルエディタを使用すると、プロセスが簡単になりますが、柔軟性は制限されます。これは、最初のポリシーを作成し、使用に慣れるのに最適な方法です。これらの機能の仕組みを理解し、ビジュアルエディタが提供するものによって制限され始めたら、JSON ポリシーテキストを自分で編集して、ポリシーに高度な機能を追加できます。ビジュアルエディタは、@@assign 値設定演算子のみを使用し、子制御演算子へのアクセスは提供しません。子制御演算子は、JSON ポリシーテキストを手動で編集した場合にのみ追加できます。

バックアップポリシーを作成するには

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 (非推奨) としてサインインする必要があります。
2. バックアップポリシーページで、[Create policy] (ポリシーの作成) を選択します。
3. [Create policy] (ポリシーの作成) ページで、ポリシー名と、オプションでポリシーの説明を入力します。

4. (オプション) [Add tag] (タグの追加) を選択してキーとオプションの値を入力することで、ポリシーに 1 つ以上のタグを追加できます。値を空白のままにすると、空の文字列が設定され、null にはなりません。1 つのポリシーに最大 50 個のタグをアタッチできます。タグ付けの詳細については、「AWS Organizations リソースのタグ付け」を参照してください。
5. この手順で説明するように、[ビジュアルエディタ] を使用してポリシーを構築できます。また、[JSON] タブにポリシーテキストを入力または貼り付けることもできます。バックアップポリシーの構文については、バックアップポリシーの構文と例 を参照してください。

   [ビジュアルエディタ] を使用する場合は、シナリオに適したバックアップオプションを選択します。バックアッププランは 3 つの部分で構成されます。こうしたバックアッププランの要素について詳しくは、AWS Backup デベロッパーガイドのバックアッププランの作成、およびリソースの割り当てを参照してください。

   a. バックアッププランの全般的な説明
      - [バックアッププラン名] には、英数字、ハイフン、下線のみを使用できます。
      - リストから少なくとも 1 つの [バックアッププランリージョン] を選択する必要があります。プランでは、選択した AWS リージョンでのみリソースをバックアップできます。

   b. AWS Backup の動作方法とタイミングを指定する 1 つ以上のバックアップルール。各バックアップルールは、次の項目を定義します。
      - バックアップの頻度、およびバックアップを実行できるタイムウィンドウを含むスケジュール。
      - 使用するバックアップボールトの名前。[バックアップボールト名] は、英数字、ハイフン、下線のみで構成できます。プランを正常に実行するには、バックアップボールトが存在している必要があります。 AWS Backup コンソールまたは AWS CLI コマンドを使用してボールトを作成します。
      - (オプション) 1 つ以上のリージョンにコピールールで、バックアップを他の AWS リージョンのボールトにもコピーします。
      - このバックアッププランを実行するたびに作成されるバックアップリカバリポイントに関連付ける 1 つ以上のタグキーと値のペア。
      - バックアップがコールドストレージに移行するタイミングとバックアップの期限を指定するライフサイクルオプション。

      [Add rule] (ルールの追加) を選択し、必要な各ルールをプランに追加します。

      バックアップルールの詳細については、AWS Backup デベロッパーガイドのバックアップルールを参照してください。

c. このプランで AWS Backup がバックアップするリソースを指定するリソース割り当て。割り当ては、 AWS Backup がリソースの検索と照合に使用するタグペアを指定することによって行われます。

- [リソースの割り当て名] には、英数字、ハイフン、下線のみを使用できます。
- AWS Backup 用の [IAM role] (IAM ロール) を指定します。バックアップはこの名前で実行されます。

  コンソールでは、Amazon リソースネーム (ARN) の全体は指定しません。ロール名とロールのタイプを指定するプレフィックスの両方を含める必要があります。通常、プレフィックスは `role` または `service-role` で、ロール名とはスラッシュ (「/」) で区切られます。例えば、`role/MyRoleName` または `service-role/MyManagedRoleName` と入力します。これは、基本となる JSON に保存される際に完全な ARN に自動で変換されます。

  > **Important**
  >
  > 指定した IAM ロールは、ポリシーが適用されるアカウントにすでに存在している必要があります。存在しない場合、バックアッププランはバックアップジョブを正常に開始する可能性がありますが、それらのバックアップジョブは失敗します。

- [Resource tag key] (リソースタグキー) と [Tag values] (タグ値) のペアを 1 つ以上指定し、バックアップするリソースを特定します。複数のタグ値がある場合は、値をカンマで区切ります。

[Add assignment] (割り当てを追加) を選択し、バックアッププランに設定した各リソース割り当てを追加します。

詳細については、AWS Backup デベロッパーガイドのバックアッププランへのリソースの割り当てを参照してください。

6. ポリシーの作成が完了したら、[Create policy] (ポリシーの作成) を選択します。使用可能なバックアップポリシーのリストにポリシーが表示されます。

AWS CLI & AWS SDKs

バックアップポリシーを作成するには

次のいずれかを使用して、バックアップポリシーを作成できます。

- AWS CLI: create-policy

  バックアッププランを次のような JSON テキストとして作成し、テキストファイルとして保存します。構文のすべてのルールについては、バックアップポリシーの構文と例 を参照してください。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" }
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "datatype": {
                            "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                            "tag_key": { "@@assign": "dataType" },
                            "tag_value": { "@@assign": [ "PII" ] }
                        }
                    }
                }
```

```
        }
    }
}
```

このバックアッププランでは、 AWS Backup AWS アカウント が、指定された にあり、 の値dataTypeを持つ タグ AWS リージョン を持つ、影響を受ける のすべてのリソースをバックアップするように指定しますPII。

次に、JSON ポリシーファイルをインポートして、組織内に新しいポリシーを作成します。出力のポリシー ARN の末尾にあるポリシー ID を書き留めます。

```
$ aws organizations create-policy \
    --name "MyBackupPolicy" \
    --type BACKUP_POLICY \
    --description "My backup policy" \
    --content file://policy.json{
    "Policy": {
        "PolicySummary": {
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/backup_policy/p-
i9j8k7l6m5",
            "Description": "My backup policy",
            "Name": "MyBackupPolicy",
            "Type": "BACKUP_POLICY"
        }
        "Content": "...a condensed version of the JSON policy document you
 provided in the file...",
    }
}
```

- AWS SDKs: CreatePolicy

タグポリシーを作成する

> **最小アクセス許可**
>
> タグポリシーを作成するには、次のアクションを実行するためのアクセス権限が必要です。
>
> - `organizations:CreatePolicy`

のタグポリシーは、次の 2 つの方法のいずれか AWS Management Console で作成できます。

- オプションを選択し、JSON ポリシーテキストを生成できるビジュアルエディタ。
- JSON ポリシーテキストを直接作成できるテキストエディタ。

ビジュアルエディタを使用すると、プロセスが簡単になりますが、柔軟性は制限されます。これは、最初のポリシーを作成し、使用に慣れるのに最適な方法です。これらの機能の仕組みを理解し、ビジュアルエディタが提供するものによって制限され始めたら、JSON ポリシーテキストを自分で編集して、ポリシーに高度な機能を追加できます。ビジュアルエディタは、@@assign 値設定演算子のみを使用し、子制御演算子へのアクセスは提供しません。子制御演算子は、JSON ポリシーテキストを手動で編集した場合にのみ追加できます。

AWS Management Console

のタグポリシーは、次の 2 つの方法のいずれか AWS Management Console で作成できます。

- オプションを選択し、JSON ポリシーテキストを生成できるビジュアルエディタ。
- JSON ポリシーテキストを直接作成できるテキストエディタ。

ビジュアルエディタを使用すると、プロセスが簡単になりますが、柔軟性は制限されます。これは、最初のポリシーを作成し、使用に慣れるのに最適な方法です。これらの機能の仕組みを理解し、ビジュアルエディタが提供するものによって制限され始めたら、JSON ポリシーテキストを自分で編集して、ポリシーに高度な機能を追加できます。ビジュアルエディタは、@@assign 値設定演算子のみを使用し、子制御演算子へのアクセスは提供しません。子制御演算子は、JSON ポリシーテキストを手動で編集した場合にのみ追加できます。

タグポリシーを作成するには

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 (非推奨) としてサインインする必要があります。
2. タグポリシーページで、[Create policy] (ポリシーの作成) を選択します。
3. [Create policy] (ポリシーの作成) ページで、ポリシー名と、オプションでポリシーの説明を入力します。
4. (オプション) ポリシーオブジェクト自体には 1 つ以上のタグを追加できます。これらのタグはポリシーの一部ではありません。これを行うには、[Add tag] (タグの追加) を選択してから、キーとオプションの値を入力します。値を空白のままにすると、空の文字列が設定され、null にはなりません。1 つのポリシーに最大 50 個のタグをアタッチできます。詳細については、「AWS Organizations リソースのタグ付け」を参照してください。

5. この手順で説明するように、ビジュアルエディタを使用してタグポリシーを構築できます。[JSON] タブでタグポリシーを入力またはペーストすることもできます。タグポリシーの構文については、タグポリシー構文 を参照してください。

   ビジュアルエディタを使用する場合は、以下を指定します。

6. [New tag key 1] (新しいタグキー 1) で、追加するタグキーの名前を指定します。

7. [コンプライアンスオプション] では、次のオプションを選択できます。

   a. [タグキーには、上記で指定したの大文字と小文字の表記を使用する] – このオプションをオフ (デフォルト) のままにすると、継承された親タグポリシーが存在する場合、タグキーの大文字と小文字の処理を定義するように指定します。

   このポリシーを使用してタグキーの大文字と小文字を区別する場合は、このオプションを有効にします。このオプションを選択すると、[タグキー] に指定した大文字と小文字は、継承された親ポリシーで指定された大文字と小文字の処理より優先されます。

   親ポリシーが存在せず、このオプションを有効にしない場合、タグキーがすべて小文字のものだけが準拠していると見なされます。親ポリシーからの継承の詳細については、「管理ポリシーの継承を理解する」を参照してください。

   > **Tip**
   >
   > タグキーとその大文字小文字の処理を定義するタグポリシーを作成する際のガイドとして、「例 1: 組織全体のタグキーの大文字小文字取り扱いの定義」に示すタグポリシーの例を使用することを検討してください。組織のルートにアタッチします。後で追加のタグポリシーを作成し、OU またはアカウントにアタッチして、追加のタグ付けルールを作成できます。

   b. [このタグの許可された値を指定する] で、このタグキーに許可される値を親ポリシーから継承された値に追加する場合は、このオプションを有効にします。

   デフォルトでは、このオプションはオフになっています。つまり、親ポリシーで定義され、親ポリシーから継承された値だけが準拠していると見なされます。親ポリシーが存在しない場合、またはタグ値を指定しない場合、すべての値 (値なしの場合を含む) が準拠していると見なされます。

   受け入れ可能なタグ値のリストを更新するには、[Specify allowed values for this tag key] (このタグキーに許可される値を指定する) を選択し、[Specify values] (値を指定) を選択し

ます。プロンプトが表示されたら、新しい値を入力し (ボックスごとに 1 つの値)、[Save changes] (変更の保存) を選択します。

8. を [強制するリソースタイプ] では、[このタグの非準拠オペレーションの防止] を選択できます。

   タグポリシーの使用経験がない場合は、このオプションをオフ (デフォルト) のままにしておくことをお勧めします。「強制について」の推奨事項を確認し、完全なテストを実施してください。そうしないと、組織のアカウントのユーザーが必要なリソースにタグ付けできなくなる可能性があります。

   このタグキーへの準拠を強制する場合は、チェックボックスをオンにしてから [Specify resource types] (リソースタイプを指定) を選択します。プロンプトが表示されたら、ポリシーに含めるリソースタイプを選択します。次に、変更の保存を選択します。

   > **Important**
   >
   > このオプションを選択すると、指定したタイプのリソースのタグを操作するオペレーションは、そのオペレーションの結果としてポリシーに準拠するタグが得られた場合にのみ成功します。

9. (オプション) このタグポリシーに別のタグキーを追加するには、[Add tag key] を選択します。次に、ステップ 6 ~ 9 を実行してタグキーを定義します。
10. タグポリシーの構築が完了したら、[Save changes] (変更を保存) を選択します。

AWS CLI & AWS SDKs

タグポリシーを作成するには

次のいずれかを使用して、タグポリシーを作成できます。

- AWS CLI: create-policy

  タグポリシーの作成には任意のテキスト工ディタを使用できます。JSON 構文を使用し、タグポリシーを任意の名前と拡張子を持つファイルとして任意の場所に保存します。タグポリシーには、スペースを含めて最大 2,500 文字を使用できます。タグポリシーの構文については、タグポリシー構文 を参照してください。

タグポリシーを作成するには

1. 以下のようなタグポリシーのテキストファイルを作成します。

   testpolicy.json の内容:

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            }
        }
    }
}
```

   このタグポリシーは、CostCenter タグキーを定義します。タグは任意の値を受け入れることができますが、値を受け入れなくても構いません。このようなポリシーでは、値の有無にかかわらず CostCenter タグの付いているリソースを準拠しているとみなします。

2. ファイルにあるポリシーの内容を含むポリシーを作成します。出力が読みやすくなるように、余分な余白は切り詰められています。

```
$ aws organizations create-policy \
    --name "MyTestTagPolicy" \
    --description "My Test policy" \
    --content file://testpolicy.json \
    --type TAG_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-a1b2c3d4e5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-a1b2c3d4e5",
            "Name": "MyTestTagPolicy",
            "Description": "My Test policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign
\":\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
```

```
}
```

- AWS SDKs: CreatePolicy

チャットアプリケーションポリシーを作成する

> **最小アクセス許可**
>
> チャットアプリケーションポリシーを作成するには、次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。
>
> - `organizations:CreatePolicy`

AWS Management Console

チャットアプリケーションポリシーは、次の 2 つの方法のいずれか AWS Management Console で で作成できます。

- オプションを選択し、JSON ポリシーテキストを生成できるビジュアルエディタ。
- JSON ポリシーテキストを直接作成できるテキストエディタ。

ビジュアルエディタを使用すると、プロセスが簡単になりますが、柔軟性は制限されます。これは、最初のポリシーを作成し、使用に慣れるのに最適な方法です。これらの機能の仕組みを理解し、ビジュアルエディタが提供するものによって制限され始めたら、JSON ポリシーテキストを自分で編集して、ポリシーに高度な機能を追加できます。ビジュアルエディタは、@@assign 値設定演算子のみを使用し、子制御演算子へのアクセスは提供しません。子制御演算子は、JSON ポリシーテキストを手動で編集した場合にのみ追加できます。

チャットアプリケーションポリシーを作成するには

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 (非推奨) としてサインインする必要があります。
2. チャットボットポリシーページで、[ポリシーの作成] を選択します。
3. 新しいチャットアプリケーションポリシーの作成ページで、ポリシー名とオプションのポリシーの説明を入力します。

4. (オプション) [Add tag] (タグの追加) を選択してキーとオプションの値を入力することで、ポリシーに 1 つ以上のタグを追加できます。値を空白のままにすると、空の文字列が設定され、null にはなりません。1 つのポリシーに最大 50 個のタグをアタッチできます。詳細については、「AWS Organizations リソースのタグ付け」を参照してください。
5. この手順で説明するように、[ビジュアルエディタ] を使用してポリシーを構築できます。また、[JSON] タブにポリシーテキストを入力または貼り付けることもできます。チャットアプリケーションポリシー構文の詳細については、「」を参照してくださいチャットアプリケーションポリシーの構文と例。

   ビジュアルエディタを使用する場合は、チャットクライアントのアクセスコントロールを指定して、チャットアプリケーションポリシーを設定します。

   a. Amazon Chime チャットクライアントアクセスを設定するには、次のいずれかを選択します。
      - Chime へのアクセスを拒否します。
      - Chime へのアクセスを許可します。

   b. Microsoft Teams チャットクライアントアクセスを設定するには、以下を選択します。
      - すべての Teams へのアクセスを拒否する
      - すべての Teams へのアクセスを許可する
      - 名前付き Teams へのアクセスを制限する

   c. Slack チャットクライアントアクセスを設定するには、次のいずれかを選択します。
      - すべての Slack ワークスペースへのアクセスを拒否する
      - すべての Slack ワークスペースへのアクセスを許可する
      - 名前付き Slack ワークパスへのアクセスを制限する

      > **Note**
      >
      > さらに、チャットアプリケーションの Amazon Q Developer の使用をプライベート Slack チャネルのみに制限することもできます。

   d. IAM アクセス許可タイプを設定するには、次のオプションを選択します。
      - [チャネルレベルの IAM ロールを有効にする] – すべてのチャネルメンバーは、チャネルでタスクを実行するための IAM ロールのアクセス許可を共有します。チャネルメンバーが同じアクセス許可を必要とする場合、チャネルロールが適切です。

- [ユーザーレベルの IAM ロールを有効にする] – チャネルメンバーはアクションを実行するために IAM ユーザーロールを選択する必要があります (ロールを選択するにはコンソールへのアクセスが必要です)。チャネルメンバーが異なるアクセス許可を必要とし、ユーザーロールを選択できる場合、ユーザーロールは適切です。

6. ポリシーの作成が完了したら、[Create policy] (ポリシーの作成) を選択します。チャットボットバックアップポリシーのリストにポリシーが表示されます。

AWS CLI & AWS SDKs

チャットアプリケーションポリシーを作成するには

次のいずれかを使用して、チャットアプリケーションポリシーを作成できます。

- AWS CLI: create-policy

  任意のテキストエディタを使用して、チャットアプリケーションポリシーを作成できます。JSON 構文を使用して、チャットアプリケーションポリシーを任意の名前と拡張子を持つファイルとして任意の場所に保存します。チャットアプリケーションポリシーには、スペースを含め、最大？文字を使用できます。タグポリシーの構文については、チャットアプリケーションポリシーの構文と例 を参照してください。

  チャットアプリケーションポリシーを作成するには

  1. 次のようなテキストファイルにチャットアプリケーションポリシーを作成します。

     testpolicy.json の内容:

```
{
   "chatbot": {
      "platforms": {
         "slack": {
            "client": {
               "@@assign": "enabled"
            },
            "workspaces": {
               "@@assign": [
                  "Slack-Workspace-Id"
               ]
            },
            "default": {
               "supported_channel_types": {
```

```
                  "@@assign": [
                     "private"
                  ]
               }
            }
         },
         "microsoft_teams": {
            "client": {
               "@@assign": "disabled"
            }
         }
      }
   }
}
```

このチャットアプリケーションポリシーでは、特定のワークスペースのプライベート Slack チャネルのみを許可し、Microsoft Teams を無効にして、すべての[ロール設定](#)をサポートします。

2. ファイルにあるポリシーの内容を含むポリシーを作成します。出力が読みやすくなるように、余分な余白は切り詰められています。

```
$ aws organizations create-policy \
    --name "MyTestChatbotPolicy" \
    --description "My Test policy" \
    --content file://testpolicy.json \
    --type CHATBOT_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-a1b2c3d4e5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
chatbot_policy/p-a1b2c3d4e5",
            "Name": "MyTestChatApplicationsPolicy",
            "Description": "My Test policy",
            "Type": "CHATBOT_POLICY",
            "AwsManaged": false
        },
        "Content": "{"chatbot":{"platforms":{"slack":{"client":
{"@@assign":"enabled"},"workspaces":{"@@assign":["Slack-Workspace-
Id"]},"supported_channel_types":{"@@assign":["private"]}},"microsoft_teams":
{"client":{"@@assign":"disabled"}}}}}"
    }
```

```
}
```

- AWS SDKs: CreatePolicy

AI サービスのオプトアウトポリシーを作成する

> **最小アクセス許可**
>
> AI サービスのオプトアウトポリシーを作成するには、次のアクションを実行するアクセス許可が必要です。
>
> - `organizations:CreatePolicy`

AWS Management Console

AI サービスのオプトアウトポリシーを作成するには

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 (非推奨) としてサインインする必要があります。
2. AI サービスのオプトアウトポリシーページで、[Create policy] (ポリシーの作成) を選択します。
3. [Create new AI services opt-out policy] (新しい AI サービスのオプトアウトポリシーの作成) ページで、ポリシー名とポリシーの説明を入力します。
4. (オプション) [Add tag] (タグの追加) を選択してキーとオプションの値を入力することで、ポリシーに 1 つ以上のタグを追加できます。値を空白のままにすると、空の文字列が設定され、null にはなりません。1 つのポリシーに最大 50 個のタグをアタッチできます。詳細については、「AWS Organizations リソースのタグ付け」を参照してください。
5. [JSON] タブで、ポリシーテキストを入力するか貼り付けます。AI サービスのオプトアウトポリシーの構文について詳しくは、AI サービスのオプトアウトポリシーの構文と例 を参照してください。開始点として使用できるサンプルポリシーについては、AI サービスのオプトアウトポリシーの例 を参照してください。
6. ポリシーの編集が完了したら、ページの右下隅の [Create policy] (ポリシーの作成) を選択します。

AWS CLI & AWS SDKs

AI サービスのオプトアウトポリシーを作成するには

次のいずれかを使用して、タグポリシーを作成できます。

- AWS CLI: create-policy

1. 次のような AI サービスのオプトアウトポリシーを作成し、テキストファイルとして保存します。「optOut」と「optIn」では大文字と小文字が区別されます。

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

この AI サービスのオプトアウトポリシーは、ポリシーの影響を受けるすべてのアカウントが、Amazon Rekognition を除くすべての AI サービスからオプトアウトされるように指定します。

2. JSON ポリシーファイルをインポートして、組織内に新しいポリシーを作成します。この例では、先に扱った JSON ファイルは policy.json という名前になっています。

```
$ aws organizations create-policy \
    --type AISERVICES_OPT_OUT_POLICY \
    --name "MyTestPolicy" \
    --description "My test policy" \
    --content file://policy.json
{
    "Policy": {
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":{\"@@assign
\":\"optOut\"}},\"rekognition\":{\"opt_out_policy\":{\"@@assign\":\"optIn
\"}}}}",
```

```
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5"
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Description": "My test policy",
            "Name": "MyTestPolicy",
            "Type": "AISERVICES_OPT_OUT_POLICY"
        }
    }
}
```

- AWS SDKs: CreatePolicy

Security Hub ポリシーを作成する

最小アクセス許可

Security Hub ポリシーを作成するには、次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。

- `organizations:CreatePolicy`

AWS Management Console

Security Hub ポリシーを作成するには

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 (非推奨) としてサインインする必要があります。
2. Security Hub ポリシーページで、ポリシーの作成を選択します。
3. 新しい Security Hub ポリシーの作成ページで、ポリシー名とオプションのポリシーの説明を入力します。
4. (オプション) [Add tag] (タグの追加) を選択してキーとオプションの値を入力することで、ポリシーに 1 つ以上のタグを追加できます。値を空白のままにすると、空の文字列が設定され、null にはなりません。1 つのポリシーに最大 50 個のタグをアタッチできます。詳細については、「AWS Organizations リソースのタグ付け」を参照してください。
5. JSON コードボックスにポリシーテキストを入力または貼り付けます。Security Hub ポリシー構文の詳細については、「」を参照してくださいSecurity Hub ポリシーの構文と例。開

始点として使用できるサンプルポリシーについては、Security Hub ポリシーの例 を参照してください。

6. ポリシーの編集が完了したら、ページの右下隅の [Create policy] (ポリシーの作成) を選択します。

AWS CLI & AWS SDKs

Security Hub ポリシーを作成するには

Security Hub ポリシーを作成するには、次のいずれかを使用します。

- AWS CLI: create-policy

  例: サポートされているすべてのリージョンで Security Hub を有効にするポリシーを作成する

  次の例は、JSON ポリシーのテキストを含む `testPolicy_enableAllSupportedRegions.json` いう名前のファイルがあることを前提としたものです。このファイルを使用して、新しい Security Hub ポリシーを作成します。

```
$ aws organizations create-policy \
    --content file://./testPolicy_enableAllSupportedRegions.json \
    --name "testPolicy_enableAllSupportedRegions" \
    --description "Test policy to enable securityhub in ALL_SUPPORTED Regions" \
    --type SECURITYHUB_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-66ev7hgcvj",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
securityhub_policy/p-66ev7hgcvj",
            "Name": "testPolicy_enableAllSupportedRegions",
            "Description": "Test policy to enable securityhub in ALL_SUPPORTED
 Regions",
            "Type": "SECURITYHUB_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":
 {\n      \"@@assign\":[\n        \"ALL_SUPPORTED\"\n      ]\n    },\n
 \"disable_in_regions\": {\n      \"@@assign\":[]\n    }\n  }\n}\n"
    }
}
```

例: サポートされているすべてのリージョンで Security Hub を有効にし、us-east-1 リージョンで無効にするポリシーを作成する

次の例は、JSON ポリシーのテキストを含む `testPolicy_enableAllSupportedRegions_Disable_us-east-1.json` いう名前のファイルがあることを前提としたものです。このファイルを使用して、新しい Security Hub ポリシーを作成します。

```
$ aws organizations create-policy \
    --content file://./testPolicy_enableAllSupportedRegions_Disable_us-east-1.json
 \
    --name "testPolicy_enableAllSupportedRegions_Disable_us-east-1" \
    --description "Test policy to enable securityhub in ALL_SUPPORTED Regions but
 disable in us-east-1 Region" \
    --type SECURITYHUB_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-66217dwpos",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
securityhub_policy/p-66217dwpos",
            "Name": "testPolicy_enableAllSupportedRegions_Disable_us-east-1",
            "Description": "Test policy to enable securityhub in ALL_SUPPORTED
 Regions but disable in us-east-1 Region",
            "Type": "SECURITYHUB_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":
 {\n      \"@@assign\":[\n        \"ALL_SUPPORTED\"\n      ]\n    },\n
 \"disable_in_regions\": {\n      \"@@assign\":[\n        \"us-east-1\"\n      ]\n
    }\n  }\n}\n"
    }
}
```

- AWS SDKs: CreatePolicy

を使用した組織ポリシーの更新 AWS Organizations

ポリシーの要件が変更された場合は、既存のポリシーを更新できます。

このトピックでは、 を使用してポリシーを更新する方法について説明します AWS Organizations。ポリシーは、グループに適用するコントロールを定義します AWS アカウント。

トピック

- サービスコントロールポリシー (SCP) を更新する
- リソースコントロールポリシー (RCP) を更新する
- 宣言ポリシーを更新する
- バックアップポリシーを更新する
- タグポリシーを更新する
- チャットアプリケーションポリシーを更新する
- AI サービスのオプトアウトポリシーを更新する
- Security Hub ポリシーを更新する

サービスコントロールポリシー (SCP) を更新する

組織の管理アカウントにサインインすると、ポリシーの名前または内容を変更することができます。SCP の内容を変更すると、すぐにアタッチされているすべてのアカウントの任意のユーザー、グループ、およびロールに影響します。

> **最小アクセス許可**
>
> SCP を更新するには、次のアクションを実行する権限が必要です。
>
> - 指定されたポリシー (または "*") の ARN を含む同じポリシーステートメントの `Resource` 要素を持つ `organizations:UpdatePolicy`。
> - 指定されたポリシー (または "*") の ARN を含む同じポリシーステートメントの `Resource` 要素を持つ `organizations:DescribePolicy`。

AWS Management Console

ポリシーを更新するには

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

2. サービスコントロールポリシーページで、更新するポリシーの名前を選択します。
3. ポリシーの詳細ページで、[Edit policy] (ポリシーの編集) を選択します。
4. 次の変更のいずれか、またはすべてを行います。

   - ポリシーの名前を変更するには、[Policy name] (ポリシー名) に新しい名前を入力します。
   - 説明を変更するには、[Policy description] (ポリシーの説明) に新しいテキストを入力します。
   - 左側のペインでポリシーを JSON 形式で編集すると、ポリシーテキストを編集できます。または、右側のエディタでステートメントを選択し、コントロールを使用して要素を変更することもできます。各コントロールの詳細については、このトピックで前述した SCP の作成手順を参照してください。
5. 完了したら、[変更の保存] を選択します。

AWS CLI & AWS SDKs

ポリシーを更新するには

ポリシーを更新するには、以下のいずれかのコマンドを使用します。

- AWS CLI: update-policy

  次の例では、ポリシーの名前を変更します。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "MyRenamedPolicy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "Blocks all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
```

```
}
```

次の例では、サービスコントロールポリシーの説明を追加または変更します。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

次の例では、新しい JSON ポリシーテキストを含むファイルを指定して、SCP のポリシードキュメントを変更します。

```
$ aws organizations update-policy \
    --policy-id p-zlfw1r64
    --content file://MyNewPolicyText.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
```

```
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AModifiedPolicy\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*
\"]}]}"
    }
}
```

- AWS SDKs: UpdatePolicy

リソースコントロールポリシー (RCP) を更新する

組織の管理アカウントにサインインすると、ポリシーの名前または内容を変更することができます。RCP の内容を変更すると、アタッチされたすべてのアカウントのリソースに直ちに影響します。

最小アクセス許可

RCP を更新するには、次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。

- 指定されたポリシー (または "*") の ARN を含む同じポリシーステートメントの `Resource` 要素を持つ `organizations:UpdatePolicy`。
- 指定されたポリシー (または "*") の ARN を含む同じポリシーステートメントの `Resource` 要素を持つ `organizations:DescribePolicy`。

AWS Management Console

ポリシーを更新するには

1. AWS Organizations コンソールにサインインします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザー (非推奨) としてサインインする必要があります。
2. リソースコントロールポリシーページで、更新するポリシーの名前を選択します。
3. ポリシーの詳細ページで、[Edit policy] (ポリシーの編集) を選択します。
4. 次の変更のいずれか、またはすべてを行います。
   - ポリシーの名前を変更するには、[Policy name] (ポリシー名) に新しい名前を入力します。
   - 説明を変更するには、[Policy description] (ポリシーの説明) に新しいテキストを入力します。

- 左側のペインでポリシーを JSON 形式で編集すると、ポリシーテキストを編集できます。または、右側のエディタでステートメントを選択し、コントロールを使用して要素を変更することもできます。各コントロールの詳細については、このトピックの前半の「RCP の作成」の手順を参照してください。

5. 完了したら、[変更の保存] を選択します。

AWS CLI & AWS SDKs

ポリシーを更新するには

ポリシーを更新するには、以下のいずれかのコマンドを使用します。

- AWS CLI: update-policy

次の例では、ポリシーの名前を変更します。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "MyRenamedPolicy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "Blocks all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

次の例では、リソースコントロールポリシーの説明を追加または変更します。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new policy description"
{
```

```
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

次の例では、新しい JSON ポリシーテキストを含むファイルを指定して RCP のポリシードキュメントを変更します。

```
$ aws organizations update-policy \
    --policy-id p-zlfw1r64
    --content file://MyNewPolicyText.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AModifiedPolicy\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*
\"]}]}"
    }
}
```

- AWS SDKs: UpdatePolicy

宣言ポリシーを更新する

最小アクセス許可

宣言ポリシーを更新するには、次のアクションを実行するアクセス許可が必要です。

- 指定されたポリシー (または "*") の ARN を含む同じポリシーステートメントの `Resource` 要素を持つ `organizations:UpdatePolicy`。
- 指定したポリシー (または "*") の Amazon リソースネーム (ARN) を含む同じポリシーステートメントの `Resource` 要素を持つ `organizations:DescribePolicy`。

AWS Management Console

宣言ポリシーを更新するには

1. AWS Organizations コンソールにサインインします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザー (非推奨) としてサインインする必要があります。
2. 宣言ポリシーページで、更新するポリシーの名前を選択します。
3. ポリシーの詳細ページで、[Edit policy] (ポリシーの編集) を選択します。
4. 新しいポリシー名とポリシーの説明を入力するか、JSON ポリシーテキストを編集します。宣言ポリシー構文の詳細については、「」を参照してください宣言型ポリシーの構文と例。
5. ポリシーの更新が完了したら、[変更を保存] を選択します。

AWS CLI & AWS SDKs

ポリシーを更新するには

次のいずれかを使用して、ポリシーを更新できます。

- AWS CLI: update-policy

  次の の例では、宣言ポリシーの名前を変更します。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
```

```
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
declarative_policy_ec2/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "DECLARATIVE_POLICY_EC2",
            "AwsManaged": false
        },
        "Content": "{"ec2-configuration":{"ec2_attributes":
{"image_block_public_access":{"state":{"@@assign":"block_new_sharing"}}}}".
    }
}
```

次の例では、宣言ポリシーの説明を追加または変更します。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
declarative_policy_ec2/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "DECLARATIVE_POLICY_EC2",
            "AwsManaged": false
        },
        "Content": "{"ec2_attributes":{"image_block_public_access":{"state":
{"@@assign":"block_new_sharing"}}}}".
    }
}
```

- AWS SDKs: UpdatePolicy

バックアップポリシーを更新する

組織の管理アカウントにサインインすると、組織内で変更が必要なポリシーを編集できます。

最小アクセス許可

バックアップポリシーを更新するには、次のアクションを実行するアクセス許可が必要です。

- 更新するポリシー (または "*") の ARN を含む同じポリシーステートメントの Resource 要素を持つ organizations:UpdatePolicy。
- 更新するポリシー (または "*") の ARN を含む同じポリシーステートメントの Resource 要素を持つ organizations:DescribePolicy。

AWS Management Console

バックアップポリシーを更新するには

1. AWS Organizations コンソールにサインインします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザー (非推奨) としてサインインする必要があります。
2. バックアップポリシーページで、更新するポリシーの名前を選択します。
3. [ポリシーの編集] を選択します。
4. 新しいポリシー名とポリシーの説明を入力できます。ポリシーの内容を変更するには、[Visual editor] (ビジュアルエディタ) を使用するか、直接 JSON を編集します。
5. ポリシーの更新が完了したら、[変更を保存] を選択します。

AWS CLI & AWS SDKs

バックアップポリシーを更新するには

次のいずれかを使用して、バックアップポリシーを更新できます。

- AWS CLI: update-policy

  次の例では、バックアップポリシーの名前を変更しています。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
```

```
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

次の例では、バックアップポリシーの説明を追加、変更しています。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
       "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

次の例では、バックアップポリシーにアタッチされた JSON ポリシードキュメントを変更しています。この例では、次のようなテキストを含む policy.json というファイルから、内容が取得されています。

```
{
    "plans": {
        "PII_Backup_Plan": {
```

```
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" },
                        "opt_in_to_archive_for_supported_resources": {"@@assign":
 false}
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" },
                                "opt_in_to_archive_for_supported_resources":
 {"@@assign": false}
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII" ] }
                    }
                }
            }
        }
    }
}
```

```
$ aws organizations update-policy \
```

```
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
}
```

- AWS SDKs: UpdatePolicy

タグポリシーを更新する

> **最小アクセス許可**
>
> タグポリシーを更新するには、次のアクションを実行する権限が必要です。
>
> - 指定されたポリシー (または "*") の ARN を含む同じポリシーステートメントの Resource 要素を持つ organizations:UpdatePolicy。
> - 指定されたポリシー (または "*") の ARN を含む同じポリシーステートメントの Resource 要素を持つ organizations:DescribePolicy。

AWS Management Console

タグポリシーを更新するには

1. AWS Organizations コンソールにサインインします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザー (非推奨) としてサインインする必要があります。
2. [Tag policies] (タグポリシー) ページで、更新するタグポリシーを選択します。
3. [ポリシーの編集] を選択します。

4. 新しいポリシー名とポリシーの説明を入力できます。ポリシーの内容を変更するには、ビジュアルエディタを使用するか、JSON を編集します。
5. タグポリシーの更新が完了したら、[Save changes] (変更を保存) を選択します。

AWS CLI & AWS SDKs

ポリシーを更新するには

次のいずれかを使用して、ポリシーを更新できます。

- AWS CLI: update-policy

次の例では、タグポリシーの名前を変更します。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed tag policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

次の例では、タグポリシーの説明を追加または変更します。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new tag policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
```

```
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
       "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

次の例では、AI サービスのオプトアウトポリシーにアタッチされた JSON ポリシードキュメントを変更しています。この例では、次のようなテキストを含む policy.json というファイルから、内容が取得されています。

```
{
  "tags": {
    "Stage": {
      "tag_key": {
        "@@assign": "Stage"
      },
      "tag_value": {
        "@@assign": [
          "Production",
          "Test"
        ]
      }
    }
  }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
```

```
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"tags\":{\"Stage\":{\"tag_key\":{\"@@assign\":\"Stage
\"},\"tag_value\":{\"@@assign\":[\"Production\",\"Test\"]},\"enforced_for\":
{\"@@assign\":[\"ec2:instance\"]}}}}"
}
```

- AWS SDKs: UpdatePolicy

チャットアプリケーションポリシーを更新する

最小アクセス許可

チャットアプリケーションポリシーを更新するには、次のアクションを実行するアクセス許可が必要です。

- 指定されたポリシー (または "*") の ARN を含む同じポリシーステートメントの Resource 要素を持つ organizations:UpdatePolicy。
- 指定されたポリシー (または "*") の ARN を含む同じポリシーステートメントの Resource 要素を持つ organizations:DescribePolicy。

AWS Management Console

チャットアプリケーションポリシーを更新するには

1. AWS Organizations コンソールにサインインします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザー (非推奨) としてサインインする必要があります。
2. Chatbot ポリシーページで、更新するチャットアプリケーションポリシーを選択します。
3. [ポリシーの編集] を選択します。
4. 新しいポリシー名とポリシーの説明を入力できます。ポリシーの内容を変更するには、ビジュアルエディタを使用するか、JSON を編集します。
5. タグポリシーの更新が完了したら、[Save changes] (変更を保存) を選択します。

AWS CLI & AWS SDKs

ポリシーを更新するには

次のいずれかを使用して、ポリシーを更新できます。

- AWS CLI: update-policy

  次の の例では、チャットアプリケーションポリシーの名前を変更します。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed chat applications policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
chatbot_policy/p-i9j8k7l6m5",
            "Name": "Renamed chat applications policy",
            "Type": "CHATBOT_POLICY",
            "AwsManaged": false
        },
        "Content": "{"chatbot":{"platforms":{"slack":{"client":
{"@@assign":"enabled"},"workspaces":{"@@assign":["Slack-Workspace-Id"]},"default":
{"supported_channel_types":{"@@assign":["private"]}}},"microsoft_teams":{"client":
{"@@assign":"disabled"}}}}}"
    }
}
```

- AWS SDKs: UpdatePolicy

AI サービスのオプトアウトポリシーを更新する

最小アクセス許可

AI サービスのオプトアウトポリシーを更新するには、次のアクションを実行するアクセス許可が必要です。

- 指定されたポリシー (または "*") の ARN を含む同じポリシーステートメントの Resource 要素を持つ organizations:UpdatePolicy。

- 指定したポリシー (または "*") の Amazon リソースネーム (ARN) を含む同じポリシーステートメントの `Resource` 要素を持つ `organizations:DescribePolicy`。

AWS Management Console

AI サービスのオプトアウトポリシーを更新するには

1. AWS Organizations コンソールにサインインします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザー (非推奨) としてサインインする必要があります。
2. AI サービスのオプトアウトポリシーページで、更新するポリシーの名前を選択します。
3. ポリシーの詳細ページで、[Edit policy] (ポリシーの編集) を選択します。
4. 新しいポリシー名とポリシーの説明を入力するか、JSON ポリシーテキストを編集します。AI サービスのオプトアウトポリシーの構文について詳しくは、AI サービスのオプトアウトポリシーの構文と例 を参照してください。開始点として使用できるサンプルポリシーについては、AI サービスのオプトアウトポリシーの例 を参照してください。
5. ポリシーの更新が完了したら、[変更を保存] を選択します。

AWS CLI & AWS SDKs

ポリシーを更新するには

次のいずれかを使用して、ポリシーを更新できます。

- AWS CLI: update-policy

  次の例では、AI サービスのオプトアウトポリシーの名前を変更しています。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
```

```
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

次の例では、AI サービスのオプトアウトポリシーの説明を追加、変更しています。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

次の例では、AI サービスのオプトアウトポリシーにアタッチされた JSON ポリシードキュメントを変更しています。この例では、次のようなテキストを含む policy.json というファイルから、内容が取得されています。

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
```

```
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
         "Content": "{\n\"services\": {\n\"default\": {\n\"   ....TRUNCATED FOR
 BREVITY....    ": \"optIn\"\n}\n}\n}\n}\n"}
}
```

- AWS SDKs: UpdatePolicy

Security Hub ポリシーを更新する

最小アクセス許可

Security Hub ポリシーを更新するには、次のアクションを実行するアクセス許可が必要です。

- 指定されたポリシー (または "*") の ARN を含む同じポリシーステートメントの `Resource` 要素を持つ `organizations:UpdatePolicy`。

- 指定したポリシー (または "*") の Amazon リソースネーム (ARN) を含む同じポリシーステートメントの `Resource` 要素を持つ `organizations:DescribePolicy`。

AWS Management Console

Security Hub ポリシーを更新するには

1. AWS Organizations コンソールにサインインします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザー (非推奨) としてサインインする必要があります。
2. Security Hub ポリシーページで、更新するポリシーの名前を選択します。
3. ポリシーの詳細ページで、[Edit policy] (ポリシーの編集) を選択します。
4. 新しいポリシー名とポリシーの説明を入力するか、JSON ポリシーテキストを編集します。Security Hub ポリシー構文の詳細については、「」を参照してくださいSecurity Hub ポリシーの構文と例。開始点として使用できるサンプルポリシーについては、Security Hub ポリシーの例 を参照してください。
5. ポリシーの更新が完了したら、[変更を保存] を選択します。

AWS CLI & AWS SDKs

ポリシーを更新するには

次のいずれかを使用して、ポリシーを更新できます。

- AWS CLI: update-policy

  次の の例では、Security Hub ポリシーの名前を変更します。

```
$ aws organizations update-policy \
    --policy-id p-66ev7hgcvj \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-66ev7hgcvj",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
securityhub_policy/p-66ev7hgcvj",
            "Name": "Renamed policy",
```

```
            "Type": "SECURITYHUB_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":
 {\n      \"@@assign\":[\n        \"ALL_SUPPORTED\"\n      ]\n    },\n
 \"disable_in_regions\": {\n      \"@@assign\":[]\n    }\n  }\n}\n"
    }
}
```

次の例では、Security Hub ポリシーの説明を追加または変更します。

```
$ aws organizations update-policy \
    --policy-id p-66ev7hgcvj \
    --name "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-66ev7hgcvj",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
securityhub_policy/p-66ev7hgcvj",
            "Name": "My new description",
            "Type": "SECURITYHUB_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":
 {\n      \"@@assign\":[\n        \"ALL_SUPPORTED\"\n      ]\n    },\n
 \"disable_in_regions\": {\n      \"@@assign\":[]\n    }\n  }\n}\n"
    }
}
```

- AWS SDKs: UpdatePolicy

AWS Organizationsを使用して組織ポリシーにアタッチされたタグを編集する

このトピックでは、タグがアタッチされたポリシーを編集する方法について説明します AWS Organizations。ポリシーは、 のグループに適用するコントロールを定義します AWS アカウント。

トピック

- サービスコントロールポリシー (SCP) にアタッチされたタグを編集する

- リソースコントロールポリシー (RCP) にアタッチされたタグを編集する
- 宣言ポリシーにアタッチされたタグを編集する
- バックアップポリシーにアタッチされたタグを編集する
- タグポリシーにアタッチされたタグを編集する
- チャットアプリケーションポリシーにアタッチされたタグを編集する
- AI サービスのオプトアウトポリシーにアタッチされたタグを編集する
- Security Hub ポリシーにアタッチされたタグを編集する

サービスコントロールポリシー (SCP) にアタッチされたタグを編集する

組織の管理アカウントにサインインすると、SCP にアタッチされるタグを追加または削除できます。タグ付けの詳細については、「AWS Organizations リソースのタグ付け」を参照してください。

> **最小アクセス許可**
>
> 組織の SCP にアタッチされたタグを編集するには、以下のアクセス許可が必要です。
>
> - `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要
> - `organizations:DescribePolicy` - Organizations コンソールを使用する場合にのみ必要
> - `organizations:TagResource`
> - `organizations:UntagResource`

AWS Management Console

SCP にアタッチされたタグを編集するには

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 (非推奨) としてサインインする必要があります。
2. サービスコントロールポリシーページで、編集するタグがアタッチされたポリシーの名前を選択します。
3. ポリシーの詳細ページで、[Tags] (タグ) タブ、[Manage tags] (タグ管理) の順に選択します。

4. 次の変更のいずれか、またはすべてを行います。

   - 古い値を新しい値で上書きして、タグの値を変更します。タグキーを直接変更することはできません。キーを変更するには、古いキーを持つタグを削除してから、新しいキーを持つタグを追加する必要があります。
   - [Remove] (削除) を選択すると、既存のタグが削除されます。
   - 新しいタグのキーと値のペアを追加します。[Add tag] (タグの追加) を選択し、表示されたボックスに新しいキー名とオプションの値を入力します。[Value] (値) ボックスを空白のままにすると、値は空の文字列に設定され、`null` にはなりません。

5. 完了したら、[変更の保存] を選択します。

AWS CLI & AWS SDKs

SCP にアタッチされたタグを編集するには

SCP にアタッチされたタグを編集するには、次のいずれかのコマンドを使用します。

- AWS CLI: tag-resource および untag-resource
- AWS SDKs: TagResource と UntagResource

リソースコントロールポリシー (RCP) にアタッチされたタグを編集する

組織の管理アカウントにサインインすると、RCP にアタッチされたタグを追加または削除できます。タグ付けの詳細については、「AWS Organizations リソースのタグ付け」を参照してください。

> **最小アクセス許可**
>
> AWS 組織内の RCP にアタッチされたタグを編集するには、次のアクセス許可が必要です。
>
> - `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要
> - `organizations:DescribePolicy` - Organizations コンソールを使用する場合にのみ必要
> - `organizations:TagResource`
> - `organizations:UntagResource`

AWS Management Console

RCP にアタッチされたタグを編集するには

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 (非推奨) としてサインインする必要があります。
2. リソースコントロールポリシーページで、編集するタグを含むポリシーの名前を選択します。
3. ポリシーの詳細ページで、タグタブを選択し、タグの管理を選択します。
4. 次の変更のいずれか、またはすべてを行います。
   - 古い値を新しい値で上書きして、タグの値を変更します。タグキーを直接変更することはできません。キーを変更するには、古いキーを持つタグを削除してから、新しいキーを持つタグを追加する必要があります。
   - [Remove] (削除) を選択すると、既存のタグが削除されます。
   - 新しいタグのキーと値のペアを追加します。[Add tag] (タグの追加) を選択し、表示されたボックスに新しいキー名とオプションの値を入力します。[Value] (値) ボックスを空白のままにすると、値は空の文字列に設定され、`null` にはなりません。
5. 完了したら、[変更の保存] を選択します。

AWS CLI & AWS SDKs

RCP にアタッチされたタグを編集するには

次のいずれかのコマンドを使用して、RCP にアタッチされたタグを編集できます。

- AWS CLI: tag-resource および untag-resource
- AWS SDKs: TagResource と UntagResource

宣言ポリシーにアタッチされたタグを編集する

組織の管理アカウントにサインインすると、宣言ポリシーにアタッチされたタグを追加または削除できます。タグ付けの詳細については、「AWS Organizations リソースのタグ付け」を参照してください。

最小アクセス許可

AWS 組織内の宣言ポリシーにアタッチされたタグを編集するには、次のアクセス許可が必要です。

- `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要
- `organizations:DescribePolicy` - Organizations コンソールを使用する場合にのみ必要
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

宣言ポリシーにアタッチされたタグを編集するには

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 (非推奨) としてサインインする必要があります。
2. 宣言ポリシーページで、編集するタグを含むポリシーの名前を選択します。
3. 選択したポリシーの詳細ページで、[Tags] (タグ) タブ、[Manage tags] (タグ管理) の順に選択します。
4. このページでは次のアクションを実行できます。
   - 古い値に上書きして新しい値を入力し、任意のタグの値を編集します。キーは変更できません。キーを変更するには、古いキーを持つタグを削除し、新しいキーを持つタグを追加する必要があります。
   - [Remove] (削除) を選択すると、既存のタグが削除されます。
   - 新しいタグのキーと値のペアを追加します。[Add tag] (タグの追加) を選択し、表示されたボックスに新しいキー名とオプションの値を入力します。[Value] (値) ボックスを空白のままにすると、値は空の文字列に設定され、`null` にはなりません。
5. 必要な追加、削除、編集をすべて終えたら、[Save changes] (変更の保存) を選択します。

AWS CLI & AWS SDKs

宣言ポリシーにアタッチされたタグを編集するには

次のいずれかのコマンドを使用して、宣言ポリシーにアタッチされたタグを編集できます。

- AWS CLI: tag-resource および untag-resource
- AWS SDKs: TagResource と UntagResource

バックアップポリシーにアタッチされたタグを編集する

組織の管理アカウントにサインインすると、バックアップポリシーにアタッチされたタグの追加と削除を行うことができます。タグ付けの詳細については、「AWS Organizations リソースのタグ付け」を参照してください。

最小アクセス許可

組織のバックアップポリシーにアタッチされたタグを編集するには、次のアクセス許可が必要です。

- `organizations:DescribeOrganization` (コンソールのみ - ポリシーに移動するために使用)
- `organizations:DescribePolicy` (コンソールのみ - ポリシーに移動するために使用)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

バックアップポリシーにアタッチされたタグを編集するには

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 (非推奨) としてサインインする必要があります。
2. バックアップポリシーページ
3. 編集するタグを含むポリシーの名前を選択します。

   ポリシーの詳細ページが表示されます。

4. [Tags (タグ)] タブで、[Manage tags (タグ管理)] を選択します。
5. このページでは次のアクションを実行できます。

   - 古い値に上書きして新しい値を入力し、任意のタグの値を編集します。キーは変更できません。キーを変更するには、古いキーを持つタグを削除し、新しいキーを持つタグを追加する必要があります。
   - [Remove] (削除) を選択すると、既存のタグが削除されます。
   - 新しいタグのキーと値のペアを追加します。[Add tag] (タグの追加) を選択し、表示されたボックスに新しいキー名とオプションの値を入力します。[Value] (値) ボックスを空白のままにすると、値は空の文字列に設定され、null にはなりません。
6. 必要な追加、削除、編集をすべて終えたら、[Save changes] (変更の保存) を選択します。

AWS CLI & AWS SDKs

バックアップポリシーにアタッチされたタグを編集するには

バックアップポリシーにアタッチされたタグを編集するには、次のいずれかのコマンドを使用します。

- AWS CLI: tag-resource および untag-resource
- AWS SDKs: TagResource と UntagResource

タグポリシーにアタッチされたタグを編集する

組織の管理アカウントにサインインすると、タグポリシーにアタッチされたタグを追加または削除できます。そのためには、以下の手順を完了します。

最小アクセス許可

組織のタグポリシーにアタッチされたタグを編集するには、次のアクセス許可が必要です。

- `organizations:DescribeOrganization` (コンソールのみ - ポリシーに移動するために使用)
- `organizations:DescribePolicy` (コンソールのみ - ポリシーに移動するために使用)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

タグポリシーにアタッチされたタグを編集するには

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 (非推奨) としてサインインする必要があります。
2. [Tag policies] (タグポリシー) ページで、タグを編集するポリシーの名前を選択します。
3. 選択したポリシーの詳細ページで、[Tags] (タグ) タブ、[Manage tags] (タグ管理) の順に選択します。
4. このページでは次のアクションを実行できます。
   - 古い値に上書きして新しい値を入力し、任意のタグの値を編集します。キーは変更できません。キーを変更するには、古いキーを持つタグを削除し、新しいキーを持つタグを追加する必要があります。
   - [Remove] (削除) を選択すると、既存のタグが削除されます。
   - 新しいタグのキーと値のペアを追加します。[Add tag] (タグの追加) を選択し、表示されたボックスに新しいキー名とオプションの値を入力します。[Value] (値) ボックスを空白のままにすると、値は空の文字列に設定され、`null` にはなりません。
5. 必要な追加、削除、編集をすべて終えたら、[Save changes] (変更の保存) を選択します。

AWS CLI & AWS SDKs

タグポリシーにアタッチされたタグを編集するには

次のいずれかのコマンドを使用して、タグポリシーにアタッチされたタグを編集できます。

- AWS CLI: tag-resource および untag-resource
- AWS SDKs: TagResource と UntagResource

チャットアプリケーションポリシーにアタッチされたタグを編集する

組織の管理アカウントにサインインすると、チャットアプリケーションポリシーにアタッチされたタグを追加または削除できます。そのためには、以下の手順を完了します。

最小アクセス許可

組織内のチャットアプリケーションポリシーにアタッチされたタグを編集するには、次のアクセス許可が必要です。

- `organizations:DescribeOrganization` (コンソールのみ - ポリシーに移動するために使用)
- `organizations:DescribePolicy` (コンソールのみ - ポリシーに移動するために使用)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

チャットアプリケーションポリシーにアタッチされたタグを編集するには

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 (非推奨) としてサインインする必要があります。
2. [チャットボットポリシーページ] ページで、タグを編集するポリシーの名前を選択します。
3. 選択したポリシーの詳細ページで、[Tags] (タグ) タブ、[Manage tags] (タグ管理) の順に選択します。
4. このページでは次のアクションを実行できます。
   - 古い値に上書きして新しい値を入力し、任意のタグの値を編集します。キーは変更できません。キーを変更するには、古いキーを持つタグを削除し、新しいキーを持つタグを追加する必要があります。
   - [Remove] (削除) を選択すると、既存のタグが削除されます。
   - 新しいタグのキーと値のペアを追加します。[Add tag] (タグの追加) を選択し、表示されたボックスに新しいキー名とオプションの値を入力します。[Value] (値) ボックスを空白のままにすると、値は空の文字列に設定され、`null` にはなりません。
5. 必要な追加、削除、編集をすべて終えたら、[Save changes] (変更の保存) を選択します。

AWS CLI & AWS SDKs

チャットアプリケーションポリシーにアタッチされたタグを編集するには

次のいずれかのコマンドを使用して、チャットアプリケーションポリシーにアタッチされたタグを編集できます。

- AWS CLI: tag-resource および untag-resource
- AWS SDKs: TagResource と UntagResource

AI サービスのオプトアウトポリシーにアタッチされたタグを編集する

組織の管理アカウントにサインインすると、AI サービスのオプトアウトポリシーにアタッチされたタグの追加と削除を行うことができます。タグ付けの詳細については、「AWS Organizations リソースのタグ付け」を参照してください。

> **最小アクセス許可**
>
> 組織の AI サービスのオプトアウトポリシーにアタッチされたタグを編集するには、次のアクセス許可が必要です。
>
> - `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要
> - `organizations:DescribePolicy` - Organizations コンソールを使用する場合にのみ必要
> - `organizations:TagResource`
> - `organizations:UntagResource`

AWS Management Console

AI サービスのオプトアウトポリシーにアタッチされたタグを編集するには

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 (非推奨) としてサインインする必要があります。
2. AI サービスのオプトアウトポリシーページで、タグを編集するポリシーの名前を選択します。
3. 選択したポリシーの詳細ページで、[Tags] (タグ) タブ、[Manage tags] (タグ管理) の順に選択します。
4. このページでは次のアクションを実行できます。

- 古い値に上書きして新しい値を入力し、任意のタグの値を編集します。キーは変更できません。キーを変更するには、古いキーを持つタグを削除し、新しいキーを持つタグを追加する必要があります。
- [Remove] (削除) を選択すると、既存のタグが削除されます。
- 新しいタグのキーと値のペアを追加します。[Add tag] (タグの追加) を選択し、表示されたボックスに新しいキー名とオプションの値を入力します。[Value] (値) ボックスを空白のままにすると、値は空の文字列に設定され、`null` にはなりません。

5. 必要な追加、削除、編集をすべて終えたら、[Save changes] (変更の保存) を選択します。

AWS CLI & AWS SDKs

AI サービスのオプトアウトポリシーにアタッチされたタグを編集するには

AI サービスのオプトアウトポリシーにアタッチされたタグを編集するには、次のいずれかのコマンドを使用します。

- AWS CLI: tag-resource および untag-resource
- AWS SDKs: TagResource と UntagResource

Security Hub ポリシーにアタッチされたタグを編集する

組織の管理アカウントにサインインすると、Security Hub ポリシーにアタッチされたタグを追加または削除できます。タグ付けの詳細については、「AWS Organizations リソースのタグ付け」を参照してください。

最小アクセス許可

組織内の Security Hub ポリシーにアタッチされたタグを編集するには、次のアクセス許可が必要です。

- `organizations:DescribeOrganization` - Organizations コンソールを使用する場合にのみ必要
- `organizations:DescribePolicy` - Organizations コンソールを使用する場合にのみ必要
- `organizations:TagResource`

- `organizations:UntagResource`

AWS Management Console

Security Hub ポリシーにアタッチされたタグを編集するには

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 (非推奨) としてサインインする必要があります。
2. Security Hub ポリシーページで、編集するタグを含むポリシーの名前を選択します。
3. 選択したポリシーの詳細ページで、[Tags] (タグ) タブ、[Manage tags] (タグ管理) の順に選択します。
4. このページでは次のアクションを実行できます。
   - 古い値に上書きして新しい値を入力し、任意のタグの値を編集します。キーは変更できません。キーを変更するには、古いキーを持つタグを削除し、新しいキーを持つタグを追加する必要があります。
   - [Remove] (削除) を選択すると、既存のタグが削除されます。
   - 新しいタグのキーと値のペアを追加します。[Add tag] (タグの追加) を選択し、表示されたボックスに新しいキー名とオプションの値を入力します。[Value] (値) ボックスを空白のままにすると、値は空の文字列に設定され、`null` にはなりません。
5. 必要な追加、削除、編集をすべて終えたら、[Save changes] (変更の保存) を選択します。

AWS CLI & AWS SDKs

Security Hub ポリシーにアタッチされたタグを編集するには

次のいずれかのコマンドを使用して、Security Hub ポリシーにアタッチされたタグを編集できます。

- AWS CLI: tag-resource および untag-resource
- AWS SDKs: TagResource と UntagResource

での組織ポリシーのアタッチ AWS Organizations

このトピックでは、 AWS Organizationsでポリシーをアタッチする方法について説明します。ポリシーは、グループに適用するコントロールを定義します AWS アカウント。

トピック

- でポリシーをアタッチする AWS Organizations

でポリシーをアタッチする AWS Organizations

最小アクセス許可

ポリシーをアタッチするには、次のアクションを実行するアクセス認可が必要です。

- `organizations:AttachPolicy`

最小アクセス許可

ルート、OU、またはアカウントに認可ポリシー (SCP または RCP) をアタッチするには、次のアクションを実行するアクセス許可が必要です。

- 特定のポリシーの "*" または Amazon リソースネーム (ARN) を含む同じポリシーステートメントの `Resource` 要素を持つ `organizations:AttachPolicy`、およびポリシーをアタッチするルート、OU、またはアカウントの ARN。

AWS Management Console

Service control policies (SCPs)

SCP をアタッチするには、ポリシーをアタッチするルート、OU、またはアカウントに移動する必要があります。

ルート、OU、またはアカウントに移動して SCP をアタッチするには

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 (非推奨) としてサインインする必要があります。

2. AWS アカウント ページで、SCP をアタッチするルート、OU、または
アカウントの横にあるチェックボックスに移動してオンにします。場合
によっては、目的の OU またはアカウントを表示するため、OU を展開
(
を選択) する必要があります。
3. [Policies] (ポリシー) タブの [Service control policies] (サービスコントロールポリシー) で、[Attach] (アタッチ) を選択します。
4. 目的のポリシーを見つけて [Attach policy] (ポリシーのアタッチ) を選択します。

   [Policies] (ポリシー) タブで、アタッチされている SCP のリストが更新され、新たに追加したものが表示されます。ポリシーの変更はすぐに有効になり、アタッチされたアカウントや、アタッチされたルートまたは OU の下のすべてのアカウントの IAM ユーザーとロールのアクセス許可に影響します。

ポリシーに移動して SCP をアタッチするには

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 (非推奨) としてサインインする必要があります。
2. サービスコントロールポリシーページで、アタッチするポリシーの名前を選択します。
3. [Targets] (ターゲット) タブで [Attach] (アタッチ) を選択します。
4. ポリシーをアタッチするルート、OU、またはアカウントの横にあるラジオボタンをクリックします。場合によっては、目的の OU またはアカウントを表示するため、OU を展開
(
を選択) する必要があります。
5. Attach policy] (ポリシーのアタッチ) を選択してください。

   [Targets] (ターゲット) タブで、アタッチされている SCP のリストが更新され、新たに追加したものが表示されます。ポリシーの変更はすぐに有効になり、アタッチされたアカウントや、アタッチされたルートまたは OU の下のすべてのアカウントの IAM ユーザーとロールのアクセス許可に影響します。

Resource control policies (RCPs)

RCP をアタッチするには、ポリシーに移動するか、ポリシーをアタッチするルート、OU、またはアカウントに移動します。

ルート、OU、またはアカウントに移動して RCP をアタッチするには

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 (非推奨) としてサインインする必要があります。
2. AWS アカウント ページで、 に移動し、RCP をアタッチするルート、OU、またはアカウントの横にあるチェックボックスをオンにします。場合によっては、目的の OU またはアカウントを表示するため、OU を展開
(
を選択) する必要があります。
3. 「ポリシー」タブの「リソースコントロールポリシー」のエントリで、「アタッチ」を選択します。
4. 目的のポリシーを見つけて [Attach policy] (ポリシーのアタッチ) を選択します。

   ポリシータブのアタッチされた RCPs のリストが更新され、新しい追加が追加されました。ポリシーの変更はすぐに有効になり、アタッチされたアカウント、またはアタッチされたルートまたは OU 下にあるすべてのアカウントのリソースのアクセス許可に影響します。

ポリシーに移動して RCP をアタッチするには

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 (非推奨) としてサインインする必要があります。
2. リソースコントロールポリシーページで、アタッチするポリシーの名前を選択します。
3. [Targets] (ターゲット) タブで [Attach] (アタッチ) を選択します。
4. ポリシーをアタッチするルート、OU、またはアカウントの横にあるラジオボタンをクリックします。場合によっては、目的の OU またはアカウントを表示するため、OU を展開
(
を選択) する必要があります。
5. Attach policy] (ポリシーのアタッチ) を選択してください。

   Targets タブのアタッチされた RCPs のリストが更新され、新しい追加が追加されました。ポリシーの変更はすぐに有効になり、アタッチされたアカウント、またはアタッチされたルートまたは OU 下にあるすべてのアカウントのリソースのアクセス許可に影響します。

Declarative policies

宣言ポリシーをアタッチするには、ポリシーに移動するか、ポリシーをアタッチするルート、OU、またはアカウントに移動します。

ルート、OU、またはアカウントに移動して宣言ポリシーをアタッチするには

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 (非推奨) としてサインインする必要があります。
2. AWS アカウント ページで、ポリシーをアタッチするルート、OU、またはアカウントを見つけ、名前を選択します。場合によっては、目的の OU またはアカウントを表示するため、OU を展開
(
を選択) する必要があります。
3. ポリシータブの宣言ポリシーのエントリで、アタッチを選択します。
4. 目的のポリシーを見つけて [Attach policy] (ポリシーのアタッチ) を選択します。

   Policies タブにアタッチされた宣言ポリシーのリストが更新され、新しい追加が追加されました。ポリシーの変更はすぐに反映されます。

ポリシーに移動して宣言ポリシーをアタッチするには

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 (非推奨) としてサインインする必要があります。
2. 宣言ポリシーページで、アタッチするポリシーの名前を選択します。
3. [Targets] (ターゲット) タブで [Attach] (アタッチ) を選択します。
4. ポリシーをアタッチするルート、OU、またはアカウントの横にあるラジオボタンをクリックします。場合によっては、目的の OU またはアカウントを表示するため、OU を展開
(
を選択) する必要があります。
5. Attach policy] (ポリシーのアタッチ) を選択してください。

   ターゲットタブにアタッチされた宣言ポリシーのリストが更新され、新しい追加が追加されました。ポリシーの変更はすぐに反映されます。

Backup policies

バックアップポリシーのアタッチには、ポリシーに移動する方法と、ポリシーをアタッチするルート、OU、またはアカウントに移動する方法があります。

ルート、OU、またはアカウントに移動してバックアップポリシーをアタッチするには

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 (非推奨) としてサインインする必要があります。
2. AWS アカウント ページで、ポリシーをアタッチするルート、OU、またはアカウントを見つけ、名前を選択します。場合によっては、目的の OU またはアカウントを表示するため、OU を展開
(
を選択) する必要があります。
3. [Policies] (ポリシー) タブの [Backup policies] (バックアップポリシー) の項目で、[Attach] (アタッチ) を選択します。
4. 目的のポリシーを見つけて [Attach policy] (ポリシーのアタッチ) を選択します。

   [Policies] (ポリシー) タブで、アタッチされているバックアップポリシーの一覧が更新され、新たに追加したものが表示されます。ポリシーの変更はすぐに反映されます。

ポリシーに移動してバックアップポリシーをアタッチするには

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 (非推奨) としてサインインする必要があります。
2. バックアップポリシーページで、アタッチするポリシーの名前を選択します。
3. [Targets] (ターゲット) タブで [Attach] (アタッチ) を選択します。
4. ポリシーをアタッチするルート、OU、またはアカウントの横にあるラジオボタンをクリックします。場合によっては、目的の OU またはアカウントを表示するため、OU を展開
(
を選択) する必要があります。
5. Attach policy] (ポリシーのアタッチ) を選択してください。

   [Targets] (ターゲット) タブで、アタッチされているバックアップポリシーの一覧が更新され、新たに追加したものが表示されます。ポリシーの変更はすぐに反映されます。

Tag policies

タグポリシーをアタッチするには、ポリシーをアタッチするルート、OU、またはアカウントに移動します。

ルート、OU、またはアカウントに移動してタグポリシーをアタッチするには

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 (非推奨) としてサインインする必要があります。
2. AWS アカウント ページで、ポリシーをアタッチするルート、OU、またはアカウントを見つけ、名前を選択します。場合によっては、目的の OU またはアカウントを表示するため、OU を展開
(
を選択) する必要があります。
3. [Policies] (ポリシー) タブの [Tag policies] (タグポリシー) で、[Attach] (アタッチ) を選択します。
4. 目的のポリシーを見つけて [Attach policy] (ポリシーのアタッチ) を選択します。

   [Policies] (ポリシー) タブで、アタッチされているタグポリシーのリストが更新され、新たに追加したものが表示されます。ポリシーの変更はすぐに反映されます。

ポリシーに移動してタグポリシーをアタッチするには

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 (非推奨) としてサインインする必要があります。
2. タグポリシーページで、アタッチするポリシーの名前を選択します。
3. [Targets] (ターゲット) タブで [Attach] (アタッチ) を選択します。
4. ポリシーをアタッチするルート、OU、またはアカウントの横にあるラジオボタンをクリックします。場合によっては、目的の OU またはアカウントを表示するため、OU を展開
(
を選択) する必要があります。
5. Attach policy] (ポリシーのアタッチ) を選択してください。

   [Targets] (ターゲット) タブで、アタッチされているタグポリシーのリストが更新され、新たに追加したものが表示されます。ポリシーの変更はすぐに反映されます。

Chat applications policies

チャットアプリケーションポリシーをアタッチするには、ポリシーに移動するか、ポリシーをアタッチするルート、OU、またはアカウントに移動します。

ルート、OU、またはアカウントに移動してチャットアプリケーションポリシーをアタッチするには

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 (非推奨) としてサインインする必要があります。
2. AWS アカウント ページで、ポリシーをアタッチするルート、OU、またはアカウントを見つけ、名前を選択します。場合によっては、目的の OU またはアカウントを表示するため、OU を展開 (
を選択) する必要があります。
3. ポリシータブのチャットアプリケーションポリシーのエントリで、アタッチを選択します。
4. 目的のポリシーを見つけて [Attach policy] (ポリシーのアタッチ) を選択します。

   ポリシータブのアタッチされたチャットアプリケーションポリシーのリストが更新され、新しい追加が追加されました。ポリシーの変更はすぐに反映されます。

ポリシーに移動してチャットアプリケーションポリシーをアタッチするには

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 (非推奨) としてサインインする必要があります。
2. チャットボットポリシーページで、アタッチするポリシーの名前を選択します。
3. [Targets] (ターゲット) タブで [Attach] (アタッチ) を選択します。
4. ポリシーをアタッチするルート、OU、またはアカウントの横にあるラジオボタンをクリックします。場合によっては、目的の OU またはアカウントを表示するため、OU を展開 (
を選択) する必要があります。
5. Attach policy] (ポリシーのアタッチ) を選択してください。

   ターゲットタブのアタッチされたチャットアプリケーションポリシーのリストが更新され、新しい追加が追加されました。ポリシーの変更はすぐに反映されます。

AI services opt-out policies

AI サービスのオプトアウトポリシーのアタッチには、ポリシーに移動する方法と、ポリシーをアタッチするルート、OU、またはアカウントに移動する方法があります。

ルート、OU、またはアカウントに移動して AI サービスのオプトアウトポリシーをアタッチするには

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 (非推奨) としてサインインする必要があります。
2. AWS アカウント ページで、ポリシーをアタッチするルート、OU、またはアカウントを見つけ、名前を選択します。場合によっては、目的の OU またはアカウントを表示するため、OU を展開
(
を選択) する必要があります。
3. [Policies] (ポリシー) タブの [AI service opt-out policies] (AI サービスのオプトアウトポリシー) の項目で、[Attach] (アタッチ) を選択します。
4. 目的のポリシーを見つけて [Attach policy] (ポリシーのアタッチ) を選択します。

   [Policies] (ポリシー) タブで、アタッチされている AI サービスのオプトアウトポリシーの一覧が更新され、新たに追加したものが表示されます。ポリシーの変更はすぐに反映されます。

ポリシーに移動して AI サービスのオプトアウトポリシーをアタッチするには

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 (非推奨) としてサインインする必要があります。
2. AI サービスのオプトアウトポリシーページで、アタッチするポリシーの名前を選択します。
3. [Targets] (ターゲット) タブで [Attach] (アタッチ) を選択します。
4. ポリシーをアタッチするルート、OU、またはアカウントの横にあるラジオボタンをクリックします。場合によっては、目的の OU またはアカウントを表示するため、OU を展開
(
を選択) する必要があります。
5. Attach policy] (ポリシーのアタッチ) を選択してください。

[Targets] (ターゲット) タブで、アタッチされている AI サービスのオプトアウトポリシーの一覧が更新され、新たに追加したものが表示されます。ポリシーの変更はすぐに反映されます。

Security Hub policies

Security Hub ポリシーをアタッチするには、ポリシーに移動するか、ポリシーをアタッチするルート、OU、またはアカウントに移動します。

ルート、OU、またはアカウントに移動して Security Hub ポリシーをアタッチするには

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 (非推奨) としてサインインする必要があります。
2. AWS アカウント ページで、ポリシーをアタッチするルート、OU、またはアカウントを見つけ、名前を選択します。場合によっては、目的の OU またはアカウントを表示するため、OU を展開 (を選択) する必要があります。
3. ポリシータブの Security Hub ポリシーのエントリで、アタッチを選択します。
4. 目的のポリシーを見つけて [Attach policy] (ポリシーのアタッチ) を選択します。

   Policies タブのアタッチされた Security Hub ポリシーのリストが更新され、新しい追加が追加されました。ポリシーの変更はすぐに反映されます。

ポリシーに移動して Security Hub ポリシーをアタッチするには

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 (非推奨) としてサインインする必要があります。
2. Security Hub ポリシーページで、アタッチするポリシーの名前を選択します。
3. [Targets] (ターゲット) タブで [Attach] (アタッチ) を選択します。
4. ポリシーをアタッチするルート、OU、またはアカウントの横にあるラジオボタンをクリックします。場合によっては、目的の OU またはアカウントを表示するため、OU を展開 (を選択) する必要があります。

5. Attach policy] (ポリシーのアタッチ) を選択してください。

   Targets タブのアタッチされた Security Hub ポリシーのリストが更新され、新しい追加が追加されました。ポリシーの変更はすぐに反映されます。

AWS CLI & AWS SDKs

ポリシーをアタッチする

次のサンプルコードは、`AttachPolicy` を使用する方法を説明しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to attach an AWS Organizations policy to an organization,
/// an organizational unit, or an account.
/// </summary>
public class AttachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then calls the
    /// AttachPolicyAsync method to attach the policy to the root
    /// organization.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
        var policyId = "p-00000000";
```

```
            var targetId = "r-0000";

            var request = new AttachPolicyRequest
            {
                PolicyId = policyId,
                TargetId = targetId,
            };

            var response = await client.AttachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully attached Policy ID {policyId} to
 Target ID: {targetId}.");
            }
            else
            {
                Console.WriteLine("Was not successful in attaching the policy.");
            }
        }
    }
```

- API の詳細については、AWS SDK for .NET API リファレンスの「AttachPolicy」を参照してください。

CLI

AWS CLI

root、OU、またはアカウントにポリシーをアタッチするには

例 1

次の例は、サービスコントロールポリシーを OU にアタッチする方法を示しています。

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id ou-examplerootid111-exampleouid111
```

例 2

次の例は、サービスコントロールポリシーをアカウントに直接アタッチする方法を示しています。

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id 333333333333
```

- API の詳細については、AWS CLI コマンドリファレンスの「AttachPolicy」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
def attach_policy(policy_id, target_id, orgs_client):
    """
    Attaches a policy to a target. The target is an organization root, account,
 or
    organizational unit.

    :param policy_id: The ID of the policy to attach.
    :param target_id: The ID of the resources to attach the policy to.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.attach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Attached policy %s to target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't attach policy %s to target %s.", policy_id, target_id
        )
        raise
```

- API の詳細については、AWS SDK for Python (Boto3) API リファレンスの「AttachPolicy」を参照してください。

ポリシーの変更はすぐに有効になり、アタッチされたアカウントや、アタッチされたルートまたは OU の下のすべてのアカウントの IAM ユーザーとロールのアクセス許可に影響します。

を使用した組織ポリシーのデタッチ AWS Organizations

このトピックでは、 AWS Organizationsでポリシーをデタッチする方法について説明します。ポリシーは、グループに適用するコントロールを定義します AWS アカウント。

トピック

- を使用してポリシーをデタッチする AWS Organizations

を使用してポリシーをデタッチする AWS Organizations

最小アクセス許可

組織ルート、OU、またはアカウントからポリシーをデタッチするには、以下のアクションを実行する権限が必要です。

- `organizations:DetachPolicy`

Note

ルート、OU、またはアカウントから最後の認可ポリシー (SCP または RCP) をデタッチすることはできません。すべてのルート、OU、アカウントに常に少なくとも 1 つの SCP と RCP がアタッチされている必要があります。

AWS Management Console

Service control policies (SCPs)

SCP をデタッチするには、ポリシーまたはそのポリシーをデタッチするルート、OU、アカウントに移動する必要があります。

SCP がアタッチされているルート、OU、またはアカウントに移動して SCP をデタッチするには

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 (非推奨) としてサインインする必要があります。
2. AWS アカウント ページで、ポリシーをデタッチするルート、OU、またはアカウントに移動します。場合によっては、目的の OU またはアカウントを表示するため、OU を展開 (
を選択) する必要があります。ルート、OU、またはアカウントの名前を選択します。
3. [Policies] (ポリシー) タブで、デタッチする SCP の横にあるラジオボタンを選択して、[Detach] (デタッチ) を選択します。
4. 確認ダイアログボックスで、[Detach policy] (ポリシーのデタッチ) を選択します。

   アタッチされている SCP のリストが更新されます。SCP のデタッチによるポリシーの変更はすぐに有効になります。例えば、SCP をデタッチすると、以前にアタッチされた 1 つ以上のアカウントの IAM ユーザーおよびロールのアクセス許可によって、以前にアタッチされた組織ルートまたは OU にすぐに影響します。

ポリシーに移動して SCP をデタッチするには

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 (非推奨) としてサインインする必要があります。
2. サービスコントロールポリシーページで、ルート、OU、またはアカウントからデタッチするポリシーの名前を選択します。
3. [Targets] (ターゲット) タブで、ポリシーをデタッチするルート、OU、またはアカウントの横にあるラジオボタンをクリックします。場合によっては、目的の OU またはアカウントを表示するため、OU を展開 (
を選択) する必要があります。

4. [Detach] (デタッチ) を選択します。
5. 確認ダイアログボックスで、[Detach] (デタッチ) を選択します。

   アタッチされている SCP のリストが更新されます。SCP のデタッチによるポリシーの変更はすぐに有効になります。例えば、SCP をデタッチすると、以前にアタッチされた 1 つ以上のアカウントの IAM ユーザーおよびロールのアクセス許可によって、以前にアタッチされた組織ルートまたは OU にすぐに影響します。

Resource control policies (RCPs)

RCP をデタッチするには、ポリシーに移動するか、ポリシーをデタッチするルート、OU、またはアカウントに移動します。エンティティから RCP をデタッチすると、その RCP は、デタッチされたエンティティの影響を受けたリソースに適用されなくなります。

> **Note**
>
> **`RCPFullAWSAccess`ポリシーをデタッチすることはできません**
> `RCPFullAWSAccess` ポリシーは、ルート、すべての OU、および組織内のすべてのアカウントに自動的にアタッチされます。このポリシーをデタッチすることはできません。

アタッチされているルート、OU、またはアカウントに移動して RCP をデタッチするには

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 (非推奨) としてサインインする必要があります。
2. AWS アカウント ページで、ポリシーをデタッチするルート、OU、またはアカウントに移動します。場合によっては、目的の OU またはアカウントを表示するため、OU を展開 (
   を選択) する必要があります。ルート、OU、またはアカウントの名前を選択します。
3. ポリシータブで、デタッチする RCP の横にあるラジオボタンを選択し、デタッチを選択します。
4. 確認ダイアログボックスで、[Detach policy] (ポリシーのデタッチ) を選択します。

   アタッチされた RCPsが更新されました。RCP のデタッチによるポリシーの変更は、すぐに有効になります。例えば、RCP をデタッチすると、以前にアタッチされたアカウントまたは

以前にアタッチされた組織のルートまたは OU のアカウントの IAM ユーザーとロールのアクセス許可にすぐに影響します。

ポリシーに移動して RCP をデタッチするには

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 (非推奨) としてサインインする必要があります。
2. リソースコントロールポリシーページで、ルート、OU、またはアカウントからデタッチするポリシーの名前を選択します。
3. [Targets] (ターゲット) タブで、ポリシーをデタッチするルート、OU、またはアカウントの横にあるラジオボタンをクリックします。場合によっては、目的の OU またはアカウントを表示するため、OU を展開
(
を選択) する必要があります。
4. [Detach] (デタッチ) を選択します。
5. 確認ダイアログボックスで、[Detach] (デタッチ) を選択します。

   アタッチされた RCPsが更新されました。RCP のデタッチによるポリシーの変更は、すぐに有効になります。例えば、RCP をデタッチすると、以前にアタッチされたアカウントまたは以前にアタッチされた組織のルートまたは OU のアカウントの IAM ユーザーとロールのアクセス許可にすぐに影響します。

Declarative policies

宣言ポリシーをデタッチするには、ポリシーに移動するか、ポリシーをデタッチするルート、OU、またはアカウントに移動します。

アタッチされているルート、OU、またはアカウントに移動して宣言ポリシーをデタッチするには

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 (非推奨) としてサインインする必要があります。
2. AWS アカウント ページで、ポリシーをデタッチするルート、OU、またはアカウントに移動します。場合によっては、目的の OU またはアカウントを表示するため、OU を展開
(
を選択) する必要があります。ルート、OU、またはアカウントの名前を選択します。

3. ポリシータブで、デタッチする宣言ポリシーの横にあるラジオボタンを選択し、デタッチを選択します。
4. 確認ダイアログボックスで、[Detach policy] (ポリシーのデタッチ) を選択します。

   アタッチされた宣言ポリシーのリストが更新されました。ポリシーの変更はすぐに反映されます。

ポリシーに移動して宣言ポリシーをデタッチするには

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 (非推奨) としてサインインする必要があります。
2. 宣言ポリシーページで、ルート、OU、またはアカウントからデタッチするポリシーの名前を選択します。
3. [Targets] (ターゲット) タブで、ポリシーをデタッチするルート、OU、またはアカウントの横にあるラジオボタンをクリックします。場合によっては、目的の OU またはアカウントを表示するため、OU を展開
   (
   を選択) する必要があります。
4. [Detach] (デタッチ) を選択します。
5. 確認ダイアログボックスで、[Detach] (デタッチ) を選択します。

   アタッチされた宣言ポリシーのリストが更新されました。ポリシーの変更はすぐに反映されます。

Backup policies

バックアップポリシーのデタッチには、ポリシーに移動する方法と、ポリシーをデタッチするルート、OU、またはアカウントに移動する方法があります。

ポリシーがアタッチされているルート、OU、またはアカウントに移動してバックアップポリシーをデタッチするには

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 (非推奨) としてサインインする必要があります。

2. AWS アカウント ページで、ポリシーをデタッチするルート、OU、またはアカウントに移動します。場合によっては、目的の OU またはアカウントを表示するため、OU を展開 (
を選択) する必要があります。ルート、OU、またはアカウントの名前を選択します。
3. [Policies] (ポリシー) タブで、デタッチするバックアップポリシーの横にあるラジオボタンを選択し、[Detach] (デタッチ) を選択します。
4. 確認ダイアログボックスで、[Detach policy] (ポリシーのデタッチ) を選択します。

   アタッチされているバックアップポリシーの一覧が更新されます。ポリシーの変更はすぐに反映されます。

ポリシーに移動してバックアップポリシーをデタッチするには

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 (非推奨) としてサインインする必要があります。
2. バックアップポリシーページで、ルート、OU、またはアカウントからデタッチするポリシーの名前を選択します。
3. [Targets] (ターゲット) タブで、ポリシーをデタッチするルート、OU、またはアカウントの横にあるラジオボタンをクリックします。場合によっては、目的の OU またはアカウントを表示するため、OU を展開 (
を選択) する必要があります。
4. [Detach] (デタッチ) を選択します。
5. 確認ダイアログボックスで、[Detach] (デタッチ) を選択します。

   アタッチされているバックアップポリシーの一覧が更新されます。ポリシーの変更はすぐに反映されます。

Tag policies

タグポリシーをデタッチするには、ポリシーをデタッチするルート、OU、またはアカウントに移動します。

タグポリシーがアタッチされているルート、OU、またはアカウントに移動してデタッチするには

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 (非推奨) としてサインインする必要があります。
2. AWS アカウント ページで、ポリシーをデタッチするルート、OU、またはアカウントに移動します。場合によっては、目的の OU またはアカウントを表示するため、OU を展開 (
を選択) する必要があります。ルート、OU、またはアカウントの名前を選択します。
3. [Policies] (ポリシー) タブで、デタッチするタグポリシーの横にあるラジオボタンをクリックし、[Detach] (デタッチ) を選択します。
4. 確認ダイアログボックスで、[Detach policy] (ポリシーのデタッチ) を選択します。

   アタッチされているタグポリシーのリストが更新されます。ポリシーの変更はすぐに反映されます。

ポリシーに移動してタグポリシーをデタッチするには

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 (非推奨) としてサインインする必要があります。
2. タグポリシーページで、ルート、OU、またはアカウントからデタッチするポリシーの名前を選択します。
3. [Targets] (ターゲット) タブで、ポリシーをデタッチするルート、OU、またはアカウントの横にあるラジオボタンをクリックします。場合によっては、目的の OU またはアカウントを表示するため、OU を展開 (
を選択) する必要があります。
4. [Detach] (デタッチ) を選択します。
5. 確認ダイアログボックスで、[Detach] (デタッチ) を選択します。

   アタッチされているタグポリシーのリストが更新されます。ポリシーの変更はすぐに反映されます。

Chat applications policies

チャットアプリケーションポリシーをデタッチするには、ポリシーに移動するか、ポリシーをデタッチするルート、OU、またはアカウントに移動します。

アタッチされているルート、OU、またはアカウントに移動してチャットアプリケーションポリシーをデタッチするには

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 (非推奨) としてサインインする必要があります。
2. AWS アカウント ページで、ポリシーをデタッチするルート、OU、またはアカウントに移動します。場合によっては、目的の OU またはアカウントを表示するため、OU を展開 (
を選択) する必要があります。ルート、OU、またはアカウントの名前を選択します。
3. ポリシータブで、デタッチするチャットアプリケーションポリシーの横にあるラジオボタンを選択し、デタッチを選択します。
4. 確認ダイアログボックスで、[Detach policy] (ポリシーのデタッチ) を選択します。

   アタッチされたチャットアプリケーションポリシーのリストが更新されました。ポリシーの変更はすぐに反映されます。

ポリシーに移動してチャットアプリケーションポリシーをデタッチするには

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 (非推奨) としてサインインする必要があります。
2. チャットボットポリシーページで、ルート、OU、またはアカウントからデタッチするポリシーの名前を選択します。
3. [Targets] (ターゲット) タブで、ポリシーをデタッチするルート、OU、またはアカウントの横にあるラジオボタンをクリックします。場合によっては、目的の OU またはアカウントを表示するため、OU を展開 (
を選択) する必要があります。
4. [Detach] (デタッチ) を選択します。
5. 確認ダイアログボックスで、[Detach] (デタッチ) を選択します。

アタッチされたチャットアプリケーションポリシーのリストが更新されました。ポリシーの変更はすぐに反映されます。

AI services opt-out policies

AI サービスのオプトアウトポリシーのデタッチには、ポリシーに移動する方法と、ポリシーをデタッチするルート、OU、またはアカウントに移動する方法があります。

ポリシーがアタッチされているルート、OU、またはアカウントに移動して AI サービスのオプトアウトポリシーをデタッチするには

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 (非推奨) としてサインインする必要があります。
2. AWS アカウント ページで、ポリシーをデタッチするルート、OU、またはアカウントに移動します。場合によっては、目的の OU またはアカウントを表示するため、OU を展開 (
を選択) する必要があります。ルート、OU、またはアカウントの名前を選択します。
3. [Policies] (ポリシー) タブで、デタッチする AI サービスのオプトアウトポリシーの横にあるラジオボタンを選択し、[Detach] (デタッチ) を選択します。
4. 確認ダイアログボックスで、[Detach policy] (ポリシーのデタッチ) を選択します。

   アタッチされている AI サービスのオプトアウトポリシーの一覧が更新されます。ポリシーの変更はすぐに反映されます。

ポリシーに移動して AI サービスのオプトアウトポリシーをデタッチするには

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 (非推奨) としてサインインする必要があります。
2. AI サービスのオプトアウトポリシーページで、ルート、OU、またはアカウントからデタッチするポリシーの名前を選択します。
3. [Targets] (ターゲット) タブで、ポリシーをデタッチするルート、OU、またはアカウントの横にあるラジオボタンをクリックします。場合によっては、目的の OU またはアカウントを表示するため、OU を展開

(
を選択) する必要があります。

4. [Detach] (デタッチ) を選択します。
5. 確認ダイアログボックスで、[Detach] (デタッチ) を選択します。

   アタッチされている AI サービスのオプトアウトポリシーの一覧が更新されます。ポリシーの変更はすぐに反映されます。

Security Hub policies

Security Hub ポリシーをデタッチするには、ポリシーに移動するか、ポリシーをデタッチするルート、OU、またはアカウントに移動します。

アタッチされているルート、OU、またはアカウントに移動して Security Hub ポリシーをデタッチするには

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 (非推奨) としてサインインする必要があります。
2. AWS アカウント ページで、ポリシーをデタッチするルート、OU、またはアカウントに移動します。場合によっては、目的の OU またはアカウントを表示するため、OU を展開
   (
   を選択) する必要があります。ルート、OU、またはアカウントの名前を選択します。
3. ポリシータブで、デタッチする Security Hub ポリシーの横にあるラジオボタンを選択し、デタッチを選択します。
4. 確認ダイアログボックスで、[Detach policy] (ポリシーのデタッチ) を選択します。

   アタッチされた Security Hub ポリシーのリストが更新されました。ポリシーの変更はすぐに反映されます。

ポリシーに移動して Security Hub ポリシーをデタッチするには

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 (非推奨) としてサインインする必要があります。
2. Security Hub ポリシーページで、ルート、OU、またはアカウントからデタッチするポリシーの名前を選択します。

3. [Targets] (ターゲット) タブで、ポリシーをデタッチするルート、OU、またはアカウントの横にあるラジオボタンをクリックします。場合によっては、目的の OU またはアカウントを表示するため、OU を展開 (
を選択) する必要があります。
4. [Detach] (デタッチ) を選択します。
5. 確認ダイアログボックスで、[Detach] (デタッチ) を選択します。

   アタッチされた Security Hub ポリシーのリストが更新されました。ポリシーの変更はすぐに反映されます。

AWS CLI & AWS SDKs

ポリシーをアタッチする

次のサンプルコードは、`DetachPolicy` を使用する方法を説明しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to detach a policy from an AWS Organizations organization,
/// organizational unit, or account.
/// </summary>
public class DetachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and uses it to call
```

```
        /// DetachPolicyAsync to detach the policy.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var policyId = "p-00000000";
            var targetId = "r-0000";

            var request = new DetachPolicyRequest
            {
                PolicyId = policyId,
                TargetId = targetId,
            };

            var response = await client.DetachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully detached policy with Policy Id:
{policyId}.");
            }
            else
            {
                Console.WriteLine("Could not detach the policy.");
            }
        }
    }
```

- API の詳細については、AWS SDK for .NET API リファレンス の「DetachPolicy」を参照してください。

CLI

AWS CLI

root、OU、またはアカウントからポリシーをデタッチするには

次のコード例は、OU からポリシーをデタッチする方法を示しています。

```
aws organizations  detach-policy  --target-id ou-examplerootid111-exampleouid111
 --policy-id p-examplepolicyid111
```

- API の詳細については、AWS CLI コマンドリファレンスの「DetachPolicy」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
def detach_policy(policy_id, target_id, orgs_client):
    """
    Detaches a policy from a target.

    :param policy_id: The ID of the policy to detach.
    :param target_id: The ID of the resource where the policy is currently
 attached.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.detach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Detached policy %s from target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't detach policy %s from target %s.", policy_id, target_id
        )
        raise
```

- API の詳細については、AWS SDK for Python (Boto3) API リファレンス の「DetachPolicy」を参照してください。

ポリシーの変更はすぐに有効になり、アタッチされたアカウント、またはアタッチされたルートまたは OU のすべてのアカウントの IAM ユーザー、ロール、リソースのアクセス許可に影響します。

組織のポリシーに関する情報の取得

このトピックでは、組織内のポリシーの詳細を取得するさまざまな方法について説明します。これらの手順は、すべてのポリシータイプに適用されます。あるタイプのポリシーを組織ルート内のエンティティにアタッチする前に、その組織ルートでそのポリシータイプを有効にする必要があります。

トピック

- すべてのポリシーの一覧表示
- ルート、OU、またはアカウントにアタッチされているポリシーを一覧表示する
- ポリシーがアタッチされているすべての root、OU、およびアカウントの一覧表示
- ポリシーの詳細の取得

すべてのポリシーの一覧表示

> 最小アクセス許可
>
> 組織内のポリシーを一覧表示するには、次のアクセス権限が必要です。
>
> - `organizations:ListPolicies`

組織内のポリシーは、 で表示 AWS Management Console することも、 AWS Command Line Interface （ AWS CLI) コマンドまたは AWS SDK オペレーションを使用して表示することもできます。

AWS Management Console

組織のすべてのポリシーを一覧表示するには

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. ポリシーページで、一覧表示するポリシーを選択します。

指定したポリシータイプが有効な場合、コンソールには、組織で現在利用できる同様のタイプのポリシーの一覧が表示されます。

3. ポリシーページに戻り、ポリシータイプごとにこれを繰り返します。

AWS CLI & AWS SDKs

次のサンプルコードは、ListPolicies を使用する方法を説明しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to list the AWS Organizations policies associated with an
/// organization.
/// </summary>
public class ListPolicies
{
    /// <summary>
    /// Initializes an Organizations client object, and then calls its
    /// ListPoliciesAsync method.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        // The value for the Filter parameter is required and must must be
        // one of the following:
```

```
            //     AISERVICES_OPT_OUT_POLICY
            //     BACKUP_POLICY
            //     SERVICE_CONTROL_POLICY
            //     TAG_POLICY
            var request = new ListPoliciesRequest
            {
                Filter = "SERVICE_CONTROL_POLICY",
                MaxResults = 5,
            };

            var response = new ListPoliciesResponse();
            try
            {
                do
                {
                    response = await client.ListPoliciesAsync(request);
                    response.Policies.ForEach(p => DisplayPolicies(p));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (AWSOrganizationsNotInUseException ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about the Organizations policies associated
        /// with an organization.
        /// </summary>
        /// <param name="policy">An Organizations policy summary to display
        /// information on the console.</param>
        private static void DisplayPolicies(PolicySummary policy)
        {
            string policyInfo = $"{policy.Id}
{policy.Name}\t{policy.Description}";

            Console.WriteLine(policyInfo);
        }
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「ListPolicies」を参照してください。

CLI

AWS CLI

特定のタイプの組織のすべてのポリシーのリストを取得するには

次の例は、フィルターパラメータで指定された SCP のリストを取得する方法を示しています。

```
aws organizations list-policies --filter SERVICE_CONTROL_POLICY
```

出力には、ポリシーのリストと概要情報が含まれます。

```
{
        "Policies": [
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllS3Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid111",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid111",
                        "Description": "Enables account admins to delegate
 permissions for any S3 actions to users and roles in their accounts."
                },
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllEC2Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid222",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid222",
                        "Description": "Enables account admins to delegate
 permissions for any EC2 actions to users and roles in their accounts."
                },
                {
```

```
                        "AwsManaged": true,
                        "Description": "Allows access to every operation",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-FullAWSAccess",
                        "Arn": "arn:aws:organizations::aws:policy/
service_control_policy/p-FullAWSAccess",
                        "Name": "FullAWSAccess"
                }
        ]
}
```

- API の詳細については、「AWS CLI Command Reference」の「ListPolicies」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
def list_policies(policy_filter, orgs_client):
    """
    Lists the policies for the account, limited to the specified filter.

    :param policy_filter: The kind of policies to return.
    :param orgs_client: The Boto3 Organizations client.
    :return: The list of policies found.
    """
    try:
        response = orgs_client.list_policies(Filter=policy_filter)
        policies = response["Policies"]
        logger.info("Found %s %s policies.", len(policies), policy_filter)
    except ClientError:
        logger.exception("Couldn't get %s policies.", policy_filter)
        raise
    else:
        return policies
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「ListPolicies」を参照してください。

ルート、OU、またはアカウントにアタッチされているポリシーを一覧表示する

> **最小アクセス許可**
>
> 組織内のルート、組織単位 (OU)、またはアカウントにアタッチされたポリシーを一覧表示するには、次のアクセス許可が必要です。
>
> - 指定されたターゲット (または "*") の Amazon リソースネーム (ARN) を含む同じポリシーステートメントの `Resource` 要素を持つ `organizations:ListPoliciesForTarget`。

AWS Management Console

指定したルート、OU、またはアカウント に直接アタッチされているすべてのポリシーを一覧表示するには

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. リポジトリの AWS アカウント ページで、ポリシーを表示するルート、OU、またはアカウントの名前を選択します。必要な OU を見つけるために、OUを展開する (
を選択する) 必要がある場合があります。
3. ルート、OU、またはアカウントページで、[Policies] (ポリシー) タブを選択します。

   [Policies] (ポリシー) タブでは、そのルート、OU、またはアカウントにアタッチされているすべてのポリシーが、ポリシータイプ別にグループ化されて表示されます。

AWS CLI & AWS SDKs

指定したルート、OU、またはアカウント に直接アタッチされているすべてのポリシーを一覧表示するには

エンティティにアタッチされているポリシーを一覧表示するには、次のいずれかのコマンドを使用します。

- AWS CLI: list-policies-for-target

  次の例では、指定された OU にアタッチされているすべてのサービスコントロールポリシーを一覧表示します。ルート、OU、またはアカウントの ID、および一覧表示するポリシーのタイプを指定する必要があります。

```
$ aws organizations list-policies-for-target \
    --target-id ou-a1b2-f6g7h222 \
    --filter SERVICE_CONTROL_POLICY
{
    "Policies": [
        {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        }
    ]
}
```

- AWS SDKs: ListPoliciesForTarget

ポリシーがアタッチされているすべての root、OU、およびアカウントの一覧表示

> **最小アクセス許可**
>
> ポリシーがアタッチされているエンティティを一覧表示するには、次のアクセス権限が必要です。

- 指定されたポリシー (または "*") の ARN を含む同じポリシーステートメントの `Resource` 要素を持つ `organizations:ListTargetsForPolicy`。

AWS Management Console

特定のポリシーがアタッチされているすべてのルート、OU、およびアカウントを一覧表示するには

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. ポリシーページで、ポリシータイプを選択してから、添付ファイルを確認するポリシーの名前を選択します。
3. [Targets] (ターゲット) タブを選択し、選択したポリシーがアタッチされているすべてのルート、OU、およびアカウントのテーブルを表示します。

AWS CLI & AWS SDKs

特定のポリシーがアタッチされているすべてのルート、OU、およびアカウントを一覧表示するには

ポリシーを含むエンティティを一覧表示するには、次のいずれかのコマンドを使用します。

- AWS CLI: list-targets-for-policy

  次の例は、指定されたポリシーのルート、OU、およびアカウントに対するすべての添付ファイルを示しています。

```
$ aws organizations list-targets-for-policy \
    --policy-id p-FullAWSAccess
{
    "Targets": [
        {
            "TargetId": "ou-a1b2-f6g7h111",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
            "Name": "testou2",
            "Type": "ORGANIZATIONAL_UNIT"
```

```
        },
        {
            "TargetId": "ou-a1b2-f6g7h222",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
            "Name": "testou1",
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
            "TargetId": "123456789012",
            "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
            "Name": "My Management Account (bisdavid)",
            "Type": "ACCOUNT"
        },
        {
            "TargetId": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "Type": "ROOT"
        }
    ]
}
```

- AWS SDKs: ListTargetsForPolicy

ポリシーの詳細の取得

最小アクセス許可

ポリシーの詳細を表示するには、次のアクセス権限が必要です。

- 指定されたポリシー (または "*") の ARN を含む同じポリシーステートメントの Resource 要素を持つ organizations:DescribePolicy。

AWS Management Console

ポリシーの詳細を取得するには

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. ポリシーページで、確認するポリシーのポリシータイプを選択してから、ポリシーの名前を選択します。

   ポリシーページには、ARN、説明、アタッチメントなど、ポリシーに関する利用可能な情報が表示されます。

   - [Content] (コンテンツ) タブには、ポリシーの現在の内容が JSON 形式で表示されます。
   - [Targets] (ターゲット) タブには、ポリシーがアタッチされているルート、OU、およびアカウントの一覧が表示されます。
   - [Tags] (タグ) タブには、ポリシーにアタッチされたタグが表示されます。注: [Tags] (タグ) タブは、 AWS 管理ポリシーでは使用できません。

   ポリシーを編集するには、[Edit policy] (ポリシーの編集) を選択します。編集要件はポリシータイプごとに異なるため、指定したポリシータイプのポリシーの作成および更新手順を参照してください。

AWS CLI & AWS SDKs

以下のコード例は、`DescribePolicy` の使用方法を示しています。

CLI

AWS CLI

ポリシーに関する情報を取得するには

次の例は、ポリシーに関する情報をリクエストする方法を示しています。

```
aws organizations describe-policy --policy-id p-examplepolicyid111
```

出力には、ポリシーの詳細を含むポリシーオブジェクトが含まれます。

```
{
        "Policy": {
                "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement
\": [\n    {\n      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n
 \"Resource\": \"*\"\n    }\n  ]\n}",
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::111111111111:policy/o-
exampleorgid/service_control_policy/p-examplepolicyid111",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-examplepolicyid111",
                        "AwsManaged": false,
                        "Name": "AllowAllS3Actions",
                        "Description": "Enables admins to delegate S3
 permissions"
                }
        }
}
```

- API の詳細については、AWS CLI コマンドリファレンスの「DescribePolicy」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
def describe_policy(policy_id, orgs_client):
    """
    Describes a policy.

    :param policy_id: The ID of the policy to describe.
    :param orgs_client: The Boto3 Organizations client.
    :return: The description of the policy.
    """
    try:
        response = orgs_client.describe_policy(PolicyId=policy_id)
```

```
        policy = response["Policy"]
        logger.info("Got policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't get policy %s.", policy_id)
        raise
    else:
        return policy
```

- API の詳細については、AWS SDK for Python (Boto3) API リファレンスの「DescribePolicy」を参照してください。

を使用した組織ポリシーの削除 AWS Organizations

ポリシーが不要になった場合、すべての組織単位 (OU) およびアカウントからポリシーをデタッチした後、ポリシーを削除できます。

このトピックでは、 を使用してポリシーを削除する方法について説明します AWS Organizations。ポリシーは、グループに適用するコントロールを定義します AWS アカウント。

トピック

- を使用してポリシーを削除する AWS Organizations

を使用してポリシーを削除する AWS Organizations

組織の管理アカウントにサインインすると、組織に不要になったポリシーを削除できます。

ポリシーを削除するには、まずそのポリシーをすべての添付エンティティからデタッチする必要があります。

> **Note**
>
> - という名前の SCP などの AWS マネージド SCP は削除できませんFullAWSAccess。
> - という名前の RCP などの AWS マネージド RCP は削除できませんRCPFullAWSAccess。

最小アクセス許可

ポリシーを削除するには、次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。

- `organizations:DeletePolicy`

AWS Management Console

Service control policies (SCPs)

SCP を削除するには

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 (非推奨) としてサインインする必要があります。
2. サービスコントロールポリシーページで、削除する SCP の名前を選択します。
3. 削除するポリシーは、まず、すべてのルート、OU、アカウントからデタッチする必要があります。[Targets] (ターゲット) タブを選択し、[Targets] (ターゲット) リストの各ルート、OU、アカウントの横にあるラジオボタンをクリックしてから、[Detach] (デタッチ) を選択します。確認ダイアログボックスで、[Detach] (デタッチ) を選択します。すべてのターゲットを削除するまで繰り返します。
4. ページの上部で、[Delete] (削除) を選択します。
5. 確認ダイアログボックスで、ポリシーの名前を入力し、[Delete] (削除) を選択します。

Resource control policies (RCPs)

RCP を削除するには

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の 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 (非推奨) としてサインインする必要があります。
2. リソースコントロールポリシーページで、削除する RCP の名前を選択します。
3. 削除するポリシーは、まず、すべてのルート、OU、アカウントからデタッチする必要があります。[Targets] (ターゲット) タブを選択し、[Targets] (ターゲット) リストの各ルート、OU、アカウントの横にあるラジオボタンをクリックしてから、[Detach] (デタッチ) を

選択します。確認ダイアログボックスで、[Detach] (デタッチ) を選択します。すべてのターゲットを削除するまで繰り返します。

4. ページの上部で、[Delete] (削除) を選択します。
5. 確認ダイアログボックスで、ポリシーの名前を入力し、[Delete] (削除) を選択します。

Declarative policies

宣言ポリシーを削除するには

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 (非推奨) としてサインインする必要があります。
2. 宣言ポリシーページで、削除するポリシーの名前を選択します。
3. 削除するポリシーは、まず、すべてのルート、OU、アカウントからデタッチする必要があります。[Targets] (ターゲット) タブを選択し、[Targets] (ターゲット) リストの各ルート、OU、アカウントの横にあるラジオボタンをクリックしてから、[Detach] (デタッチ) を選択します。確認ダイアログボックスで、[Detach] (デタッチ) を選択します。すべてのターゲットを削除するまで繰り返します。
4. ページの上部で、[Delete] (削除) を選択します。
5. 確認ダイアログボックスで、ポリシーの名前を入力し、[Delete] (削除) を選択します。

Backup policies

バックアップポリシーを削除するには

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 (非推奨) としてサインインする必要があります。
2. バックアップポリシーページから、削除するバックアップポリシーの名前を選択します。
3. 削除するバックアップポリシーは、まず、すべてのルート、OU、アカウントからデタッチする必要があります。[Targets] (ターゲット) タブを選択し、[Targets] (ターゲット) リストの各ルート、OU、アカウントの横にあるラジオボタンをクリックしてから、[Detach] (デタッチ) を選択します。確認ダイアログボックスで、[Detach] (デタッチ) を選択します。すべてのターゲットを削除するまで繰り返します。
4. ページの上部で、[Delete] (削除) を選択します。

5. 確認ダイアログボックスで、ポリシーの名前を入力し、[Delete] (削除) を選択します。

Tag policies

タグポリシーを削除するには

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 (非推奨) としてサインインする必要があります。
2. タグポリシーページで、削除するポリシーを選択します。
3. 削除するポリシーは、まず、すべてのルート、OU、アカウントからデタッチする必要があります。[Targets] (ターゲット) タブで、[Targets] (ターゲット) リストに表示されている各ルート、OU、またはアカウントの横にあるラジオボタンをクリックしてから、[Detach] (デタッチ) を選択します。確認ダイアログボックスで、[Detach] (デタッチ) を選択します。すべてのターゲットを削除するまで繰り返します。
4. ページの上部で、[Delete] (削除) を選択します。
5. 確認ダイアログボックスで、ポリシーの名前を入力し、[Delete] (削除) を選択します。

Chat applications policies

チャットアプリケーションポリシーを削除するには

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 (非推奨) としてサインインする必要があります。
2. チャットボットポリシーページで、削除するポリシーの名前を選択します。
3. 削除するポリシーは、まず、すべてのルート、OU、アカウントからデタッチする必要があります。[Targets] (ターゲット) タブを選択し、[Targets] (ターゲット) リストの各ルート、OU、アカウントの横にあるラジオボタンをクリックしてから、[Detach] (デタッチ) を選択します。確認ダイアログボックスで、[Detach] (デタッチ) を選択します。すべてのターゲットを削除するまで繰り返します。
4. ページの上部で、[Delete] (削除) を選択します。
5. 確認ダイアログボックスで、ポリシーの名前を入力し、[Delete] (削除) を選択します。

AI services opt-out policies

AI サービスのオプトアウトポリシーを削除するには

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 (非推奨) としてサインインする必要があります。
2. AI サービスのオプトアウトポリシーページで、削除するポリシーの名前を選択します。
3. 削除するポリシーは、まず、すべてのルート、OU、アカウントからデタッチする必要があります。[Targets] (ターゲット) タブを選択し、[Targets] (ターゲット) リストの各ルート、OU、アカウントの横にあるラジオボタンをクリックしてから、[Detach] (デタッチ) を選択します。確認ダイアログボックスで、[Detach] (デタッチ) を選択します。すべてのターゲットを削除するまで繰り返します。
4. ページの上部で、[Delete] (削除) を選択します。
5. 確認ダイアログボックスで、ポリシーの名前を入力し、[Delete] (削除) を選択します。

Security Hub policies

Security Hub ポリシーを削除するには

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 (非推奨) としてサインインする必要があります。
2. Security Hub ポリシーページで、削除するポリシーの名前を選択します。
3. 削除するポリシーは、まず、すべてのルート、OU、アカウントからデタッチする必要があります。[Targets] (ターゲット) タブを選択し、[Targets] (ターゲット) リストの各ルート、OU、アカウントの横にあるラジオボタンをクリックしてから、[Detach] (デタッチ) を選択します。確認ダイアログボックスで、[Detach] (デタッチ) を選択します。すべてのターゲットを削除するまで繰り返します。
4. ページの上部で、[Delete] (削除) を選択します。
5. 確認ダイアログボックスで、ポリシーの名前を入力し、[Delete] (削除) を選択します。

AWS CLI & AWS SDKs

ポリシーを削除する

次のサンプルコードは、DeletePolicy を使用する方法を説明しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Deletes an existing AWS Organizations policy.
/// </summary>
public class DeletePolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// delete the policy with the specified policyId.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var policyId = "p-00000000";

        var request = new DeletePolicyRequest
        {
            PolicyId = policyId,
        };

        var response = await client.DeletePolicyAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
```

```
                Console.WriteLine($"Successfully deleted Policy: {policyId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete Policy: {policyId}.");
            }
        }
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「DeletePolicy」を参照してください。

CLI

AWS CLI

ポリシーを削除するには

次の例は、組織からポリシーを削除する方法を示しています。この例では、ポリシーをすべてのエンティティから事前にデタッチしたことを前提としています。

```
aws organizations delete-policy --policy-id p-examplepolicyid111
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「DeletePolicy」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
def delete_policy(policy_id, orgs_client):
    """
```

```
    Deletes a policy.

    :param policy_id: The ID of the policy to delete.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.delete_policy(PolicyId=policy_id)
        logger.info("Deleted policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't delete policy %s.", policy_id)
        raise
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「DeletePolicy」を参照してください。

AWS Organizations リソースのタグ付け

タグは、 AWS リソースを識別、整理、検索しやすくするために リソースに追加するカスタム属性ラベルです。各タグは 2 つの部分で構成されます。

- タグキー (例： `CostCenter`、`Environment`、または `Project`)。タグキーの長さは最大 128 文字で、大文字と小文字は区別されます。
- タグ値 (例: `111122223333` または `Production`)。タグ値の長さは最大 256 文字で、タグキーと同様に大文字と小文字は区別されます。タグの値を空の文字列に設定することはできますが、タグの値を null に設定することはできません。タグ値を省略すると、空の文字列を使用した場合と同じになります。

タグのキーまたは値で許可される文字の詳細についてはResource Groups のタグ付け API リファレンスの「タグ付け API の タグパラメータ」を参照してください。

タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。詳細については、AWS 「リソースのタグ付けのベストプラクティス」を参照してください。

> **Tip**
>
> タグポリシーを使用すると、組織のアカウント内のリソース間でタグの実装を標準化できます。

トピック

- 考慮事項
- タグの使用
- タグの追加、更新、削除

考慮事項

AWS Organizations は、管理アカウントにログインすると、次のタグ付けオペレーションをサポートします。

以下の組織のリソースにタグを追加できます

- AWS アカウント
- 組織単位
- 組織のルート
- ポリシー

タグは次のタイミングで追加できます

- リソースを作成するとき — Organizations コンソールでタグを指定するか、Create API オペレーションの 1 つで Tags パラメータを使用します。これは、組織のルートには適用されません。
- リソースを作成した後 — Organizations コンソールを使用するか、TagResource オペレーションを呼び出します。

その他の考慮事項

コンソール AWS Organizations を使用するか、 ListTagsForResourceオペレーションを呼び出すことで、 のタグ付け可能なリソースのタグを表示できます。

リソースからタグを削除するには、コンソールを使用して削除するキーを指定するか、UntagResource オペレーションを呼び出します。

タグの使用

タグを使用すると、役に立つカテゴリ別にリソースをグループ化でき、組織内のリソースリソースを整理できます。例えば、所有部門を追跡する「部門」タグを割り当てることができます。「Environment」タグを割り当てると、特定のリソースがアルファ、ベータ、ガンマ、または本番環境の一部であるかどうかを追跡できます。

タグを使用して以下のこともできます。

- リソースにタグ付け基準を適用します。
- 誰がリソースにアクセスできるかを制御します。

タグの追加、更新、削除

組織の管理アカウントにサインインすると、組織のリソースにタグを追加できます。

リソースの作成時にタグを追加する

最小アクセス許可

リソースの作成時にリソースにタグを追加するには、次のアクセス許可が必要です。

- 特定のタイプのリソースを作成するためのアクセス許可
- `organizations:TagResource`
- `organizations:ListTagsForResource` - Organizations コンソールを使用する場合にのみ必要

作成時に、以下のリソースにアタッチされたタグキーと値を含めることができます。

- AWS アカウント
  - 作成したアカウント
  - 招待されたアカウント
- 組織単位 (OU)
- ポリシー
  - サービスコントロールポリシー
  - リソースコントロールポリシー
  - 宣言ポリシー
  - バックアップポリシー
  - タグポリシー
  - チャットアプリケーションポリシー
  - AI サービスのオプトアウトポリシー

組織ルートは、最初に組織を作成する際に作成されるため、既存のリソースとしてのみタグを追加できます。

既存のリソースにタグを追加または更新する

新しいタグを追加したり、既存のリソースにアタッチされているタグの値を更新することもできます。

最小アクセス許可

組織のリソースにタグを追加または更新するには、次のアクセス許可が必要です。

- `organizations:TagResource`
- `organizations:ListTagsForResource` - Organizations コンソールを使用する場合にのみ必要

組織のリソースからタグを削除するには、次のアクセス許可が必要です。

- `organizations:UntagResource`

AWS Management Console

既存のリソースのタグを追加、更新、または削除するには

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の 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 (非推奨) としてサインインする必要があります。
2. アカウント、Root、OU、またはポリシーに移動して選択し、名前をクリックして詳細ページを開きます。
3. [Tags (タグ)] タブで、[Manage tags (タグ管理)] を選択します。
4. 新しいタグの追加、既存のタグの値の変更、またはタグの削除ができます。

   (オプション) タグを追加するには、[タグを追加] を選択してキーを入力し、オプションでタグの値を入力します。

   タグを削除するには[削除] を選択してください。

   タグのキーと値では、大文字と小文字が区別されます。大文字と小文字の区別は標準化して使用します。適用されるタグポリシーの要件を順守することも必要です。
5. 前のステップを必要な回数繰り返します。
6. [Save changes] (変更の保存) をクリックします。

AWS CLI & AWS SDKs

既存のリソースにタグを追加または更新するには

組織のタグ付け可能なリソースにタグを追加するには、次のいずれかのコマンドを使用します。

- AWS CLI: タグリソース
- AWS SDKs: TagResource

組織のリソースからタグを削除するには

タグを削除するには、次のいずれかのコマンドを使用します。

- AWS CLI: タグなしリソース
- AWS SDKs: UntagResource

のマルチパーティー承認 AWS Organizations

マルチパーティー承認は、分散承認プロセスを通じて事前定義されたオペレーションのリストを保護AWS Organizationsできる の一機能です。マルチパーティー承認を使用して承認ワークフローを確立し、セキュリティプロセスをチームベースの決定に変換します。

マルチパーティー承認を使用する場合：

- 「信頼しない、常に検証する」というゼロトラストの原則に従う必要があります。
- 適切な人間が適切な方法で適切なモノにアクセスできることを確認する必要があります。
- 機密性の高いオペレーションや重要なオペレーションには、分散された意思決定が必要です。
- 機密または重要なリソースに対する意図しないオペレーションから保護する必要があります
- 監査またはコンプライアンス上の理由から、正式なレビューと承認が必要です

詳細については、「マルチパーティー承認ユーザーガイド」の「マルチパーティー承認とは」を参照してください。

を他の AWS Organizations で使用する AWS のサービス

信頼されたアクセスを使用して、信頼された AWS サービスと呼ばれる、指定したサービスを有効にし、ユーザーに代わって組織とそのアカウントでタスクを実行できます。これには、信頼されたサービスに許可を付与する必要がありますが、ユーザーまたはロールの許可に影響はありません。アクセスを有効にすると、信頼されたサービスは、組織の各アカウントにサービスにリンクされたロールと呼ばれる IAM ロール を必要なときに作成できるようになります。このロールには、信頼されたサービスを使用して、該当サービスのドキュメントに記載されているタスクの実行を可能にするアクセス許可ポリシーが含まれています。これにより、信頼されたサービスを使用して、ユーザーに代わって組織のアカウントで管理する設定や構成の詳細を指定できます。信頼されたサービスは、アカウントに対して管理アクションを実行する必要がある場合にのみ、サービスにリンクされたロールを作成します。必ずしも組織のすべてのアカウントで管理アクションを実行する必要はありません。

Important

オプションが使用可能な場合は、信頼されたサービスのコンソール、またはその AWS CLI または API オペレーションの同等のもののみを使用して、信頼されたアクセスを有効または無効にすることを強くお勧めします。これにより、信頼できるアクセスの有効化に必要なすべての初期化処理が信頼できるサービスによって実行可能になります。例えば、必要なリソースの作成や、信頼できるアクセスの無効にする際のリソースのクリーンアップなどです。

信頼されたサービスを使用し、信頼されたサービスによる組織へのアクセスを有効または無効にする方法については、AWS のサービス で使用できる AWS Organizations の [Supports Trusted Access] (信頼されたアクセスをサポート) 列の [Learn more] (詳細はこちら) リンクを参照してください。

Organizations コンソール、CLI コマンド、API オペレーションを使用してアクセスを無効にした場合の結果は次のようになります。

- そのサービスでは、サービスにリンクされたロールを組織のアカウントに作成できなくなります。つまり、組織の新しいアカウントに対するオペレーションをサービスがユーザーに代わって実行できなくなります。そのサービスによる AWS Organizationsのクリーンアップが完了するまでは、古いアカウントに対するオペレーションは引き続き実行可能です。
- そのサービスでは、ロールにアタッチされている IAM ポリシーによって明示的に許可されていない限り、組織のメンバーアカウントのタスクを実行できなくなります。これには、

メンバーアカウントから管理アカウントまたは委任管理者アカウント (該当する場合) へのデータ集約が含まれます。

- 一部のサービスはこれを検出し、統合に関連する残りのデータやリソースをクリーンアップします。一方、組織へのアクセスを停止するものの、統合を再び有効にする場合のために履歴データと設定を残しておくサービスもあります。

そうしたサービスであっても、コンソールまたはコマンドを使用して統合を無効にすると、その統合以外に用途のないリソースがクリーンアップされるようになります。組織のアカウントのリソースをクリーンアップする仕組みは、サービスによって異なります。詳しくは、AWS の他のサービスのドキュメントを参照してください。

信頼されたアクセスを有効にするために必要なアクセス許可

信頼されたアクセスには、 AWS Organizations と信頼されたサービスの 2 つのサービスに対するアクセス許可が必要です。信頼されたアクセスを有効にするには、次のいずれかのシナリオを選択します。

- AWS Organizations と信頼されたサービスの両方にアクセス許可を持つ認証情報がある場合は、信頼されたサービスが提供するツール (コンソールまたは AWS CLI) を使用してアクセスを有効にします。これにより、サービスが AWS Organizations ユーザーに代わって で信頼されたアクセスを有効にし、サービスが組織内で動作するために必要なリソースを作成できます。

  これらの認証情報に必要な最小限のアクセス権限は次のとおりです。

  - `organizations:EnableAWSServiceAccess`。また、このオペレーションに `organizations:ServicePrincipal` 条件キーを使用し、承認されたサービスプリンシパル名のリストに対してオペレーションが行うリクエストを制限することもできます。詳細については、「条件キー」を参照してください。
  - `organizations:ListAWSServiceAccessForOrganization` – AWS Organizations コンソールを使用する場合に必要です。
  - 信頼されたサービスで必要な最小限のアクセス権限は、サービスによって異なります。詳細については、信頼されたサービスのドキュメントを参照してください。
- あるユーザーが でアクセス許可を持つ認証情報を持っている AWS Organizations が、別のユーザーが信頼されたサービスでアクセス許可を持つ認証情報を持っている場合は、以下の順序で以下の手順を実行します。

1. のアクセス許可を持つ認証情報を持つユーザーは、 AWS Organizations コンソール AWS CLI、、または AWS SDK を使用して、信頼されたサービスの信頼されたアクセスを有効にする AWS Organizations 必要があります。これにより、次のステップ (ステップ 2) を実行すると、組織の必要な設定を実行するためのアクセス権限が他のサービスに付与されます。

   最小限の AWS Organizations アクセス許可は次のとおりです。

   - `organizations:EnableAWSServiceAccess`
   - `organizations:ListAWSServiceAccessForOrganization` – AWS Organizations コンソールを使用する場合にのみ必要です

   で信頼されたアクセスを有効にする手順については AWS Organizations、「」を参照してください信頼されたアクセスを有効または無効にする方法。

2. 信頼されたサービスのアクセス許可を含む認証情報をユーザーに設定すると、そのサービスで AWS Organizationsを操作できます。これにより、信頼されたサービスを使用して、組織で操作するために必要なリソースの作成など、必要な初期化を行うようサービスに指示されます。詳細については、サービス固有の手順 (AWS のサービス で使用できる AWS Organizations) を参照してください。

信頼されたアクセスを無効にするために必要なアクセス許可

信頼されたサービスを使用して、組織またはそのアカウントで操作する必要がなくなった場合は、次のいずれかのシナリオを選択します。

> **Important**
>
> サービスへの信頼されたアクセスを無効にすると、適切なアクセス権限を含むユーザーやロールは、そのサービスを使用できなくなります。ユーザーとロールによる AWS サービスへのアクセスを完全にブロックするには、そのアクセスを許可する IAM アクセス許可を削除するか、 でサービスコントロールポリシー (SCPs) を使用できます AWS Organizations。SCP はメンバーアカウントにのみ適用できます。SCP は管理アカウントには適用されません。管理アカウントではサービスを実行しないことをお勧めします。代わりに、SCP を使用してセキュリティを制御できるメンバーアカウントで実行します。

- AWS Organizations と信頼されたサービスの両方にアクセス許可を持つ認証情報がある場合は、信頼されたサービスで使用できるツール (コンソールまたは AWS CLI) を使用してアクセスを無効

にします。無効になると、サービスは、ユーザーの代わりに、不要になったリソースを削除し、AWS Organizations のサービスの信頼されたアクセスを無効にしてクリーンアップします。

これらの認証情報に必要な最小限のアクセス権限は次のとおりです。

- `organizations:DisableAWSServiceAccess`。また、このオペレーションに `organizations:ServicePrincipal` 条件キーを使用し、承認されたサービスプリンシパル名のリストに対してオペレーションが行うリクエストを制限することもできます。詳細については、「条件キー」を参照してください。
- `organizations:ListAWSServiceAccessForOrganization` – AWS Organizations コンソールを使用する場合に必要です。
- 信頼されたサービスで必要な最小限のアクセス権限は、サービスによって異なります。詳細については、信頼されたサービスのドキュメントを参照してください。

- のアクセス許可を持つ認証情報 AWS Organizations が、信頼されたサービスのアクセス許可を持つ認証情報ではない場合は、次の手順を次の順序で実行します。

  1. まず、信頼されたサービスのアクセス権限を含むユーザーを使用して、このサービスを使用するアクセスを無効にします。これにより、信頼されたアクセスに必要なリソースを削除してクリーンアップするよう、信頼されたサービスに指示されます。詳細については、サービス固有の手順 (AWS のサービス で使用できる AWS Organizations) を参照してください。
  2. のアクセス許可を持つユーザーは、 コンソール、または AWS SDK を使用して AWS Organizations AWS CLI、信頼されたサービスへのアクセスを無効に AWS Organizations できます。これにより、信頼されたサービスのアクセス許可は、組織やそのアカウントより削除されます。

     最小限の AWS Organizations アクセス許可は次のとおりです。

     - `organizations:DisableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization` – AWS Organizations コンソールを使用する場合にのみ必要です

     で信頼されたアクセスを無効にする手順については AWS Organizations、「」を参照してください信頼されたアクセスを有効または無効にする方法。

信頼されたアクセスを有効または無効にする方法

のアクセス許可のみがあり、他の AWS サービスの管理者に代わって組織への信頼されたアクセスを有効または無効に AWS Organizations する場合は、次の手順を使用します。

Important

オプションが使用可能な場合は、信頼されたサービスのコンソール、またはその AWS CLI または API オペレーションの同等のもののみを使用して、信頼されたアクセスを有効または無効にすることを強くお勧めします。これにより、信頼できるアクセスの有効化に必要なすべての初期化処理が信頼できるサービスによって実行可能になります。例えば、必要なリソースの作成や、信頼できるアクセスの無効にする際のリソースのクリーンアップなどです。

信頼されたサービスを使用し、信頼されたサービスによる組織へのアクセスを有効または無効にする方法については、AWS のサービス で使用できる AWS Organizations の [Supports Trusted Access] (信頼されたアクセスをサポート) 列の [Learn more] (詳細はこちら) リンクを参照してください。

Organizations コンソール、CLI コマンド、API オペレーションを使用してアクセスを無効にした場合の結果は次のようになります。

- そのサービスでは、サービスにリンクされたロールを組織のアカウントに作成できなくなります。つまり、組織の新しいアカウントに対するオペレーションをサービスがユーザーに代わって実行できなくなります。そのサービスによる AWS Organizationsのクリーンアップが完了するまでは、古いアカウントに対するオペレーションは引き続き実行可能です。
- そのサービスでは、ロールにアタッチされている IAM ポリシーによって明示的に許可されていない限り、組織のメンバーアカウントのタスクを実行できなくなります。これには、メンバーアカウントから管理アカウントまたは委任管理者アカウント (該当する場合) へのデータ集約が含まれます。
- 一部のサービスはこれを検出し、統合に関連する残りのデータやリソースをクリーンアップします。一方、組織へのアクセスを停止するものの、統合を再び有効にする場合のために履歴データと設定を残しておくサービスもあります。

そうしたサービスであっても、コンソールまたはコマンドを使用して統合を無効にすると、その統合以外に用途のないリソースがクリーンアップされるようになります。組織のアカウントのリソースをクリーンアップする仕組みは、サービスによって異なります。詳細については、他の AWS サービスのドキュメントを参照してください。

AWS Management Console

信頼されたサービスの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. サービスページで、有効にするサービスの行を探し、その名前を選択します。
3. [Enable trusted access (信頼されたアクセスを有効にする)] を選択します。
4. 確認ダイアログボックスで、[Show the option to enable trusted access] (信頼されたアクセスを有効にするオプションを表示する) チェックボックスをオンにし、ボックスに「**enable**」と入力してから、[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. アクセスを有効にする場合は、他の AWS サービスの管理者に、他の サービスが動作できるようになりました AWS Organizations。

信頼されたサービスのアクセスを無効にするには

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. サービスページで、無効にするサービスの行を探し、その名前を選択します。
3. もう一方のサービスの管理者から、サービスが無効になり、そのリソースのクリーンアップが完了したことが知らされるまで待ちます。
4. 確認ダイアログボックスで、ボックスに「**disable**」と入力してから、[Disable trusted access] (信頼されたアクセスを無効にする) を選択します。

AWS CLI, AWS API

信頼されたサービスのアクセスを有効または無効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効または無効にできます。

- AWS CLI: AWS 組織の enable-aws-service-access
- AWS CLI: AWS 組織の disable-aws-service-access

- AWS API: EnableAWSServiceAccess
- AWS API: DisableAWSServiceAccess

AWS Organizations およびサービスにリンクされたロール

AWS Organizations は、IAM サービスにリンクされたロールを使用して、信頼されたサービスが組織のメンバーアカウントでユーザーに代わってタスクを実行できるようにします。信頼されたサービスを設定して、組織との統合のためにそのサービスを承認すると、サービスにリンクされたロールをメンバーアカウントに作成するようにそのサービスから AWS Organizations にリクエストできます。信頼されたサービスによって必要に応じて非同期的に行われますが、組織のすべてのアカウントで必ずしも同時に必要とは限りません。サービスにリンクされたロールには IAM 許可が事前定義されており、信頼されたサービスは、そのアカウント内の特定のタスクだけを実行する許可が与えられます。一般的に、サービスにリンクされたロールはすべて AWS によって管理されます。つまり、通常、ロールまたはアタッチされたポリシーを変更することはできません。

こうした変更を行えるようにするため、組織内にアカウントを作成するとき、または組織への既存のアカウントの招待が承諾されたときに、 AWS Organizations は、サービスにリンクされたロール (AWSServiceRoleForOrganizations) を使用してメンバーアカウントをプロビジョニングします。このロールを引き受けることができるのは、 AWS Organizations サービス自体のみです。ロールには、 が他の のサービスにリンクされたロールを作成 AWS Organizations できるようにするアクセス許可があります AWS のサービス。このサービスにリンクされたロールは、すべての組織に存在します。

組織で一括請求機能のみ有効になっている場合、サービスにリンクされたロール (AWSServiceRoleForOrganizations) は使用されないため、削除できます。ただし、推奨されません。組織のすべての機能を後に有効にする場合はこのロールが必要になるため、復元する必要があります。次のチェックは、すべての機能を有効にするプロセスを開始するときに実行されます。

- 組織に参加するように招待された各メンバーアカウント - アカウント管理者には、すべての機能を有効にすることへの同意を求めるリクエストが送信されます。サービスにリンクされたロール (AWSServiceRoleForOrganizations) が存在しない場合に適切にリクエストに同意するには、organizations:AcceptHandshake 許可および iam:CreateServiceLinkedRole 許可の両方がアカウント管理者に必要です。AWSServiceRoleForOrganizations ロールが既に存在する場合、管理者がリクエストに同意するには、organizations:AcceptHandshake アクセス権限のみが管理者に必要です。管理者がリクエストに同意すると、サービスにリンクされたロールがまだ存在しない場合、 AWS Organizations によって作成されます。

- 組織に作成された各メンバーアカウント - サービスにリンクされたロールの再作成リクエストがアカウント管理者に送信されます。(メンバーアカウントの管理者には、すべての機能を有効にするリクエストが届きません。これは、管理アカウント (旧称は「マスターアカウント」) の管理者が、作成されたメンバーアカウントの所有者と見なされるためです)。サービスにリンクされたロールは、メンバーアカウント管理者がリクエストに同意すると AWS Organizations によって作成されます。ハンドシェイクを適切に承諾するには、`organizations:AcceptHandshake` アクセス権限と `iam:CreateServiceLinkedRole` アクセス権限の両方が管理者に必要です。

組織内のすべての機能を有効にすると、サービスにリンクされたロール `AWSServiceRoleForOrganizations` はどのアカウントからも削除できなくなります。

> **Important**
>
> AWS Organizations SCPsサービスにリンクされたロールに影響を与えることはありません。これらのロールは、SCP 制限の対象外であるためです。

AWSServiceRoleForDeclarativePoliciesEC2Report サービスにリンクされたロールの使用

サービスにリンクされたロールは、Organizations `AWSServiceRoleForDeclarativePoliciesEC2Report`がメンバーアカウントのアカウント属性の状態を記述して宣言ポリシーレポートを作成するために使用されます。ロールのアクセス許可は、で定義されていますAWS 管理ポリシー: DeclarativePoliciesEC2Report。

AWS のサービス で使用できる AWS Organizations

AWS Organizations では、複数の を 1 つの組織に統合することで、アカウント管理アクティビティを大規模 AWS アカウント に実行できます。アカウントを統合すると、他のアカウントの使用方法が簡素化されます AWS のサービス。Select AWS Organizations で で使用できるマルチアカウント管理サービスを活用して AWS のサービス 、組織のメンバーであるすべてのアカウントでタスクを実行できます。

次の表に、 で使用できる AWS のサービス と AWS Organizations、組織全体レベルで各サービスを使用する利点を示します。

信頼されたアクセス – 互換性のある AWS サービスを有効にして、組織内のすべての AWS アカウント でオペレーションを実行できます。詳細については、「を他の AWS Organizations で使用する AWS のサービス」を参照してください。

の委任管理者 AWS のサービス – 互換性のある AWS サービスは、組織内の AWS メンバーアカウントを、そのサービス内の組織のアカウントの管理者として登録できます。詳細については、「Organizations と連携 AWS のサービス する の委任管理者」を参照してください。

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS アカウント管理 AWS アカウント 組織のすべての の詳細とメタデータを管理します。	組織 AWS アカウント 内のすべてのアカウントの詳細、代替連絡先、リージョンを管理します。	 はい 詳細はこちら	 はい 詳細はこちら	
AWS Application Migration Service AWS Application Migration Service を使用すると、企業は互換性の問題、パフォーマンスの中断、または長い	複数のアカウントにわたる、大規模な移行を管理できます。	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
カットオーバーウィンドウなしに、AWS 多数の物理サーバー、仮想サーバー、またはクラウドサーバーにlift-and-shiftできます。				
AWS Artifact ISO レポートや PCI レポートなどの AWS セキュリティコンプライアンスレポートをダウンロードします。	契約を組織内のすべてのアカウントに代わって受諾できます。	 はい 詳細はこちら	 いえ	い

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Audit Manager クラウドサービスの使用の監査に役立てられるよう、エビデンスの継続的な収集を自動化します。	組織内の複数のアカウントで AWS 使用を継続的に監査し、リスクとコンプライアンスの評価方法を簡素化します。	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Backup 組織内のすべてのアカウントのバックアップを管理およびモニタリングします。	組織全体、または組織単位 (OU) におけるアカウントのグループのバックアッププランを設定および管理できます。すべてのアカウントのバックアップを一元的にモニタリングできます。	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Billing and Cost Management AWS クラウド財務管理データの概要と、より迅速で情報に基づいた意思決定に役立ちます。	該当する場合は、分割コスト配分データによる AWS Organizations 情報の取得と、オプトインした分割コスト配分データサービスのテレメトリデータの収集を許可します。 詳細については、「 Billing and Cost Management ユーザーガイド」の「What is AWS Billing	 はい 詳細はこちら	 いえ	い

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
	and Cost Management?」を参照してください。			
AWS CloudFormation スタック・セット 1 回の操作で、複数のアカウントとリージョンにまたがるスタックを作成、更新、または削除できます。	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、組織内のアカウントにスタックインスタンスを配備する、サービスによって管理されたアクセス許可を持つスタックセットを作成できます。	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS CloudTrail アカウントのガバナンス、コンプライアンス、および運用とリスクの監査を実行できます。	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、組織のアカウントに関するすべてのイベントを口グに記録するイベントデータストアまたは組織の証跡を作成できます。	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
Amazon CloudWatch AWS リソースと で実行しているアプリケーションを AWS リアルタイムでモニタリングします。CloudWatch を使用して、リソースとアプリケーションに対して測定できる変数であるメトリクスを収集および追跡できます。	Organizations との統合には、CloudWatch で 2 つの利点があります。まず、Organizations と統合することで、CloudWatch を使用してCloudWatch コンソールの中央ビューから AWS リソースのテレメトリ設定の状態を検出して理解できます。	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
	次に、CloudWatch で Network Flow Monitor を使用してネットワークパフォーマンスメトリクスを可視化できる場合、Organizations と統合することで、1 つのアカウントだけでなく、複数のアカウントのリソースのネットワークパフォーマンス情報を表			

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
	示できます。			
AWS Compute Optimizer AWS コンピューティング最適化の推奨事項を取得します。	組織のアカウントにあるすべてのリソースを分析して、最適化の推奨事項を取得できます。 詳細については、AWS Compute Optimizer ユーザーガイドの Compute Optimizer によってサポートされるアカウントを参照してください。	 はい 詳細はこちら	 はい 詳細はこちら	は

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Config AWS リソースの設定を診断、監査、評価します。	コンプライアンスステータスに関する組織全体のビューを取得できます。AWS Config API オペレーションを使用して、組織内のすべての AWS アカウントで AWS Config ルールとコンフォーマンスパックを管理することもできます。	 はい 詳細はこちら	 はい 詳細はこちら: 設定 ルール コンフォーマンスパック マルチアカウント、マルチリージョンのデータ集計	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
	委任管理者アカウントを使用し、 AWS Organizationsの組織のメンバーアカウント全体を対象に、リソース構成とコンプライアンス・データを集約できます。詳細については、 AWS Config デベロッパーガイドの委任された管理者の登録を参照			

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
	してください。			

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Control Tower 基準に準拠した安全な AWS マルチアカウント環境をセットアップして管理します。	すべての AWS リソースのマルチアカウント環境であるランディングゾーンを設定できます。この環境には、組織および組織のエンティーティが含まれています。この環境を使用して、すべての にコンプライアンス規制を適用できます AWS アカウント。	 はい 詳細はこちら	 いえ	い

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
	詳細については、AWS Control Tower ユーザーガイドのAWS Control Towerの仕組みおよびAWS Organizations によるアカウントの管理を参照してください。			

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Cost Optimization Hub AWS 最適化製品全体でコストに関する推奨事項を収集します。	AWS Organizations メンバーアカウントと AWS リージョン全体で、AWS コスト最適化の推奨事項を簡単に特定、フィルタリング、集計できます。 詳細については、「Cost Optimization Hub user guide」の「Cost Optimization Hub」を参照し	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
	てください。			
Amazon Detective ログデータから可視化を生成して、セキュリティに関する検出結果や疑わしいアクティビティの根本原因の分析、調査、および迅速な特定を行います。	Amazon Detective を と統合 AWS Organizations することで、Detective 動作グラフがすべての組織アカウントのアクティビティを可視化できます。	 はい 詳細はこちら	 はい 詳細はこちら	は

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
Amazon DevOps Guru 運用データとアプリケーションのメトリクスおよびイベントを分析し、通常の運用パターンから逸脱する動作を特定します。DevOps Guru が運用上の問題またはリスクを検出すると、ユーザーに通知されます。	を と統合 AWS Organizations して、組織全体のすべてのアカウントからのインサイトを管理できます。管理者を委任すると、すべてのアカウントから取得したインサイトを表示、ソート、およびフィルタリングし、すべての監視対象アプリケーションの組織全体	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
	の健全性を取得できます。			
AWS Directory Service AWS クラウドでディレクトリをセットアップして実行するか、リソースを AWS 既存のオンプレミス Microsoft Active Directory に接続します。	AWS Directory Service を と統合 AWS Organizations して、リージョン内の複数のアカウントと任意の VPC 間でディレクトリをシームレスに共有できます。	 はい 詳細はこちら	 いえ	い

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
Amazon EventBridge AWS リソースと で実行しているアプリケーションを AWS リアルタイムでモニタリングします。	組織のすべてのアカウント間で、すべての Amazon EventBridge (旧 Amazon CloudWatch Events) の共有を有効にできます。 詳細については、Amazon EventBridge ユーザーガイドの「AWS アカウント間での Amazon EventBridge イベントの送受信」を参	 いいえ	 いいえ	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
	照してください。			
Amazon Elastic Compute Cloud Amazon VPC IP Address Manager (IPAM) は、AWS クラウドでオンデマンドでスケーラブルなコンピューティング容量を提供します。	Organizations 管理者が宣言ポリシー機能を使用する際に、組織全体のアカウントの既存の設定に関するレポートを作成できるようにします。	 はい 詳細はこちら	 いえ	い

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
Amazon Elastic Kubernetes Service Amazon EKS Dashboard は、 AWS クラウド全体の Kubernetes クラスターの集約された可視性と管理を提供します。	Organizations 管理者が、組織全体のバージョンディストリビューション、ヘルスステータス、アップグレード要件など、クラスターリソースに関する統合ダッシュボードデータを表示できるようにします。	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Firewall Manager アカウントやアプリケーション間でウェブアプリケーションのファイアウォールルールを一元的に設定、管理します。	組織内のアカウント全体で AWS WAF ルールを一元的に設定および管理できます。	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
Amazon GuardDuty GuardDuty は、さまざまなデータソースからの情報を分析および処理する継続的セキュリティモニタリングサービスです。脅威インテリジェンスフィードおよび機械学習を使用して、AWS 環境内の予期しないアクティビティ、不正の可能性があるアクティビティ、悪意のあるアクティビティを識別します。	組織内のすべてのアカウントに対して、GuardDuty を確認および管理するメンバーアカウントを指定できます。メンバーアカウントを追加すると、選択したのアカウントの GuardDuty が自動的に有効になります AWS リージョン。また、組織に追加された新しいア	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
	カウントに対して GuardDuty のアクティベーションを自動化することもできます。 詳細については、Amazon GuardDuty ユーザーガイドの GuardDuty and Organizations を参照してください。			

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Health リソースのパフォーマンスに影響する可能性のあるイベントや、AWS のサービスの可用性に関する問題を可視化します。	組織内のアカウント間で AWS Health イベントを集約できます。	はい 詳細はこちら	はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Identity and Access Management AWS リソースへのアクセスを安全に制御します。	IAM のサービスの最後にアクセスされたデータを使用することで、組織全体の AWS アクティビティをより詳しく把握できます。このデータを使用してサービスコントロールポリシー (SCP) を作成、更新し、組織のアカウントが使用する AWS サービスだけにアクセ	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
	スを限定することができます。 設定例については、IAM ユーザーガイドの情報を使用した組織単位のアクセス許可の調整を参照してください。 IAM ルートアクセス管理を使用すると、ルートユーザーの認証情報を一元管理し、メンバーア			

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
	カウントで特権タスクを実行できます。			
IAM Access Analyzer AWS 環境内のリソースベースのポリシーを分析して、信頼ゾーン外のプリンシパルにアクセスを許可するポリシーを特定します。	IAM Access Analyzer の管理者には、メンバーアカウントを指定できます。 詳細については、IAM ユーザーガイド の Access Analyzer の有効化を参照してください。	 はい 詳細はこちら	 はい 詳細はこちら	は

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
Amazon Inspector AWS ワークロードの脆弱性を自動的にスキャンして、Amazon ECR に存在する Amazon EC2 インスタンスとコンテナイメージを検出し、ソフトウェアの脆弱性と意図しないネットワークへの露出を検出します。	管理者を委任することで、メンバーアカウントのスキャンの有効化または無効化、組織全体の集約された調査結果データの表示、抑制ルールの作成および管理などが可能になります。 詳細については、「Amazon Inspector ユーザーガイド」の「AWS Organizat	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
	ionsで複数のアカウントを管理する」を参照してください。			
AWS License Manager ソフトウェアライセンスをクラウドに移動するプロセスを効率化します。	組織全体でコンピューティングリソースのクロスアカウントの検出を有効にすることができます。	 はい 詳細はこちら	 はい 詳細はこちら	は

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
Amazon Macie 機械学習を使用してビジネスクリティカルなコンテンツを検出および分類し、データのセキュリティとプライバシーの要件を満たすのに役立ちます。Amazon S3 に保存されているコンテンツを継続的に評価し、潜在的な問題があれば通知します。	組織内のすべてのアカウントに対して Amazon Macie を設定し、指定された Macie 管理者アカウントのすべてのアカウントで、Amazon S3 のすべてのデータを一括表示することができます。組織の成長に合わせて新しいアカウントのリソースを自動的に保護す	 はい 詳細はこちら	 はい 詳細はこちら	は

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
	るように Macie を設定できます。組織全体の S3 バケット間でポリシーの設定ミスを修正するよう求めるアラートが生成されます。			

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Managed Services (AMS) セルフサービスレポート (SSR) さまざまなネイティブ AWS サービスからデータを収集し、主要な AMS サービスに関するレポートへのアクセスを提供します。SSR は、オペレーション、設定管理、アセット管理、セキュリティ管理、コンプライアンスをサポートするために使用できる情報を提供します。	集約 SSR を有効にできます。これは、顧客が管理アカウントまたは委任された管理者アカウントを通じて組織全体の統合セルフサービスレポートを表示できるようにする機能です。	はい 詳細はこちら	はい 詳細はこちら	はい

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Marketplace 厳選されたデジタルカタログで、ここからサードパーティーのソフトウェア、データ、サービスを検索、購入、配置、管理し、ソリューションの構築やビジネス運営に活用することができます。	AWS Marketplace サブスクリプションと購入のライセンスは、組織内のアカウント間で共有できます。	 はい 詳細はこちら	 いえ	い

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Marketplace プライベートマーケットプレイス で利用可能な製品の幅広いカタログと AWS Marketplace、それらの製品のきめ細かな制御を提供します。	組織全体、一つ以上の OU、または、組織内の 1 つ以上のアカウントに関連付けられた 1 つ以上のプライベートマーケットプレイスエクスペリエンスを作成し、それぞれに独自の承認済み製品セットを設定できます。AWS 管理者は、会社またはチームのロゴ、	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
	メッセージング、カラースキームを使用して、各プライベートマーケットプレイスエクスペリエンスに会社のブランドを適用することもできます。			

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Marketplace 調達インサイトダッシュボード 組織内の AWS アカウント全体のすべての AWS Marketplace 購入の契約とコスト分析データを表示できます。	AWS Marketplace 調達インサイトダッシュボードは、組織に参加するアカウントなどの組織の変更を聞き、対応する契約のデータを集約してダッシュボードを構築します。	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Network Manager AWS アカウント、リージョン、オンプレミスロケーション間で AWS Cloud WAN コアネットワークと AWS Transit Gateway ネットワークを一元管理できます。	組織内の複数の AWS アカウントのトランジットゲートウェイとそのアタッチされたリソースを使用して、グローバルネットワークを一元管理およびモニタリングできます。	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
Amazon Q Developer Amazon Q Developer は、生成 AI を活用した会話アシスタントであり、 AWS アプリケーションの理解、構築、拡張、運用に役立ちます。	Amazon Q Developer の有料サブスクリプションバージョンには、Organizations の統合が必要です。	 はい 詳細はこちら	 いえ	い

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Resource Access Manager 所有している指定された AWS リソースを他のアカウントと共有します。	組織内で、追加の招待を交換することなくリソースを共有できます。共有できるリソースには、Route 53 リゾルバーのルール、オンデマンドキャパシティーの予約などがあります。 キャパシティ予約の共有については、「Amazon EC2 ユーザーガ	 はい 詳細はこちら	 いえ	い

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
	イド」または「Amazon EC2 ユーザーガイド」を参照してください。 共有可能なリソースの一覧については、AWS RAM ユーザーガイドの共有可能なリソースを参照してください。			

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Resource Explorer インターネット検索エンジンのようなエクスペリエンスを使用してリソースを調べます。	マルチアカウント検索を有効にします。	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Security Hub でセキュリティ状態を表示 AWS し、セキュリティ業界標準とベストプラクティスに照らして環境を確認します。	Security Hub は、追加した新しいアカウントを含む組織のすべてのアカウントに対し、自動的に有効にすることができます。これにより、Security Hub のチェックと検出がより広範囲に行えるようになり、セキュリティ体制の全体像をより正確に把握できます。	 はい 詳細はこちら	 はい 詳細はこちら	はい

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
Amazon S3 Storage Lens Amazon S3 ストレージの使用状況とアクティビティに関するメトリクスを可視化し、ストレージを最適化する実用的な推奨事項を提供します。	Amazon S3 Storage Lens を設定することで、Amazon S3 ストレージの使用状況とアクティビティの傾向を可視化するとともに、組織のすべてのメンバーアカウントに向けた推奨事項を取得することが可能になります。	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS セキュリティインシデント対応 AWS セキュリティサービスは、お客様が認証情報の盗難やランサムウェア攻撃などのサイバーセキュリティインシデントに迅速に対応できるように、24 時間 365 日ライブでヒューマンアシストされたセキュリティインシデントサポートを提供します。	組織全体のセキュリティカバレッジ。	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
Amazon Security Lake Amazon Security Lake は、クラウド、オンプレミス、カスタムソースのセキュリティデータを、アカウントに保存されているデータレイクに一元化します。	アカウント全体からログとイベントを収集するデータレイクを作成します。	はい 詳細はこちら	はい 詳細はこちら	は
AWS Service Catalog AWSでの使用が承認されたIT サービスのカタログを作成および管理します。	ポートフォリオ ID を共有することなく、アカウント間でより簡単にポートフォリオの共有と製品のコピーができます。	はい 詳細はこちら	はい 詳細はこちら	は

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
Service Quotas 一元的な場所から、サービスクォータ (制限とも呼ばれます) を表示および管理します。	クォータリクエストテンプレートを作成して、組織のアカウントの作成時に自動的にクォータの引き上げをリクエストできます。	 はい 詳細はこちら	 いえ	い

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS IAM Identity Center すべてのアカウントとクラウドアプリケーションに対してシングルサインオンサービスを提供します。	ユーザーは、企業の認証情報を使用して AWS アクセスポータルにサインインし、割り当てられた管理アカウントまたはメンバーアカウントのリソースにアクセスできます。	はい 詳細はこちら	はい 詳細はこちら	は

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Systems Manager AWS リソースの可視性と制御を有効にします。	Systems Manager Explorer を使用して、組織内のすべての AWS アカウント でオペレーションデータを同期できます。 また、Systems Manager Change Manager を使用すれば、委任管理者アカウントから、組織内のすべてのメンバーアカウントを対象に、変更	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
	のテンプレート、承認、レポート作成を管理できます。			
AWS User Notifications AWS 通知の中心的な場所。	通知は、組織内のアカウント間で一元的に設定および表示できます。	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
タグポリシー 組織のアカウントのリソース間でタグを標準化するのに役立ちます。	タグポリシーを作成して特定のリソースおよびリソースタイプのタグ付けルールを定義し、そのポリシーを組織とアカウントにアタッチして適用できます。	 はい 詳細はこちら	 いえ	い

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Trusted Advisor Trusted Advisor は AWS 環境を検査し、コスト削減、システムの可用性とパフォーマンスの向上、セキュリティギャップの解消に役立つ機会が存在する場合にレコメンデーションを行います。	組織 AWS アカウント 内のすべての の Trusted Advisor チェックを実行します。	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
AWS Well-Architected Tool AWS Well-Architected Tool は、ワークロードの状態を文書化し、最新の AWS アーキテクチャのベストプラクティスと比較するのに役立ちます。	AWS WA Tool と Organizations の両方のお客様が、組織の他のメンバーと AWS WA Tool リソースを共有するプロセスを簡素化できるようにします。	 はい 詳細はこちら	 いえ	い

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
Amazon VPC IP Address Manager (IPAM) IPAM は、AWS ワークロードの IP アドレスの計画、追跡、モニタリングを容易にする VPC 機能です。	組織全体の IP アドレスの使用状況をモニタリングし、メンバーアカウント間で IP アドレスプールを共有します。	 はい 詳細はこちら	 はい 詳細はこちら	

AWS サービス	で を使用する利点 AWS Organizations	信頼されたアクセスをサポート	委任管理者をサポート	
Amazon VPC Reachability Analyzer Reachability Analyzer は、仮想プライベートクラウド (VPC) 内のソースリソースと送信先リソース間の接続テストを実行できるようにする設定分析ツールです。	組織内のアカウント間のパスを追跡できます。	 はい 詳細はこちら	 はい 詳細はこちら	

AWS アカウント管理 および AWS Organizations

AWS アカウント管理 は、組織 AWS アカウント 内のすべての のアカウント情報とメタデータを管理するのに役立ちます。組織の各メンバーアカウントの代替連絡先情報を設定、変更、または削除できます。詳細については、AWS アカウント管理 ユーザーガイドの「組織で AWS アカウント管理 を使用する」を参照してください。

次の情報は、 AWS アカウント管理 との統合に役立ちます AWS Organizations。

Account Management で信頼されたアクセスを有効にするには

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

アカウント管理では、メンバーアカウントを組織のこのサービスの委任管理者に指定 AWS Organizations する前に、 への信頼されたアクセスが必要です。

信頼されたアクセスは、Organizations ツールを使用してのみ有効にできます。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・ インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [AWS 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. 「 の信頼されたアクセスを有効にする AWS アカウント管理」ダイアログボックスで、「確認のために を有効にする」と入力し、「信頼されたアクセスを有効にする」を選択します。
6. の管理者のみである場合は AWS Organizations、 の管理者に、サービスコンソール からそのサービスが と AWS Organizations 連携できるようになった AWS アカウント管理 ことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS アカウント管理 としてを有効にします。

```
$ aws organizations enable-aws-service-access \
    --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。

- AWS API: EnableAWSServiceAccess

Account Management で信頼されたアクセスを無効にするには

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

で信頼されたアクセスを無効にすることができるのは、 AWS Organizations 管理アカウントの管理者のみです AWS アカウント管理。

信頼されたアクセスは、Organizations ツールを使用してのみ無効にできます。

信頼されたアクセスを無効にするには、 AWS Organizations コンソールを使用するか、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを無効にするには

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 アカウント管理] を選択します。
4. Disable trusted access (信頼されたアクセスを無効にする) を選択します。
5. 「 の信頼されたアクセスを無効にする AWS アカウント管理」ダイアログボックスで、「無効にして確認」と入力し、「信頼されたアクセスを無効にする」を選択します。
6. の管理者のみの場合は AWS Organizations、 の管理者 AWS アカウント管理 に、サービスコンソールまたはツール を使用して、そのサービスが で AWS Organizations 動作することを無効にできることを伝えます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを無効にすることができます。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS アカウント管理 としてを無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --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。

- AWS API: DisableAWSServiceAccess

Account Management 用の委任管理者アカウントの有効化

メンバーアカウントを組織の委任管理者として指定すると、指定されたアカウントのユーザーおよびロールは組織のその他のメンバーアカウントの AWS アカウント メタデータを管理できるようになります。委任された管理者アカウントを有効にしない場合、これらのタスクは組織の管理アカウントによってのみ実行できます。この手法は、組織の管理からアカウントの詳細の管理を分離するのに有効です。

> **最小アクセス許可**
>
> Organizations 管理アカウントのユーザーまたはロールのみが、組織内で Account Management の委任管理者としてメンバーアカウントを設定できます

委任ポリシーを設定する方法については、「を使用してリソースベースの委任ポリシーを作成する AWS Organizations」を参照してください。

AWS CLI, AWS API

CLI またはいずれかの AWS SDKs を使用して AWS 委任管理者アカウントを設定する場合は、次のコマンドを使用できます。

- AWS CLI:

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

- AWS SDK: Organizations `RegisterDelegatedAdministrator`オペレーションとメンバーアカウントの ID 番号を呼び出し、アカウントサービスプリンシパルをパラメータ`account.amazonaws.com`として識別します。

AWS Application Migration Service（ アプリケーション移行サービス) および AWS Organizations

AWS Application Migration Service は、 へのアプリケーションの移行を簡素化、迅速化し、コストを削減します AWS。Organizations と統合することで、グローバルビュー機能を使用して複数のアカウントにまたがる大規模な移行を管理できます。詳細については、「Application Migration Service user guide」の「Setting up your AWS Organizations」を参照してください。

次の情報は、 AWS Application Migration Service との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、Application Migration Service はサポートされているオペレーションを組織内のアカウントで実行できます。

このロールを削除または変更できるのは、Application Migration Service と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleForApplicationMigrationService`

Application Migration Service で使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。Application Migration Service によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `mgn.amazonaws.com`

Application Migration Service による信頼されたアクセスの有効化

Application Migration Service で信頼されたアクセスを有効にすると、グローバルビュー機能を使用できます。これにより、複数のアカウントにまたがる大規模な移行を管理できます。グローバ

ルビューは、さまざまな AWS アカウントのソースサーバー、アプリ、ウェーブに対して特定のアクションを実行するための可視性と機能を提供します。詳細については、「 AWS Application Migration Service ユーザーガイド」のAWS 「Organizations のセットアップ」を参照してください。

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、 AWS Application Migration Service コンソールまたは AWS Organizations コンソールを使用して有効にできます。

> **Important**
>
> 可能な限り、 AWS Application Migration Service コンソールまたはツールを使用して Organizations との統合を有効にすることを強くお勧めします。これにより、 は、サービスに必要なリソースの作成など、必要な設定 AWS Application Migration Service を実行できます。ここに示す手順は、統合の有効化に AWS Application Migration Serviceが提供するツールを使用できない場合にのみ実施してください。詳細については、この注意を参照してください。
>
> AWS Application Migration Service コンソールまたはツールを使用して信頼されたアクセスを有効にする場合、これらのステップを実行する必要はありません。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・ インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [AWS Application Migration Service] 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. 「 の信頼されたアクセスを有効にする AWS Application Migration Service」ダイアログボックスで、「確認のために を有効にする」と入力し、「信頼されたアクセスを有効にする」を選択します。

6. の管理者のみである場合は AWS Organizations、 の管理者に、そのサービスがサービスコンソール から と AWS Organizations 連携できるようになった AWS Application Migration Service ことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Application Migration Service として を有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal mgn.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。
- AWS API: EnableAWSServiceAccess

Application Migration Service による信頼されたアクセスの無効化

Application Migration Service との信頼されたアクセスを無効にできるのは、Organizations の管理アカウントの管理者だけです。

信頼されたアクセスは、 AWS Application Migration Service または AWS Organizations ツールを使用して無効にできます。

> **Important**
>
> 可能な限り、 AWS Application Migration Service コンソールまたはツールを使用して Organizations との統合を無効にすることを強くお勧めします。これにより、 は、サービスで不要になったリソースやアクセスロールの削除など、必要なクリーンアップ AWS Application Migration Service を実行できます。ここに示す手順は、統合の無効化に AWS Application Migration Serviceが提供するツールを使用できない場合にのみ実施してください。

AWS Application Migration Service コンソールまたはツールを使用して信頼されたアクセスを無効にする場合は、これらのステップを実行する必要はありません。

信頼されたアクセスを無効にするには、 AWS Organizations コンソールを使用するか、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを無効にするには

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 Application Migration Service] を選択します。
4. Disable trusted access (信頼されたアクセスを無効にする) を選択します。
5. 「 の信頼されたアクセスを無効にする AWS Application Migration Service」ダイアログボックスで、「無効にして確認」と入力し、「信頼されたアクセスを無効にする」を選択します。
6. の管理者のみの場合は AWS Organizations、 の管理者 AWS Application Migration Service に、サービスコンソールまたはツール を使用して、そのサービスが で AWS Organizations 動作することを無効にできることを伝えます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを無効にすることができます。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Application Migration Service として を無効にします。

```
$ aws organizations disable-aws-service-access \
    --service-principal mgn.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。

- AWS API: DisableAWSServiceAccess

Application Migration Service の委任管理者アカウントの有効化

メンバーアカウントを組織の委任管理者として指定すると、そのアカウントのユーザーおよびロールは、Application Migration Service の管理アクションを実行できるようになります。通常この管理アクションは、組織の管理アカウントのユーザーとロールだけが実行できるものです。この手法は、Application Migration Service の管理から組織の管理を分離するのに有効です。詳細については、「Application Migration Service user guide」の「Setting up your AWS Organizations」を参照してください。

> **最小アクセス許可**
>
> Organizations 管理アカウントのユーザーまたはロールのみが、組織内で Application Migration Service の委任管理者としてメンバーアカウントを設定できます

AWS CLI, AWS API

CLI またはいずれかの AWS SDKs を使用して AWS 委任管理者アカウントを設定する場合は、次のコマンドを使用できます。

- AWS CLI:

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

- AWS SDK: Organizations `RegisterDelegatedAdministrator`オペレーションとメンバーアカウントの ID 番号を呼び出し、アカウントサービスをパラメータ`mgn.amazonaws.com`として識別します。

Application Migration Service の委任管理者の無効化

Application Migration Service の委任管理者を削除できるのは、Organizations 管理アカウントの管理者だけです。Organizations の `DeregisterDelegatedAdministrator` CLI または SDK オペレーションを使用して、委任された管理者を削除できます。

AWS Artifact および AWS Organizations

AWS Artifact は、ISO レポートや PCI レポートなどの AWS セキュリティコンプライアンスレポートをダウンロードできるサービスです。を使用すると AWS Artifact、組織の管理アカウントのユーザーは、新しいレポートやアカウントが追加されても、組織内のすべてのメンバーアカウントに代わって契約を自動的に受諾できます。メンバーアカウントのユーザーは、契約を表示および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 での複数のアカウントの契約の管理」を参照してください。

次の情報は、 AWS Artifact との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより AWS Artifact 、 はサポートされているオペレーションを組織内のアカウント内で実行できます。

このロールを削除または変更できるのは、 AWS Artifact と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

組織からメンバーアカウントを削除すると、このロールを削除または変更できますが、お勧めしません。

サービス間での混乱した代理などのセキュリティ上の問題を引き起こす可能性があるため、ロールの変更は推奨されません。混乱した使節に対する保護の詳細については、「AWS Artifact ユーザーガイド」の「Cross-service deputy prevention」(サービス間での使節の防止) を参照してください。

- `AWSServiceRoleForArtifact`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。で使用されるサービスにリンクされたロールは、次のサービスプリンシパルへのアクセス AWS Artifact を許可します。

- `artifact.amazonaws.com`

AWS Artifactとの信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、Organizations ツールを使用してのみ有効にできます。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・ インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [AWS Artifact] 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. 「信頼されたアクセスを有効にする AWS Artifact」ダイアログボックスで、「確認のためにを有効にする」と入力し、「信頼されたアクセスを有効にする」を選択します。
6. の管理者のみである場合は AWS Organizations、 の管理者に、そのサービスがサービスコンソール から と AWS Organizations 連携できるようになった AWS Artifact ことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Artifact として を有効にします。

```
$ aws organizations enable-aws-service-access \
```

```
    --service-principal artifact.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。

- AWS API: EnableAWSServiceAccess

AWS Artifactとの信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

で信頼されたアクセスを無効にすることができるのは、 AWS Organizations 管理アカウントの管理者のみです AWS Artifact。

信頼されたアクセスを無効にするには、Organizations ツールを使用する必要があります。

AWS Artifact では、組織契約を使用するために AWS Organizations との信頼されたアクセスが必要です。組織契約 AWS Artifact で を使用している AWS Organizations ときに を使用して信頼されたアクセスを無効にすると、組織にアクセスできないため、機能しなくなります。で受諾した組織契約は AWS Artifact 残りますが、 からはアクセスできません AWS Artifact。が AWS Artifact 作成する AWS Artifact ロールは残ります。その後、信頼されたアクセスを再度有効にすると、 AWS Artifact は以前のように動作し続けます。サービスを再設定する必要はありません。

スタンドアロンアカウントは組織から削除され、組織契約にアクセスできなくなります。

信頼されたアクセスを無効にするには、 AWS Organizations コンソールを使用するか、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを無効にするには

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 Artifact] を選択します。
4. Disable trusted access (信頼されたアクセスを無効にする) を選択します。
5. 「 の信頼されたアクセスを無効にする AWS Artifact」ダイアログボックスで、「無効化」と入力して確認し、「信頼されたアクセスを無効にする」を選択します。

6. の管理者のみの場合は AWS Organizations、 の管理者 AWS Artifact に、サービスコンソールまたはツール を使用して、そのサービスが で AWS Organizations 動作することを無効にできることを伝えます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを無効にすることができます。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Artifact として を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal artifact.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。

- AWS API: DisableAWSServiceAccess

AWS Audit Manager および AWS Organizations

AWS Audit Manager は、 AWS 使用状況を継続的に監査し、リスクと規制や業界標準への準拠を評価する方法を簡素化するのに役立ちます。Audit Manager はエビデンスの収集を自動化するため、ポリシー、手順、アクティビティが効果的に機能しているかどうかの評価が容易になります。監査が実施される際には、Audit Manager を使用し、コントロールについてのステークホルダーレビューを管理できます。また、監査用のレポートの作成に費やす手間を大幅に削減できます。

Audit Manager を と統合すると AWS Organizations、評価の範囲内に組織の複数の を含めることで、より広範なソース AWS アカウント から証拠を収集できます。

詳細については、「Audit Manager ユーザーガイド」の AWS 「組織を有効にする」を参照してください。

次の情報は、 AWS Audit Manager との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、Audit Manager はサポートされているオペレーションを組織内のアカウントで実行できます。

このロールを削除または変更できるのは、Audit Manager と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合です。

Audit Manager でこのロールを使用する方法について詳しくは、AWS Audit Manager ユーザーガイドの Using service-linked roles を参照してください。

- `AWSServiceRoleForAuditManager`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。Audit Manager によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `auditmanager.amazonaws.com`

Audit Manager との信頼されたアクセスを有効にするには

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

Audit Manager では、メンバーアカウントを組織の委任管理者として指定 AWS Organizations する前に、 への信頼されたアクセスが必要です。

信頼されたアクセスは、 AWS Audit Manager コンソールまたは AWS Organizations コンソールを使用して有効にできます。

> **Important**
>
> 可能な限り、 AWS Audit Manager コンソールまたはツールを使用して Organizations との統合を有効にすることを強くお勧めします。これにより、 は、サービスに必要なリソースの作成など、必要な設定 AWS Audit Manager を実行できます。ここに示す手順は、統合の有効

化に AWS Audit Managerが提供するツールを使用できない場合にのみ実施してください。詳細については、この注意を参照してください。
AWS Audit Manager コンソールまたはツールを使用して信頼されたアクセスを有効にする場合、これらのステップを実行する必要はありません。

Audit Manager コンソールを使用して信頼されたアクセスを有効にするには

信頼されたアクセスを有効にする手順については、AWS Audit Manager ユーザーガイドのセットアップを参照してください。

> **Note**
>
> AWS Audit Manager コンソールを使用して委任管理者を設定すると、 によって信頼されたアクセス AWS Audit Manager が自動的に有効になります。

信頼されたアクセスを有効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Audit Manager として を有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal auditmanager.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。

- AWS API: EnableAWSServiceAccess

Audit Manager との信頼されたアクセスを無効にするには

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

で信頼されたアクセスを無効にすることができるのは、 AWS Organizations 管理アカウントの管理者のみです AWS Audit Manager。

信頼されたアクセスを無効にするには、Organizations ツールを使用する必要があります。

信頼されたアクセスを無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Audit Manager として を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal auditmanager.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。

- AWS API: DisableAWSServiceAccess

Audit Manager 用の委任管理者アカウントの有効化

メンバーアカウントを組織の委任管理者として指定すると、そのアカウントのユーザーおよびロールは、Audit Manager の管理アクションを実行できるようになります。通常この管理アクションは、組織の管理アカウントのユーザーとロールだけが実行できるものです。この手法は、組織の管理から Audit Manager の管理を分離するのに有効です。

> **最小アクセス許可**
>
> 次の許可を持つ Organizations 管理アカウントのユーザーまたはロールのみが、組織内で Audit Manager の委任管理者としてメンバーアカウントを設定できます。`audit-manager:RegisterAccount`

Audit Manager 用に委任管理者アカウントを有効にする手順については、AWS Audit Manager ユーザーガイドのセットアップを参照してください。

AWS Audit Manager コンソールを使用して委任管理者を設定すると、Audit Manager は信頼されたアクセスを自動的に有効にします。

AWS CLI, AWS API

CLI またはいずれかの AWS SDKs を使用して AWS 委任管理者アカウントを設定する場合は、次のコマンドを使用できます。

- AWS CLI:

```
$  aws audit-manager register-account \
    --delegated-admin-account 123456789012
```

- AWS SDK: `RegisterAccount`オペレーションを呼び出し、管理者アカウントを委任するためのパラメータ`delegatedAdminAccount`として を指定します。

AWS Backup および AWS Organizations

AWS Backup は、組織内の AWS Backup ジョブを管理およびモニタリングできるサービスです。を使用して AWS Backup、組織の管理アカウントのユーザーとしてサインインすると、組織全体のバックアップ保護とモニタリングを有効にできます。バックアップポリシーを使用して、組織内のすべてのアカウントでリソースに AWS Backup プランを一元的に適用することで、コンプライアンスを達成できます。 AWS Backup と の両方を AWS Organizations 一緒に使用すると、次の利点が得られます。

保護

組織でバックアップポリシータイプを有効にし、バックアップポリシーを作成して、組織のルート、OU、またはアカウントにアタッチできます。バックアップポリシーは、 AWS Backup プ

ランと、そのプランをアカウントに自動的に適用するために必要なその他の詳細を組み合わせます。アカウントに直接アタッチされたポリシーは、組織のルートおよび親 OUs から継承されたポリシーとマージされ、アカウントに適用される有効なポリシーが作成されます。ポリシーには、アカウントのリソース AWS Backup で を実行するアクセス許可を持つ IAM ロールの ID が含まれます。 は、有効なポリシーのバックアッププランで指定されているように、IAM ロール AWS Backup を使用してユーザーに代わってバックアップを実行します。

モニタリング

組織で AWS Backupに対して信頼されたアクセスを有効にすると、 AWS Backup コンソールを使用して、組織内の任意のアカウントのバックアップ、復元、およびコピージョブの詳細を表示できます。詳細については、AWS Backup デベロッパーガイドの Monitor your backup jobs を参照してください。

詳細については AWS Backup、「 AWS Backup デベロッパーガイド」を参照してください。

次の情報は、 AWS Backup との統合に役立ちます AWS Organizations。

AWS Backupとの信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、 AWS Backup コンソールまたは AWS Organizations コンソールを使用して有効にできます。

> **Important**
>
> 可能な限り、 AWS Backup コンソールまたはツールを使用して Organizations との統合を有効にすることを強くお勧めします。これにより、 は、サービスに必要なリソースの作成など、必要な設定 AWS Backup を実行できます。ここに示す手順は、統合の有効化に AWS Backupが提供するツールを使用できない場合にのみ実施してください。詳細については、この注意を参照してください。
> AWS Backup コンソールまたはツールを使用して信頼されたアクセスを有効にする場合、これらのステップを実行する必要はありません。

を使用して信頼されたアクセスを有効にするには AWS Backup、「 AWS Backup デベロッパーガイド」の「複数の でバックアップを有効にする AWS アカウント」を参照してください。

AWS Backupとの信頼されたアクセスの無効化

信頼されたアクセスの有効化に必要なアクセス許可に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

AWS Backup では、組織のアカウント全体のバックアップ、復元、コピージョブのモニタリングを可能にする AWS Organizations ために、 との信頼されたアクセスが必要です。信頼されたアクセスを無効にすると AWS Backup、現在のアカウント以外のジョブを表示できなくなります。が AWS Backup 作成する AWS Backup ロールは残ります。後で信頼されたアクセスを再度有効にすると、はサービスを再設定することなく、以前と同じように動作し AWS Backup 続けます。

信頼されたアクセスは、Organizations ツールを使用してのみ無効にできます。

信頼されたアクセスを無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Backup として を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal backup.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。

- AWS API: DisableAWSServiceAccess

の委任管理者アカウントの有効化 AWS Backup

「AWS Backup デベロッパーガイド」の「委任管理者」を参照してください。

AWS Billing and Cost Management および AWS Organizations

AWS Billing and Cost Management には、請求の設定、請求書の取得と支払い、コストの分析、整理、計画、最適化に役立つ一連の機能が用意されています。Billing and Cost Management を で使用する AWS Organizations と、分割コスト配分データで、必要に応じて AWS Organizations 情報を取得し、オプトインした分割コスト配分データサービスのテレメトリデータを収集できます。

次の情報は、 AWS Billing and Cost Management との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、Billing and Cost Management はサポートされているオペレーションを組織内のアカウントで実行できます。

このロールを削除または変更できるのは、Billing and Cost Management と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

詳細については、「Billing and Cost Management ユーザーガイド」の「Service-linked role permissions for Billing and Cost Management」を参照してください。

- `AWSServiceRoleForSplitCostAllocationData`

Billing and Cost Management で使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。Billing and Cost Management によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

Billing and Cost Management は、 `billing-cost-management.amazonaws.com` サービスプリンシパルを使用します。

Billing and Cost Management による信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

管理アカウントを介して信頼されたアクセスを有効にすると、お客様は Billing and Cost Management の分割コスト配分データ機能を利用できます。お客様が Amazon Managed Service for

Prometheus で Amazon Elastic Kubernetes Service の分割コスト配分データを有効にすると、信頼されたアクセスが呼び出され、組織内のすべてのメンバーアカウントに対してサービスにリンクされたロールが作成されます。これにより、分割コスト配分データは、顧客の Amazon Managed Service for Prometheus ワークスペースからテレメトリデータを収集し、それらのメトリクスに基づいてコスト配分を実行できます。

信頼されたアクセスは、Organizations ツールを使用してのみ有効にできます。

信頼されたアクセスを有効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Billing and Cost Management として を有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal  billing-cost-management.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。

- AWS API: EnableAWSServiceAccess

信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスを無効にするには、Organizations ツールを使用する必要があります。

信頼されたアクセスを無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Billing and Cost Management として を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal  billing-cost-management.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。
- AWS API: DisableAWSServiceAccess

AWS CloudFormation StackSets と AWS Organizations

AWS CloudFormation StackSets を使用すると、1 回のオペレーション AWS リージョン で複数の AWS アカウント と にまたがるスタックを作成、更新、または削除できます。StackSets と AWS Organizations の統合により、サービスマネージド型のアクセス許可が付与されたスタックセットの作成が可能になります。これには、各メンバーアカウントの、関連するアクセス許可を持つサービスにリンクされたロールが使用されます。これにより、組織内のメンバーアカウントにスタックインスタンスをデプロイできるようになります。必要な AWS Identity and Access Management ロールを作成する必要はありません。StackSets はユーザーに代わって各メンバーアカウントに IAM ロールを作成します。

また、将来組織に追加されるアカウントへの自動デプロイを有効にすることもできます。自動デプロイを有効にすると、今後その OU に追加されるすべてのアカウントにロールと関連するスタックセットインスタンスのデプロイが自動的に追加されるようになります。

StackSets と Organizations 間の信頼されたアクセスが有効になっていると、管理アカウントには、組織のスタックセットを作成および管理するためのアクセス許可が与えられます。管理アカウントは、委任管理者として最大 5 つのメンバーアカウントを登録できます。信頼されたアクセスが有効になっていると、組織のスタックセットを作成および管理するためのアクセス許可が委任管理者にも付与されます。サービスマネージド型のアクセス許可を持つスタックセットは、委任された管理者によって作成されたスタックセットを含め、管理アカウントに作成されます。

> **Important**
>
> 委任された管理者は、組織内のアカウントにデプロイするための完全なアクセス許可を持っています。管理アカウントでは、特定の OU にデプロイしたり、特定のスタックセットの操作を実行したりする、委任された管理者のアクセス許可を制限することはできません。

StackSets と Organizations の統合の詳細については、 AWS CloudFormation ユーザーガイドのAWS CloudFormation StackSets の使用」を参照してください。

AWS CloudFormation StackSets を と統合するには、次の情報を使用します AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、Stacksets AWS CloudFormation はサポートされているオペレーションを組織内のアカウント内で実行できます。

このロールを削除または変更できるのは、 AWS CloudFormation StackSets と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- 管理アカウント: `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`

サービスにリンクされたロール `AWSServiceRoleForCloudFormationStackSetsOrgMember` を組織内のメンバーアカウントに作成するには、始めに管理アカウントにスタックセットを作成する必要があります。これにより、スタックセットインスタンスが作成され、メンバーアカウントにロールが作成されます。

- メンバーアカウント: `AWSServiceRoleForCloudFormationStackSetsOrgMember`

スタックセットの作成の詳細については、「AWS CloudFormation ユーザーガイド」の「AWS CloudFormation StackSet の操作」を参照してください。

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。 AWS CloudFormation

Stacksets で使用されるサービスにリンクされたロールは、次のサービスプリンシパルへのアクセスを許可します。

- 管理アカウント: `stacksets.cloudformation.amazonaws.com`

  このロールを変更または削除できるのは、StackSets と Organizations 間の信頼されたアクセスを無効にした場合だけです。
- メンバーアカウント: `member.org.stacksets.cloudformation.amazonaws.com`

  アカウントのこのロールを変更または削除できるのは、 StackSets と Organizations 間の信頼されたアクセスが無効になっている場合か、アカウントがターゲット組織または組織単位 (OU) から削除されている場合だけです。

AWS CloudFormation StackSets との信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

Organizations 管理アカウントの管理者のみが、別の AWS サービスで信頼されたアクセスを有効にするアクセス許可を持っています。 AWS CloudFormation コンソールまたは Organizations コンソールを使用して、信頼されたアクセスを有効にできます。

信頼されたアクセスは、 AWS CloudFormation StackSets を使用してのみ有効にできます。

Stacksets コンソールを使用して信頼されたアクセスを有効にするには、 AWS CloudFormation AWS CloudFormation 「 ユーザーガイド」の「 で信頼されたアクセスを有効にする AWS Organizations」を参照してください。

AWS CloudFormation StackSets との信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

Organizations 管理アカウントの管理者のみが、別の AWS サービスでの信頼されたアクセスを無効にするアクセス許可を持っています。信頼されたアクセスの無効化には、Organizations コンソールを使用する必要があります。StackSets の使用中に Organizations との信頼されたアクセスを無効にすると、以前に作成されたすべてのスタックインスタンスが保持されます。ただし、サービスにリンクされたロールのアクセス許可を使用してデプロイされたスタックセットは、Organizations によって管理されるアカウントへのデプロイを実行できなくなります。

信頼されたアクセスは、 AWS CloudFormation コンソールまたは Organizations コンソールを使用して無効にできます。

> **Important**
>
> 信頼されたアクセスをプログラムで (AWS CLI または API などで) 無効にすると、 アクセス許可が削除されることに注意してください。 AWS CloudFormation コンソールで信頼されたアクセスを無効にすることをお勧めします。

信頼されたアクセスを無効にするには、 AWS Organizations コンソールを使用するか、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを無効にするには

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 CloudFormation StackSets] を選択します。
4. Disable trusted access (信頼されたアクセスを無効にする) を選択します。
5. AWS CloudFormation StackSets の信頼されたアクセスを無効にする」ダイアログボックスで、「無効にして確認」と入力し、「信頼されたアクセスを無効にする」を選択します。
6. の管理者のみの場合は AWS Organizations、 AWS CloudFormation StackSets の管理者に、サービスコンソールまたはツール を使用して、そのサービスが で AWS Organizations 動作することを無効にできることを伝えます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを無効にすることができます。

- AWS CLI: disable-aws-service-access

次のコマンドを実行して、 AWS CloudFormation StackSets を Organizations の信頼されたサービスとして無効にします。

```
$ aws organizations disable-aws-service-access \
    --service-principal stacksets.cloudformation.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。

- AWS API: DisableAWSServiceAccess

Stacksets AWS CloudFormation の委任管理者アカウントの有効化

メンバーアカウントを組織の委任管理者として指定すると、そのアカウントのユーザーおよびロールは、 AWS CloudFormation StackSets の管理アクションを実行できるようになります。通常この管理アクションは、組織の管理アカウントのユーザーとロールだけが実行できるものです。これにより、組織の管理と Stacksets AWS CloudFormation の管理を分離できます。

メンバーアカウントを組織の AWS CloudFormation StackSets の委任管理者として指定する手順については、AWS CloudFormation ユーザーガイドの委任された管理者の登録を参照してください。

AWS CloudTrail および AWS Organizations

AWS CloudTrail は、 のガバナンス、コンプライアンス、運用およびリスクの監査を可能にする AWS のサービスです AWS アカウント。管理アカウントのユーザーは AWS CloudTrail、 を使用して、その組織 AWS アカウント 内のすべての のすべてのイベントを記録する組織の証跡を作成できます。組織の証跡は、組織内のすべてのメンバーアカウントに自動的に適用されます。メンバーアカウントは組織の証跡を表示できますが、これを変更または削除することはできません。デフォルトでは、メンバーアカウントは Amazon S3 バケット内にある組織の証跡のログファイルにはアクセスできません。これにより、組織内のすべてのアカウントに対してイベントのログ記録戦略を一律に適用および実施できます。

組織の証跡については、AWS CloudTrail ユーザーガイドの組織の証跡の作成を参照してください。

次の情報は、 AWS CloudTrail との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、CloudTrail はサポートされているオペレーションを組織内のアカウントで実行できます。

このロールを削除または変更できるのは、CloudTrail と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleForCloudTrail`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。CloudTrail によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `cloudtrail.amazonaws.com`

CloudTrail との信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

AWS CloudTrail コンソールから証跡を作成して信頼されたアクセスを有効にすると、信頼されたアクセスが自動的に設定されます (推奨)。 AWS Organizations コンソールを使用して信頼されたアクセスを有効にすることもできます。組織の証跡を作成するには、 AWS Organizations 管理アカウントでサインインする必要があります。

AWS CLI または AWS API を使用して組織の証跡を作成する場合は、信頼されたアクセスを手動で設定する必要があります。詳細については、AWS CloudTrail ユーザーガイドの Enabling CloudTrail as a trusted service in AWS Organizationsを参照してください。

> **Important**
>
> 可能な限り、 AWS CloudTrail コンソールまたはツールを使用して Organizations との統合を有効にすることを強くお勧めします。

信頼されたアクセスを有効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS CloudTrail として を有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal cloudtrail.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。

- AWS API: EnableAWSServiceAccess

CloudTrail との信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

AWS CloudTrail では、組織の証跡や組織のイベントデータストアを操作する AWS Organizations ために、 との信頼されたアクセスが必要です。の使用中に を使用して AWS Organizations 信頼されたアクセスを無効にすると AWS CloudTrail、CloudTrail は組織にアクセスできないため、メンバーアカウントのすべての組織の証跡が削除されます。すべての管理アカウントの組織証跡と組織イベントデータストアは、アカウントレベルの証跡とイベントデータストアに変換されます。CloudTrail と AWS Organizations の統合用に作成された `AWSServiceRoleForCloudTrail` ロールは、アカウント内に残ります。信頼されたアクセスを再度有効にした場合、CloudTrail は既存の証跡やイベントデータストアに対してアクションを実行しません。管理アカウントは、アカウントレベルの証跡とイベントデータストアを更新して、組織に適用する必要があります。

アカウントレベルの証跡またはイベントデータストアを組織証跡または組織イベントデータストアに変換するには、以下を実行します。

- CloudTrail コンソールから、証跡またはイベントデータストアを更新し、[組織内のすべてのアカウントの有効化] オプションを選択します。
- から AWS CLI、次の操作を行います。
  - 証跡を更新するには、update-trail コマンドを実行し、`--is-organization-trail` パラメータを含めます。
  - イベントデータストアを更新するには、update-event-data-store コマンドを実行し、`--organization-enabled` パラメータを含めます。

で信頼されたアクセスを無効にすることができるのは、 AWS Organizations 管理アカウントの管理者のみです AWS CloudTrail。信頼されたアクセスを無効にするには、 AWS Organizations コンソールを使用するか、Organizations CLI コマンドを実行するか、いずれかの SDK で Organizations API AWS オペレーションを呼び出します。 AWS SDKs

信頼されたアクセスを無効にするには、 AWS Organizations コンソールを使用するか、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを無効にするには

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 CloudTrail] を選択します。
4. Disable trusted access (信頼されたアクセスを無効にする) を選択します。
5. 「 の信頼されたアクセスを無効にする AWS CloudTrail」ダイアログボックスで、「無効化」と入力して確認してから、「信頼されたアクセスを無効にする」を選択します。
6. の管理者のみの場合は AWS Organizations、 の管理者 AWS CloudTrail に、サービスコンソールまたはツール を使用して、そのサービスが で AWS Organizations 動作することを無効にできることを伝えます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを無効にすることができます。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS CloudTrail として を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal cloudtrail.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。

- AWS API: DisableAWSServiceAccess

CloudTrail 用の委任管理者アカウントの有効化

Organizations で CloudTrail を使用する場合、CloudTrail の委任管理者として組織内の任意のアカウントを登録できます。このアカウントは、組織に代わって組織の証跡やイベントデータストアを管理できます。委任管理者は、管理アカウントと同じ管理タスクを CloudTrail で実行できる組織のメンバーアカウントです。

> **最小アクセス許可**
>
> CloudTrail の委任管理者を登録できるのは、Organizations 管理アカウントの管理者だけです。

CloudTrail コンソール、あるいは Organizations `RegisterDelegatedAdministrator` CLI または SDK オペレーションを使用して委任管理者アカウントを登録できます。CloudTrail コンソールを使用して委任管理者を登録するには、「Add a CloudTrail delegated administrator」(委任管理者を登録する) を参照してください。

CloudTrail 用の委任された管理者の無効化

CloudTrail の委任管理者を削除できるのは、Organizations 管理アカウントの管理者だけです。CloudTrail コンソール、あるいは Organizations `DeregisterDelegatedAdministrator` CLI または SDK オペレーションを使用して、委任管理者を削除できます。CloudTrail コンソールを使

用して委任管理者を削除する方法については、「Remove a CloudTrail delegated administrator」(CloudTrail の委任管理者を削除する) を参照してください。

Amazon CloudWatch および AWS Organizations

Amazon CloudWatch AWS Organizations の は、次のユースケースで使用できます。

- CloudWatch コンソールの中央ビューから、リソースのテレメトリ設定の状態を検出して理解します AWS 。これにより、 AWS 組織全体またはアカウント全体で複数のリソースタイプのテレメトリコレクション設定を監査するプロセスが簡素化されます。組織全体でテレメトリ設定を使用するには、信頼されたアクセスを有効にする必要があります。

  詳細については、Amazon CloudWatch ユーザーガイドの「CloudWatch テレメトリ設定の監査」を参照してください。

- Amazon CloudWatch Network Monitoring の機能である Network Flow Monitor で複数のアカウントを操作します。Network Flow Monitor は、Amazon EC2 インスタンス間のトラフィックのネットワークパフォーマンスをほぼリアルタイムで可視化します。Organizations と統合するための信頼されたアクセスを有効にしたら、モニターを作成して、複数のアカウントにわたるネットワークパフォーマンスの詳細を視覚化できます。

  詳細については、「Amazon CloudWatch ユーザーガイド」の「マルチアカウントモニタリング用のネットワークフローモニターの初期化」を参照してください。 Amazon CloudWatch

次の情報は、Amazon CloudWatch を と統合するのに役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

組織の管理アカウントに次のサービスにリンクされたロールを作成します。信頼されたアクセスを有効にすると、サービスにリンクされたロールがメンバーアカウントに自動的に作成されます。このロールにより、CloudWatch は組織内のアカウント内でサポートされているオペレーションを実行できます。このロールを削除または変更できるのは、CloudWatch と Organizations 間の信頼されたアクセスを無効にした場合、または組織からメンバーアカウントを削除した場合のみです。

- `AWSServiceRoleForObservabilityAdmin`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。CloudWatch で使用されるサービスにリンクされたロールは、次のサービスプリンシパルへのアクセスを許可します。

- `observabilityadmin.amazonaws.com`
- `networkflowmonitor.amazonaws.com`
- `topology.networkflowmonitor.amazonaws.com`

CloudWatch による信頼されたアクセスの有効化

信頼されたアクセスを有効にするために必要なアクセス許可については、「」を参照してください信頼されたアクセスを有効にするために必要なアクセス許可。

Amazon CloudWatch コンソールまたは コンソールを使用して、信頼された AWS Organizations アクセスを有効にできます。

> **Important**
>
> 可能な限り、Amazon CloudWatch コンソールまたはツールを使用して Organizations との統合を有効にすることを強くお勧めします。これにより、Amazon CloudWatch は、サービスに必要なリソースの作成など、必要な設定を実行できます。Amazon CloudWatch が提供するツールを使用して統合を有効にできない場合にのみ、これらのステップを実行します。詳細については、この注意を参照してください。
> Amazon CloudWatch コンソールまたはツールを使用して信頼されたアクセスを有効にする場合、これらのステップを実行する必要はありません。

CloudWatch コンソールを使用して信頼されたアクセスを有効にするには

「Amazon CloudWatch ユーザーガイド」の「CloudWatch テレメトリ監査を有効にする」を参照してください。 Amazon CloudWatch

CloudWatch で信頼されたアクセスを有効にすると、テレメトリ監査が有効になり、Network Flow Monitor で複数のアカウントを操作できます。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザー (非推奨) としてサインインする必要があります。
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 Amazon CloudWatch 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. Amazon CloudWatch の信頼されたアクセスを有効にするダイアログボックスで、確認のために有効化と入力し、信頼されたアクセスを有効にするを選択します。
6. の管理者のみの場合は AWS Organizations、Amazon CloudWatch の管理者に、そのサービスがサービスコンソール から と AWS Organizations 連携できるようになったことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

信頼されたサービスアクセスを有効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Amazon CloudWatch を Organizations の信頼されたサービスとして有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal observabilityadmin.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。

- AWS API: EnableAWSServiceAccess

CloudWatch で信頼されたアクセスをオフにする

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

Amazon CloudWatch または AWS Organizations ツールを使用して、信頼されたアクセスを無効にすることができます。

> **Important**
>
> 可能な限り、Amazon CloudWatch コンソールまたはツールを使用して Organizations との統合を無効にすることを強くお勧めします。これにより、Amazon CloudWatch は、サービスで不要になったリソースやアクセスロールの削除など、必要なクリーンアップを実行できます。これらのステップは、Amazon CloudWatch が提供するツールを使用して統合を無効にすることができない場合にのみ実行してください。
> Amazon CloudWatch コンソールまたはツールを使用して信頼されたアクセスを無効にする場合、これらのステップを実行する必要はありません。

CloudWatch コンソールを使用して信頼されたアクセスを無効にするには

「Amazon CloudWatch ユーザーガイド」の「CloudWatch テレメトリ監査の無効化」を参照してください。 Amazon CloudWatch

CloudWatch で信頼されたアクセスをオフにすると、テレメトリ監査はアクティブでなくなり、Network Flow Monitor で複数のアカウントを操作できなくなります。

信頼されたアクセスを無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations の信頼されたサービスとして Amazon CloudWatch を無効にします。

```
$ aws organizations disable-aws-service-access \
    --service-principal observabilityadmin.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。

- AWS API: DisableAWSServiceAccess

CloudWatch の委任管理者アカウントの登録

メンバーアカウントを組織の委任管理者アカウントとして登録すると、そのアカウントのユーザーとロールは CloudWatch の管理アクションを実行できます。それ以外の場合は、組織の管理アカウントでサインインしたユーザーまたはロールのみが実行できます。委任管理者アカウントを使用すると、組織の管理と CloudWatch の機能の管理を分離できます。

> **最小アクセス許可**
>
> Organizations 管理アカウントの管理者のみが、組織内の CloudWatch の委任管理者アカウントとしてメンバーアカウントを登録できます。

CloudWatch コンソールを使用するか、 または AWS Command Line Interface SDK で Organizations `RegisterDelegatedAdministrator` API オペレーションを使用して、委任管理者アカウントを登録できます。

CloudWatch コンソールを使用して委任管理者アカウントを登録する方法については、「Amazon CloudWatch ユーザーガイド」の「CloudWatch テレメトリ監査を有効にする」を参照してください。 Amazon CloudWatch

CloudWatch に委任管理者アカウントを登録すると、テレメトリ監査と Network Flow Monitor による管理オペレーションにアカウントを使用できます。

CloudWatch の委任管理者の登録を解除する

> **最小アクセス許可**
>
> Organizations 管理アカウントでサインインした管理者のみが、組織内の CloudWatch の委任管理者アカウントの登録を解除できます。

委任管理者アカウントの登録を解除するには、CloudWatch コンソールを使用するか、 または AWS Command Line Interface SDK で Organizations `DeregisterDelegatedAdministrator` API オペレーションを使用します。詳細については、「Amazon CloudWatch ユーザーガイド」の「委任管理者アカウントの登録解除」を参照してください。 Amazon CloudWatch

CloudWatch で委任管理者アカウントの登録を解除すると、テレメトリ監査と Network Flow Monitor による管理オペレーションにアカウントを使用できなくなります。

AWS Compute Optimizer および AWS Organizations

AWS Compute Optimizer は、 AWS リソースの設定と使用率のメトリクスを分析するサービスです。リソースの例には、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスや Auto Scaling グループがあります。Compute Optimizer は、リソースが最適かどうかを報告します。また、コストを削減し、ワークロードのパフォーマンスを向上させるための最適化に関する推奨事項を生成します。Compute Optimizer について詳しくは、AWS Compute Optimizer ユーザーガイドを参照してください。

次の情報は、 AWS Compute Optimizer との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、Compute Optimizer はサポートされているオペレーションを組織内のアカウントで実行できます。

このロールを削除または変更できるのは、Compute Optimizer と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleForComputeOptimizer`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。Compute Optimizer によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `compute-optimizer.amazonaws.com`

Compute Optimizer との信頼されたアクセスを有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、 AWS Compute Optimizer コンソールまたは AWS Organizations コンソールを使用して有効にできます。

> **Important**
>
> 可能な限り、 AWS Compute Optimizer コンソールまたはツールを使用して Organizations との統合を有効にすることを強くお勧めします。これにより、 は、サービスに必要なリソースの作成など、必要な設定 AWS Compute Optimizer を実行できます。ここに示す手順は、統合の有効化に AWS Compute Optimizerが提供するツールを使用できない場合にのみ実施してください。詳細については、この注意を参照してください。
> AWS Compute Optimizer コンソールまたはツールを使用して信頼されたアクセスを有効にする場合、これらのステップを実行する必要はありません。

Compute Optimizer コンソールを使用して信頼されたアクセスを有効にするには

組織の管理アカウントを使用して Compute Optimizer コンソールにサインインする必要があります。組織を代表してオプトインするには、AWS Compute Optimizer ユーザーガイドのアカウントにオプトインするの指示に従います。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [AWS Compute Optimizer] 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. 「 の信頼されたアクセスを有効にする AWS Compute Optimizer」ダイアログボックスで、「確認のために を有効にする」と入力し、「信頼されたアクセスを有効にする」を選択します。
6. の管理者のみである場合は AWS Organizations、 の管理者に、サービスコンソール からそのサービスが と AWS Organizations 連携できるようになった AWS Compute Optimizer ことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Compute Optimizer として を有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal compute-optimizer.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。
- AWS API: EnableAWSServiceAccess

Compute Optimizer との信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

で信頼されたアクセスを無効にすることができるのは、 AWS Organizations 管理アカウントの管理者のみです AWS Compute Optimizer。

信頼されたアクセスを無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Compute Optimizer として を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal compute-optimizer.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。

- AWS API: DisableAWSServiceAccess

Compute Optimizer の委任された管理者アカウントの有効化

メンバーアカウントを組織の委任管理者として指定すると、指定されたアカウントのユーザーおよびロールは組織のその他のメンバーアカウントの AWS アカウント メタデータを管理できるようになります。委任された管理者アカウントを有効にしない場合、これらのタスクは組織の管理アカウントによってのみ実行できます。この手法は、組織の管理からアカウントの詳細の管理を分離するのに有効です。

> **最小アクセス許可**
>
> Organizations 管理アカウントのユーザーまたはロールのみが、組織内で Computer Optimizer の委任管理者としてメンバーアカウントを設定できます

Compute Optimizer の委任された管理者アカウントを有効にする手順については、AWS Compute Optimizer ユーザーガイドの https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html を参照してください。

AWS CLI, AWS API

CLI またはいずれかの AWS SDKs を使用して AWS 委任管理者アカウントを設定する場合は、次のコマンドを使用できます。

- AWS CLI:

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

- AWS SDK: Organizations `RegisterDelegatedAdministrator`オペレーションとメンバーアカウントの ID 番号を呼び出し、アカウントサービスプリンシパルをパラメータ`account.amazonaws.com`として識別します。

Compute Optimizer の委任された管理者の無効化

Compute Optimizer の委任された管理者を設定できるのは、組織管理アカウントの管理者だけです。

Compute Optimizer コンソールを使用して、委任された管理者 Compute Optimizer アカウントを無効にするには、AWS Compute Optimizer ユーザーガイドの https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html を参照してください。

を使用して委任管理者を削除するには AWS AWS CLI、AWS AWS CLI 「 コマンドリファレンス」のderegister-delegated-administrator」を参照してください。

AWS Config および AWS Organizations

のマルチアカウント、マルチリージョンのデータ集約 AWS Config を使用すると、複数のアカウントと の AWS Config データを AWS リージョン 1 つのアカウントに集約できます。マルチアカウント、マルチリージョンのデータ集約は、中央の IT 管理者がエンタープライズの複数の AWS アカウント のコンプライアンスをモニタリングするうえで役立ちます。アグリゲータは、複数のソースアカウントとリージョンから AWS Config データを収集 AWS Config する のリソースタイプです。集計 AWS Config データを表示するリージョンにアグリゲータを作成します。アグリゲータの作成中、個々のアカウント ID、または組織の追加を選択できます。詳細については AWS Config、「 AWS Config デベロッパーガイド」を参照してください。

AWS Config APIs を使用して、組織内のすべての AWS アカウント でルールを管理する AWS Config こともできます。詳細については、「 AWS Config デベロッパーガイド」の「組織内のすべてのアカウントで AWS Config ルールを有効にする」を参照してください。

次の情報は、 AWS Config との統合に役立ちます AWS Organizations。

サービスにリンクされた役割

次のサービスにリンクされたロールでは AWS Config 、 が組織内のアカウント内でサポートされているオペレーションを実行できます。

- `AWSServiceRoleForConfig`

このロールの作成の詳細については、「 デベロッパーガイド」の「 に割り当てられた IAM ロールのアクセス許可 AWS Config」を参照してください。 AWS Config

でサービスにリンクされたロール AWS Config を使用する方法については、「 AWS Config デベロッパーガイド」の「 でサービスにリンクされたロールを使用する AWS Config」を参照してください。

このロールを削除または変更できるのは、 AWS Config と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

AWS Configとの信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、 AWS Config コンソールまたは AWS Organizations コンソールを使用して有効にできます。

> **Important**
>
> 可能な限り、 AWS Config コンソールまたはツールを使用して Organizations との統合を有効にすることを強くお勧めします。これにより、 はサービスに必要なリソースの作成など、必要な設定 AWS Config を実行できます。ここに示す手順は、統合の有効化に AWS Config が提供するツールを使用できない場合にのみ実施してください。詳細については、この注意を参照してください。
>
> AWS Config コンソールまたはツールを使用して信頼されたアクセスを有効にする場合、これらのステップを実行する必要はありません。

AWS Config コンソールを使用して信頼されたアクセスを有効にするには

AWS Organizations を使用して への信頼されたアクセスを有効にするには AWS Config、マルチアカウントアグリゲータを作成し、組織を追加します。マルチアカウントアグリゲータの設定方法については、「AWS Config 開発者ガイド」の「Creating Aggregators」を参照してください。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・ インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [AWS Config] 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. 「 の信頼されたアクセスを有効にする AWS Config」ダイアログボックスで、「確認のために を有効にする」と入力し、「信頼されたアクセスを有効にする」を選択します。
6. の管理者のみである場合は AWS Organizations、 の管理者に、サービスコンソール からそのサービスが と AWS Organizations 連携できるようになった AWS Config ことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Config として を有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal config.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。

- AWS API: EnableAWSServiceAccess

AWS Configとの信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスを無効にするには、Organizations ツールを使用する必要があります。

信頼されたアクセスを無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Config として を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal config.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。
- AWS API: DisableAWSServiceAccess

AWS Cost Optimization Hub および AWS Organizations

AWS Cost Optimization Hub は、 AWS アカウントと AWS リージョン全体でコスト最適化の推奨事項を統合して優先順位を付けるのに役立つ AWS 請求情報とコスト管理機能です。これにより、AWS 支出を最大限に活用できます。で Cost Optimization Hub を使用すると、Organizations メンバーアカウントと AWS リージョン全体で AWS コスト最適化の推奨事項 AWS Organizations を簡単に識別、フィルタリング、集計できます。

詳細については、「AWS Cost Management User Guide」の「Cost Optimization Hub」を参照してください。

次の情報は、 AWS Cost Optimization Hub との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、Cost Optimization Hub はサポートされているオペレーションを組織内のアカウントで実行できます。

このロールを削除または変更できるのは、Cost Optimization Hub と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

詳細については、「AWS Cost Management ユーザーガイド」の「Service-linked role permissions for Cost Optimization Hub」を参照してください。

- `AWSServiceRoleForCostOptimizationHub`

Cost Optimization Hub で使用されるサービスプリンシパル

Cost Optimization Hub は `cost-optimization-hub.bcm.amazonaws.com` サービスプリンシパルを使用します。

Cost Optimization Hub で信頼されたアクセスを有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

組織の管理アカウントを使用してオプトインし、組織内のすべてのメンバーアカウントを含めると、Cost Optimization Hub の信頼されたアクセスが組織アカウントで自動的に有効になります。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・ インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [AWS Cost Optimization Hub] 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. 「 の信頼されたアクセスを有効にする AWS Cost Optimization Hub」ダイアログボックスで、「確認のために を有効にする」と入力し、「信頼されたアクセスを有効にする」を選択します。
6. の管理者のみである場合は AWS Organizations、 の管理者に、サービスコンソール からそのサービスが と AWS Organizations 連携できるようになった AWS Cost Optimization Hub ことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Cost Optimization Hub として を有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal cost-optimization-hub.bcm.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。
- AWS API: EnableAWSServiceAccess

信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスを無効にするには、Organizations ツールを使用する必要があります。

> **Important**
>
> オプトインした後に Cost Optimization Hub の信頼されたアクセスを無効にすると、Cost Optimization Hub は組織のメンバー アカウントのレコメンデーションへのアクセスを拒否します。さらに、組織内のメンバーアカウントは Cost Optimization Hub にオプトイン

されていません。詳細については、「AWS Cost Management ユーザーガイド」の「Cost Optimization Hub and Organizations trusted access」を参照してください。

信頼されたアクセスを無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Cost Optimization Hub として を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal cost-optimization-hub.bcm.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。
- AWS API: DisableAWSServiceAccess

Cost Optimization Hub の委任された管理者アカウントの有効化

メンバーアカウントを組織の委任管理者に指定すると、指定されたアカウントは、組織内のすべてのアカウントの Cost Optimization Hub レコメンデーションを取得し、Cost Optimization Hub の設定を管理できるため、リソース最適化の機会を一元的に特定する柔軟性が高まります。

最小アクセス許可

次の許可を持つ Organizations 管理アカウントのユーザーまたはロールのみが、組織内で Cost Optimization Hub の委任管理者としてメンバーアカウントを設定できます。

Cost Optimization Hub の委任管理者アカウントを有効にする方法については、「AWS Cost Management ユーザーガイド」の「Delegate an administrator account」を参照してください。

Cost Optimization Hub の委任管理者の無効化

Cost Optimization Hub の委任管理者を削除できるのは、Organizations 管理アカウントの管理者だけです。

Cost Optimization Hub コンソールを使用して委任管理者の Cost Optimization Hub アカウントを無効にするには、「AWS Cost Management User Guide」の「Delegate an administrator account」を参照してください。

CLI を使用して委任管理者を削除するには、 CLI AWS リファレンスの`deregister-delegated-administrator`「」を参照してください。 AWS Config

AWS Control Tower および AWS Organizations

AWS Control Tower は、規範的なベストプラクティスに従って、 AWS マルチアカウント環境を簡単にセットアップして管理する方法を提供します。 AWS Control Tower オーケストレーションは、 の機能を拡張 AWS Organizationsします。 は、組織とアカウントがベストプラクティス (ドリフト) から逸脱しないように、予防コントロールと検出コントロール (ガードレール) AWS Control Tower を適用します。

AWS Control Tower オーケストレーションは の機能を拡張します AWS Organizations。

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

次の情報は、 AWS Control Tower との統合に役立ちます AWS Organizations。

統合に必要な役割

`AWSControlTowerExecution` ロールは、登録されたすべてのアカウントに存在する必要があります。これにより、 AWS Control Tower は個々のアカウントを管理し、それらの情報を監査アカウントとログアーカイブアカウントにレポートできます。

で使用されるロールの詳細については AWS Control Tower、「 AWS Control Tower がロールと連携してアカウントを作成および管理する方法」および「 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 Control Tower」を参照してください。

で使用されるサービスプリンシパル AWS Control Tower

AWS Control Tower は`controltower.amazonaws.com`サービスプリンシパルを使用します。

AWS Control Towerとの信頼されたアクセスの有効化

AWS Control Tower は信頼されたアクセスを使用して、予防コントロールのドリフトを検出し、ドリフトの原因となるアカウントと OU の変更を追跡します。

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、Organizations ツールを使用してのみ有効にできます。

Organizations コンソールから信頼されたアクセスを有効にするには、AWS Control Tower の隣の **`Enable access`** を選択します。

信頼されたアクセスを有効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Control Tower として を有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal controltower.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。
- AWS API: EnableAWSServiceAccess

AWS Control Towerとの信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスを無効にするには、Organizations ツールを使用する必要があります。

> **Important**
>
> AWS Control Tower信頼されたアクセスを無効にすると、 AWS Control Tower ランディングゾーンにドリフトが発生します。ドリフトを修正する唯一の方法は、 AWS Control Towerのランディングゾーンの修理を利用することです。Organizations での信頼できるアクセスを再度有効にしても、ドリフトは解決しません。ドリフトの詳細については、「AWS Control Tower 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を無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Control Tower として を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal controltower.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。

- AWS API: DisableAWSServiceAccess

Amazon Detective と AWS Organizations

Amazon Detective がログデータを使用して可視化を生成することにより、セキュリティに関する検出結果や疑わしいアクティビティの根本原因を分析、調査、および特定できるようになります。

AWS Organizations を使用すると、Detective 動作グラフがすべての組織アカウントのアクティビティを可視化できます。

Detective への信頼されたアクセスを許可すると、組織のメンバーシップに変更があった場合、Detective サービスが自動的に対応します。委任管理者が、任意の組織アカウントを動作グラフのメンバーアカウントとして有効にできます。Detective では、新しい組織アカウントをメンバーアカウントとして自動的に有効化することもできます。組織アカウントの動作グラフとの関連付けを解除することはできません。

詳細については、「Amazon Detective 管理ガイド」の「Using Amazon Detective in your organization」(組織内で Amazon Detective を使用する) を参照してください。

Amazon Detective を と統合するには、次の情報を使用します AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、Detective はサポートされているオペレーションを組織内のアカウントで実行できます。

このロールを削除または変更できるのは、Detective と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleForDetective`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。Detective によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `detective.amazonaws.com`

Detective との信頼されたアクセスを有効にするには

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

> **Note**
>
> Amazon Detective の委任管理者を指定すると、組織の Detective に対する信頼されたアクセスが自動的に有効になります。
> Detective では、メンバーアカウントを組織のこのサービスの委任管理者に指定 AWS Organizations する前に、 への信頼されたアクセスが必要です。

信頼されたアクセスは、Organizations ツールを使用してのみ有効にできます。

AWS Organizations コンソールを使用して、信頼されたアクセスを有効にできます。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [Amazon Detective] 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. [Amazon Detective の信頼されたアクセスを有効にする] ダイアログボックスで、[有効にする] と入力して確定し、[信頼されたアクセスを有効にする] を選択します。
6. の管理者のみである場合は AWS Organizations、Amazon Detective の管理者に、サービスコンソール AWS Organizations からそのサービスが と連携できるようになったことを知らせます。

Detective との信頼されたアクセスを無効にするには

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

Amazon Detective での信頼されたアクセスを無効にすることができるのは、 AWS Organizations 管理アカウントの管理者のみです。

信頼されたアクセスを無効にするには、Organizations ツールを使用する必要があります。

AWS Organizations コンソールを使用して、信頼されたアクセスを無効にすることができます。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを無効にするには

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 [Amazon Detective] を選択します。
4. Disable trusted access (信頼されたアクセスを無効にする) を選択します。
5. Amazon Detective の信頼されたアクセスを無効にするダイアログボックスで、「確認のために無効化」と入力し、「信頼されたアクセスを無効にする」を選択します。
6. の管理者のみである場合は AWS Organizations、Amazon Detective の管理者に、サービスコンソールまたはツールを使用して、そのサービスが で AWS Organizations 動作することを無効にできることを伝えます。

Detective 用の委任管理者アカウントの有効化

Detective 用の委任管理者アカウントは、Detective 動作グラフの管理者アカウントになります。委任管理者は、その動作グラフのメンバーアカウントとして有効または無効にする組織アカウントを決定します。委任管理者は、新しい組織アカウントが組織に追加されたときに、メンバーアカウントとして自動的に有効にするように Detective を設定できます。委任管理者が組織アカウントを管理する方法については、「Amazon Detective 管理ガイド」の「組織アカウントをメンバーアカウントとして管理する」を参照してください。

Detective 用の委任管理者を設定できるのは、組織管理アカウントの管理者だけです。

委任管理者アカウントを指定する場合は、Detective コンソールまたは API を介して、あるいは Organizations CLI または SDK オペレーションを使用して行います。

> **最小アクセス許可**
>
> Organizations 管理アカウントのユーザーまたはロールのみが、組織内で Detective の委任管理者としてメンバーアカウントを設定できます

Detective コンソールまたは API を使用して委任管理者を設定するには、「Amazon Detective 管理ガイド」の「組織の Detective 管理者アカウントの指定」を参照してください。

AWS CLI, AWS API

CLI またはいずれかの AWS SDKs を使用して AWS 委任管理者アカウントを設定する場合は、次のコマンドを使用できます。

- AWS CLI:

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

- AWS SDK: Organizations `RegisterDelegatedAdministrator`オペレーションとメンバーアカウントの ID 番号を呼び出し、アカウントサービスプリンシパルをパラメータ`account.amazonaws.com`として識別します。

Detective 用の委任管理者の無効化

委任管理者アカウントを削除する場合は、Detective コンソールまたは API を使用して、あるいは Organizations `DeregisterDelegatedAdministrator` CLI または SDK オペレーションを使用して行います。Detective コンソールまたは API、あるいは Organizations API を使用して委任管理者を削除する方法については、「Amazon Detective 管理ガイド」の「組織の Detective 管理者アカウントの指定」を参照してください。

Amazon DevOpsGuru と AWS Organizations

Amazon DevOps Guru は、運用データとアプリケーションのメトリクスおよびイベントを分析し、通常の運用パターンから逸脱する動作を特定します。DevOps Guru が運用上の問題またはリスクを検出すると、ユーザーに通知されます。

DevOpsGuru を使用すると、 でのマルチアカウントサポートが有効になるため AWS Organizations、組織全体のインサイトを管理するメンバーアカウントを指定できます。この委任管理者は、組織内のすべてのアカウントから取得したインサイトを表示、ソート、フィルタリングして、追加のカスタマイズを必要とせずに、組織内のすべてのモニタリング対象アプリケーションの状態に関する全体像を作成できます。

詳細については、「Amazon DevOps Guru ユーザーガイド」の「組織全体のアカウントをモニタリングする」を参照してください。

次の情報は、Amazon DevOpsGuru と の統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、DevOps Guru はサポートされているオペレーションを組織内のアカウントで実行できます。

このロールを削除または変更できるのは、DevOps Guru と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleForDevOpsGuru`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。DevOps Guru によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `devops-guru.amazonaws.com`

詳細については、「Amazon DevOps Guru ユーザーガイド」の「DevOps Guru でのサービスにリンクされたロールの使用」を参照してください。

DevOps Guru との信頼されたアクセスを有効にするには

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

> **Note**
>
> Amazon DevOps Guru の委任管理者を指定すると、組織の DevOps に対する信頼されたアクセスが自動的に有効になります。
> DevOpsGuru では、メンバーアカウントを組織のこのサービスの委任管理者に指定 AWS Organizations する前に、 への信頼されたアクセスが必要です。

> **Important**
>
> Organizations との統合の有効化には、可能な場合は常に Amazon DevOps Guru のコンソールまたはツールを使用することを強くお勧めします。そうすることで、サービスに必要なリソースの作成など、必要な設定が Amazon DevOps Guru で実行可能になります。ここに示す手順は、統合の有効化に Amazon DevOps Guru が提供するツールを使用できない場合にのみ実施してください。詳細については、この注意を参照してください。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールまたは DevOpsGuru コンソールを使用します。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. [Services] (サービス) ページで Amazon DevOps Guru の行を探し、サービスの名前を選択してから、[Enable trusted access] (信頼されたアクセスを有効にする) を選択します。
3. 確認ダイアログボックスで、[Show the option to enable trusted access] (信頼されたアクセスを有効にするオプションを表示する) を有効にし、ボックスに「**enable**」と入力してから、[Enable trusted access] (信頼されたアクセスを有効にする) を選択します。
4. の管理者のみである場合は AWS Organizations、Amazon DevOpsGuru の管理者に、コンソールを使用してそのサービスを有効にして操作できることを伝えます AWS Organizations。

DevOps Guru console

DevOps Guru コンソールを使用してサービスへの信頼されたアクセスを有効にするには

1. 管理アカウントに管理者としてサインインし、DevOps Guru コンソール (Amazon DevOps Guru コンソール) を開きます。
2. [Enable trusted access (信頼されたアクセスを有効にする)] を選択します。

DevOps Guru との信頼されたアクセスを無効にするには

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

Amazon DevOpsGuru での信頼されたアクセスを無効にすることができるのは、 AWS Organizations 管理アカウントの管理者のみです。

信頼されたアクセスは、Organizations ツールを使用してのみ無効にできます。

AWS Organizations コンソールを使用して、信頼されたアクセスを無効にすることができます。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを無効にするには

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 [Amazon DevOps Guru] を選択します。
4. Disable trusted access (信頼されたアクセスを無効にする) を選択します。
5. Amazon DevOpsGuru の信頼されたアクセスを無効にするダイアログボックスで、「Disable」と入力して確認し、「信頼されたアクセスを無効にする」を選択します。
6. の管理者のみの場合は AWS Organizations、Amazon DevOpsGuru の管理者に、サービスコンソールまたはツールを使用してそのサービスが で AWS Organizations 動作することを無効にできることを伝えます。

DevOps Guru 用の委任管理者アカウントの有効化

DevOps Guru 用の委任管理者アカウントは、組織から DevOps Guru にオンボーディングされているすべてのメンバーアカウントから取得したインサイトデータを表示できます。委任管理者が組織アカウントを管理する方法については、「Amazon DevOps Guru ユーザーガイド」の「組織全体のアカウントをモニタリングする」を参照してください。

DevOps Guru 用の委任管理者を設定できるのは、組織管理アカウントの管理者だけです。

委任管理者アカウントを指定する場合は、DevOps Guru コンソールを介して、あるいは Organizations `RegisterDelegatedAdministrator` CLI または SDK オペレーションを使用して行います。

> **最小アクセス許可**
>
> Organizations 管理アカウントのユーザーまたはロールのみが、組織内で DevOps Guru の委任管理者としてメンバーアカウントを設定できます

DevOps Guru console

DevOps Guru コンソールで委任管理者を設定するには

1. 管理アカウントに管理者としてサインインし、DevOps Guru コンソール (Amazon DevOps Guru コンソール) を開きます。
2. [Register delegated administrator (委任管理者の登録)] を選択します。管理アカウントまたは任意のメンバーアカウントのいずれかを、委任管理者として選択できます。

AWS CLI, AWS API

CLI またはいずれかの AWS SDKs を使用して AWS 委任管理者アカウントを設定する場合は、次のコマンドを使用できます。

- AWS CLI:

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

- AWS SDK: Organizations `RegisterDelegatedAdministrator`オペレーションとメンバーアカウントの ID 番号を呼び出し、アカウントサービスプリンシパルをパラメータ`account.amazonaws.com`として識別します。

DevOps Guru 用の委任管理者の無効化

DevOps Guru コンソール、あるいは Organizations `DeregisterDelegatedAdministrator` CLI または SDK オペレーションを使用して、委任管理者を削除できます。DevOps Guru コンソールを使

用して委任管理者を削除する方法については、「Amazon DevOps Guru ユーザーガイド」の「組織全体のアカウントをモニタリングする」を参照してください。

AWS Directory Service および AWS Organizations

AWS Directory Service for Microsoft Active Directory、または を使用すると AWS Managed Microsoft AD、Microsoft Active Directory (AD) をマネージドサービスとして実行できます。 AWS Directory Service を使用すると、 AWS クラウドでディレクトリを簡単にセットアップして実行したり、 AWS リソースを既存のオンプレミスの Microsoft Active Directory に接続したりできます。 AWS Managed Microsoft AD また、 と緊密に統合 AWS Organizations されているため、リージョン内の複数の VPC AWS アカウント と任意の VPC 間でディレクトリをシームレスに共有できます。詳細については、AWS Directory Service 管理ガイドを参照してください。

組織全体 AWS Directory Service で を共有するには、組織ですべての機能が有効になっている必要があり、ディレクトリは組織管理アカウントにある必要があります。

次の情報は、 AWS Directory Service との統合に役立ちます AWS Organizations。

AWS Directory Serviceとの信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、 AWS Directory Service コンソールまたは AWS Organizations コンソールを使用して有効にできます。

> **Important**
>
> 可能な限り、 AWS Directory Service コンソールまたはツールを使用して Organizations との統合を有効にすることを強くお勧めします。これにより、 は、サービスに必要なリソースの作成など、必要な設定 AWS Directory Service を実行できます。ここに示す手順は、統合の有効化に AWS Directory Serviceが提供するツールを使用できない場合にのみ実施してください。詳細については、この注意を参照してください。
> AWS Directory Service コンソールまたはツールを使用して信頼されたアクセスを有効にする場合、これらのステップを実行する必要はありません。

AWS Directory Service コンソールを使用して信頼されたアクセスを有効にするには

ディレクトリを共有するには、AWS Directory Service 管理ガイドのディレクトリの共有を参照してください。ディレクトリを共有すると、信頼されたアクセスが自動的に有効になります。step-by-step手順については、「チュートリアル: AWS Managed Microsoft AD ディレクトリの共有」を参照してください。

AWS Organizations コンソールを使用して、信頼されたアクセスを有効にできます。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・ インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [AWS Directory Service] 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 Directory Serviceの信頼されたアクセスを有効にする] ダイアログボックスで、[有効にする] と入力して確定し、[信頼されたアクセスを有効にする] を選択します。
6. の管理者のみである場合は AWS Organizations、 の管理者に、サービスコンソール AWS Organizations からそのサービスが と連携できるようになった AWS Directory Service ことを知らせます。

AWS Directory Serviceとの信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

の使用 AWS Organizations 中に を使用して信頼されたアクセスを無効にすると AWS Directory Service、以前に共有されたディレクトリはすべて通常どおり動作し続けます。ただし、信頼されたアクセスを再度有効化するまでは、組織内で新しいディレクトリを共有することはできなくなります。

信頼されたアクセスは、Organizations ツールを使用してのみ無効にできます。

AWS Organizations コンソールを使用して、信頼されたアクセスを無効にすることができます。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを無効にするには

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 Directory Service] を選択します。
4. Disable trusted access (信頼されたアクセスを無効にする) を選択します。
5. 「 の信頼されたアクセスを無効にする AWS Directory Service」ダイアログボックスで、「無効にして確認」と入力し、「信頼されたアクセスを無効にする」を選択します。
6. の管理者のみである場合は AWS Organizations、 の管理者に、そのサービスコンソールまたはツールを使用して、そのサービスの の使用 AWS Organizations を無効にすることができる AWS Directory Service ようになったことを知らせます。

Amazon Elastic Compute Cloudおよび AWS Organizations

Amazon Elastic Compute Cloud は、 AWS クラウドでオンデマンドでスケーラブルなコンピューティング能力を提供します。Organizations で Amazon EC2 を使用する場合、Organizations 管理者は、Amazon EC2 の宣言ポリシー機能を使用した後、組織全体のアカウントの既存の設定に関するレポートを作成できます。

Amazon Elastic Compute Cloud を と統合するには、次の情報を使用します AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、Amazon EC2 は組織内のアカウント内でサポートされているオペレーションを実行できます。

このロールを削除または変更できるのは、Amazon EC2 と Organizations 間の信頼されたアクセスを無効にした場合、または組織からメンバーアカウントを削除した場合のみです。

- `AWSServiceRoleForDeclarativePoliciesEC2Report`

Amazon EC2 で使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。Amazon EC2 で使用されるサービスにリンクされたロールは、次のサービスプリンシパルへのアクセスを許可します。

- `ec2.amazonaws.com`

Amazon EC2 での信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

Organizations 管理者が組織全体のアカウントの既存の設定に関するレポートを作成できるようにするには、信頼されたアクセスを有効にする必要があります。

Organizations ツールを使用してのみ、信頼されたアクセスを有効にできます。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・インします。組織の管理アカウントの 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 (非推奨) としてサインインする必要があります。
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 Amazon Elastic Compute Cloud 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. Amazon Elastic Compute Cloud の信頼されたアクセスを有効にするダイアログボックスで、確認のために有効化と入力し、信頼されたアクセスを有効にするを選択します。
6. の管理者のみである場合は AWS Organizations、Amazon Elastic Compute Cloud の管理者に、サービスコンソール からそのサービスが と AWS Organizations 連携できるようになったことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Amazon Elastic Compute Cloud を Organizations の信頼されたサービスとして有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal ec2.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。
- AWS API: EnableAWSServiceAccess

信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

Organizations ツールを使用してのみ、信頼されたアクセスを無効にできます。

Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs で Organizations API オペレーションを呼び出すことで、信頼されたアクセスを無効にすることができます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを無効にします。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations の信頼されたサービスとして Amazon Elastic Compute Cloud を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
  ```

```
    --service-principal ec2.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。

- AWS API: DisableAWSServiceAccess

Amazon Elastic Kubernetes Service および AWS Organizations

Amazon Elastic Kubernetes Service Dashboard は、複数の AWS リージョンと AWS アカウントにわたる Kubernetes クラスターをモニタリング、管理、可視化するために使用できる統合ダッシュボードです。EKS ダッシュボードは、一元化されたインターフェイスを通じて Amazon EKS インフラストラクチャの包括的な制御とインサイトを提供します。

Amazon Elastic Kubernetes Service Dashboard を使用すると、アップグレードが予定されているクラスターの追跡、プロジェクトコントロールプレーンのコスト、クラスターインサイトの確認、組織全体のノードグループのディストリビューションのモニタリングを行うことができます。 AWS 管理者は、グラフ、リソースリスト、地理的マップなどのさまざまな視覚化オプションを使用して、ヘルスステータス、バージョンディストリビューション、アドオン設定など、クラスターリソースに関する集計データを表示できます。ダッシュボードは AWS Organizations と統合され、EKS リソースの安全なクロスアカウントおよびクロスリージョン可視性を提供します。

次の情報は、Amazon Elastic Kubernetes Service を と統合するのに役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

Amazon Elastic Kubernetes Service コンソールを使用して信頼されたアクセスを有効にすると、次のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、Amazon EKS はサポートされているオペレーションを組織内のアカウント内で実行できます。このロールを削除または変更できるのは、Amazon Elastic Kubernetes Service と Organizations 間の信頼されたアクセスを無効にした場合のみです。

Organizations コンソール、CLI、または SDK から直接信頼されたアクセスを有効にすると、サービスにリンクされたロールは自動的に作成されません。

- `AWSServiceRoleForAmazonEKSDashboard`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。Amazon EKS で使用されるサービスにリンクされたロールは、次のサービスプリンシパルへのアクセスを許可します。

- `dashboard.eks.amazonaws.com`

Amazon EKS での信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

Amazon EKS コンソールを使用して信頼されたアクセスを有効にするには

「Amazon EKS ユーザーガイド」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。

Amazon EKS での信頼されたアクセスの無効化

Amazon EKS コンソールを使用して信頼されたアクセスを無効にするには

Amazon EKS ユーザーガイドの「信頼されたアクセスを無効にする」を参照してください。

Amazon EKS の委任管理者アカウントの有効化

管理アカウント管理者は、Amazon EKS 管理権限を委任管理者と呼ばれる指定されたメンバーアカウントに委任できます。

管理アカウントと委任管理者アカウントは、Amazon EKS ダッシュボードを表示できます。

委任管理者アカウントを有効にするには

「Amazon EKS ユーザーガイド」の「委任管理者アカウントの有効化」を参照してください。

Amazon EKS の委任管理者の無効化

Amazon EKS の委任管理者を設定できるのは、組織管理アカウントの管理者のみです。

委任管理者アカウントを無効にするには

「Amazon EKS ユーザーガイド」の「委任管理者アカウントの無効化」を参照してください。

AWS Firewall Manager および AWS Organizations

AWS Firewall Manager は、組織内の およびアプリケーション全体でファイアウォールルールやその他の保護を一元的に設定 AWS アカウント および管理するために使用するセキュリティ管理サービスです。Firewall Manager を使用すると、 AWS WAF ルールのロールアウト、保護の作成 AWS Shield Advanced 、Amazon Virtual Private Cloud (Amazon VPC) セキュリティグループの設定と監査、 AWS Network Firewallのデプロイを行うことができます。Firewall Manager を使用すれば、保護を一度設定するだけで、新しいリソースやアカウントが追加されているかどうかにかかわらず、組織内のすべてのアカウントとリソースに保護が自動的に適用されます。詳細については AWS Firewall Manager、「 AWS Firewall Manager デベロッパーガイド」を参照してください。

次の情報は、 AWS Firewall Manager との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、Firewall Manager はサポートされているオペレーションを組織内のアカウントで実行できます。

このロールを削除または変更できるのは、Firewall Manager と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleForFMS`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。Firewall Manager によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `fms.amazonaws.com`

Firewall Manager との信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、 AWS Firewall Manager コンソールまたは AWS Organizations コンソールを使用して有効にできます。

> **Important**
>
> 可能な限り、 AWS Firewall Manager コンソールまたはツールを使用して Organizations との統合を有効にすることを強くお勧めします。これにより、 はサービスに必要なリソースの作成など、必要な設定 AWS Firewall Manager を実行できます。ここに示す手順は、統合の有効化に AWS Firewall Managerが提供するツールを使用できない場合にのみ実施してください。詳細については、この注意を参照してください。
> AWS Firewall Manager コンソールまたはツールを使用して信頼されたアクセスを有効にする場合、これらのステップを実行する必要はありません。

AWS Organizations 管理アカウントでサインインし、組織内のアカウントを AWS Firewall Manager 管理者アカウントとして設定する必要があります。詳細については、AWS Firewall Manager デベロッパーガイドの Set the AWS Firewall Manager Administrator Account を参照してください。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [AWS Firewall Manager] 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. 「信頼されたアクセスを有効にする AWS Firewall Manager」ダイアログボックスで、「確認のために を有効にする」と入力し、「信頼されたアクセスを有効にする」を選択します。
6. の管理者のみである場合は AWS Organizations、 の管理者に、サービスコンソール からそのサービスが と AWS Organizations 連携できるようになった AWS Firewall Manager ことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Firewall Manager としてを有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal fms.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。

- AWS API: EnableAWSServiceAccess

Firewall Manager との信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、 AWS Firewall Manager または AWS Organizations ツールを使用して無効にできます。

> **Important**
>
> 可能な限り、 AWS Firewall Manager コンソールまたはツールを使用して Organizations との統合を無効にすることを強くお勧めします。これにより、 は、サービスで不要になったリソースやアクセスロールの削除など、必要なクリーンアップ AWS Firewall Manager を実行できます。ここに示す手順は、統合の無効化に AWS Firewall Managerが提供するツールを使用できない場合にのみ実施してください。
> AWS Firewall Manager コンソールまたはツールを使用して信頼されたアクセスを無効にする場合、これらのステップを実行する必要はありません。

Firewall Manager コンソールを使用して信頼されたアクセスを無効にするには

AWS Firewall Manager 管理者アカウントを変更または取り消すには、「 AWS Firewall Manager デベロッパーガイド」の「管理者アカウントとして別の AWS Firewall Manager アカウントを指定する」の手順に従います。

管理者アカウントを取り消す場合は、 AWS Organizations 管理アカウントにサインインし、新しい管理者アカウントを設定する必要があります AWS Firewall Manager。

信頼されたアクセスを無効にするには、 AWS Organizations コンソールを使用するか、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを無効にするには

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 Firewall Manager] を選択します。
4. Disable trusted access (信頼されたアクセスを無効にする) を選択します。
5. 「 の信頼されたアクセスを無効にする AWS Firewall Manager」ダイアログボックスで、「無効にして確認」と入力し、「信頼されたアクセスを無効にする」を選択します。
6. の管理者のみの場合は AWS Organizations、 の管理者に、サービスコンソールまたはツール を使用して、そのサービスが で AWS Organizations 動作することを無効にできるようになった AWS Firewall Manager ことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを無効にすることができます。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Firewall Manager としてを無効にします。

```
$ aws organizations disable-aws-service-access \
```

```
    --service-principal fms.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。

- AWS API: DisableAWSServiceAccess

Firewall Manager 用の委任管理者アカウントの有効化

メンバーアカウントを組織の委任管理者として指定すると、そのアカウントのユーザーおよびロールは、 Firewall Manager の管理アクションを実行できるようになります。通常この管理アクションは、組織の管理アカウントのユーザーとロールだけが実行できるものです。この手法は、組織の管理から Firewall Manager の管理を分離するのに有効です。

> **最小アクセス許可**
>
> Organizations 管理アカウントのユーザーまたはロールのみが、組織内で Firewall Manager の委任管理者としてメンバーアカウントを設定できます。

メンバーアカウントを組織の Firewall Manager 管理者として指定する方法については、「 AWS Firewall Manager デベロッパーガイド」のAWS Firewall Manager 「管理者アカウントの設定」を参照してください。

Amazon GuardDuty と AWS Organizations

Amazon GuardDuty は、さまざまなデータソースを分析および処理する継続的セキュリティモニタリングサービスです。脅威インテリジェンスフィードおよび機械学習を使用して、 AWS 環境内の予期しないアクティビティ、不正の可能性があるアクティビティ、悪意のあるアクティビティを識別します。これには、権限のエスカレーション、公開された認証情報の使用、悪意のある IP アドレス、URL、またはドメインとの通信、Amazon Elastic Compute Cloud インスタンスおよびコンテナワークロードでのマルウェアの存在などの問題が含まれる場合があります。

Organizations を使用し、組織のすべてのアカウントを対象に GuardDuty を管理することで、GuardDuty の管理を簡素化できます。

詳細については、Amazon GuardDuty ユーザーガイドの Managing GuardDuty accounts with AWS Organizations を参照してください。

以下の情報は、Amazon GuardDuty との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、GuardDuty はサポートされているオペレーションを組織内の組織アカウントで実行できます。このロールを削除できるのは、GuardDuty と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleForAmazonGuardDuty` サービスにリンクされたロールは、GuardDuty をOrganizations と統合したアカウントで自動的に作成されます。詳細については、Amazon GuardDuty ユーザーガイドの Managing GuardDuty accounts with Organizations を参照してください。
- `AmazonGuardDutyMalwareProtectionServiceRolePolicy` サービスにリンクされたロールは、GuardDuty Malware Protection が有効になっているアカウントで自動的に作成されます。詳細については、Amazon GuardDuty ユーザーガイドの GuardDuty マルウェア保護のためのサービスにリンクされたロールの許可を参照してください。

サービスにリンクされたロールで使用されるサービスプリンシパル

- `guardduty.amazonaws.com`、`AWSServiceRoleForAmazonGuardDuty` サービスにリンクされたロールによって使用される。
- `malware-protection.guardduty.amazonaws.com`、`AmazonGuardDutyMalwareProtectionServiceRole` サービスにリンクされたロールによって使用される。

GuardDuty との信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

Amazon GuardDuty を使用してのみ、信頼されたアクセスを有効にできます。

Amazon GuardDuty では、メンバーアカウントを組織の GuardDuty 管理者として指定 AWS Organizations する前に、 への信頼されたアクセスが必要です。GuardDuty コンソールを使用して委任管理者を設定すると、信頼されたアクセスが GuardDuty によって自動的に有効になります。

ただし、 AWS CLI またはいずれかの AWS SDKs を使用して委任管理者アカウントを設定する場合は、EnableAWSServiceAccess オペレーションを明示的に呼び出し、サービスプリンシパルを

パラメータとして指定する必要があります。次に、EnableOrganizationAdminAccount を呼び出し、GuardDuty の管理者アカウントを委任します。

GuardDuty との信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、Organizations ツールを使用してのみ無効にできます。

信頼されたアクセスを無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で Amazon GuardDuty を信頼されたサービスとして無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal guardduty.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。

- AWS API: DisableAWSServiceAccess

GuardDuty 用の委任管理者アカウントの有効化

メンバーアカウントを組織の委任管理者として指定すると、そのアカウントのユーザーおよびロールは、GuardDuty の管理アクションを実行できるようになります。通常この管理アクションは、組織の管理アカウントのユーザーとロールだけが実行できるものです。この手法は、組織の管理から GuardDuty の管理を分離するのに有効です。

> **最小アクセス許可**
>
> メンバーアカウントを委任管理者として指定するために必要なアクセス許可については、Amazon GuardDuty ユーザーガイドの委任された管理者の指定に必要な権限を参照してください。

GuardDuty の委任管理者としてメンバーアカウントを指定するには

Designate a delegated administrator and add member accounts (console)、および Designate a delegated administrator and add member accounts (API) を参照してください。

AWS Health および AWS Organizations

AWS Health は、リソースのパフォーマンスと、 AWS のサービス および アカウントの可用性を継続的に可視化します。 は、 AWS リソースとサービスが問題の影響を受けているか、今後の変更の影響を受ける場合にイベント AWS Health を提供します。組織ビューを有効にすると、組織の管理アカウントのユーザーは、組織内のすべてのアカウントで AWS Health イベントを集約できます。組織ビューには、機能が有効になった後に配信された AWS Health イベントのみが表示され、90 日間保持されます。

組織ビューを有効にするには、 AWS Health コンソール、 (AWS CLI)、 AWS Command Line Interface または AWS Health API を使用します。

詳細については、「 AWS Health ユーザーガイド」の AWS Health 「イベントの集約」を参照してください。

次の情報は、 AWS Health との統合に役立ちます AWS Organizations。

統合のためのサービスにリンクされたロール

`AWSServiceRoleForHealth_Organizations` サービスにリンクされたロールにより AWS Health 、 はサポートされているオペレーションを組織内のアカウント内で実行できます。

このロールは、EnableHealthServiceAccessForOrganization API オペレーションを呼び出して信頼されたアクセスを有効にすると、組織の管理アカウントに自動的に作成されます。それ以外の場合は、「IAM ユーザーガイド」の「サービスにリンクされたロールの作成」の説明に従って、 AWS Health コンソール、API、または CLI を使用してロールを作成します。 https://docs.aws.amazon.com/IAM/latest/UserGuide/using-service-linked-roles.html#create-service-linked-role

このロールを削除または変更できるのは、 AWS Health と Organizations 間の信頼されたアクセスを無効にした場合、または組織からメンバーアカウントを削除した場合のみです。

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。で使用されるサービスにリンクされたロールは、次のサービスプリンシパルへのアクセス AWS Health を許可します。

- `health.amazonaws.com`

AWS Healthとの信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

の組織ビュー機能を有効にすると AWS Health、信頼されたアクセスも自動的に有効になります。

信頼されたアクセスは、 AWS Health コンソールまたは AWS Organizations コンソールを使用して有効にできます。

> **Important**
>
> 可能な限り、 AWS Health コンソールまたはツールを使用して Organizations との統合を有効にすることを強くお勧めします。これにより、 は、サービスに必要なリソースの作成など、必要な設定 AWS Health を実行できます。ここに示す手順は、統合の有効化に AWS Healthが提供するツールを使用できない場合にのみ実施してください。詳細については、この注意を参照してください。
> AWS Health コンソールまたはツールを使用して信頼されたアクセスを有効にする場合、これらのステップを実行する必要はありません。

AWS Health コンソールを使用して信頼されたアクセスを有効にするには

と次のいずれかのオプションを使用して AWS Health 、信頼されたアクセスを有効にできます。

- AWS Health コンソールを使用します。詳細については、AWS Health ユーザーガイドの組織ビュー (コンソール) を参照してください。
- AWS CLIを使用します。詳細については、AWS Health ユーザーガイドの組織ビュー (CLI) を参照してください。

- EnableHealthServiceAccessForOrganization API オペレーションを呼び出します。

信頼されたアクセスを有効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Health として を有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal health.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。
- AWS API: EnableAWSServiceAccess

AWS Healthとの信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

組織ビュー機能を無効にすると、 は組織内の他のすべてのアカウントのイベントの集計を AWS Health 停止します。また、信頼されたアクセスは自動的に無効になります。

信頼されたアクセスは、 AWS Health または AWS Organizations ツールを使用して無効にできます。

> **Important**
>
> 可能な限り、 AWS Health コンソールまたはツールを使用して Organizations との統合を無効にすることを強くお勧めします。これにより、 は、サービスで不要になったリソースやアクセスロールの削除など、必要なクリーンアップ AWS Health を実行できます。ここに示す

手順は、統合の無効化に AWS Healthが提供するツールを使用できない場合にのみ実施してください。
AWS Health コンソールまたはツールを使用して信頼されたアクセスを無効にする場合は、これらのステップを実行する必要はありません。

AWS Health コンソールを使用して信頼されたアクセスを無効にするには

信頼されたアクセスを無効にする方法には次のようなものがあります。

- AWS Health コンソールを使用します。詳細については、AWS Health ユーザーガイドの組織ビューの無効化 (コンソール) を参照してください。
- AWS CLIを使用します。詳細については、AWS Health ユーザーガイドの組織ビューの無効化 (CLI) を参照してください。
- DisableHealthServiceAccessForOrganization API オペレーションを呼び出します。

信頼されたアクセスを無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Health として を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal health.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。

- AWS API: DisableAWSServiceAccess

の委任管理者アカウントの有効化 AWS Health

メンバーアカウントを組織の委任管理者として指定すると、そのアカウントのユーザーおよびロールは、 AWS Health の管理アクションを実行できるようになります。通常この管理アクションは、組織の管理アカウントのユーザーとロールだけが実行できるものです。この手法は、 AWS Healthの管理から 組織の管理を分離するのに有効です。

メンバーアカウントを AWS Health の委任管理者として指定するには

「組織ビューに委任管理者を登録する」を参照してください。

AWS Health の委任管理者を削除するにほ

「組織ビューから委任管理者を削除する」を参照してください。

AWS Identity and Access Management and AWS Organizations

AWS Identity and Access Management は、 サービスへのアクセスを安全に制御するためのウェブ AWS サービスです。

IAM のサービスの最後にアクセスされたデータを使用することで、組織全体の AWS アクティビティをより詳しく把握できます。このデータを使用してサービスコントロールポリシー (SCP) を作成、更新し、組織のアカウントが使用する AWS サービスだけにアクセスを限定することができます。

設定例については、IAM ユーザーガイドの情報を使用した組織単位のアクセス許可の調整を参照してください。

IAM を使用すると、ルートユーザーの認証情報を一元管理し、メンバーアカウントで特権タスクを実行できます。で IAM の信頼されたアクセスを有効にするルートアクセス管理を有効にすると AWS Organizations、メンバーアカウントのルートユーザー認証情報を一元的に保護できます。メンバーアカウントは、ルートユーザーにサインインしたり、ルートユーザーのパスワードリカバリを実行したりできません。IAM の管理アカウントまたは委任管理者アカウントは、短期ルートアクセスを使用してメンバーアカウントでいくつかの特権タスクを実行することもできます。短期の特権セッションでは、組織内のメンバーアカウントで特権アクションを実行する範囲を絞り込むことができる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「メンバーアカウントのルートアクセスを一元管理する」を参照してください。

次の情報は、 AWS Identity and Access Management との統合に役立ちます AWS Organizations。

IAM による信頼されたアクセスの有効化

ルートアクセス管理を有効にすると、 で IAM に対して信頼されたアクセスが有効になります AWS Organizations。

IAM による信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

で信頼されたアクセスを無効にすることができるのは、 AWS Organizations 管理アカウントの管理者のみです AWS Identity and Access Management。

信頼されたアクセスは、Organizations ツールを使用してのみ無効にできます。

信頼されたアクセスを無効にするには、 AWS Organizations コンソールを使用するか、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを無効にするには

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 Identity and Access Management] を選択します。
4. Disable trusted access (信頼されたアクセスを無効にする) を選択します。
5. 「 の信頼されたアクセスを無効にする AWS Identity and Access Management」ダイアログボックスで、「Disable to confirm」と入力し、「Disable trusted access」を選択します。
6. の管理者のみの場合は AWS Organizations、 の管理者 AWS Identity and Access Management に、サービスコンソールまたはツール を使用して、そのサービスが で AWS Organizations 動作することを無効にできることを伝えます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを無効にすることができます。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Identity and Access Management として を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal iam.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。

- AWS API: DisableAWSServiceAccess

IAM の委任管理者アカウントの有効化

メンバーアカウントを組織の委任管理者として指定すると、そのアカウントのユーザーとロールは、メンバーアカウントで特権タスクを実行できます。それ以外の場合は、組織の管理アカウントのユーザーまたはロールのみが実行できます。詳細については、「IAM ユーザーガイド」の「Organizations メンバーアカウントで特権タスクを実行する」を参照してください。

IAM の委任管理者を設定できるのは、組織管理アカウントの管理者のみです。

委任管理者アカウントは、IAM コンソールまたは API から、または Organizations CLI または SDK オペレーションを使用して指定できます。

IAM の委任管理者の無効化

Organizations 管理アカウントまたは IAM 委任管理者アカウントの管理者のみが、組織から委任管理者アカウントを削除できます。Organizations CLI または SDK `DeregisterDelegatedAdministrator` オペレーションを使用して、委任管理を無効にすることができます。

Amazon Inspector と AWS Organizations

Amazon Inspector は、Amazon EC2 とコンテナのワークロードを継続的にスキャンして、ソフトウェアの脆弱性や意図しないネットワークの公開 (ネットワークエクスポージャー) を検出する、自動化された脆弱性管理サービスです。

Amazon Inspector を使用すると、Amazon Inspector の管理者アカウントを委任 AWS Organizations するだけで、 を介して関連付けられている複数のアカウントを管理できます。委任管理者は、組織

の Amazon Inspector を管理し、組織に代わって次のようなタスクを実行するための特別なアクセス許可が付与されます。

- メンバーアカウントへのスキャンを有効または無効にする
- 組織全体の集約された調査結果データを表示する
- 抑制ルールを作成して管理する

詳細については、「Amazon Inspector ユーザーガイド」の「AWS Organizationsで複数のアカウントを管理する」を参照してください。

Amazon Inspector を と統合するには、次の情報を使用します AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、Amazon Inspector は、サポートされているオペレーションを組織内の組織のアカウントで実行できます。

このロールを削除または変更できるのは、Amazon Inspector と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleForAmazonInspector2`

詳細については、「Amazon Inspector ユーザーガイド」の「Amazon Inspector でのサービスにリンクされたロールの使用」を参照してください。

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。Amazon Inspector によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `inspector2.amazonaws.com`

Amazon Inspector との信頼されたアクセスを有効にするには

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

Amazon Inspector では、メンバーアカウントを組織のこのサービスの委任管理者に指定 AWS Organizations する前に、 への信頼されたアクセスが必要です。

Amazon Inspector の委任管理者を指定すると、組織の Amazon Inspector に対する信頼されたアクセスが自動的に有効になります。

ただし、 CLI またはいずれかの AWS SDKs を使用して AWS 委任管理者アカウントを設定する場合は、 `EnableAWSServiceAccess`オペレーションを明示的に呼び出し、サービスプリンシパルをパラメータとして指定する必要があります。次に、`EnableDelegatedAdminAccount` を呼び出して Inspector 管理者アカウントを委任します。

信頼されたアクセスを有効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Amazon Inspector を Organizations の信頼されたサービスとして有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal inspector2.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。

- AWS API: EnableAWSServiceAccess

> **Note**
>
> `EnableAWSServiceAccess` API を使用している場合、`EnableDelegatedAdminAccount` も呼び出して Inspector 管理者アカウントを委任する必要があります。

Amazon Inspector との信頼されたアクセスを無効にするには

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

Amazon Inspector での信頼されたアクセスを無効にすることができるのは、 AWS Organizations 管理アカウントの管理者のみです。

信頼されたアクセスを無効にするには、Organizations ツールを使用する必要があります。

信頼されたアクセスを無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で Amazon Inspector を信頼されたサービスとして無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal inspector2.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。

- AWS API: DisableAWSServiceAccess

Amazon Inspector 用の委任管理者アカウントの有効化

Amazon Inspector では、 AWS Organizations サービスで委任された管理者を使用して、組織内の複数のアカウントを管理できます。

AWS Organizations 管理アカウントは、組織内のアカウントを Amazon Inspector の委任管理者アカウントとして指定します。委任管理者は、組織の Amazon Inspector を管理し、組織に代わってタスクを実行するための特別なアクセス許可が付与されます。タスクには、メンバーアカウントのスキャ

ンの有効化または無効化、組織全体の集約された調査結果データの表示、抑制ルールの作成および管理などが含まれます

委任管理者が組織アカウントを管理する方法については、「Amazon Inspector ユーザーガイド」の「管理者とメンバーアカウントの関係について」を参照してください。

Amazon Inspector 用の委任管理者を設定できるのは、組織管理アカウントの管理者だけです。

委任管理者アカウントを指定する場合は、Amazon Inspector コンソールまたは API を介して、あるいは Organizations CLI または SDK オペレーションを使用して行います。

> **最小アクセス許可**
>
> Organizations 管理アカウントのユーザーまたはロールのみが、組織内で Amazon Inspector の委任管理者としてメンバーアカウントを設定できます

Amazon Inspector コンソールを使用して委任管理者を設定するには、「Amazon Inspector ユーザーガイド」の「ステップ 1: Amazon Inspector を有効にする – Multi-account environment」を参照してください。

> **Note**
>
> Amazon Inspector を使用する各リージョンで、`inspector2:enableDelegatedAdminAccount` を呼び出す必要があります。

AWS CLI, AWS API

CLI またはいずれかの AWS SDKs を使用して AWS 委任管理者アカウントを設定する場合は、次のコマンドを使用できます。

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal inspector2.amazonaws.com
```

- AWS SDK: Organizations `RegisterDelegatedAdministrator`オペレーションとメンバーアカウントの ID 番号を呼び出し、アカウントサービスプリンシパルをパラメータ`account.amazonaws.com`として識別します。

Amazon Inspector 用の委任管理者の無効化

組織から委任された管理者アカウントを削除できるのは、 AWS Organizations 管理アカウントの管理者のみです。

委任管理者を削除する場合は、Amazon Inspector コンソールまたは API を介して、あるいは Organizations `DeregisterDelegatedAdministrator` CLI または SDK オペレーションを使用して行います。Amazon Inspector コンソールを使用して委任管理者を削除するには、「Amazon Inspector ユーザーガイド」の「委任管理者の削除」を参照してください。

AWS License Manager および AWS Organizations

AWS License Manager は、ソフトウェアベンダーライセンスをクラウドに持ち込むプロセスを合理化します。でクラウドインフラストラクチャを構築する際 AWS、BYOL (bring-your-own-license) の機会を使用すること、つまり、クラウドリソースで使用する既存のライセンスインベントリを再利用することで、コストを削減できます。管理者は、ライセンスの使用でルールベースのコントロールを使用することにより、新規および既存のクラウドのデプロイにソフト制限またはハード制限を設定し、準拠していないサーバーの使用を事前に停止できます。

License Manager について詳しくは、License Manager ユーザーガイドを参照してください。

License Manager を にリンクすることで AWS Organizations、次のことができます。

- 組織全体でコンピューティングリソースのクロスアカウントの検出を有効にすることができます。
- 所有して AWSに実行している商用 Linux サブスクリプションを表示および管理します。詳細については、「AWS License Managerの Linux サブスクリプション」を参照してください。

次の情報は、 AWS License Manager との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、次の「サービスにリンクされたロール」が組織の管理アカウントに自動的に作成されます。これらのロールにより、License Manager はサポートされているオペレーションを組織内のアカウントで実行できます。

ロールを削除または変更できるのは、License Manager と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合のみです。

- `AWSLicenseManagerMasterAccountRole`

- `AWSLicenseManagerMemberAccountRole`
- `AWSServiceRoleForAWSLicenseManagerRole`
- `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService`

詳細については、「License Manager における管理アカウントロール」、「License Manager におけるメンバーアカウントロール」、「License Manager における Linux サブスクリプションロール」を参照してください。

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。License Manager によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `license-manager.amazonaws.com`
- `license-manager.member-account.amazonaws.com`
- `license-manager-linux-subscriptions.amazonaws.com`

License Manager との信頼されたアクセスの有効化

を使用してのみ、信頼されたアクセスを有効にできます AWS License Manager。

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

License Manager との信頼されたアクセスを有効にするには

AWS Organizations 管理アカウントを使用して License Manager コンソールにサインインし、License Manager アカウントに関連付ける必要があります。詳細については、「 の設定 AWS License Manager」を参照してください。

License Manager との信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、Organizations ツールを使用してのみ無効にできます。

信頼されたアクセスを無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを無効にすることができます。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS License Manager としてを無効にできます。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal license-manager.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。

  Linux サブスクリプション用の信頼されたアクセスを無効にする手順は、次のとおりです。

  ```
  $  aws organizations disable-aws-service-access \
      --service-principal license-manager-linux-subscriptions.amazonaws.com
  ```

- AWS API: DisableAWSServiceAccess

License Manager 用の委任管理者アカウントの有効化

メンバーアカウントを組織の委任管理者として指定すると、そのアカウントのユーザーおよびロールは、 License Manager の管理アクションを実行できるようになります。通常この管理アクションは、組織の管理アカウントのユーザーとロールだけが実行できるものです。この手法は、組織の管理から License Manager の管理を分離するのに有効です。

License Manager の管理者をメンバーアカウントに委任するには、License Manager ユーザーガイドの委任された管理者の登録を参照してください。

AWS Managed Services (AMS) セルフサービスレポート (SSR) と AWS Organizations

AWS Managed Services (AMS) セルフサービスレポート (SSR) は、さまざまなネイティブ AWS サービスからデータを収集し、主要な AMS サービスに関するレポートへのアクセスを提供します。SSR は、オペレーション、設定管理、アセット管理、セキュリティ管理、コンプライアンスをサポートするために使用できる情報を提供します。

と統合したら AWS Organizations、集約セルフサービスレポート (SSR) を有効にできます。これは、Advanced および Accelerate のお客様が組織レベルで集計された既存のセルフサービスレポートをクロスアカウントで表示できるようにする AMS 機能です。これにより、パッチコンプライアンス、バックアップカバレッジ、インシデントなどの主要な運用メトリクスを、 内のすべての AMS マネージドアカウントで可視化できます AWS Organizations。

以下の情報は、 AWS Managed Services (AMS) セルフサービスレポート (SSR) と の統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、AMS はサポートされているオペレーションを組織内のアカウント内で実行できます。

このロールを削除または変更できるのは、AMS と Organizations 間の信頼されたアクセスを無効にした場合、または組織からメンバーアカウントを削除した場合のみです。

- `AWSServiceRoleForManagedServices_SelfServiceReporting`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。AMS で使用されるサービスにリンクされたロールは、次のサービスプリンシパルへのアクセスを許可します。

- `selfservicereporting.managedservices.amazonaws.com`

AMS による信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスを有効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、 AWS Managed Services (AMS) セルフサービスレポート (SSR) を Organizations の信頼されたサービスとして有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal selfservicereporting.managedservices.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。

- AWS API: EnableAWSServiceAccess

AMS での信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、Organizations ツールを使用してのみ無効にできます。

信頼されたアクセスを無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations の信頼されたサービスとして AWS Managed Services (AMS) セルフサービスレポート (SSR) を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal selfservicereporting.managedservices.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。
- AWS API: DisableAWSServiceAccess

AMS の委任管理者アカウントの有効化

委任された管理者アカウントは、すべてのアカウントの AMS レポート (パッチやバックアップなど) を AMS コンソールの単一の集約ビューで表示できます。

AMS コンソールまたは API を使用するか、Organizations CLI または SDK `RegisterDelegatedAdministrator` オペレーションを使用して、委任管理者を追加できます。

AMS の委任管理者の無効化

AMS の委任管理者を設定できるのは、組織管理アカウントの管理者のみです。

AMS コンソールまたは API を使用するか、Organizations CLI または SDK `DeregisterDelegatedAdministrator` オペレーションを使用して、委任管理者を削除できます。

Amazon Macie と AWS Organizations

Amazon Macie は、フルマネージド型のデータセキュリティおよびデータプライバシーサービスです。機械学習とパターンマッチングを使用して、Amazon Simple Storage Service (Amazon S3) 内の機密データを検出、モニタリングし、適切な保護を支援します。Macie は、組織が Amazon S3 に保存している個人を特定できる情報 (PII) や知的財産などの機密データを詳細に把握できるよう、そうしたデータの検出を自動化します。

詳細については、Amazon Macie ユーザーガイドの「Managing Amazon Macie accounts with AWS Organizations」を参照してください。

Amazon Macie を と統合するには、次の情報を使用します AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の委任された Macie 管理アカウントに自動的に作成されます。このロールにより、Macie はサポートされているオペレーションを組織内のアカウントに対して実行できます。

このロールを削除できるのは、Macie と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleRorAmazonMacie`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。Macie によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `macie.amazonaws.com`

Macie との信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要なアクセス許可に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

Amazon Macie コンソールまたは AWS Organizations コンソールを使用して、信頼されたアクセスを有効にできます。

> **Important**
>
> Organizations との統合の有効化には、可能な場合は常に Amazon Macie のコンソールまたはツールを使用することを強くお勧めします。そうすることで、サービスに必要なリソースの作成など、必要な構成が Amazon Macie で実行可能になります。ここに示す手順は、統合の有効化に Amazon Macie が提供するツールを使用できない場合にのみ実施してください。詳細については、この注意を参照してください。
> Amazon Macie のコンソールまたはツールを使用して信頼されたアクセスを有効にする場合、これらのステップを実施する必要はありません。

Macie コンソールを使用して信頼されたアクセスを有効にするには

Amazon Macie では、メンバーアカウントを組織の Macie 管理者として指定 AWS Organizations するために、 への信頼されたアクセスが必要です。Macie マネジメントコンソールを使用して委任管理者を設定すると、信頼されたアクセスが Macie によって自動的に有効になります。

詳細については、Amazon Macie ユーザーガイドの「Integrating and configuring an organization in Amazon Macie」を参照してください。

信頼されたアクセスを有効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Amazon Macie を Organizations の信頼されたサービスとして有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal macie.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。

- AWS API: EnableAWSServiceAccess

Macie 用の委任管理者アカウントの有効化

メンバーアカウントを組織の委任管理者として指定すると、そのアカウントのユーザーおよびロールは、 Macie の管理アクションを実行できるようになります。通常この管理アクションは、組織の管理アカウントのユーザーとロールだけが実行できるものです。この手法は、組織の管理から Macie の管理を分離するのに有効です。

最小アクセス許可

次の許可を持つ Organizations 管理アカウントのユーザーまたはロールのみが、組織内で Macie の委任管理者としてメンバーアカウントを設定できます。

- `organizations:EnableAWSServiceAccess`
- `macie:EnableOrganizationAdminAccount`

メンバーアカウントを Macie の委任管理者として指定するには

Amazon Macie では、メンバーアカウントを組織の Macie 管理者として指定 AWS Organizations するために、 への信頼されたアクセスが必要です。Macie マネジメントコンソールを使用して委任管理者を設定すると、信頼されたアクセスが Macie によって自動的に有効になります。

詳細については、「https://docs.aws.amazon.com/macie/latest/user/macie-organizations.html#register-delegated-admin」を参照してください

AWS Marketplace および AWS Organizations

AWS Marketplace は厳選されたデジタルカタログで、ソリューションを構築してビジネスを運営するために必要なサードパーティーのソフトウェア、データ、サービスを検索、購入、デプロイ、管理するために使用できます。

AWS Marketplace は、 での購入 AWS License Manager に を使用してライセンスを作成および管理します AWS Marketplace。組織内の他のアカウントとライセンスを共有 (アクセスを許可) すると、AWS Marketplace はそのアカウント用に新しいライセンスを作成し、管理します。

詳細については、AWS Marketplace 購入者ガイドの Service-linked roles for AWS Marketplace を参照してください。

次の情報は、 AWS Marketplace との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより AWS Marketplace 、 はサポートされているオペレーションを組織内のアカウント内で実行できます。

このロールを削除または変更できるのは、 AWS Marketplace と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleForMarketplaceLicenseManagement`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。で使用されるサービスにリンクされたロールは、次のサービスプリンシパルへのアクセス AWS Marketplace を許可します。

- `license-management.marketplace.amazonaws.com`

AWS Marketplaceとの信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、 AWS Marketplace コンソールまたは AWS Organizations コンソールを使用して有効にできます。

> **Important**
>
> 可能な限り、 AWS Marketplace コンソールまたはツールを使用して Organizations との統合を有効にすることを強くお勧めします。これにより、 は、サービスに必要なリソースの作成など、必要な設定 AWS Marketplace を実行できます。ここに示す手順は、統合の有効化に AWS Marketplaceが提供するツールを使用できない場合にのみ実施してください。詳細については、この注意を参照してください。
> AWS Marketplace コンソールまたはツールを使用して信頼されたアクセスを有効にする場合、これらのステップを実行する必要はありません。

AWS Marketplace コンソールを使用して信頼されたアクセスを有効にするには

「AWS Marketplace 購入者ガイド」の「AWS Marketplaceのサービスにリンクされたロールの作成」を参照してください。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [AWS Marketplace] 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. 「 の信頼されたアクセスを有効にする AWS Marketplace」ダイアログボックスで、「確認のために を有効にする」と入力し、「信頼されたアクセスを有効にする」を選択します。
6. の管理者のみである場合は AWS Organizations、 の管理者に、サービスコンソール からそのサービスが と AWS Organizations 連携できるようになった AWS Marketplace ことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Marketplace として を有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal license-management.marketplace.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。

- AWS API: EnableAWSServiceAccess

AWS Marketplaceとの信頼されたアクセスの無効化

信頼されたアクセスの有効化に必要なアクセス許可に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、Organizations ツールを使用してのみ有効にできます。

信頼されたアクセスを無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Marketplace として を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal license-management.marketplace.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。
- AWS API: DisableAWSServiceAccess

AWS Marketplace Private Marketplace と AWS Organizations

AWS Marketplace は厳選されたデジタルカタログで、ソリューションを構築してビジネスを運営するために必要なサードパーティーのソフトウェア、データ、サービスを検索、購入、デプロイ、管理するために使用できます。プライベートマーケットプレイスでは、 で利用可能な幅広い製品カタログと AWS Marketplace、それらの製品のきめ細かな制御が提供されます。

AWS Marketplace Private Marketplace を使用すると、組織全体、1 つ以上の OUs、または組織内の 1 つ以上のアカウントに関連付けられた複数のプライベートマーケットプレイスエクスペリエンスを作成し、それぞれに独自の承認済み製品のセットを作成できます。 AWS 管理者は、会社またはチームのロゴ、メッセージング、カラースキームを使用して、各プライベートマーケットプレイスエクスペリエンスに会社のブランドを適用することもできます。

詳細については、「AWS Marketplace 購入者ガイド」の「Using roles to configure Private Marketplace in AWS Marketplace」を参照してください。

AWS Marketplace Private Marketplace を と統合するには、次の情報を参考にしてください AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

AWS Marketplace Private Marketplace コンソールを使用して信頼されたアクセスを有効にすると、次のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、Private Marketplace はサポートされているオペレーションを組織内のアカウントで実行できます。Private Marketplace と Organizations AWS Marketplace 間の信頼されたアクセスを無効にし、組織内のすべてのプライベートマーケットプレイスエクスペリエンスの関連付けを解除する場合にのみ、このロールを削除または変更できます。

Organizations コンソール、CLI、または SDK から直接信頼されたアクセスを有効にすると、サービスにリンクされたロールは自動的に作成されません。

- `AWSServiceRoleForPrivateMarketplaceAdmin`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。Private Marketplace によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `private-marketplace.marketplace.amazonaws.com`

Private Marketplace による信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

Private Marketplace コンソールまたは AWS Marketplace コンソールを使用して、信頼された AWS Organizations アクセスを有効にできます。

> **Important**
>
> 可能な限り、 AWS Marketplace Private Marketplace コンソールまたはツールを使用して Organizations との統合を有効にすることを強くお勧めします。これにより、サービスに必要なリソースの作成など、必要な設定を AWS Marketplace Private Marketplace で実行できます。 AWS Marketplace Private Marketplace が提供するツールを使用して統合を有効にできない場合にのみ、これらのステップに進みます。詳細については、この注意を参照してください。
> AWS Marketplace Private Marketplace コンソールまたはツールを使用して信頼されたアクセスを有効にする場合、これらのステップを実行する必要はありません。

Private Marketplace コンソールを使用して信頼されたアクセスを有効にするには

「AWS Marketplace 購入者ガイド」の「Getting started with Private Marketplace」を参照してください。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・ インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [AWS Marketplace Private Marketplace] 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 Marketplace 「プライベートマーケットプレイスの信頼されたアクセスを有効にする」ダイアログボックスで、「確認のために有効にする」と入力し、「信頼されたアクセスを有効にする」を選択します。
6. の管理者のみである場合は AWS Organizations、サービスコンソール からそのサービスを操作 AWS Organizations できるようになったことを AWS Marketplace Private Marketplace の管理者に伝えます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、 Private Marketplace AWS Marketplace を Organizations の信頼されたサービスとして有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal private-marketplace.marketplace.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。
- AWS API: EnableAWSServiceAccess

Private Marketplace での信頼されたアクセスの無効化

信頼されたアクセスの有効化に必要なアクセス許可に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、Organizations ツールを使用してのみ無効にできます。

信頼されたアクセスを無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations の信頼されたサービスとして AWS Marketplace Private Marketplace を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
  ```

```
    --service-principal private-marketplace.marketplace.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。

- AWS API: DisableAWSServiceAccess

Private Marketplace 用の委任管理者アカウントの有効化

管理アカウント管理者は、委任された管理者と呼ばれる指定されたメンバーアカウントに Private Marketplace 管理アクセス許可を委任できます。アカウントをプライベートマーケットプレイスの委任管理者として登録するには、管理アカウント管理者は、信頼されたアクセスとサービスにリンクされたロールが有効になっていることを確認し、新しい管理者の登録を選択し、12 桁の AWS アカウント番号を指定して、送信を選択する必要があります。

管理アカウントと委任された管理者アカウントは、エクスペリエンスの作成、ブランド設定の更新、オーディエンスの関連付けまたは関連付け解除、製品の追加または削除、保留中のリクエストの承認または拒否などの Private Marketplace 管理タスクを実行できます。

Private Marketplace コンソールを使用して委任管理者を設定するには、「AWS Marketplace 購入者ガイド」の「Creating and managing a private marketplace」を参照してください。

Organizations `RegisterDelegatedAdministrator` API を使用して、委任された管理者を設定することもできます。詳細については、「Organizations Command Reference」(Organizations コマンドリファレンス) で、「RegisterDelegatedAdministrator」を参照してください。

Private Marketplace の委任された管理者の無効化

Private Marketplace の委任管理者を構成できるのは、組織管理アカウントの管理者のみです。

委任管理者アカウントを削除する場合は、Private Marketplace コンソールまたは API を使用して、あるいは Organizations `DeregisterDelegatedAdministrator` CLI または SDK オペレーションを使用して行います。

Private Marketplace コンソールを使用して委任管理者 Private Marketplace アカウントを無効にするには、「AWS Marketplace 購入者ガイド」の「Creating and managing a private marketplace」を参照してください。

AWS Marketplace 調達インサイトダッシュボードと AWS Organizations

AWS Marketplace 調達インサイトダッシュボードを使用して、組織内のすべての AWS アカウントの契約とコスト分析データを表示します。Organizations と統合すると、 AWS Marketplace 調達イン

サイトダッシュボードは、組織に参加するアカウントなどの組織の変更を聞き、対応する契約のデータを集約してダッシュボードを構築します。

詳細については、「AWS Marketplace 購入者ガイド」の「Procurement insights」を参照してください。

調達 AWS Marketplace インサイトダッシュボードを と統合するには、次の情報を使用します AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロールと管理ポリシー

AWS Marketplace 調達インサイトダッシュボードをアクティブ化すると、AWSServiceRoleForProcurementInsightsPolicyサービスにリンクされたロールとAWSServiceRoleForProcurementInsightsPolicy AWS 管理ポリシーが作成されます。

AWS Marketplace 調達インサイトによる信頼されたアクセスの有効化

信頼されたアクセスを有効にすると、 AWS Marketplace 調達インサイトダッシュボードはお客様の Organizations サービスと統合できます。 AWS Marketplace 調達インサイトダッシュボードは、組織に参加するアカウントなどの組織の変更を聞き、対応する契約のデータを集約してダッシュボードを構築します。

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

AWS Marketplace 調達インサイトダッシュボードコンソールまたは コンソールを使用して、信頼された AWS Organizations アクセスを有効にできます。

> **Important**
>
> 可能な限り、 AWS Marketplace 調達インサイトダッシュボードコンソールまたはツールを使用して Organizations との統合を有効にすることを強くお勧めします。これにより、 AWS Marketplace 調達インサイトダッシュボードは、サービスに必要なリソースの作成など、必要な設定を実行できます。これらのステップは、 AWS Marketplace 調達インサイトダッシュボードが提供するツールを使用して統合を有効にできない場合にのみ実行してください。詳細については、この注意を参照してください。
> AWS Marketplace 調達インサイトダッシュボードコンソールまたはツールを使用して信頼されたアクセスを有効にする場合、これらのステップを実行する必要はありません。

AWS Marketplace 調達インサイトダッシュボードを有効にして信頼されたアクセスを有効にするには

「 AWS Marketplace 購入者ガイド」の AWS Marketplace 「調達インサイトダッシュボードの有効化」を参照してください。

Organizations ツールを使用して、信頼されたアクセスを有効するには

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [AWS Marketplace 調達インサイトダッシュボード] 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 Marketplace 「調達インサイトの信頼されたアクセスを有効にする」ダッシュボードダイアログボックスで、「確認のために を有効にする」と入力し、「信頼されたアクセスを有効にする」を選択します。
6. の管理者のみである場合は AWS Organizations、 AWS Marketplace 調達インサイトダッシュボードの管理者に、サービスコンソール からそのサービスが と AWS Organizations 連携できるようになったことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations の信頼されたサービスとして AWS Marketplace 調達インサイトダッシュボードを有効にします。

```
$ aws organizations enable-aws-service-access \
    --service-principal procurement-insights.marketplace.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。

- AWS API: EnableAWSServiceAccess

AWS Marketplace 調達インサイトによる信頼されたアクセスの無効化

信頼されたアクセスの有効化に必要なアクセス許可に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、Organizations ツールを使用してのみ無効にできます。

信頼されたアクセスを無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations の信頼されたサービスとして AWS Marketplace 調達インサイトダッシュボードを無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal procurement-insights.marketplace.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。
- AWS API: DisableAWSServiceAccess

AWS Marketplace 調達インサイトの委任管理者アカウントの有効化

AWS Marketplace 調達インサイトコンソールで委任管理者を設定するには、「 AWS Marketplace 購入者ガイド」の「委任管理者の登録 > 」を参照してください。

Organizations `RegisterDelegatedAdministrator` API を使用して、委任された管理者を設定することもできます。詳細については、「Organizations Command Reference」(Organizations コマンドリファレンス) で、「RegisterDelegatedAdministrator」を参照してください。

AWS Marketplace 調達インサイトの委任管理者の無効化

組織管理アカウントの管理者のみが、 AWS Marketplace 調達インサイトの委任管理者を設定できます。

AWS Marketplace 調達インサイトコンソールから委任管理者を削除するには、「 購入者ガイド」の「委任管理者の登録解除」を参照してください。 AWS Marketplace

Organizations の `DeregisterDelegatedAdministrator` CLI または SDK オペレーションを使用して、委任管理者を削除することもできます。

AWS Network Manager と AWS Organizations

Network Manager を使用すると、 AWS アカウント、リージョン、オンプレミスロケーション間で AWS Cloud WAN コアネットワークと Transit Gateway ネットワークを AWS 一元管理できます。マルチアカウントサポートを使用すると、任意の AWS アカウントに単一のグローバルネットワークを作成し、Network Manager コンソールを使用して複数のアカウントからグローバルネットワークにトランジットゲートウェイを登録できます。

Network Manager と Organizations 間の信頼されたアクセスを有効にすると、登録された委任管理者と管理アカウントは、メンバーアカウントに展開されたサービスリンクの役割を利用して、グローバルネットワークに接続されたリソースを説明できます。Network Manager コンソールから、登録された委任管理者と管理アカウントは、メンバーアカウントに展開されたカスタム IAM ロール (マルチアカウントの監視とイベント、およびマルチアアクウントリソースの表示と管理のためのコンソールスイッチのロールアクセス) を引き受けることができます。

> **Important**
>
> - Network Manager コンソールを使用してマルチアカウント設定 (信頼されたアクセスの有効化/無効化、委任された管理者の登録/解除)を管理することを強くお勧めします。コンソールからこれらの設定を管理すると、マルチアカウント· アクセスに必要なメンバーアカウントに、必要なすべてのサービスにリンクされたロールとカスタム IAM ロールが自動的に配備され、管理されます。
> - Network Manager コンソールで Network Manager の信頼されたアクセスを有効にすると、コンソールは AWS CloudFormation StackSets サービスも有効にします。ネットワー

ク· マネージャーは StackSets を使用して、マルチアカウント管理に必要なカスタム IAM ロールを配備にします。

Network Manager とOrganizations の統合の詳細については、「Amazon VPC User Guide」の「ネットワークマネージャで複数のアカウントを管理する」を参照してください。

Network AWS Manager を と統合するには、次の情報を使用します AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、リストされた組織アカウントに以下のようなサービスにリンクされたロールが自動的に作成されます。これらのロールにより、Nettwork Managerは組織のアカウント内でサポートされている操作を実行できます。信頼されたアクセスを無効にした場合、Network Manager は組織内のアカウントからこれらのロールを削除しません。IAM コンソールを使用して手動で削除できます。

管理アカウント

- `AWSServiceRoleForNetworkManager`
- `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`
- `AWSServiceRoleForCloudWatchCrossAccount`

メンバーアカウント

- `AWSServiceRoleForNetworkManager`
- `AWSServiceRoleForCloudFormationStackSetsOrgMember`

メンバーアカウントを委任された管理者として登録すると、委任された管理者アカウントに次の追加ロールが自動的に作成されます。

- `AWSServiceRoleForCloudWatchCrossAccount`

サービスにリンクされたロールで使用されるサービスプリンシパル

サービスにリンクされたロールは、そのロールに定義された信頼関係によって承認されたサービスプリンシパルのみが担うことができる。

- ロールの場合、アクセス権を持つ唯一のサービスプリンシパルです。
- サービスにリンクされたロールの場合、アクセス権を持つ唯一のサービスプリンシパルです。
- サービスにリンクされたロールの場合、アクセス権を持つ唯一のサービスプリンシパルです。
- サービスにリンクされたロールの場合、アクセス権を持つ唯一のサービスプリンシパルです。

これらのロールを削除すると、ネットワーク・マネージャのマルチ・アカウント機能が損なわれます。

ネットワーク・マネージャーで信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

Organizations 管理アカウントの管理者のみが、別の AWS サービスで信頼されたアクセスを有効にするアクセス許可を持っています。権限の問題を回避するために、ネットワーク・マネージャを必ず使用して、信頼されたアクセスを有効にします。詳細については、「Amazon VPC ユーザーガイド」の 「Manage multiple accounts in Network Manager with」を参照してください。

Network Manager との信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

Organizations 管理アカウントの管理者のみが、別の AWS サービスでの信頼されたアクセスを無効にするアクセス許可を持っています。

> **Important**
>
> 信頼されたアクセスを無効にするには、Network Manager コンソールを使用することを強くお勧めします。API や AWS CloudFormation コンソール AWS CLIなどで信頼されたアクセスを無効にすると、デプロイされた AWS CloudFormation StackSets とカスタム IAM ロールが適切にクリーンアップされない場合があります。信頼されたサービスのアクセスを無効にするには、Network Manager コンソールにサイン・インします。

Network Manager 用の委任管理者アカウントの有効化

メンバーアカウントを組織の委任管理者として指定すると、そのアカウントのユーザーおよびロールは、 Network Manager の管理アクションを実行できるようになります。それ以外の場合は、この

管理アクションは、組織の管理アカウントのユーザーとロールだけが実行できるものです。この手法は、Network Manager の管理を組織の管理から分離するのに有効です。

メンバーアカウントを組織の StackSets の委任管理者として指定する手順については、 ユーザーガイドの委任された管理者の登録を参照してください。

Amazon Q Developer と AWS Organizations

Amazon Q Developer は、生成 AI を活用した会話型アシスタントで、 AWS アプリケーションの理解、構築、拡張、運用に役立ちます。また Amazon Q Developer は、リアルタイムでコードの推奨を提供する汎用の機械学習を利用したコードジェネレーターでもあります。Amazon Q Developer の有料サブスクリプションバージョンには、Organizations の統合が必要です。詳細については、「Amazon Q ユーザーガイド」の「Account, IAM Identity Center, and Organizations setup」を参照してください。

Amazon Q Developer を と統合するには、次の情報を使用します AWS Organizations。

サービスにリンクされた役割

`AWSServiceRoleForAmazonQDeveloper` サービスにリンクされたロールにより、Amazon Q Developer は組織内でサポートされているオペレーションを実行できます。「IAM ユーザーガイド」の「サービスにリンクされたロールの作成」の説明に従って、Amazon Q Developer コンソール、API、または CLI を使用してロールを作成します。

メンバーアカウントを使用している場合、このロールを削除または変更できるのは、Amazon Q Developer と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

Amazon Q Developer で使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。Amazon Q Developer によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `q.amazonaws.com`

Amazon Q Developer での信頼されたアクセスの有効化

Amazon Q Developer Pro は、信頼されたアクセスを使用して、Organizations 管理アカウントで行われた設定を同じ組織のメンバーアカウントと共有します。

例えば、Amazon Q Developer Pro 管理者は Organizations 管理アカウントで作業し、コード参照を使用して提案を有効にできます。信頼されたアクセスが有効になっている場合、その組織内のすべてのメンバーアカウントでもコードリファレンスを含む提案が有効になります。

Amazon Q Developer を使用してのみ、信頼されたアクセスを有効にできます。

Amazon Q Developer の信頼されたアクセスを有効にするには、この手順を使用します。

1. Amazon Q Developer [設定] ページの [メンバーアカウント設定] で、[編集] を選択します。
2. ポップアップウィンドウで [確認] を選択します。
3. [Save] を選択します。

詳細については、「Amazon Q Developer user guide」の「Enabling trusted access」を参照してください。

Amazon Q Developer での信頼されたアクセスの無効化

信頼されたアクセスを無効にするには、Amazon Q Developer ツールを使用する必要があります。

Amazon Q Developer の信頼されたアクセスを無効にするには、この手順を使用します。

1. Amazon Q Developer [設定] ページの [メンバーアカウント設定] で、[編集] を選択します。
2. ポップアップウィンドウで [オフ] を選択します。
3. [Save] を選択します。

詳細については、「Amazon Q Developer user guide」の「Enabling trusted access」を参照してください。

AWS Resource Access Manager および AWS Organizations

AWS Resource Access Manager （ AWS RAM) を使用すると、所有している指定された AWS リソースを他の と共有できます AWS アカウント。これは、複数のアカウント間でさまざまなタイプ

の AWS リソースを共有するための一貫したエクスペリエンスを提供する一元化されたサービスです。

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

次の情報は、 AWS Resource Access Manager との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより AWS RAM 、 はサポートされているオペレーションを組織内のアカウント内で実行できます。

このロールを削除または変更できるのは、 AWS RAM と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleForResourceAccessManager`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。で使用されるサービスにリンクされたロールは、次のサービスプリンシパルへのアクセス AWS RAM を許可します。

- `ram.amazonaws.com`

AWS RAMとの信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、 AWS Resource Access Manager コンソールまたは AWS Organizations コンソールを使用して有効にできます。

> **Important**
>
> 可能な限り、 AWS Resource Access Manager コンソールまたはツールを使用して Organizations との統合を有効にすることを強くお勧めします。これにより、 はサービスに

必要なリソースの作成など、必要な設定 AWS Resource Access Manager を実行できます。ここに示す手順は、統合の有効化に AWS Resource Access Managerが提供するツールを使用できない場合にのみ実施してください。詳細については、この注意を参照してください。AWS Resource Access Manager コンソールまたはツールを使用して信頼されたアクセスを有効にする場合、これらのステップを実行する必要はありません。

AWS RAM コンソールまたは CLI を使用して信頼されたアクセスを有効にするには

AWS RAM ユーザーガイドの Enable Sharing with AWS Organizations を参照してください。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [AWS Resource Access Manager] 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. 「信頼されたアクセスを有効にする AWS Resource Access Manager」ダイアログボックスで、「確認のために を有効にする」と入力し、「信頼されたアクセスを有効にする」を選択します。
6. の管理者のみである場合は AWS Organizations、 の管理者に、サービスコンソール からそのサービスが と AWS Organizations 連携できるようになった AWS Resource Access Manager ことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Resource Access Manager として を有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal ram.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。

- AWS API: EnableAWSServiceAccess

AWS RAMとの信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、 AWS Resource Access Manager または AWS Organizations ツールを使用して無効にできます。

> **Important**
>
> 可能な限り、 AWS Resource Access Manager コンソールまたはツールを使用して Organizations との統合を無効にすることを強くお勧めします。これにより、 は、サービスで不要になったリソースやアクセスロールの削除など、必要なクリーンアップ AWS Resource Access Manager を実行できます。ここに示す手順は、統合の無効化に AWS Resource Access Managerが提供するツールを使用できない場合にのみ実施してください。AWS Resource Access Manager コンソールまたはツールを使用して信頼されたアクセスを無効にする場合、これらのステップを実行する必要はありません。

AWS Resource Access Manager コンソールまたは CLI を使用して信頼されたアクセスを無効にするには

AWS RAM ユーザーガイドの Enable Sharing with AWS Organizations を参照してください。

信頼されたアクセスを無効にするには、 AWS Organizations コンソールを使用するか、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを無効にするには

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 Resource Access Manager] を選択します。
4. Disable trusted access (信頼されたアクセスを無効にする) を選択します。
5. 「 の信頼されたアクセスを無効にする AWS Resource Access Manager」ダイアログボックスで、「確認のために無効化」と入力し、「信頼されたアクセスを無効にする」を選択します。
6. の管理者のみの場合は AWS Organizations、 の管理者 AWS Resource Access Manager に、サービスコンソールまたはツール を使用して、そのサービスが で AWS Organizations 動作することを無効にできることを伝えます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを無効にすることができます。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Resource Access Manager として を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ram.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。

- AWS API: DisableAWSServiceAccess

AWS Resource Explorer および AWS Organizations

AWS Resource Explorer はリソース検索および検出サービスです。Resource Explorer では、インターネット検索エンジンのようなエクスペリエンスを使用して、Amazon Elastic Compute Cloud インスタンス、Amazon Kinesis Data Streams、または Amazon DynamoDB テーブルなどのリソースを調べることができます。リソースは、名前、タグ、および ID などのリソースメタデータを使用して検索できます。Resource Explorer は、 アカウントの AWS リージョン間で動作し、クロスリージョンワークロードを簡素化します。

Resource Explorer を と統合すると AWS Organizations、評価の範囲内に組織の複数の を含めることで、より広範なソース AWS アカウント から証拠を収集できます。

次の情報は、 AWS Resource Explorer との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールは、組織内のアカウントでサポートされている操作を Resource Explorer が実行できるようにします。

このロールを削除または変更できるのは、Resource Explorer と Organizations 間における信頼されたアクセスを無効にした場合か、組織からメンバーアカウントを削除した場合のみです。

Resource Explorer がこのロールを使用する方法の詳細については、「AWS Resource Explorer ユーザーガイド」の「サービスリンクロールの使用」を参照してください。

- `AWSServiceRoleForResourceExplorer`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。Resource Explorer が使用するサービスリンクロールは、次のサービスプリンシパルにアクセス許可を付与します。

- `resource-explorer-2.amazonaws.com`

AWS Resource Explorerとの信頼されたアクセスを有効にする

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

Resource Explorer では、メンバーアカウントを組織の委任管理者として指定 AWS Organizations する前に、 への信頼されたアクセスが必要です。

信頼されたアクセスは、Resource Explorer コンソールまたは Organizations コンソールを使用して有効にできます。可能な場合は常に、Resource Explorer のコンソールまたはツールを使用して Organizations との統合を有効にすることを強くお勧めします。これにより、 はサービスに必要なリソースの作成など、必要な設定 AWS Resource Explorer を実行できます。

Resource Explorer コンソールを使用して信頼されたアクセスを有効にする

信頼されたアクセスを有効にする手順については、「AWS Resource Explorer ユーザーガイド」の「Resource Explorer の使用に対する前提条件」を参照してください。

> **Note**
>
> AWS Resource Explorer コンソールを使用して委任管理者を設定すると、 によって信頼されたアクセス AWS Resource Explorer が自動的に有効になります。

信頼されたアクセスを有効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Resource Explorer として を有効にします。

```
$ aws organizations enable-aws-service-access \
```

```
    --service-principal resource-explorer-2.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。

- AWS API: EnableAWSServiceAccess

Resource Explorer との信頼されたアクセスを無効にする

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

で信頼されたアクセスを無効にすることができるのは、 AWS Organizations 管理アカウントの管理者のみです AWS Resource Explorer。

信頼されたアクセスは、 AWS Resource Explorer または AWS Organizations ツールを使用して無効にできます。

> **Important**
>
> 可能な限り、 AWS Resource Explorer コンソールまたはツールを使用して Organizations との統合を無効にすることを強くお勧めします。これにより、 は、サービスで不要になったリソースやアクセスロールの削除など、必要なクリーンアップ AWS Resource Explorer を実行できます。ここに示す手順は、統合の無効化に AWS Resource Explorerが提供するツールを使用できない場合にのみ実施してください。
> AWS Resource Explorer コンソールまたはツールを使用して信頼されたアクセスを無効にする場合、これらのステップを実行する必要はありません。

信頼されたアクセスを無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: disable-aws-service-access

次のコマンドを実行して、Organizations で信頼されたサービス AWS Resource Explorer として を無効にします。

```
$ aws organizations disable-aws-service-access \
    --service-principal resource-explorer-2.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。

- AWS API: DisableAWSServiceAccess

Resource Explorer 用の委任管理者アカウントの有効化

委任管理者アカウントを使用してマルチアカウントリソースビューを作成し、組織単位または組織全体にスコープします。リソース共有を作成 AWS Resource Access Manager することで、 を介して組織内の任意のアカウントとマルチアカウントビューを共有できます。

> **最小アクセス許可**
>
> 組織内の Resource Explorer 用の委任管理者としてメンバーアカウントを設定できるのは、以下の許可を持つ Organizations 管理アカウントのユーザーまたはロールのみです。`resource-explorer:RegisterAccount`

Resource Explorer 用の委任管理者アカウントを有効にする手順については、「AWS Resource Explorer ユーザーガイド」の「セットアップ」を参照してください。

AWS Resource Explorer コンソールを使用して委任管理者を設定すると、Resource Explorer によって信頼されたアクセスが自動的に有効になります。

AWS CLI, AWS API

CLI またはいずれかの AWS SDKs を使用して AWS 委任管理者アカウントを設定する場合は、次のコマンドを使用できます。

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal resource-explorer-2.amazonaws.com
```

- AWS SDK: Organizations `RegisterDelegatedAdministrator`オペレーションとメンバーアカウントの ID 番号を呼び出し、アカウントサービスをパラメータ`resource-explorer-2.amazonaws.com`として識別します。

Resource Explorer 用の委任管理者の無効化

Resource Explorer 用の委任管理者を削除できるのは、Organizations の管理アカウント、または Resource Explorer の委任管理者アカウントの管理者のみです。信頼されたアクセスは、Organizations `DeregisterDelegatedAdministrator` CLI または SDK 操作を使用して無効にできます。

AWS Security Hub および AWS Organizations

AWS Security Hub は、 のセキュリティ状態を包括的に把握 AWS し、セキュリティ業界標準とベストプラクティスに照らして環境をチェックするのに役立ちます。

Security Hub は、 全体 AWS アカウント、 AWS のサービス 使用する 、およびサポートされているサードパーティーパートナー製品からセキュリティデータを収集します。セキュリティの傾向を分析し、特に優先度の高いセキュリティ問題を特定するのに役立ちます。

Security Hub と の両方を同時に使用すると AWS Organizations 、追加された新しいアカウントを含め、すべてのアカウントに対して Security Hub を自動的に有効にできます。これにより、Security Hub のチェックと検出がより広範囲に行えるようになり、セキュリティ体制の全体像をより包括的かつ正確に把握できます。

Security Hub について詳しくは、AWS Security Hub ユーザーガイドを参照してください。

次の情報は、 AWS Security Hub との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、Security Hub はサポートされているオペレーションを組織内のアカウントで実行できます。

このロールを削除または変更できるのは、Security Hub と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleForSecurityHub`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。Security Hub によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `securityhub.amazonaws.com`

Security Hub との信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要なアクセス許可に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

Security Hub に委任管理者を指定すると、Security Hub に対する信頼されたアクセスが Security Hub によって自動的に有効になります。

Security Hub との信頼できるアクセスの無効化

信頼されたアクセスを無効にするために必要なアクセス許可については、「AWS Organizations ユーザーガイド」の「Permissions required to disable trusted access」を参照してください。

信頼されたアクセスを無効にする前に、必要に応じて組織の委任管理者に連絡して、メンバーアカウントの Security Hub を無効にし、それらのアカウントの Security Hub リソースをクリーンアップしてください。

信頼されたアクセスを無効にするには、 AWS Organizations コンソール、Organizations API、または を使用します AWS CLI。Security Hub との信頼されたアクセスを無効にできるのは、Organizations の管理アカウントの管理者だけです。

Security Hub で信頼されたアクセスを無効にする手順については、「Disabling Security Hub integration with AWS Organizations」を参照してください。

Security Hub 用の委任管理者の有効化

メンバーアカウントを組織の委任管理者として指定すると、そのアカウントのユーザーおよびロールは、Security Hub の管理アクションを実行できるようになります。通常この管理アクションは、組織の管理アカウントのユーザーとロールだけが実行できるものです。この手法は、組織の管理から Security Hub の管理を分離するのに有効です。

詳細については、AWS Security Hub ユーザーガイドの Security Hub 管理者アカウントの指定を参照してください。

メンバーアカウントを Security Hub の委任管理者として指定するには

1. Organizations の管理アカウントでサインインします。
2. 次のいずれかを実行します。
   - 管理アカウントで Security Hub が有効になっていない場合は、Security Hub コンソールで [Go to Security Hub] (Security Hub に移動) を選択します。
   - 管理アカウントで Security Hub が有効になっている場合は、Security Hub コンソールの [一般] で [設定] を選択します。
3. [Delegated Administrator] (委任管理者) に、アカウント ID を入力します。

Security Hub の委任管理者の無効化

委任 Security Hub 管理者アカウントを削除することができるのは、組織管理アカウントでのみです。

委任 Security Hub 管理者を変更するには、まず現在の委任された管理者アカウントを削除してから、新しいアカウントを指定する必要があります。

Security Hub コンソールを使用して、あるリージョンの委任管理者を削除すると、その管理者はすべてのリージョンから自動的に削除されます。

Security Hub API は、API コールまたはコマンドが発行されたリージョンでのみ委任 Security Hub 管理者アカウントを削除します。他のリージョンでもこの操作を繰り返す必要があります。

Organizations API を使用して委任 Security Hub 管理者アカウントを削除すると、すべてのリージョンで自動的に削除されます。

委任 Security Hub 管理者を無効にする手順については、「Removing or changing the delegated administrator」を参照してください。

Amazon S3 Storage Lens と AWS Organizations

Amazon S3 Storage Lens に組織への信頼されたアクセスを許可することで、組織 AWS アカウント内のすべての でメトリクスを収集および集計できます。S3 Storage Lens は、これを実行するにあたり、組織に属するアカウントのリストにアクセスします。そして、すべてのアカウントのストレージ、使用状況、アクティビティのメトリクスを収集して分析します。

詳細については、Amazon S3 Storage Lens ユーザーガイドの Amazon S3 Storage Lens でのサービスにリンクされたロールの使用を参照してください。

Amazon S3 Storage Lens を と統合するには、次の情報を使用します AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にし、Storage Lens の設定が組織に適用されていると、以下のサービスにリンクされたロールが組織の代理管理者アカウントに自動的に作成されます。このロールにより、Amazon S3 Storage Lens はサポートされているオペレーションを組織内のアカウントで実行できます。

このロールを削除または変更できるのは、Amazon S3 Storage Lens と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleForS3StorageLens`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。Amazon S3 Storage Lens によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `storage-lens.s3.amazonaws.com`

Amazon S3 Storage Lens との信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要なアクセス許可に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

Amazon S3 Storage Lens コンソールまたは AWS Organizations コンソールを使用して、信頼されたアクセスを有効にできます。

> **Important**
>
> Organizations との統合の有効化には、可能な場合は常に Amazon S3 Storage Lens のコンソールまたはツールを使用することを強くお勧めします。そうすることで、サービスに必要

なリソースの作成など、必要な構成が Amazon S3 Storage Lens で実行可能になります。ここに示す手順は、統合の有効化に Amazon S3 Storage Lens が提供するツールを使用できない場合にのみ実施してください。詳細については、こちらの注意事項を参照してください。詳細については、この注意を参照してください。
Amazon S3 Storage Lens のコンソールまたはツールを使用して信頼されたアクセスを有効にする場合、これらのステップを実施する必要はありません。

Amazon S3 コンソールを使用して信頼されたアクセスを有効にするには

「Amazon Simple Storage Service ユーザーガイド」の「S3 ストレージレンズのため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。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・ インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [Amazon S3 ストレージレンズ] 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. Amazon S3 Storage Lens の信頼されたアクセスを有効にするダイアログボックスで、確認のために enable と入力し、信頼されたアクセスを有効にするを選択します。
6. の管理者のみである場合は AWS Organizations、Amazon S3 Storage Lens の管理者に、サービスコンソール からそのサービスが と AWS Organizations 連携できるようになったことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Amazon S3 Storage Lens を Organizations の信頼されたサービスとして有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal storage-lens.s3.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。
- AWS API: EnableAWSServiceAccess

Amazon S3 Storage Lens との信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

Amazon S3 Storage Lens ツールを使用してのみ、信頼されたアクセスを無効にできます。

Amazon S3 コンソール、、 AWS CLI または任意の AWS SDKs を使用して、信頼されたアクセスを無効にできます。

Amazon S3 コンソールを使用して信頼されたアクセスを無効にするには

「Amazon Simple Storage Service ユーザーガイド」の「S3 ストレージレンズのための信頼されたアクセスを無効にする」を参照してください。

Amazon S3 Storage Lens 用の代理管理者アカウントの有効化

メンバーアカウントを組織の代理管理者として指定すると、そのアカウントのユーザーおよびロールは、 Amazon S3 Storage Lens の管理アクションを実行できるようになります。通常この管理アクションは、組織の管理アカウントのユーザーとロールだけが実行できるものです。この手法は、組織の管理から Amazon S3 Storage Lens の管理を分離するのに有効です。

> **最小アクセス許可**
>
> 次の許可を持つ Organizations 管理アカウントのユーザーまたはロールのみが、組織内で Amazon S3 ストレージレンズの委任管理者としてメンバーアカウントを設定できます。
> `organizations:RegisterDelegatedAdministrator`
> `organizations:DeregisterDelegatedAdministrator`

Amazon S3 Storage Lens は、組織内の代理管理者アカウントを最大で 5 つまでサポートしています。

Amazon S3 Storage Lens の代理管理者としてメンバーアカウントを指定するには

委任された管理者は、Amazon S3 コンソール、、 AWS CLI または任意の AWS SDKs を使用して登録できます。Amazon S3 コンソールを使用して、組織の代理管理者アカウントとしてメンバーアカウントを登録するには、「Amazon Simple Storage Service ユーザーガイド」の「Registering a delegated administrator for S3 Storage Lens」を参照してください。

Amazon S3 Storage Lens の代理管理者の登録を解除するには

Amazon S3 コンソール、、 AWS CLI または任意の AWS SDKs を使用して、委任管理者の登録を解除できます。Amazon S3 コンソールを使用して委任管理者の登録を解除するには、「Amazon Simple Storage Service ユーザーガイド」の「S3 ストレージレンズでの委任管理者の登録を解除する」を参照してください。

AWS セキュリティインシデント対応と AWS Organizations

AWS Security Incident Response は、24 時間 365 日のライブで、人によるセキュリティインシデントサポートを提供するセキュリティサービスです。これにより、お客様は認証情報の盗難やランサムウェア攻撃などのサイバーセキュリティインシデントに迅速に対応できます。Organizations と統合することで、組織全体のセキュリティカバレッジを有効にします。詳細については、AWS「 Security Incident Response ユーザーガイド」の「Managing Security Incident Response accounts with AWS Organizations 」を参照してください。

次の情報は、 AWS セキュリティインシデント対応を と統合するのに役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、次の「サービスにリンクされたロール」が組織の管理アカウントに自動的に作成されます。

- `AWSServiceRoleForSecurityIncidentResponse` - Security Incident Response メンバーシップの作成に使用されます - を通じたサービスへのサブスクリプション AWS Organizations。
- `AWSServiceRoleForSecurityIncidentResponse_Triage` - サインアップ中にトリアージ機能を有効にした場合にのみ使用されます。

セキュリティインシデント対応で使用されるサービスプリンシパル

前のセクションのサービスにリンクされたロールは、ロールに定義された信頼関係によって承認されたサービスプリンシパルのみが引き受けることができます。Security Incident Response で使用されるサービスにリンクされたロールは、次のサービスプリンシパルへのアクセスを許可します。

- `security-ir.amazonaws.com`

セキュリティインシデント対応への信頼されたアクセスの有効化

Security Incident Response への信頼されたアクセスを有効にすると、サービスが組織の構造を追跡し、組織内のすべてのアカウントにアクティブなセキュリティインシデントカバレッジがあることを確認できます。また、トリアージ機能を有効にすると、サービスにリンクされたロールをメンバーアカウントで使用して、機能のトリアージを行うこともできます。

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

セキュリティ AWS インシデント対応コンソールまたは コンソールを使用して、信頼された AWS Organizations アクセスを有効にできます。

> **Important**
>
> 可能な限り、 AWS セキュリティインシデント対応コンソールまたはツールを使用して Organizations との統合を有効にすることを強くお勧めします。これにより、 AWS Security Incident Response は、サービスに必要なリソースの作成など、必要な設定を実行できます。 AWS セキュリティインシデント対応が提供するツールを使用して統合を有効にできない場合にのみ、これらのステップに進みます。詳細については、この注意を参照してください。
>
> AWS Security Incident Response コンソールまたはツールを使用して信頼されたアクセスを有効にする場合、これらのステップを実行する必要はありません。

Organizations は、セットアップと管理に Security Incident Response コンソールを使用すると、Organizations の信頼されたアクセスを自動的に有効にします。セキュリティインシデント対応 CLI/SDK を使用する場合は、EnableAWSServiceAccess API を使用して、信頼されたアクセスを手動で有効にする必要があります。セキュリティインシデント対応コンソールを使用して信頼されたアクセスを有効にする方法については、「セキュリティインシデント対応ユーザーガイド」の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。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・ インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストでAWS セキュリティインシデント対応を選択します。
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 セキュリティインシデント対応の信頼されたアクセスを有効にするダイアログボックスで、確認のために enable と入力し、信頼されたアクセスを有効にするを選択します。
6. の管理者のみである場合は AWS Organizations、 AWS セキュリティインシデント対応の管理者に、サービスコンソール からそのサービスが と AWS Organizations 連携できるようになったことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations の信頼されたサービスとして AWS Security Incident Response を有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal security-ir.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。

- AWS API: EnableAWSServiceAccess

セキュリティインシデント対応による信頼されたアクセスの無効化

セキュリティインシデント対応による信頼されたアクセスを無効にすることができるのは、Organizations 管理アカウントの管理者のみです。

信頼されたアクセスを無効にするには、Organizations ツールを使用する必要があります。

信頼されたアクセスを無効にするには、 AWS Organizations コンソールを使用するか、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを無効にするには

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 セキュリティインシデント対応を選択します。
4. Disable trusted access (信頼されたアクセスを無効にする) を選択します。
5. AWS セキュリティインシデント対応の信頼されたアクセスを無効にするダイアログボックスで、「確認のために無効化」と入力し、「信頼されたアクセスを無効にする」を選択します。
6. の管理者のみの場合は AWS Organizations、 AWS セキュリティインシデント対応の管理者に、サービスコンソールまたはツール を使用して、そのサービスが で AWS Organizations 動作することを無効にできることを伝えます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを無効にすることができます。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations の信頼されたサービスとして AWS Security Incident Response を無効にします。

```
$ aws organizations disable-aws-service-access \
    --service-principal security-ir.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。

- AWS API: DisableAWSServiceAccess

セキュリティインシデント対応の委任管理者アカウントの有効化

メンバーアカウントを組織の委任管理者として指定すると、そのアカウントのユーザーとロールは、組織の管理アカウントのユーザーまたはロールのみが実行できるセキュリティインシデント対応の管理アクションを実行できます。これにより、組織の管理とセキュリティインシデント対応の管理を分離できます。詳細については、AWS 「 Security Incident Response User Guide」の「Managing Security Incident Response accounts with AWS Organizations 」を参照してください。

> **最小アクセス許可**
>
> Organizations 管理アカウントのユーザーまたはロールのみが、組織内のセキュリティインシデント対応の委任管理者としてメンバーアカウントを設定できます。

セキュリティインシデント対応コンソールを使用して委任管理者を設定する方法については、「セキュリティインシデント対応ユーザーガイド」の「委任セキュリティインシデント対応管理者アカウントの指定」を参照してください。

AWS CLI, AWS API

CLI またはいずれかの AWS SDKs を使用して AWS 委任管理者アカウントを設定する場合は、次のコマンドを使用できます。

- AWS CLI:

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

- AWS SDK: Organizations `RegisterDelegatedAdministrator`オペレーションとメンバーアカウントの ID 番号を呼び出し、アカウントサービスをパラメータ`security-ir.amazonaws.com`として識別します。

セキュリティインシデント対応の委任管理者の無効化

> **Important**
>
> メンバーシップが委任された管理者アカウントから作成された場合、委任された管理者の登録解除は破壊的なアクションであり、サービスの中断を引き起こします。DA を再登録するには：
>
> 1. https://console.aws.amazon.com/security-ir/home#/membership/settings でセキュリティインシデント対応コンソールにサインインします。
> 2. サービスコンソールからメンバーシップをキャンセルします。メンバーシップは、請求サイクルが終了するまで有効です。
> 3. メンバーシップがキャンセルされると、Organizations コンソール、CLI、または SDK によるサービスアクセスが無効になります。

セキュリティインシデント対応の委任された管理者を削除できるのは、Organizations 管理アカウントの管理者のみです。Organizations の `DeregisterDelegatedAdministrator` CLI または SDK オペレーションを使用して、委任された管理者を削除できます。

Amazon Security Lake と AWS Organizations

Amazon Security Lake は、クラウド、オンプレミス、カスタムソースのセキュリティデータを、アカウントに保存されているデータレイクに一元化します。Organizations と統合することで、アカウント全体からログとイベントを収集するデータレイクを作成できます。詳細については、「Amazon Security Lake ユーザーガイド」の「AWS Organizationsで複数のアカウントを管理する」を参照してください。

Amazon Security Lake を と統合するには、次の情報を使用します AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

RegisterDataLakeDelegatedAdministrator API を呼び出すと、次のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、Amazon Security Lake はサポートされているオペレーションを組織内のアカウントで実行できます。

このロールを削除または変更できるのは、Amazon Security Lake と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleForSecurityLake`

> ⚠ 推奨事項: Security Lake の RegisterDataLakeDelegatedAdministrator API を使用して、Security Lake による Organization へのアクセスを許可し、Organizations の委任管理者を登録します。
>
> Organizations の API を使用して委任管理者を登録すると、Organizations のサービスにリンクされたロールが正常に作成されない可能性があります。完全な機能を確保するには、Security Lake APIs を使用します。

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。Amazon Security Lake によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `securitylake.amazonaws.com`

Amazon Security Lake との信頼されたアクセスの有効化

Security Lake との信頼されたアクセスを有効化すると、組織のメンバーシップに変更があった場合、Security Lake が自動的に対応するようになります。委任管理者は、任意の組織アカウントでサポートされているサービスからの AWS ログ収集を有効にできます。詳細については、「Amazon Security Lake ユーザーガイド」の「Amazon Security Lake のサービスにリンクされたロール」を参照してください。

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、Organizations ツールを使用してのみ有効にできます。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [Amazon Security Lake] 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. Amazon Security Lake の信頼されたアクセスを有効にするダイアログボックスで、確認のために有効化と入力し、信頼されたアクセスを有効にするを選択します。
6. の管理者のみである場合は AWS Organizations、Amazon Security Lake の管理者に、サービスコンソール からそのサービスが と AWS Organizations 連携できるようになったことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Amazon Security Lake を Organizations の信頼されたサービスとして有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal securitylake.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。

- AWS API: EnableAWSServiceAccess

Amazon Security Lake との信頼できるアクセスの無効化

Amazon Security Lake との信頼されたアクセスを無効にできるのは、Organizations の管理アカウントの管理者だけです。

信頼されたアクセスを無効にするには、Organizations ツールを使用する必要があります。

信頼されたアクセスを無効にするには、 AWS Organizations コンソールを使用するか、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを無効にするには

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 [Amazon Security Lake] を選択します。
4. Disable trusted access (信頼されたアクセスを無効にする) を選択します。
5. Amazon Security Lake の信頼されたアクセスを無効にするダイアログボックスで、「確認のために無効化」と入力し、「信頼されたアクセスを無効にする」を選択します。
6. の管理者のみの場合は AWS Organizations、Amazon Security Lake の管理者に、サービスコンソールまたはツール を使用して、そのサービスが で AWS Organizations 動作することを無効にできることを伝えます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを無効にすることができます。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で Amazon Security Lake を信頼されたサービスとして無効にします。

```
$ aws organizations disable-aws-service-access \
```

```
    --service-principal securitylake.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。

- AWS API: DisableAWSServiceAccess

Amazon Security Lake の委任された管理者アカウントの有効化

Amazon Security Lake の委任された管理者は、組織内の他のアカウントをメンバーアカウントとして追加します。委任された管理者は、Amazon Security Lake を有効にし、メンバーアカウントの Amazon Security Lake の設定を行うことができます。委任管理者は、Amazon Security Lake が有効になっているすべての AWS リージョン (現在使用しているリージョンエンドポイントに関係なく) の組織全体の口グを収集できます。

委任された管理者を設定して、組織の新しいアカウントをメンバーとして自動的に追加することもできます。Amazon Security Lake の委任された管理者は、関連するメンバーアカウントの口グとイベントにアクセスできます。そのため、関連するメンバーアカウントが所有するデータを収集するように Amazon Security Lake を設定することができます。また、関連するメンバーアカウントが所有するデータを使用する権限をサブスクライバーに付与することもできます。

詳細については、「Amazon Security Lake ユーザーガイド」の「AWS Organizationsで複数のアカウントを管理する」を参照してください。

> **最小アクセス許可**
>
> 組織内のメンバーアカウントを Amazon Security Lake の委任された管理者として設定できるのは、Organizations 管理アカウントの管理者だけです。

委任された管理者アカウントは、Amazon Security Lake コンソールや Amazon Security Lake `CreateDatalakeDelegatedAdmin` API アクション、または `create-datalake-delegated-admin` CLI コマンドを使用して指定できます。または、Organizations `RegisterDelegatedAdministrator` CLI または SDK オペレーションを使用できます。Amazon Security Lake の委任管理者アカウントを有効にする手順については、「Amazon Security Lake ユーザーガイド」の「Designating the delegated Security Lake administrator and adding member accounts」を参照してください。

AWS CLI, AWS API

CLI またはいずれかの AWS SDKs を使用して AWS 委任管理者アカウントを設定する場合は、次のコマンドを使用できます。

- AWS CLI:

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

- AWS SDK: Organizations `RegisterDelegatedAdministrator`オペレーションとメンバーアカウントの ID 番号を呼び出し、アカウントサービスプリンシパルをパラメータ`account.amazonaws.com`として識別します。

Amazon Security Lake の委任管理者の無効化

組織から委任された管理者アカウントを削除できるのは、Organizations の管理者アカウントまたは Amazon Security Lake の委任された管理者アカウントのいずれかの管理者のみです。

委任された管理者を削除するには、Amazon Security Lake `DeregisterDataLakeDelegatedAdministrator` API オペレーションや、`deregister-data-lake-delegated-administrator` CLI コマンドを使用するか、Organizations `DeregisterDelegatedAdministrator` CLI または SDK オペレーションを使用します。Amazon Security Lake を使用して委任された管理者を削除するには、「Amazon Security Lake ユーザーガイド」の「Removing the Amazon Security Lake delegated administrator 」を参照してください。

AWS Service Catalog および AWS Organizations

Service Catalog では、 AWSでの使用が承認された IT サービスのカタログを作成および管理できます。

Service Catalog と の統合により、組織全体でのポートフォリオの共有と製品のコピー AWS Organizations が簡素化されます。Service Catalog 管理者は、ポートフォリオを共有する AWS Organizations ときに で既存の組織を参照し、組織のツリー構造内の信頼された組織単位 (OU) とポートフォリオを共有できます。これにより、ポートフォリオ ID を共有する必要がなくなり、受信側アカウントはポートフォリオをインポートするときに手動でポートフォリオ ID を参照する必要がなくなります。このメカニズムで共有されるポートフォリオは、Service Catalog の管理者の [Imported Portfolio] (インポートされたポートフォリオ) ビューに、共有先アカウントとして表示されます。

Service Catalog の詳細については、「Service Catalog 管理者ガイド」を参照してください。

次の情報は、 AWS Service Catalog との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

AWS Service Catalog は、信頼されたアクセスの有効化の一環として、サービスにリンクされたロールを作成しません。

アクセス許可を付与するために使用されるサービスプリンシパル

信頼されたアクセスを有効にするには、次のサービスプリンシパルを指定する必要があります。

- `servicecatalog.amazonaws.com`

Service Catalog を使用して信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、 AWS Service Catalog コンソールまたは AWS Organizations コンソールを使用して有効にできます。

> **Important**
>
> 可能な限り、 AWS Service Catalog コンソールまたはツールを使用して Organizations との統合を有効にすることを強くお勧めします。これにより、 は、サービスに必要なリソースの作成など、必要な設定 AWS Service Catalog を実行できます。ここに示す手順は、統合の有効化に AWS Service Catalogが提供するツールを使用できない場合にのみ実施してください。詳細については、この注意を参照してください。
> AWS Service Catalog コンソールまたはツールを使用して信頼されたアクセスを有効にする場合、これらのステップを実行する必要はありません。

Service Catalog CLI または AWS SDK を使用して信頼されたアクセスを有効にするには

以下のいずれかのコマンドまたはオペレーションを呼び出します。

- AWS CLI: aws servicecatalog enable-aws-organizations-access

- AWS SDKs: AWSServiceCatalog::EnableAWSOrganizationsAccess

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [AWS Service Catalog] 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. 「 の信頼されたアクセスを有効にする AWS Service Catalog」ダイアログボックスで、「確認のために を有効にする」と入力し、「信頼されたアクセスを有効にする」を選択します。
6. の管理者のみである場合は AWS Organizations、 の管理者に、サービスコンソール からそのサービスが と AWS Organizations 連携できるようになった AWS Service Catalog ことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Service Catalog としてを有効にします。

```
$ aws organizations enable-aws-service-access \
    --service-principal servicecatalog.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。

- AWS API: EnableAWSServiceAccess

Service Catalog を使用して信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

Service Catalog の使用 AWS Organizations 中に を使用して信頼されたアクセスを無効にしても、現在の共有は削除されませんが、組織全体で新しい共有を作成することはできません。このアクションを呼び出した後で変更した場合、現在の共有は組織構造と同期されません。

Service Catalog CLI または AWS SDK を使用して信頼されたアクセスを無効にするには

以下のいずれかのコマンドまたはオペレーションを呼び出します。

- AWS CLI:aws servicecatalog disable-aws-organizations-access
- AWS SDKs: DisableAWSOrganizationsAccess

信頼されたアクセスを無効にするには、 AWS Organizations コンソールを使用するか、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを無効にするには

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 Service Catalog] を選択します。
4. Disable trusted access (信頼されたアクセスを無効にする) を選択します。
5. 「 の信頼されたアクセスを無効にする AWS Service Catalog」ダイアログボックスで、「無効にして確認」と入力し、「信頼されたアクセスを無効にする」を選択します。
6. の管理者のみの場合は AWS Organizations、 の管理者 AWS Service Catalog に、サービスコンソールまたはツール を使用して、そのサービスが で AWS Organizations 動作することを無効にできることを伝えます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを無効にすることができます。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Service Catalog としてを無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal servicecatalog.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。
- AWS API: DisableAWSServiceAccess

Service Quotas と AWS Organizations

Service Quotas は、クォータを一元的に表示および管理できる AWS のサービスです。クォータ (制限とも呼ばれます) は、 AWS アカウントのリソース、アクション、アイテムの最大値です。

Service Quotas が に関連付けられている場合 AWS Organizations、アカウントの作成時にクォータの引き上げを自動的にリクエストするクォータリクエストテンプレートを作成できます。

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

Service Quotas を と統合するには、次の情報を使用します AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、Service Quotas はサポートされているオペレーションを組織内のアカウントで実行できます。

このロールを削除または変更できるのは、Service Quotas と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleForServiceQuotas`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。Service Quotas によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `servicequotas.amazonaws.com`

Service Quotas との信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

Service Quotas を使用してのみ、信頼されたアクセスを有効にできます。

Service Quotas コンソール AWS CLI または SDK を使用して、信頼されたアクセスを有効にできます。

- Service Quotas コンソールを使用して信頼されたアクセスを有効にするには

  AWS Organizations 管理アカウントでサインインし、Service Quotas コンソールでテンプレートを設定します。詳細については、Service Quotas ユーザーガイドの Using the Service Quota Template を参照してください。
- Service Quotas AWS CLI または SDK を使用して信頼されたアクセスを有効にするには

  以下のコマンドまたはオペレーションを呼び出します。
  - AWS CLI: aws service-quotas associate-service-quota-template
  - AWS SDKs: AssociateServiceQuotaTemplate

AWS IAM Identity Center および AWS Organizations

AWS IAM Identity Center は、すべての AWS アカウント およびクラウドアプリケーションにシングルサインオンアクセスを提供します。を介して Microsoft Active Directory に接続 AWS Directory Service し、そのディレクトリ内のユーザーが既存の Active Directory ユーザー名とパスワードを使用してパーソナライズされた AWS アクセスポータルにサインインできるようにします。 AWS アクセスポータルから、ユーザーはアクセス許可を持つすべての AWS アカウント およびクラウドアプリケーションにアクセスできます。

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

次の情報は、 AWS IAM Identity Center との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、IAM Identity Center はサポートされているオペレーションを組織内の組織アカウントで実行できます。

このロールを削除または変更できるのは、IAM Identity Center と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleForSSO`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。IAM Identity Center によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `sso.amazonaws.com`

IAM Identity Center との信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、 AWS IAM Identity Center コンソールまたは AWS Organizations コンソールを使用して有効にできます。

> **Important**
>
> 可能な限り、 AWS IAM Identity Center コンソールまたはツールを使用して Organizations との統合を有効にすることを強くお勧めします。これにより、 は、サービスに必要なリソースの作成など、必要な設定 AWS IAM Identity Center を実行できます。ここに示す手順は、統

合の有効化に AWS IAM Identity Centerが提供するツールを使用できない場合にのみ実施してください。詳細については、この注意を参照してください。
AWS IAM Identity Center コンソールまたはツールを使用して信頼されたアクセスを有効にする場合、これらのステップを実行する必要はありません。

IAM Identity Center を使用するには AWS Organizations 、 との信頼されたアクセスが必要です。IAM Identity Center をセットアップすると、信頼されたアクセスが有効になります。詳細については、AWS IAM Identity Center ユーザーガイドの Getting Started - Step 1: Enable AWS IAM Identity Center を参照してください。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・ インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [AWS IAM Identity Center] 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. 「 の信頼されたアクセスを有効にする AWS IAM Identity Center」ダイアログボックスで「確認のために を有効にする」と入力し、「信頼されたアクセスを有効にする」を選択します。
6. の管理者のみである場合は AWS Organizations、 の管理者に、サービスコンソール からそのサービスが と AWS Organizations 連携できるようになった AWS IAM Identity Center ことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS IAM Identity Center として を有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal sso.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。
- AWS API: EnableAWSServiceAccess

IAM Identity Center との信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

IAM Identity Center を使用するには、 との信頼 AWS Organizations されたアクセスが必要です。IAM Identity Center の使用 AWS Organizations 中に を使用して信頼されたアクセスを無効にすると、組織にアクセスできないため、機能しなくなります。ユーザーは IAM Identity Center を使用してアカウントにアクセスできません。IAM Identity Center によって作成されるロールは残りますが、 サービスからアクセスすることはできません。IAM Identity Center のサービスにリンクされたロールは残ります。その後、信頼されたアクセスを再度有効にすると、IAM Identity Center は以前のように動作し続けます。サービスを再設定する必要はありません。

組織からアカウントを削除すると、サービスにリンクされたロールなど、すべてのメタデータとリソースが IAM Identity Center によって自動的にクリーンアップされます。スタンドアロンアカウントを組織から削除した場合は、IAM Identity Center で機能しなくなります。

信頼されたアクセスは、Organizations ツールを使用してのみ無効にできます。

信頼されたアクセスを無効にするには、 AWS Organizations コンソールを使用するか、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを無効にするには

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 IAM Identity Center] を選択します。
4. Disable trusted access (信頼されたアクセスを無効にする) を選択します。
5. 「 の信頼されたアクセスを無効にする AWS IAM Identity Center」ダイアログボックスで、「無効にして確認」と入力し、「信頼されたアクセスを無効にする」を選択します。
6. の管理者のみである場合は AWS Organizations、 の管理者に、サービスコンソールまたはツール を使用して、そのサービスが で AWS Organizations 動作することを無効にできるようになった AWS IAM Identity Center ことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを無効にすることができます。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS IAM Identity Center として を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal sso.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。

- AWS API: DisableAWSServiceAccess

IAM Identity Center 用の委任管理者アカウントの有効化

メンバーアカウントを組織の委任管理者として指定すると、そのアカウントのユーザーおよびロールは、IAM Identity Center の管理アクションを実行できるようになります。通常この管理アクションは、組織の管理アカウントのユーザーとロールだけが実行できるものです。この手法は、IAM Identity Center の管理から組織の管理を分離するのに有効です。

> **最小アクセス許可**
>
> Organizations 管理アカウントのユーザーまたはロールのみが、組織内で IAM Identity Center の委任管理者としてメンバーアカウントを設定できます。

IAM Identity Center の委任管理者アカウントを有効にする方法については、AWS IAM Identity Center ユーザーガイドの委任された管理を参照してください。

AWS Systems Manager および AWS Organizations

AWS Systems Manager は、 リソースの可視性と制御を可能にする機能のコレクションです AWS 。次の Systems Manager 機能は、組織内のすべての AWS アカウント にわたって組織と連携します。

- Systems Manager Explorer は、 AWS リソースに関する情報をレポートするカスタマイズ可能なオペレーションダッシュボードです。Organizations と Systems Manager Explorer を使用して、組織内のすべての AWS アカウント でオペレーションデータを同期できます。詳細については、AWS Systems Manager ユーザーガイドの Systems Manager Explorer を参照してください。
- Systems Manager Change Manager は、アプリケーションの設定とインフラストラクチャに対する運用上の変更をリクエスト、承認、実装、レポートするためのエンタープライズ変更管理フレームワークです。詳細については、「AWS Systems Manager ユーザーガイド」の「AWS Systems Manager Change Manager」を参照してください。
- Systems Manager OpsCenter は、オペレーションエンジニアや IT プロフェッショナルが AWS リソースに関連する運用作業項目 (OpsItems) を表示、調査、解決できる一元的な場所を提供します。組織で OpsCenter を使用する場合、管理アカウント (組織の管理アカウントまたは Systems Manager 委任管理者アカウントのいずれか) と 1 つの他のアカウントからの OpsItems の単一セッションでの作業がサポートされます。設定が完了すると、ユーザーは次のタイプのアクションを実行できます。
  - 別のアカウントで OpsItems を作成、表示、および更新します。
  - 別のアカウントの OpsItems で指定された AWS リソースに関する詳細情報を表示します。
  - Systems Manager Automation ランブックを起動して、別のアカウントの AWS リソースに関する問題を修正します。

  詳細については、「AWS Systems Manager ユーザーガイド」の「AWS Systems Manager OpsCenter」を参照してください。

- 高速セットアップを使用すると、頻繁に使用する AWS サービスと機能を、推奨されるベストプラクティスですばやく設定できます。詳細については、「AWS Systems Manager ユーザーガイド」の「AWS Systems Manager Quick Setup」を参照してください。

  Systems Manager の AWS Organizations 委任管理者アカウントを登録すると、組織内の組織単位をターゲットとする高速セットアップ設定マネージャーを作成、更新、表示、削除できます。詳細については、「 ユーザーガイド」の「高速セットアップに委任管理者を使用する」を参照してください。 AWS Systems Manager
- Systems Manager の統合コンソールを設定するときは、委任管理者アカウントを入力します。このアカウントは、Quick Setup、Explorer、CloudFormation StackSets、Resource Explorer に AWS Organizations 委任管理者アカウントを登録するために使用されます。詳細については、「組織AWS Systems Manager ユーザーガイド」の「Systems Manager 統合コンソールの設定」を参照してください。

次の情報は、 AWS Systems Manager との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、Systems Manager はサポートされているオペレーションを組織内のアカウントで実行できます。

このロールを削除または変更できるのは、Systems Manager と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleForAmazonSSM_AccountDiscovery`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。Systems Manager によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `ssm.amazonaws.com`

Systems Manager との信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、Organizations ツールを使用してのみ有効にできます。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・ インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [AWS Systems Manager] 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. 「 の信頼されたアクセスを有効にする AWS Systems Manager」ダイアログボックスで、「確認のために を有効にする」と入力し、「信頼されたアクセスを有効にする」を選択します。
6. の管理者のみである場合は AWS Organizations、 の管理者に、サービスコンソール からそのサービスが と AWS Organizations 連携できるようになった AWS Systems Manager ことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Systems Manager として を有効にします。

```
$ aws organizations enable-aws-service-access \
    --service-principal ssm.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。

- AWS API: EnableAWSServiceAccess

Systems Manager との信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

Systems Manager では、組織 AWS アカウント 内の 間でオペレーションデータを同期 AWS Organizations するために、 との信頼されたアクセスが必要です。信頼されたアクセスを無効にすると、Systems Manager によるオペレーションデータの同期は失敗し、エラーが報告されます。

信頼されたアクセスを無効にするには、Organizations ツールを使用する必要があります。

信頼されたアクセスを無効にするには、 AWS Organizations コンソールを使用するか、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを無効にするには

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 Systems Manager] を選択します。
4. Disable trusted access (信頼されたアクセスを無効にする) を選択します。
5. 「 の信頼されたアクセスを無効にする AWS Systems Manager」ダイアログボックスで、「無効にして確認」と入力し、「信頼されたアクセスを無効にする」を選択します。
6. の管理者のみの場合は AWS Organizations、 の管理者 AWS Systems Manager に、サービスコンソールまたはツール を使用して、そのサービスが で AWS Organizations 動作することを無効にできることを伝えます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを無効にすることができます。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Systems Manager として を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ssm.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。

- AWS API: DisableAWSServiceAccess

Systems Manager 用の委任管理者アカウントの有効化

メンバーアカウントを組織の委任管理者として指定すると、そのアカウントのユーザーおよびロールは、Systems Manager の管理アクションを実行できるようになります。通常この管理アクションは、組織の管理アカウントのユーザーとロールだけが実行できるものです。この手法は、組織の管理から Systems Manager の管理を分離するのに有効です。

組織全体で Change Manager を使用する場合は、委任管理者アカウントを使用します。これは、Change Manager で変更テンプレート、変更リクエスト、変更ランブック、承認ワークフローを管理するためのアカウントとして指定されている AWS アカウント です。この委任アカウントにより、組織全体の変更アクティビティが管理されます。Change Manager を使用するように組織をセットアップするときは、どのアカウントがこのロールを担うかを指定します。組織の管理アカウントである必要はありません。Change Manager を単一のアカウントのみで使用する場合、委任管理者アカウントは必要ありません。

メンバーアカウントを代理管理者として指定するには、「AWS Systems Manager ユーザーガイド」の以下のトピックを参照してください。

- Explorer と OpsCenter については、「Configuring a Delegated Administrator」(委任管理者の構成)を参照してください。

- 変更マネージャーについては、「Setting up an organization and delegated account for Change Manager」(の組織と委任されたアカウントの設定) を参照してください。
- 高速セットアップについては、「高速セットアップの委任管理者を登録する」を参照してください。

Systems Manager の委任管理者アカウントの無効化

委任された管理者の登録を解除するには、 AWS Systems Manager ユーザーガイドの以下のトピックを参照してください。

- Explorer と OpsCenter については、「Explorer 委任管理者の登録を解除する」を参照してください。
- 変更マネージャーについては、「Setting up an organization and delegated account for Change Manager」(の組織と委任されたアカウントの設定) を参照してください。
- 高速セットアップについては、「高速セットアップの委任管理者の登録解除」を参照してください。

AWS User Notifications および AWS Organizations

AWS User Notifications は通知の中心的な場所です AWS 。

と統合すると AWS Organizations、組織内のアカウント間で通知を一元的に設定および表示できます。

次の情報は、 AWS User Notifications との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより User Notifications 、 はサポートされているオペレーションを組織内のアカウント内で実行できます。

このロールを削除または変更できるのは、 User Notifications と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleForAWSUserNotifications`

詳細については、「 AWS User Notifications ユーザーガイド」の「サービスにリンクされたロールの使用」を参照してください。

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。で使用されるサービスにリンクされたロールは、次のサービスプリンシパルへのアクセス User Notifications を許可します。

- `notifications.amazon.com`

User Notificationsとの信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、 を使用してのみ有効にできます AWS User Notifications。

User Notifications コンソールを使用して信頼されたアクセスを有効にするには、「 User Notifications ユーザーガイド」のAWS Organizations 「 での有効化 AWS User Notifications」を参照してください。

User Notificationsとの信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、 を使用してのみ有効にできます AWS User Notifications。

User Notifications コンソールを使用して信頼されたアクセスを無効にするには、「 User Notifications ユーザーガイド」のAWS Organizations 「 での有効化 AWS User Notifications」を参照してください。

の委任管理者アカウントの有効化 User Notifications

管理アカウント管理者は、委任 User Notifications 管理者と呼ばれる指定されたメンバーアカウントに管理権限を委任できます。アカウントをプライベートマーケットプレイスの委任管理者として登録するには、管理アカウント管理者は、信頼されたアクセスとサービスにリンクされたロールが有効になっていることを確認し、新しい管理者の登録を選択し、12 桁の AWS アカウント番号を指定して、送信を選択する必要があります。

管理アカウントと委任管理者アカウントは、エクスペリエンスの作成、ブランド設定の更新、対象者の関連付けまたは関連付け解除、製品の追加または削除、保留中のリクエストの承認または拒否などの User Notifications 管理タスクを実行できます。

User Notifications コンソールを使用して委任管理者を設定するには、「 User Notifications ユーザーガイド」の「 での委任管理者の登録 AWS User Notifications」を参照してください。

Organizations `RegisterDelegatedAdministrator` API を使用して、委任された管理者を設定することもできます。詳細については、「Organizations Command Reference」(Organizations コマンドリファレンス) で、「RegisterDelegatedAdministrator」を参照してください。

の委任管理者の無効化 User Notifications

組織管理アカウントの管理者のみが、委任された管理者を設定できます User Notifications。

User Notifications コンソールまたは API を使用するか、Organizations CLI または SDK `DeregisterDelegatedAdministrator` オペレーションを使用して、委任管理者を削除できます。

User Notifications コンソールを使用して委任管理者 User Notifications アカウントを無効にするには、「 User Notifications ユーザーガイド」の「 での委任管理者の削除 AWS User Notifications」を参照してください。

タグポリシーと AWS Organizations

タグポリシーは、組織のアカウント内のリソース間でタグを標準化するのに役立つ AWS Organizations のポリシーの一種です。ポリシーの詳細については、「タグポリシー」を参照してください。

次の情報は、タグポリシーを と統合するのに役立ちます AWS Organizations。

サービスにリンクされたロールで使用されるサービスプリンシパル

Organizations は、次のサービスプリンシパルを使用して、リソースにアタッチされたタグを操作します。

- `tagpolicies.tag.amazonaws.com`

タグポリシー用の信頼されたアクセスの有効化

信頼されたアクセスを有効にするには、組織でタグポリシーを有効にするか、 AWS Organizations コンソールを使用します。

> **Important**
>
> タグポリシーを有効にして、信頼されたアクセスを有効にすることを強くお勧めします。そうすることで、Organizations で必要な設定タスクが実行可能になります。

タグポリシー用に信頼されたアクセスを有効にするには、 AWS Organizations コンソールでタグポリシーのタイプを有効にします。詳細については、「ポリシータイプの有効化」を参照してください。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・ インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [タグポリシー] 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. タグポリシーの信頼されたアクセスを有効にするダイアログボックスで、確認のために enable と入力し、信頼されたアクセスを有効にするを選択します。
6. の管理者のみである場合は AWS Organizations、タグポリシーの管理者に、サービスコンソール からそのサービスが と AWS Organizations 連携できるようになったことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、タグポリシーを Organizations の信頼されたサービスとして有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal tagpolicies.tag.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。
- AWS API: EnableAWSServiceAccess

タグポリシーとの信頼されたアクセスの無効化

AWS Organizations コンソールでタグポリシータイプを無効にすることで、タグポリシーの信頼されたアクセスを無効にできます。詳細については、「ポリシータイプの無効化」を参照してください。

AWS Trusted Advisor および AWS Organizations

AWS Trusted Advisor は AWS 、環境を検査し、コスト削減、システムの可用性とパフォーマンスの向上、セキュリティギャップの解消に役立つ機会があればレコメンデーションを行います。Organizations と統合すると、組織内のすべてのアカウントの Trusted Advisor チェック結果を受け取り、レポートをダウンロードして、チェックの概要と影響を受けるリソースを表示できます。

詳細については、AWS サポート ユーザーガイドの Organizational view for AWS Trusted Advisor を参照してください。

次の情報は、 AWS Trusted Advisor との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより Trusted Advisor 、 はサポートされているオペレーションを組織内のアカウント内で実行できます。

このロールを削除または変更できるのは、 Trusted Advisor と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleForTrustedAdvisorReporting`

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。で使用されるサービスにリンクされたロールは、次のサービスプリンシパルへのアクセス Trusted Advisor を許可します。

- `reporting.trustedadvisor.amazonaws.com`

Trusted Advisorとの信頼されたアクセスの有効化

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、 を使用してのみ有効にできます AWS Trusted Advisor。

Trusted Advisor コンソールを使用して信頼されたアクセスを有効にするには

AWS サポート ユーザーガイドの組織ビューの有効化を参照してください。

Trusted Advisorとの信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

この機能を無効にすると、 は組織内の他のすべてのアカウントのチェック情報の記録を Trusted Advisor 停止します。既存のレポートの表示やダウンロード、新しいレポートの作成はできなくなります。

信頼されたアクセスは、 AWS Trusted Advisor または AWS Organizations ツールを使用して無効にできます。

> **Important**
>
> 可能な限り、 AWS Trusted Advisor コンソールまたはツールを使用して Organizations との統合を無効にすることを強くお勧めします。これにより、 は、サービスで不要になったリソースやアクセスロールの削除など、必要なクリーンアップ AWS Trusted Advisor を実行できます。ここに示す手順は、統合の無効化に AWS Trusted Advisorが提供するツールを使用できない場合にのみ実施してください。

AWS Trusted Advisor コンソールまたはツールを使用して信頼されたアクセスを無効にする場合は、これらのステップを実行する必要はありません。

Trusted Advisor コンソールを使用して信頼されたアクセスを無効にするには

AWS サポート ユーザーガイドの組織ビューの無効化を参照してください。

信頼されたアクセスを無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Trusted Advisor としてを無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal reporting.trustedadvisor.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。

- AWS API: DisableAWSServiceAccess

の委任管理者アカウントの有効化 Trusted Advisor

メンバーアカウントを組織の委任管理者として指定すると、指定されたアカウントのユーザーおよびロールは組織のその他のメンバーアカウントの AWS アカウント メタデータを管理できるようになります。委任された管理者アカウントを有効にしない場合、これらのタスクは組織の管理アカウントによってのみ実行できます。この手法は、組織の管理からアカウントの詳細の管理を分離するのに有効です。

> **最小アクセス許可**
>
> Organizations 管理アカウントのユーザーまたはロールのみが、組織 Trusted Advisor 内の の委任管理者としてメンバーアカウントを設定できます。

の委任管理者アカウントを有効にする手順については Trusted Advisor、「 サポート ユーザーガイド」の「委任管理者の登録」を参照してください。

AWS CLI, AWS API

CLI またはいずれかの AWS SDKs を使用して AWS 委任管理者アカウントを設定する場合は、次のコマンドを使用できます。

- AWS CLI:

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

- AWS SDK: Organizations `RegisterDelegatedAdministrator`オペレーションとメンバーアカウントの ID 番号を呼び出し、アカウントサービスプリンシパルをパラメータ`account.amazonaws.com`として識別します。

の委任管理者の無効化 Trusted Advisor

委任された管理者は、 Trusted Advisor コンソールを使用するか、Organizations CLI または SDK `DeregisterDelegatedAdministrator` オペレーションを使用して削除できます。 Trusted Advisor コンソールを使用して委任管理者 Trusted Advisor アカウントを無効にする方法については、 サポート ユーザーガイドの委任管理者の登録解除を参照してください。

AWS Well-Architected Tool および AWS Organizations

AWS Well-Architected Tool は、ワークロードの状態を文書化し、最新の AWS アーキテクチャのベストプラクティスと比較するのに役立ちます。

Organizations AWS Well-Architected Tool で を使用すると、 AWS Well-Architected Tool と Organizations のお客様は、組織の他のメンバーと AWS Well-Architected Tool リソースを共有するプロセスを簡素化できます。

詳しくは、AWS Well-Architected Tool ユーザーガイドの「AWS Well-Architected Tool リソースを共有する」を参照してください。

次の情報は、 AWS Well-Architected Tool との統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより AWS WA Tool 、 はサポートされているオペレーションを組織内のアカウント内で実行できます。

このロールを削除または変更できるのは、 AWS WA Tool と Organizations 間の信頼されたアクセスを無効にした場合か、組織から当該のメンバーアカウントを削除した場合だけです。

- `AWSServiceRoleForWellArchitected`

サービスロールポリシーは `AWSWellArchitectedOrganizationsServiceRolePolicy` です

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。で使用されるサービスにリンクされたロールは、次のサービスプリンシパルへのアクセス AWS WA Tool を許可します。

- `wellarchitected.amazonaws.com`

AWS WA Toolとの信頼されたアクセスの有効化

組織の階層的な変更を反映する AWS WA Tool ために を更新できるようにします。

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、 AWS Well-Architected Tool コンソールまたは AWS Organizations コンソールを使用して有効にできます。

> **Important**
>
> 可能な限り、 AWS Well-Architected Tool コンソールまたはツールを使用して Organizations との統合を有効にすることを強くお勧めします。これにより、 はサービスに必要なリソース

の作成など、必要な設定 AWS Well-Architected Tool を実行できます。ここに示す手順は、統合の有効化に AWS Well-Architected Toolが提供するツールを使用できない場合にのみ実施してください。詳細については、この注意を参照してください。
AWS Well-Architected Tool コンソールまたはツールを使用して信頼されたアクセスを有効にする場合、これらのステップを実行する必要はありません。

AWS WA Tool コンソールを使用して信頼されたアクセスを有効にするには

AWS Well-Architected Tool 「 ユーザーガイド」の「 AWS Well-Architected Tool リソースの共有」を参照してください。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・ インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで [Services (サービス)] を選択します。
3. サービスのリストで [AWS Well-Architected Tool] 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. 「信頼されたアクセスを有効にする AWS Well-Architected Tool」ダイアログボックスで、「確認のために を有効にする」と入力し、「信頼されたアクセスを有効にする」を選択します。
6. の管理者のみである場合は AWS Organizations、 の管理者に、サービスコンソール からそのサービスが と AWS Organizations 連携できるようになった AWS Well-Architected Tool ことを知らせます。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にします。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Well-Architected Tool として を有効にします。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal wellarchitected.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。

- AWS API: EnableAWSServiceAccess

AWS WA Toolとの信頼されたアクセスの無効化

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

信頼されたアクセスは、 AWS Well-Architected Tool または AWS Organizations ツールを使用して無効にできます。

> **Important**
>
> 可能な限り、 AWS Well-Architected Tool コンソールまたはツールを使用して Organizations との統合を無効にすることを強くお勧めします。これにより、 は、サービスで不要になったリソースやアクセスロールの削除など、必要なクリーンアップ AWS Well-Architected Tool を実行できます。ここに示す手順は、統合の無効化に AWS Well-Architected Toolが提供するツールを使用できない場合にのみ実施してください。
> AWS Well-Architected Tool コンソールまたはツールを使用して信頼されたアクセスを無効にする場合は、これらのステップを実行する必要はありません。

AWS WA Tool コンソールを使用して信頼されたアクセスを無効にするには

AWS Well-Architected Tool 「 ユーザーガイド」の「 AWS Well-Architected Tool リソースの共有」を参照してください。

信頼されたアクセスを無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations で信頼されたサービス AWS Well-Architected Tool として を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal wellarchitected.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。
- AWS API: DisableAWSServiceAccess

Amazon VPC IP Address Manager (IPAM) と AWS Organizations

Amazon VPC IP Address Manager (IPAM) は、 AWS ワークロードの IP アドレスの計画、追跡、モニタリングを容易にする VPC 機能です。

AWS Organizations を使用すると、組織全体の IP アドレスの使用状況をモニタリングし、メンバーアカウント間で IP アドレスプールを共有できます。

詳細については、Amazon VPC IPAM ユーザーガイドの「Integrate IPAM with AWS Organizations」を参照してください。

次の情報は、Amazon VPC IP Address Manager (IPAM) と の統合に役立ちます AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

IPAM コンソールまたは IPAM の `EnableIpamOrganizationAdminAccount` API のいずれかを使用して IPAM を AWS Organizations に統合すると、以下のサービスにリンクされたロールが組織の管理アカウントと各メンバーアカウント内に自動的に作成されます。

- `AWSServiceRoleForIPAM`

詳細については、Amazon VPC IPAM ユーザーガイドの「Service-linked roles for IPAM」を参照してください。

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。IPAM によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `ipam.amazonaws.com`

IPAM で信頼されたアクセスを有効にする

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

> **Note**
>
> IPAM の委任管理者を指定すると、組織の IPAM に対する信頼されたアクセスが自動的に有効になります。
> IPAM では、メンバーアカウントを組織のこのサービスの委任管理者として指定 AWS Organizations する前に、 への信頼されたアクセスが必要です。

信頼されたアクセスを有効にするには、Amazon VPC IP Address Manager (IPAM) ツールのみを使用します。

IPAM コンソールまたは IPAM `EnableIpamOrganizationAdminAccount` API を使用して IPAM AWS Organizations を と統合すると、IPAM への信頼されたアクセスが自動的に付与されます。信頼されたアクセスを付与すると、サービスにリンクされたロール `AWS ServiceRoleForIPAM` が組織の管理アカウントおよびすべてのメンバーアカウントに作成されます。IPAM は、サービスにリンクされたロールを使用して、組織の EC2 ネットワークリソースに関連付けられた CIDR のモニタリングを行い、IPAM に関連付けられたメトリクスを Amazon CloudWatch に保存します。詳細については、Amazon VPC IPAM ユーザーガイドの「Service-linked roles for IPAM」を参照してください。

信頼されたアクセスを有効にする手順については、Amazon VPC IP アドレス管理ユーザーガイドの「Integrate IPAM with AWS Organizations」を参照してください。

> **Note**
>
> AWS Organizations コンソールまたは `EnableAWSServiceAccess` API を使用して、IPAM で信頼されたアクセスを有効にすることはできません。

IPAM で信頼されたアクセスを無効にするには

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

API を使用して IPAM との信頼されたアクセスを無効にすることができるのは AWS Organizations `disable-aws-service-access`、 AWS Organizations 管理アカウントの管理者のみです。

IP アドレス管理アカウントのアクセス許可を無効にし、サービスにリンクされたロールの削除の詳細については、Amazon VPC IPAM ユーザーガイドの「Service-linked roles for IPAM」を参照してください。

信頼されたアクセスを無効にするには、Organizations AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、次の AWS CLI コマンドまたは API オペレーションを使用します。

- AWS CLI: disable-aws-service-access

  次のコマンドを実行して、Organizations の信頼されたサービスとして Amazon VPC IP Address Manager (IPAM) を無効にします。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ipam.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。

- AWS API: DisableAWSServiceAccess

IPAM 用の委任管理者アカウントの有効化

IPAM の委任管理者アカウントは、IPAM および IP アドレスのプールの作成、組織での IP アドレスの使用状況のモニタリング、およびメンバーメンバーアカウント間の IP アドレスプールの共有を行います。詳細については、Amazon VPC IPAM ユーザーガイドの「Integrate IPAM with AWS Organizations」を参照してください。

IPAM の委任管理者を構成できるのは、組織管理アカウントの管理者のみです。

委任された管理者アカウントは、IPAM コンソールから指定するか、`enable-ipam-organization-admin-account` API を使用して指定します。詳細については、 AWS AWS CLI 「 コマンドリファレンス」の「enable-ipam-organization-admin-account」を参照してください。

> **最小アクセス許可**
>
> Organizations 管理アカウントのユーザーまたはロールのみが、組織内で IPAM の委任管理者としてメンバーアカウントを設定できます

IPAM コンソールを使用して委任管理者を設定するには、「Amazon VPC IPAM ユーザーガイド 」の「IPAM を AWS Organizationsと統合する」を参照してください。

IPAM の委任された管理者の無効化

IPAM の委任管理者を構成できるのは、組織管理アカウントの管理者のみです。

を使用して委任管理者を削除するには AWS AWS CLI、AWS AWS CLI 「 コマンドリファレンス」のdisable-ipam-organization-admin-account」を参照してください。

IPAM コンソールを使用して委任管理者 IPAM アカウントを無効にするには、「Amazon VPC IPAM ユーザーガイド」の「IPAM を AWS Organizationsと統合する」を参照してください。

Amazon VPC Reachability Analyzer と AWS Organizations

Reachability Analyzer は、仮想プライベートクラウド (VPC) 内のソースリソースと送信先リソース間の接続テストを実行できるようにする設定分析ツールです。

Reachability Analyzer AWS Organizations で を使用すると、組織内のアカウント間のパスをトレースできます。

詳細については、「Reachability Analyzer user guide」の「Manage delegated administrator accounts in Reachability Analyzer」を参照してください。

Reachability Analyzer を と統合するには、次の情報を使用します AWS Organizations。

統合を有効にする際に作成されるサービスにリンクされたロール

信頼されたアクセスを有効にすると、以下のサービスにリンクされたロールが組織の管理アカウントに自動的に作成されます。このロールにより、Reachability Analyzer は組織内のアカウントでサポートされているオペレーションを実行できます。

このロールを削除または変更できるのは、Reachability Analyzer と Organizations 間の信頼されたアクセスを無効にする場合、または組織からメンバーアカウントを削除する場合だけです。

- `AWSServiceRoleForReachabilityAnalyzer`

詳細については、「Reachability Analyzer ユーザーガイド」の「Cross-account analyses for Reachability Analyzer」(Reachability Analyzer のクロスアカウント分析) を参照してください。

サービスにリンクされたロールで使用されるサービスプリンシパル

前のセクションで説明したサービスにリンクされたロールを引き受けることができるのは、ロールに定義された信頼関係によって承認されたサービスプリンシパルだけです。Reachability Analyzer によって使用されるサービスにリンクされたロールには、次のサービスプリンシパルへのアクセス許可が付与されます。

- `reachabilityanalyzer.networkinsights.amazonaws.com`

Reachability Analyzer で信頼されたアクセスを有効にするには

信頼されたアクセスの有効化に必要な権限に関しては、信頼されたアクセスを有効にするために必要なアクセス許可 を参照してください。

Reachability Analyzer の委任管理者を指定すると、組織の Reachability Analyzer に対する信頼されたアクセスが自動的に有効になります。

Reachability Analyzer では、メンバーアカウントを組織のこのサービスの委任管理者として指定 AWS Organizations する前に、 への信頼されたアクセスが必要です。

> **Important**
>
> - Reachability Analyzer コンソールまたは Organizations コンソールを使用して、信頼されたアクセスを有効にできます。ただし、Reachability Analyzer コンソールまたは `EnableMultiAccountAnalysisForAwsOrganization` API を使用して、Organizations との統合を有効にすることを強くお勧めします。そうすることで、サービスに必要なリソースの作成などの設定が Reachability Analyzer で実行可能になります。
> - 信頼されたアクセスを付与すると、サービスにリンクされたロール `AWSServiceRoleForReachabilityAnalyzer` が組織の管理アカウントおよびすべてのメンバーアカウントに作成されます。Reachability Analyzer はサービスにリンクされたロールを使用して管理を許可し、委任管理者は組織内の任意のリソース間の接続分析を実行できるようになります。Reachability Analyzer は接続に関するクエリに応答するため、組織内のアカウントにおけるネットワーク要素のスナップショットを取得できます。
> - 詳細および Reachability Analyzer で信頼されたアクセスを有効にする手順については、「Reachability Analyzer ユーザーガイド」の「Cross-account analyses for Reachability Analyzer」(Reachability Analyzer のクロスアカウント分析) を参照してください。

信頼されたアクセスを有効にするには、 AWS Organizations コンソールを使用するか、 AWS CLI コマンドを実行するか、いずれかの AWS SDKs。

AWS Management Console

Organizations コンソールを使用して信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサイン・インします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. [サービス] ページで、[VPC Reachability Analyzer] の行を探し、サービスの名前を選択してから [信頼されたアクセスを有効化] を選択します。
3. 確認ダイアログボックスで、[Show the option to enable trusted access] (信頼されたアクセスを有効にするオプションを表示する) を有効にし、ボックスに「**`enable`**」と入力してから、[Enable trusted access] (信頼されたアクセスを有効にする) を選択します。
4. の管理者のみである場合は AWS Organizations、Reachability Analyzer の管理者に、コンソールを使用してそのサービスを有効にして操作できることを伝えます AWS Organizations。

AWS CLI, AWS API

Organizations CLI/SDK を使用して信頼されたアクセスを有効にするには

次の AWS CLI コマンドまたは API オペレーションを使用して、信頼されたサービスアクセスを有効にできます。

- AWS CLI: enable-aws-service-access

  次のコマンドを実行し、Reachability Analyzer を Organizations で信頼されたサービスとして有効にできます。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal reachabilityanalyzer.networkinsights.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。
- AWS API: EnableAWSServiceAccess

Reachability Analyzer で信頼されたアクセスを無効にするには

信頼されたアクセスの無効化に必要なアクセス権限に関しては、信頼されたアクセスを無効にするために必要なアクセス許可 を参照してください。

Reachability Analyzer コンソール (推奨) または Organizations コンソールを使用して、信頼されたアクセスを無効にできます。Reachability Analyzer コンソールを使用して信頼されたアクセスを無効にするには、「Reachability Analyzer ユーザーガイド」の「Cross-account analyses for Reachability Analyzer」(Reachability Analyzer のクロスアカウント分析) を参照してください。

Reachability Analyzer 用の委任管理者アカウントの有効化

委任管理者アカウントは、組織内のどのリソースでも接続分析を実行できます。詳細については、「Reachability Analyzer ユーザーガイド」の「Reachability Analyzer を AWS Organizationsと統合する」を参照してください。

Reachability Analyzer の委任管理者を設定できるのは、組織の管理アカウントの管理者のみです。

委任管理者アカウントは、Reachability Analyzer コンソールから、または `RegisterDelegatedAdministrator` API を使用して指定できます。詳細については、「Organizations Command Reference」(Organizations コマンドリファレンス) で、「RegisterDelegatedAdministrator」を参照してください。

最小アクセス許可

Organizations 管理アカウントのユーザーまたはロールのみが、組織内で Reachability Analyzer の委任管理者としてメンバーアカウントを設定できます

Reachability Analyzer コンソールを使用して委任管理者を設定するには、「Reachability Analyzer ユーザーガイド」の「Reachability Analyzer を AWS Organizationsと統合する」を参照してください。

Reachability Analyzer 用の委任管理者の無効化

Reachability Analyzer の委任管理者を設定できるのは、組織の管理アカウントの管理者のみです。

Reachability Analyzer コンソールまたは API、あるいは Organizations `DeregisterDelegatedAdministrator` CLI または SDK オペレーションを使用して、委任管理者アカウントを削除できます。

Reachability Analyzer コンソールを使用して委任管理者の Reachability Analyzer アカウントを無効にするには、「Reachability Analyzer ユーザーガイド」の「Cross-account analyses for Reachability Analyzer」(Reachability Analyzer のクロスアカウント分析) を参照してください。

Organizations と連携 AWS のサービス する の委任管理者

AWS Organizations 管理アカウントとそのユーザーとロールは、そのアカウントで実行する必要があるタスクにのみ使用することをお勧めします。また、 AWS リソースを組織内の他のメンバーアカウントに保存し、管理アカウントから遠ざけることをお勧めします。これは、Organizations のサービスコントロールポリシー (SCP) などのセキュリティ機能は、管理アカウントのユーザーやロールに制限を加えることができないためです。また、リソースを管理アカウントから分離することで、請求書に記載される請求額が理解しやすくなります。

Organizations と統合 AWS のサービス されている多くの では、管理アカウントの使用量を減らすことができます。これらのサービスでは、サービスで使用される組織のアカウントをすべて管理できる管理者として 1 つ以上のメンバーアカウントを登録できます。これらのアカウントは、その特定のサービスの委任管理者と呼ばれます。メンバーアカウントを AWS サービスの委任管理者として登録すると、そのアカウントに、そのサービスに対する一部の管理者権限と、Organizations の読み取り専用アクションの権限が付与されます。

アカウントをあるサービスの委任管理者として登録する前に:

- そのサービスが委任管理者をサポートしていることを確認します。どのサービスが委任管理者をサポートしているかについては、AWS のサービス で使用できる AWS Organizations の表を参照してください。
- そのサービスでの信頼されたアクセスを有効にします。

> **Note**
>
> 委任管理者にサービスを有効にする方法については、AWS のサービス で使用できる AWS Organizations の表を参照して、そのサービスの [委任管理者のサポート] 列にある [詳細] リンクを選択してください。

委任管理者アカウントに付与された権限

各サービス固有の委任管理者アカウントには、そのサービスによって権限が付与されます。詳細については、AWS のサービス で使用できる AWS Organizations の表を参照して、そのサービスの [委任管理者のサポート] 列にある [詳細] リンクを選択してください。

委任管理者アカウントには、次の読み取り専用権限もあります。

- `DescribeAccount`
- `DescribeCreateAccountStatus`
- `DescribeEffectivePolicy`
- `DescribeHandshake`
- `DescribeOrganization`
- `DescribeOrganizationalUnit`
- `DescribePolicy`
- `DescribeResourcePolicy`
- `ListAccounts`
- `ListAccountsForParent`
- `ListAWSServiceAccessForOrganization`
- `ListChildren`
- `ListCreateAccountStatus`
- `ListDelegatedAdministrators`

- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget
- ListRoots
- ListTagsForResource
- ListTargetsForPolicy

これらの権限により、次のコンソール項目を表示できますが、変更はできません。

- 組織構造、すべてのアカウントと OU、組織ポリシー
- メンバーシップ
- すべてのアカウントと OU
- 組織方針

のセキュリティ AWS Organizations

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、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を活用できます。

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

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

このドキュメントは、Organizations.を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます 以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するように Organizations を設定する方法を説明します。また、Organizations リソースのモニタリングと保護 AWS のサービス に役立つ他の の使用方法についても説明します。

トピック

- AWS PrivateLink の AWS Organizations
- の Identity and Access Management AWS Organizations
- でのログ記録とモニタリング AWS Organizations
- AWS Organizationsのコンプライアンス検証
- の耐障害性 AWS Organizations
- のインフラストラクチャセキュリティ AWS Organizations

AWS PrivateLink の AWS Organizations

AWS PrivateLink for を使用すると AWS Organizations、パブリックインターネットを経由することなく、Virtual Private Cloud (VPC) 内から AWS Organizations サービスにアクセスできます。

Amazon VPC では、カスタム仮想ネットワークで AWS リソースを起動できます。VPC を使用して、IP アドレス範囲、サブネット、ルートテーブル、ネットワークゲートウェイなどのネットワーク設定を制御できます。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 に接続するには AWS Organizations、まずインターフェイス VPC エンドポイント (インターフェイスエンドポイント) を定義する必要があります。インターフェイスエンドポイントは、VPC 内のサブネットからプライベート IP アドレスが割り当てられた 1 つ以上の Elastic Network Interface (ENI) で表されます。インターフェイスエンドポイント AWS Organizations を介した VPC から へのリクエストは、Amazon ネットワーク上に残ります。

インターフェイスエンドポイントの一般的な情報については、「Amazon VPC ユーザーガイド」の「インターフェイス VPC エンドポイントを使用して AWS サービスにアクセスする」を参照してください。

トピック

- for の制限と制限 AWS PrivateLinkAWS Organizations
- の VPC エンドポイントの作成 AWS Organizations
- AWS Organizations用の VPC エンドポイントポリシーの作成

for の制限と制限 AWS PrivateLinkAWS Organizations

AWS PrivateLink for には VPC の制限が適用されます AWS Organizations。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 エンドポイントとクォータを使用して AWS サービスにアクセスする」を参照してください。 AWS PrivateLinkまた、以下の制限も適用されます。

- `us-east-1` リージョンでのみ利用可能です。
- Transport Layer Security (TLS) 1.1 をサポートしていません。

の VPC エンドポイントの作成 AWS Organizations

Amazon VPC コンソール、 AWS Command Line Interface （ AWS CLI ）、または を使用して、VPC に AWS Organizations エンドポイントを作成できます AWS CloudFormation。

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

い。 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、「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。

AWS Organizations エンドポイントを作成するときは、サービス名として以下を使用します。

```
com.amazonaws.us-east-1.organizations
```

アクセス時に FIPS 140-2 検証済み暗号化モジュールが必要な場合は AWS、次の AWS Organizations FIPS サービス名を使用します。

```
com.amazonaws.us-east-1.organizations-fips
```

AWS Organizations用の VPC エンドポイントポリシーの作成

VPC エンドポイントには、Organizations へのアクセスを制御するエンドポイントポリシーをアタッチできます。このポリシーでは、以下の情報を指定します。

- アクションを実行できるプリンシパル。
- 実行可能なアクション。
- アクションを実行できるリソース。

詳細については、「Amazon VPC ユーザーガイド」の「エンドポイントポリシーを使用して VPC エンドポイントへのアクセスを制御する」を参照してください。

例: AWS Organizations アクション用の VPC エンドポイントポリシー

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "Organizations:DescribeAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

の Identity and Access Management AWS Organizations

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 Organizations リソースの使用を承認 (アクセス許可を付与する) するかを制御します。IAM は、追加料金なしで使用できる AWS のサービス です。

トピック

- 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
- が IAM と AWS Organizations 連携する方法
- を使用した組織のアクセス許可の管理 AWS Organizations
- AWS Organizationsのアイデンティティベースのポリシーの例
- のリソースベースのポリシーの例 AWS Organizations
- AWS の 管理ポリシー AWS Organizations
- AWS Organizationsのタグによる属性ベースのアクセスコントロール
- AWS Organizations ID 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、Organizations で行う作業によって異なります。

サービスユーザー – Organizations 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。使用する Organizations 機能が増えると、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すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。Organizations の機能にアクセスできない場合は、「AWS Organizations ID 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 Organizations リソースを担当している場合は、おそらく Organizations へのフルアクセスがあります。サービスのユーザーがどの Organizations 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解して

ください。会社で Organizations を使用して IAM を利用する方法の詳細については、「が IAM と AWS Organizations 連携する方法」を参照してください。

IAM 管理者 – IAM 管理者は、Organizations へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できる Organizations アイデンティティベースのポリシーの例を表示するには、「AWS Organizations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 ロールを引き受けることによって、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 認証情報は、フェデレーション 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、「 AWS サインイン ユーザーガイド」の「 へのサインイン AWS アカウント方法」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、 はソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストを暗号化して署名します。AWS ツールを使用しない場合は、自分でリクエストに署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対するAWS Signature Version 4」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。たとえば、 では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用する AWS ことをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「IAM のAWS 多要素認証」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 およびリソースへの AWS のサービス 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、ID プロバイダーとのフェデレーションを使用して一時的な認証情報 AWS のサービス を使用して にアクセスすることを要求します。

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 ソースを介し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、ロールを引き受け、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か、独自の ID ソースのユーザーとグループのセットに接続して同期し、すべての AWS アカウント とアプリケーションで使用できます。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 ID 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 ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内の ID 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。で IAM ロールを一時的に引き受けるには AWS Management Console、ユーザーから IAM ロール (コンソール) に切り替えることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 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「ロールを引き受けるための各種方法」を参照してください。

IAM ロール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ロールについては、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」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 User Guide」の「Permission sets」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、 (プロキシとしてロールを使用する代わりに) リソースに直接ポリシーをアタッチできます。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 へのリクエストをリクエストする 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「AWS のサービスに許可を委任するロールを作成する」を参照してください。
- サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールの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。EC2 インスタンスに AWS ロールを割り当て、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。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限によ

り、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

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

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受けることができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。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ポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

アイデンティティベースのポリシーは、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「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。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、および Amazon VPC は AWS WAF、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) の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、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 AWS アカウント 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「サービスコントロールポリシー (SCP)」を参照してください。
- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定する

ために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースのアクセス許可を制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID の有効なアクセス許可に影響を与える可能性があります。RCP をサポートする のリストを含む Organizations と RCP の詳細については、AWS Organizations RCPs「リソースコントロールポリシー (RCPs」を参照してください。 AWS のサービス

- 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。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、「IAM ユーザーガイド」の「ポリシー評価ロジック」を参照してください。

が IAM と AWS Organizations 連携する方法

IAM を使用して Organizations へのアクセスを管理するときは、事前に、Organizations で使用できる IAM の機能について理解しておきます。

IAM の機能	Organizations のサポート
アイデンティティベースポリシー	はい
リソースベースのポリシー	あり
ポリシーアクション	はい
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	はい
ACL	いいえ

IAM の機能	Organizations のサポート
ABAC (ポリシー内のタグ)	あり
一時的な認証情報	なし
転送アクセスセッション (FAS)	あり
サービスロール	はい
サービスリンクロール	あり

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

Organizations のアイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザーグループ、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。ID ベースのポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。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。

Organizations のアイデンティティベースのポリシーの例

Organizations アイデンティティベースのポリシーの例については、「AWS Organizations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。

Organizations 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: あり

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。

Organizations サービスは、リソースベースの委任ポリシーと呼ばれる 1 つのタイプのリソースベースのポリシーのみをサポートします。これは、ポリシーに対してアクションを実行できるメンバーアカウントを指定するものです。ポリシーに複数のステートメントを追加して、メンバーアカウントにさまざまなアクセス許可を示すことができます。

詳細については、「の委任管理者 AWS Organizations」を参照してください。

Organizations 内のリソースベースのポリシーの例

Organizations リソースベースのポリシーの例については、「のリソースベースのポリシーの例 AWS Organizations」を参照してください。

Organizations のポリシーアクション

ポリシーアクションのサポート:あり

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

JSON ポリシーの Action 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。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アクセス許可を付与するポリシーで使用されます。

Organizations アクションのリストを確認するには、「Service Authorization Reference」の「Actions defined by AWS Organizations」を参照してください。

Organizations のポリシーアクションは、アクションの前に以下のプレフィックスを使用します。

```
organizations
```

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": [
      "organizations:action1",
      "organizations:action2"
         ]
```

Organizations アイデンティティベースのポリシーの例については、「AWS Organizations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。

Organizations のポリシーリソース

ポリシーリソースのサポート: あり

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

Resource JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。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": "*"
```

Organizations リソースのタイプとその ARN のリストを確認するには、「Service Authorization Reference」の「Resources defined by AWS Organizations」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 Organizationsで定義されるアクション」を参照してください。

Organizations アイデンティティベースのポリシーの例については、「AWS Organizations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。

Organizations のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

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

`Condition` 要素 (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して、ポリシーの条件とリクエスト内の値を一致させることができます。

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ています。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「グローバル条件コンテキストキー」を参照してください。

Organizations の条件キーのリストを確認するには、「Service Authorization Reference」の「Condition keys for AWS Organizations」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、「 で定義されるアクション AWS Organizations」を参照してください。

Organizations アイデンティティベースのポリシーの例については、「AWS Organizations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。

Organizations における ACL

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。

Organizations を使用した ABAC

ABAC (ポリシー内のタグ) のサポート: あり

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。では AWS、これらの属性はタグと呼ばれます。IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにタグをアタッチできます。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 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順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。

Organizations 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: なし

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。一時的な認証情報と AWS のサービス 連携する などの詳細については、AWS のサービス IAM ユーザーガイドの「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は、一時的な認証情報を使用します。たとえば、会社のシングルサインオン (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「ユーザーから IAM ロールに切り替える (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 アクセスできます AWS。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 AWS することをお勧めします。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。

Organizations の転送アクセスセッション

転送アクセスセッション (FAS) のサポート: 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 へのリクエストをリクエストする 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。

Organizations のサービスロール

サービスロールのサポート: あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」を参照してください。

> **Warning**
>
> サービスロールの許可を変更すると、Organizations の機能性が損なわれる可能性があります。Organizations が指示する場合以外は、サービスロールを編集しないでください。

Organizations のサービスにリンクされたロール

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、「IAM と提携するAWS のサービス」を参照してください。表の「サービスリンクロール」列に Yes と記載されたサービスを見つけます。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

を使用した組織のアクセス許可の管理 AWS Organizations

組織内のルート、OUs、アカウント、ポリシーを含むすべての AWS リソースは によって所有され AWS アカウント、リソースを作成またはアクセスするアクセス許可はアクセス許可ポリシーによって管理されます。組織では、管理アカウントはすべてのリソースを所有します。アカウント管理者は、IAM ID (ユーザー、グループ、ロール) にアクセス許可ポリシーをアタッチすることで、 AWS リソースへのアクセスを制御できます。

> **Note**
>
> アカウント管理者 (または管理者ユーザー) は、管理者アクセス許可を持つユーザーです。詳細については、「 AWS アカウント管理 リファレンスガイド」の「IAM 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。

アクセス許可を付与する場合、アクセス許可を取得するユーザー、取得するアクセス許可の対象となるリソース、およびそれらのリソースに対して許可される特定のアクションを決定します。

デフォルトでは、IAM ユーザー、グループ、ロールにはアクセス許可がありません。組織の管理アカウントの管理者として管理タスクを行うか、管理アカウントの他の IAM ユーザーまたはロールに管理者のアクセス許可を委任できます。そのためには、IAM ユーザー、グループ、またはロールに IAM アクセス許可ポリシーをアタッチします。デフォルトでは、ユーザーにこれらを行う権限はありません。これは、暗黙的な拒否と呼ばれます。このポリシーによって、暗黙的な拒否は、ユーザーが実行するアクションや、アクションを実行できるリソースを指定する明示的な許可に上書きされます。ロールにアクセス許可が付与されている場合は、組織内の他のアカウントのユーザーはそのロールを引き受けることができます。

AWS Organizations リソースとオペレーション

このセクションでは、 AWS Organizations 概念が IAM と同等の概念にどのようにマッピングされるかについて説明します。

リソース

では AWS Organizations、次のリソースへのアクセスを制御できます。

- 組織の階層構造を構成するルートおよび OU
- 組織のメンバーであるアカウント
- 組織のエンティティにアタッチするポリシー
- 組織の状態の変更に使用するハンドシェイク

このようなリソースにはそれぞれ、一意の Amazon リソースネーム (ARN) が関連付けられています。IAM アクセス許可ポリシーの `Resource` 要素の ARN を指定して、リソースへのアクセスをコントロールします。で使用されるリソースの ARN 形式の詳細なリストについては AWS Organizations、「サービス認可リファレンス」の「 で定義されるリソースタイプ AWS Organizations」を参照してください。

オペレーション

AWS は、組織内のリソースを操作するための一連のオペレーションを提供します。そのため、リソースの作成、一覧表示、変更、内容へのアクセス、削除などを行うことができます。ほとんどのオペレーションは、オペレーションの実行権限を制御する IAM ポリシーの `Action` 要素で参照できます。IAM ポリシーでアクセス許可として使用できる AWS Organizations オペレーションのリストに

ついては、「Service Authorization Reference」の「Actions defined by organizations」をご覧ください。

Action と Resource を 1 つのアクセス許可ポリシー Statement で組み合わせると、特定のアクションを使用できるリソースが正確に制御されます。

条件キー

AWS には、特定のアクションをより詳細に制御するためにクエリできる条件キーが用意されています。IAM ポリシーの Condition 要素でこれらの条件キーを参照し、ステートメントが一致しているとみなされる条件を満たすように追加条件を指定することができます。

以下の条件キーは、特に で役立ちます AWS Organizations。

- aws:PrincipalOrgID - リソースベースのポリシーの Principal 要素の指定を簡素化します。このグローバルキーは、組織内のすべての AWS アカウント のすべてのアカウント ID を一覧表示する代わりに使用できます。組織のメンバーであるすべてのアカウントを一覧表示せずに、Condition 要素に組織 ID を指定することができます。

  > **Note**
  >
  > このグローバル条件は、組織の管理アカウントにも適用されます。

  詳細については、「IAM ユーザーガイド」で「AWS グローバル条件コンテキストキー」の PrincipalOrgID の説明を参照してください。
- aws:PrincipalOrgPaths - この条件キーを使用して、特定の組織ルート、OU、またはその子のメンバーを照合します。リクエストを行うプリンシパル (ルートユーザー、IAM ユーザー、またはロール) が指定された組織パスにある場合、aws:PrincipalOrgPaths 条件キーは true を返します。パスは、 AWS Organizations エンティティの構造のテキスト表現です。パスの詳細については、IAM ユーザーガイドの AWS Organizations 「エンティティパスを理解する」を参照してください。この条件キーの使用の詳細については、IAM ユーザーガイドの「aws:PrincipalOrgPaths」を参照してください。

  例えば次の条件要素は、同じ組織内の 2 つの OU のいずれかのメンバーと一致します。

```
            "Condition": {
                "ForAnyValue:StringLike": {
                    "aws:PrincipalOrgPaths": [
                        "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
```

```
                    "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-jkl0-awsddddd/"
                ]
            }
        }
```

- organizations:PolicyType - この条件キーを使用して、Organization ポリシー関連 API オペレーションを、指定したタイプの Organization ポリシーでのみ動作するように制限できます。この条件キーは、Organizations ポリシーとやり取りするアクションを含むポリシーステートメントに適用できます。

  この条件キーでは、次の値を使用できます。

  - SERVICE_CONTROL_POLICY
  - RESOURCE_CONTROL_POLICY
  - DECLARATIVE_POLICY_EC2
  - BACKUP_POLICY
  - TAG_POLICY
  - CHATBOT_POLICY
  - AISERVICES_OPT_OUT_POLICY

  例えば、次のポリシー例では、ユーザーが任意の Organizations オペレーションを実行できます。ただし、ポリシー引数を取るオペレーションをユーザーが実行した場合、指定したポリシーがタグ付けポリシーである場合にのみオペレーションが許可されます。ユーザーが他のタイプのポリシーを指定した場合、オペレーションは失敗します。

  JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IfTaggingAPIThenAllowOnOnlyTaggingPolicies",
            "Effect": "Allow",
            "Action": "organizations:*",
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [ "TAG_POLICY" ]
                }
            }
        }
```

```
    ]
}
```

- `organizations:ServicePrincipal` - EnableAWSServiceAccess オペレーションまたは DisableAWSServiceAccess オペレーションで、他の AWS のサービスを使用して信頼されたアクセスを有効または無効にする場合の条件として使用できます。`organizations:ServicePrincipal` を使用して、これらのオペレーションからのリクエストを、承認されたサービスプリンシパル名のリストに制限できます。

  たとえば、次のポリシーでは、 で信頼されたアクセスを有効または無効に AWS Firewall Manager する場合にのみ を指定できます AWS Organizations。

  JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyAWSFirewallIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [ "fms.amazonaws.com" ]
                }
            }
        }
    ]
}
```

IAM ポリシーでアクセス許可として使用できる AWS Organizations特定の条件キーのリストについては、「サービス認可リファレンス」の「 の条件キー AWS Organizations」を参照してください。

リソース所有権についての理解

は、リソースを作成したユーザーに関係なく、アカウントで作成されたリソース AWS アカウントを所有します。具体的には、リソース所有者は、リソース作成リクエストを認証するプリンシパルエンティティ (ルートユーザー、IAM ユーザー、または IAM ロール) AWS アカウント の です。組織の場合は、これは常に管理アカウントになります。組織のリソースの作成またはアクセスを行うほとんどのオペレーションは、メンバーアカウントから呼び出すことができません。次の例は、この仕組みを示しています。

- 管理アカウントのルートアカウントの認証情報を使用して OU を作成する場合の管理アカウントは、リソースの所有者です。(では AWS Organizations、リソースは OU です) 。
- 管理アカウントに IAM ユーザーを作成し、そのユーザーに OU を作成するためのアクセス権限を付与する場合、そのユーザーは OU を作成できます。ただし、OU リソースを所有しているのは、このユーザーが属する管理アカウントです。
- OU を作成するためのアクセス権限を持つ管理アカウントに IAM ロールを作成する場合は、ロールを引き受けることのできるユーザーはいずれも OU を作成できます。OU リソースを所有するのは、ロール (引き受けるユーザーではない) が属する管理アカウントです。

リソースへのアクセスの管理

アクセス権限ポリシー では、誰が何にアクセスできるかを記述します。以下のセクションで、アクセス許可ポリシーを作成するために使用可能なオプションについて説明します。

> **Note**
>
> このセクションでは、 のコンテキストでの IAM の使用について説明します AWS Organizations。ここでは、IAM サービスに関する詳細情報を提供しません。完全な IAM ドキュメントについては、「IAM ユーザーガイド」を参照してください。IAM ポリシー構文の詳細と説明については、「IAM ユーザーガイド」の「IAM JSON ポリシーリファレンス」を参照してください。

IAM ID にアタッチされているポリシーは、ID ベース のポリシー (IAM ポリシー) と呼ばれます。リソースにアタッチされているポリシーは、リソースベース のポリシーと呼ばれます。

トピック

- ID ベースのアクセス許可ポリシー (IAM ポリシー)

ID ベースのアクセス許可ポリシー (IAM ポリシー)

IAM ID にポリシーをアタッチして、それらの ID が AWS リソースに対してオペレーションを実行することを許可できます。例えば、次のオペレーションを実行できます。

- アカウントのユーザーまたはグループにアクセス許可ポリシーをアタッチする – サービスコントロールポリシー (SCP) や OU などの AWS Organizations リソースを作成するアクセス許可をユーザーに付与するには、ユーザーまたはユーザーが属するグループにアクセス許可ポリシーをアタッチできます。ユーザーまたはグループを組織の管理アカウントにする必要があります。
- アクセス許可ポリシーをロールにアタッチする (クロスアカウントのアクセス許可を付与する) - アイデンティティベースのアクセス許可ポリシーを IAM ロールにアタッチして、クロスアカウントのアクセス許可を組織に付与することができます。例えば、管理アカウントの管理者はロールを作成し、次のようにクロスアカウントのアクセス許可をメンバーアカウントのユーザーに付与できます。

  1. 管理アカウントの管理者は IAM ロールを作成し、ロールにアクセス許可ポリシーをアタッチして組織のリソースにアクセス許可を付与します。
  2. 管理アカウントの管理者は、そのロールを引き受ける `Principal` として、メンバーアカウントの ID を識別するロールに信頼ポリシーをアタッチします。
  3. その後、メンバーアカウント管理者は、ロールを引き受けるアクセス権限をメンバーアカウントのユーザーに委任できます。これにより、メンバーアカウントのユーザーは、管理アカウントや組織のリソースを作成し、アクセスできるようになります。ロールを引き受けるアクセス許可を AWS サービスに付与する場合は、信頼ポリシーのプリンシパルを AWS サービスプリンシパルにすることもできます。

  IAM を使用した許可の委任の詳細については、「IAM ユーザーガイド」の「アクセス管理」を参照してください。

以下に示しているのは、組織の `CreateAccount` アクションの実行をユーザーに許可するポリシーの例です。

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Stmt1OrgPermissions",
```

```
         "Effect":"Allow",
         "Action":[
            "organizations:CreateAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

ポリシーの Resource 要素に部分的な ARN を指定して、リソースのタイプを示すこともできます。

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowCreatingAccountsOnResource",
         "Effect":"Allow",
         "Action":"organizations:CreateAccount",
         "Resource":"arn:aws:organizations::*:account/*"
      }
   ]
}
```

作成するアカウントに特定のタグを含まないアカウントの作成を拒否することもできます。

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyCreatingAccountsOnResourceBasedOnTag",
         "Effect":"Deny",
         "Action":"organizations:CreateAccount",
         "Resource":"*",
         "Condition":{
```

```
            "StringEquals":{
               "aws:ResourceTag/key":"value"
            }
         }
      }
   ]
}
```

ユーザー、グループ、ロール、アクセス許可の詳細については、「IAM ユーザーガイド」の「IAM identities (users, user groups, and roles)」を参照してください。

ポリシー要素の指定: アクション、条件、効果、リソース

サービスは、 AWS Organizations リソースごとに、そのリソースと何らかの方法でやり取りまたは操作できる一連の API オペレーションまたはアクションを定義します。これらのオペレーションのアクセス許可を付与するために、 はポリシーで指定できる一連のアクション AWS Organizations を定義します。たとえば、OU リソースの場合、 は次のようなアクション AWS Organizations を定義します。

- `AttachPolicy` および `DetachPolicy`
- `CreateOrganizationalUnit` および `DeleteOrganizationalUnit`
- `ListOrganizationalUnits` および `DescribeOrganizationalUnit`

場合によっては、API オペレーションを実行する際、アクションまたはリソースのアクセス許可が 2 つ以上必要になることがあります。

IAM アクセス許可ポリシーで使用できる最もベーシックなポリシーは、次のとおりです。

- Action - このキーワードを使用して、許可または拒否するオペレーション (アクション) を識別します。たとえば、指定された に応じて`Effect`、 は `CreateAccount`オペレーションを実行するためのユーザーアクセス許可`organizations:CreateAccount`を許可または拒否します AWS Organizations 。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素 Action」を参照してください。
- Resource - このキーワードを使用して、ポリシー構文が適用されるリソースの ARN を指定します。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素 Resource」を参照してください。
- Condition - ポリシーステートメントを満たす必要がある条件を指定するために、このキーワードを使用します。`Condition` は通常、ポリシーが一致するために満たす必要がある追加条件を指定

します。詳細については、IAM ユーザーガイド」の「IAM JSON ポリシー要素: 条件」を参照してください。

- Effect - このキーワードを使用して、ポリシー構文でリソースのアクションを許可または拒否するかどうかを指定します。リソースへのアクセス権を明示的に付与 (または許可) していない場合、アクセスは暗黙的に拒否されます。また、リソースへのアクセスを明示的に拒否することもできます。これにより、別のポリシーによってアクセスが許可されていても、ユーザーは、指定のリソースで指定のアクションを実行できないことがあります。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素 Effect」を参照してください。
- Principal - アイデンティティベースのポリシー (IAM ポリシー) では、ポリシーがアタッチされているユーザーが自動的かつ暗黙的にプリンシパルとなります。リソースベースのポリシーでは、アクセス許可 (リソースベースのポリシーにのみ適用) を受け取りたいユーザー、アカウント、サービス、またはその他のエンティティを指定します。

IAM ポリシーの構文と記述の詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシーリファレンス」を参照してください。

AWS Organizations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 Organizations 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継ぐことができます。

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 ポリシーを作成する (コンソール)」を参照してください。

Organizations が定義するアクションとリソースタイプ (リソースタイプごとの ARN の形式を含む) の詳細については、「Service Authorization Reference」の「Actions, resources, and condition keys for AWS Organizations」を参照してください。

トピック

- ポリシーに関するベストプラクティス
- Organizations コンソールの使用
- 自分の権限の表示をユーザーに許可する
- 完全な管理者権限をユーザーに付与する

- 制限付きのアクセス許可をアクションごとに付与する
- 特定のリソースへのアクセス許可の付与
- 制限付きサービスプリンシパルに信頼されたアクセスを有効にするための権限を付与する

ポリシーに関するベストプラクティス

ID ベースのポリシーは、あるユーザーがアカウント内で Organizations 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の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能のAWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで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、サービスアクションが などの特定の を通じて使用されている場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素:条件」を参照してください。
- IAM 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 でポリシーを検証する」を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、MFA をオンにしてセキュリティを強化します。API オペレーション

が呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA を使用した安全な API アクセス」を参照してください。

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

Organizations コンソールの使用

AWS Organizations コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 の Organizations リソース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制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (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。

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

ユーザーとロールが引き続き Organizations コンソールを使用できるようにするには、Organizations `AWSOrganizationsFullAccess`または `AWSOrganizationsReadOnlyAccess` AWS 管理ポリシーもエンティティにアタッチします。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

自分の権限の表示をユーザーに許可する

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
```

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

完全な管理者権限をユーザーに付与する

組織内の IAM ユーザーに完全な AWS Organizations 管理者権限を付与する IAM ポリシーを作成できます。これを行うには、IAM コンソールの JSON ポリシーエディタを使用します。

JSON ポリシーエディタでポリシーを作成するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。
2. 左側のナビゲーションペインで、[ポリシー] を選択します。

   初めて [ポリシー] を選択する場合には、[管理ポリシーにようこそ] ページが表示されます。[今すぐ始める] を選択します。
3. ページの上部で、[ポリシーを作成] を選択します。
4. [ポリシーエディタ] セクションで、[JSON] オプションを選択します。
5. 次の JSON ポリシードキュメントを入力します。

```
{
    "Version": "2012-10-17",
```

```
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*"
    }
}
```

6. [次へ] をクリックします。

> **Note**
>
> いつでも [Visual] と [JSON] エディタオプションを切り替えることができます。ただし、[Visual] エディタで [次へ] に変更または選択した場合、IAM はポリシーを再構成して visual エディタに合わせて最適化することがあります。詳細については、「IAM ユーザーガイド」の「ポリシーの再構成」を参照してください。

7. [確認と作成] ページで、作成するポリシーの [ポリシー名] と [説明] (オプション) を入力します。[このポリシーで定義されているアクセス許可] を確認して、ポリシーによって付与されたアクセス許可を確認します。
8. [ポリシーの作成] をクリックして、新しいポリシーを保存します。

IAM ポリシーの作成の詳細については、「IAM ユーザーガイド」の「IAM ポリシーを作成する」を参照してください。

制限付きのアクセス許可をアクションごとに付与する

完全なアクセス許可ではなく制限されたアクセス許可を付与する場合は、IAM アクセス許可ポリシーの `Action` 要素で許可する個々のアクセス許可をリストするポリシーを作成できます。次の例に示すように、ワイルドカード (*) 文字を使用して `Describe*` および `List*` のアクセス権限のみを付与することができます。この方法では通常、読み取り専用アクセスが組織に付与されます。

> **Note**
>
> サービスコントロールポリシー (SCP) では、`Action` 要素のワイルドカード (*) 文字は、ポリシー自体、または文字列の末尾にのみ使用できます。文字列の先頭または中間には表示されません。そのため、`"servicename:action*"` は有効ですが、`"servicename:*action"` と `"servicename:some*action"` はいずれも、SCP で無効です。

JSON

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

IAM ポリシーで割り当てることができるすべてのアクセス許可のリストについては、「サービス認可リファレンス」のAWS 「Organizations で定義されるアクション」を参照してください。

特定のリソースへのアクセス許可の付与

特定のアクションへのアクセスの制限に加えて、組織内の特定のエンティティへのアクセスを制限できます。前のセクションの例の `Resource` 要素は、両方ワイルドカード文字 (*) を指定します。つまり、「アクションがアクセスできる任意のリソース」を意味します。代わりに、「*」をアクセスを許可する特定のエンティティの Amazon リソースネーム (ARN) で置き換えることができます。

例: 単一の OU にアクセス許可を付与する

次のポリシーの最初のステートメントは、IAM ユーザーに組織全体への読み取りアクセスを許可していますが、2 番目のステートメントでは、ユーザーは指定された単一の組織単位 (OU) 内でのみ AWS Organizations 管理アクションの実行が許可されます。これは、子 OU には適用されません。請求へのアクセスは付与されません。これにより、OU AWS アカウント の への管理アクセスは許可されないことに注意してください。指定された OU 内のアカウントに対して AWS Organizations オペレーションを実行するアクセス許可のみを付与します。

JSON

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

```
            "Effect": "Allow",
            "Action": [
                "organizations:Describe*",
                "organizations:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "organizations:*",
            "Resource": "arn:aws:organizations::123456789012:ou/o-
<organizationId>/ou-<organizationalUnitId>"
        }
    ]
}
```

OU と組織の IDs は、 AWS Organizations コンソールから、または `List*` APIs。このポリシーを適用されたユーザーまたはグループは、OU に直接含まれるエンティティに対して任意のアクション (`"organizations:*"`) を実行できます。OU は Amazon リソースネーム (ARN) によって識別されます。

ARN に関するその他リソースについては、「Service Authorization Reference」の「Resources types defined by AWS Organizations」を参照してください。

制限付きサービスプリンシパルに信頼されたアクセスを有効にするための権限を付与する

ポリシーステートメントの `Condition` 要素を使用して、ポリシーステートメントの一致をさらに制限することができます。

例: 特定した 1 つのサービスに信頼されたアクセスを有効にするための権限を付与する

次のステートメントは、特定したサービスのみに信頼されたアクセスを有効にするための制限方法を示しています。ユーザーが別のサービスプリンシパルで API を呼び出そうとした場合 AWS IAM Identity Center、このポリシーは一致せず、リクエストは拒否されます。

JSON

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
                "StringEquals" : {
                    "organizations:ServicePrincipal" : "sso.amazonaws.com"
                }
            }
        }
    ]
}
```

ARN に関するその他リソースについては、「Service Authorization Reference」の「Resources types defined by AWS Organizations」を参照してください。

のリソースベースのポリシーの例 AWS Organizations

以下はリソースベースの委任ポリシーを使用する方法の例です。詳細については、「の委任管理者 AWS Organizations」を参照してください。

トピック

- 例: 組織、OU、アカウント、ポリシーの表示
- 例: ポリシーの作成、読み取り、更新、削除
- 例: タグとタグ解除ポリシー
- 例: 単一の OU またはアカウントにポリシーをアタッチする
- 例: 組織のバックアップポリシーを管理するための一括アクセス許可

例: 組織、OU、アカウント、ポリシーの表示

ポリシーの管理を委任する前に、組織の階層構造を移動したり、組織単位 (OU)、アカウント、およびそれらにアタッチされているポリシーを表示するために、アクセス許可を委任する必要があります。

以下は、これらのアクセス許可をメンバーアカウント *AccountId* のリソースベースの委任ポリシーに含める方法の例です。

> **Important**
>
> このポリシーを使用して Organizations 読み取り専用アクションを委任することは可能ですが、この例で示されているように、必要最小限のアクションのみにアクセス許可を付与することをおすすめします。

この委任ポリシーの例では、 AWS API または からプログラムでアクションを完了するために必要なアクセス許可を付与します AWS CLI。この委任ポリシーを使用するには、*AccountId* の AWS プレースホルダーテキストを独自の情報に置き換えます。次に、の委任管理者 AWS Organizations の指示に従ってください。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DelegatingNecessaryDescribeListActions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribePolicy",
                "organizations:DescribeEffectivePolicy",
                "organizations:ListRoots",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:ListTagsForResource"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

例: ポリシーの作成、読み取り、更新、削除

リソースベースの委任ポリシーを作成して、管理アカウントが任意のポリシータイプの create、read、update、および delete アクションを委任できるようにします。この例では、サービスコントロールポリシーのこれらのアクションをメンバーアカウントである *MemberAccountId* に委任する方法を示しています。この例に示す 2 つのリソースは、それぞれカスタマー管理ポリシーと AWS マネージドサービスコントロールポリシーへのアクセスを許可します。

> **Important**
>
> このポリシーにより、委任管理者は管理アカウントを含む組織内の任意のアカウントで作成したポリシーに対して指定されたアクションを実行できます。
> 委任された管理者は、organizations:AttachPolicy および organizations:DetachPolicy アクションを実行するために必要なアクセス許可が含まれていないため、ポリシーをアタッチまたはデタッチすることはできません。

この委任ポリシーの例では、 AWS API または からプログラムでアクションを完了するために必要なアクセス許可を付与します AWS CLI。*MemberAccountId*、*ManagementAccountId*、および *OrganizationId* の AWS プレースホルダーテキストを独自の情報に置き換えます。次に、の委任管理者 AWS Organizations の指示に従ってください。

例: タグとタグ解除ポリシー

この例では、委任された管理者がバックアップポリシーにタグ付けまたはタグ解除できるようにするリソースベースの委任ポリシーを作成する方法を紹介します。 AWS API または からプログラムでアクションを実行するために必要なアクセス許可を付与します AWS CLI。

この委任ポリシーを使用するには、*MemberAccountId*、*ManagementAccountId*、および *OrganizationId*、の AWS プレースホルダーテキストを独自の情報に置き換えます。次に、の委任管理者 AWS Organizations の指示に従ってください。

例: 単一の OU またはアカウントにポリシーをアタッチする

この例では、指定された組織単位 (OU) または指定されたアカウントから attach または detach Organizations ポリシーへの委任管理者を許可するリソースベースの委任ポリシーを作成する方法を示します。これらのアクションを委任する前に、組織の構造をナビゲートするアクセス許可を委任し、その下のアカウントを確認する必要があります。詳細については、「例: 組織、OU、アカウント、ポリシーの表示」を参照してください。

> **Important**
>
> - このポリシーでは、指定された OU またはアカウントからのポリシーのアタッチまたはデタッチが許可されますが、子 OU および子 OU の下のアカウントは除外されます。
> - このポリシーにより、委任管理者は管理アカウントを含む組織内の任意のアカウントで作成したポリシーに対して指定されたアクションを実行できます。

この委任ポリシーの例では、 AWS API または からプログラムでアクションを完了するために必要なアクセス許可を付与します AWS CLI。この委任ポリシーを使用するには、*MemberAccountId*、*ManagementAccountId*、*OrganizationId*、および *TargetAccountId* の AWS プレースホルダーテキストを独自の情報に置き換えます。次に、の委任管理者 AWS Organizations の指示に従ってください。

Organizations の任意の OU またはアカウントにポリシーのアタッチとデタッチを委任するには、前の例のリソースを次のリソースに置き換えます。

```
"Resource": [
    "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
    "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
    "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/backup_policy/
*"
]
```

例: 組織のバックアップポリシーを管理するための一括アクセス許可

以下は create、read、update、delete アクションや attach、detach のポリシーアクションなど、組織内のバックアップポリシーを管理するために必要なすべてのアクセス許可を管理アカウントが委任できるようにする、リソースベースの委任ポリシーを作成する方法の例です。

> **Important**
>
> このポリシーにより、委任管理者は管理アカウントを含む組織内の任意のアカウントで作成したポリシーに対して指定されたアクションを実行できます。

この委任ポリシーの例では、 AWS API または からプログラムでアクションを完了するために必要なアクセス許可を付与します AWS CLI。この委任ポリシーを使用するには、*MemberAccountId*、*ManagementAccountId*、*OrganizationId*、および *RootId* の AWS プレースホルダーテキストを独自の情報に置き換えます。次に、の委任管理者 AWS Organizations の指示に従ってください。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DelegatingNecessaryDescribeListActions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListRoots",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListTagsForResource"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "DelegatingNecessaryDescribeListActionsForSpecificPolicyType",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "organizations:DescribePolicy",
                "organizations:DescribeEffectivePolicy",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": "BACKUP_POLICY"
                }
            }
        },
        {
            "Sid": "DelegatingAllActionsForBackupPolicies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "organizations:CreatePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy",
                "organizations:AttachPolicy",
                "organizations:DetachPolicy",
                "organizations:EnablePolicyType",
                "organizations:DisablePolicyType"
            ],
            "Resource": [
                "arn:aws:organizations::111122223333:root/o-OrganizationId/
r-RootId",
                "arn:aws:organizations::111122223333:ou/o-OrganizationId/*",
                "arn:aws:organizations::111122223333:account/o-OrganizationId/*",
                "arn:aws:organizations::111122223333:policy/o-OrganizationId/
backup_policy/*"
```

```
            ],
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": "BACKUP_POLICY"
                }
            }
        }
    ]
}
```

AWS の 管理ポリシー AWS Organizations

このセクションでは、組織の管理に使用する AWSマネージドポリシーについて説明します。 AWS 管理ポリシーを変更または削除することはできませんが、必要に応じて組織内のエンティティにアタッチまたはデタッチできます。

AWS OrganizationsAWS Identity and Access Management (IAM) で使用する マネージドポリシー

IAM管理ポリシーは、 AWSによって提供され、維持されます。管理ポリシーは、管理ポリシーを適切な IAM ユーザーまたはロールオブジェクトにアタッチすることでユーザーに割り当てることができる、一般的なタスクに対するアクセス許可を提供します。ポリシーを自分で記述する必要はありません。 が新しいサービスをサポートするために必要に応じてポリシー AWS を更新すると、自動的にすぐに更新のメリットが得られます。

AWS 管理ポリシーのリストは、IAM コンソールの [Policies] (ポリシー) ページで確認できます。[Filter policies] (フィルターポリシー) のドロップダウンを使用して、[AWS managed] (マネージド) を選択します。

以下の管理ポリシーを使用して、組織のユーザーにアクセス許可を付与できます

AWS 管理ポリシー: AWSOrganizationsFullAccess

組織を作成し、完全に管理するために必要なすべてのアクセス許可を提供します。

ポリシーを表示: AWSOrganizationsFullAccess。

AWS 管理ポリシー: AWSOrganizationsReadOnlyAccess

組織に関する情報への読み取り専用アクセスを提供します。ユーザーがこれに変更を加えることはできません。

ポリシーを表示: AWSOrganizationsReadOnlyAccess。

AWS 管理ポリシー: DeclarativePoliciesEC2Report

このポリシーは、AWSServiceRoleForDeclarativePoliciesEC2Report サービスにリンクされたロールによって使用され、メンバーアカウントのアカウント属性の状態を記述できるようにします。

ポリシーを表示する: DeclarativePoliciesEC2Report。

Organizations AWS 管理ポリシーの更新

次の表は、このサービスがこれらの変更の追跡を開始してからの AWS マネージドポリシーの更新の詳細を示しています。このページの変更に関する自動通知については、ドキュメントの履歴ページの 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
AWSOrganizationsFullAccess – Organizations コンソールを介してアカウント名を表示または変更するために必要なアカウント API アクセス許可を許可するように更新されました。	組織内の任意のアカウントのアカウント名を表示するアクセスaccount:GetAccountInformation を有効にするアクションと、組織内の任意のアカウント名を変更するアクセスを有効にするaccount:PutAccountName アクションを追加しました。	2025 年 4 月 22 日
DeclarativePoliciesEC2Report – 新しい管理ポリシー	AWSServiceRoleForDeclarativePoliciesEC2Report サービスにリンクされたロールの機能を有効にするDeclarativePoliciesEC2Report ポリシーを追加しました。	2024 年 11 月 22 日
AWSOrganizationsReadOnlyAccess – ルートユーザーの E メールアドレスを表示するために必要なアカウント API アクセス許可を許可するように更新。	組織内の任意のメンバーアカウントのルートユーザーの E メールアドレスを表示するアクセスを有効にするaccount:GetPrimaryEmail アクションと、組織内の任	2024 年 6 月 6 日

変更	説明	日付
	意のメンバーアカウントの有効なリージョンを表示するアクセスを有効にするaccount:GetRegionOptStatus アクションを追加しました。	
AWSOrganizationsFullAccess – ポリシーステートメントを記述する Sid 要素を含めるように更新されました。	AWSOrganizationsFullAccess 管理ポリシーのSid要素を追加しました。	2024 年 2 月 6 日
AWSOrganizationsReadOnlyAccess – ポリシーステートメントを記述する Sid 要素を含めるように更新されました。	AWSOrganizationsReadOnlyAccess 管理ポリシーのSid要素を追加しました。	2024 年 2 月 6 日
AWSOrganizationsFullAccess - Organizations コンソールを介して AWS リージョン を有効化または無効化するために必要な API アクセス許可をアカウントに付与できるように更新されました。	アカウントのリージョンを有効または無効にする書き込みアクセスを有効にする account:ListRegions 、account:EnableRegion 、および account:DisableRegion アクションをポリシーに追加しました。	2022 年 12 月 22 日
AWSOrganizationsReadOnlyAccess – Organizations コンソール AWS リージョン を介した一覧表示に必要なアカウント API アクセス許可を許可するように更新されました。	アカウントのリージョンを表示するためのアクセスを有効にするaccount:ListRegions アクションをポリシーに追加しました。	2022 年 12 月 22 日

変更	説明	日付
AWSOrganizationsFullAccess - Organizations コンソールを介してアカウントの連絡先を追加または編集するために必要な API アクセス許可をアカウントに付与できるように更新されました。	アカウントの連絡先を変更するための書き込みアクセスを有効にする account:GetContactInformation および account:PutContactInformation アクションをポリシーに追加しました。	2022 年 10 月 21 日
AWSOrganizationsReadOnlyAccess - Organizations コンソールを介してアカウントの連絡先を表示するために必要な API アクセス許可をアカウントに付与できるように更新されました。	アカウントの連絡先を表示するためのアクセスを有効にするaccount:GetContactInformation アクションをポリシーに追加しました。	2022 年 10 月 21 日
AWSOrganizationsFullAccess — 組織を作成できるように更新されました。	組織の作成に必要なサービスにリンクされたロールの作成を有効にするアクセスCreateServiceLinkedRole 許可をポリシーに追加しました。アクセス許可は、organizations.amazonaws.com のサービスのみで使用できるロールの作成に制限されています。	2022 年 8 月 24 日
AWSOrganizationsFullAccess – Organizations コンソールでアカウントの代替連絡先を追加、編集、または削除するために必要な API アクセス許可をアカウントに付与できるように更新されました。	アカウントの代替連絡先を変更するための書き込みアクセスを有効にする account:GetAlternateContact 、account:DeleteAlternateContact 、 account:PutAlternateContact アクションをポリシーに追加しました。	2022 年 2 月 7 日

変更	説明	日付
AWSOrganizationsReadOnlyAccess – Organizations コンソールでアカウントの代替連絡先を表示するために必要な API アクセス許可をアカウントに付与できるように更新されました。	アカウントの代替連絡先を表示するためのアクセスを有効にするaccount:GetAlternateContact アクションをポリシーに追加しました。	2022 年 2 月 7 日

AWS マネージド認可ポリシー

認可ポリシーは IAM アクセス許可ポリシーに似ていますが、IAM AWS Organizations ではなく の機能です。認可ポリシーを使用して、メンバーアカウントのプリンシパルとリソースのアクセスを一元的に設定および管理します。

Organizations コンソール の [Policies] (ポリシー) ページに、組織内のポリシーのリストが表示されます。

ポリシー名	説明	ARN
FullAWSAccess	すべてのオペレーションへのアクセスを許可します。	arn:aws:organizations::aws:policy/service_control_policy/p-FullAWSAccess
RCPFullAWSAccess	すべてのリソースへのアクセスを許可します。	arn:aws:organizations::aws:policy/resource_control_policy/p-RCPFullAWSAccess

AWS Organizationsのタグによる属性ベースのアクセスコントロール

属性ベースのアクセスコントロールを使用すると、 AWS リソースと ID AWS の両方にアタッチされたタグなどの管理者管理属性を使用して、それらのリソースへのアクセスを制御できます。例えば、ユーザーとリソースの両方に特定のタグの同じ値がアタッチされている場合には、ユーザーがリソースにアクセスできるように指定できます。

AWS Organizations タグ付け可能なリソースには AWS アカウント、組織のルート、組織単位 (OUs)、またはポリシーが含まれます。Organizations リソースにタグをアタッチすると、そのタグ

を使用して、それらのリソースにアクセスできるユーザーを制御できます。これを行うには、アクションを許可する前に特定のタグキーと値が存在するかどうかをチェックするCondition要素をAWS Identity and Access Management (IAM) アクセス許可ポリシーステートメントに追加します。これにより、「キー X と値 Y を含むタグがアタッチされた OU のみの管理をユーザに許可する」または「ユーザにアタッチされたタグキー Z と同じ値を含むキー Z でタグ付けされた OU のみの管理をユーザに許可する」という効果的な IAM ポリシーを作成することができます。

IAM ポリシーのさまざまなタイプのタグリファレンスに基づいて Condition テストを行うことができます。

- リクエストによって指定されたリソースにアタッチされたタグのチェック
- リクエストを行う IAM ユーザーまたはロールにアタッチされているタグを確認する
- リクエストのパラメータとして含まれているタグをチェックする

ポリシーによるアクセスコントロールでタグを使用する方法の詳細については、「リソースタグを使用した IAM ユーザーおよびロールへのアクセスのコントロール」を参照してください。IAM アクセス許可ポリシーの完全な構文については、「IAM JSON ポリシーリファレンス」を参照してください。

リクエストによって指定されたリソースにアタッチされたタグのチェック

AWS Management Console、 AWS Command Line Interface （ AWS CLI ）、またはいずれかの AWS SDKs を使用してリクエストを行うときは、そのリクエストでアクセスするリソースを指定します。利用可能な特定のタイプのリソースの一覧表示、リソースの読み取り、リソースの書き込み、変更、更新のいずれかを行う場合は、アクセスするリソースをリクエストのパラメータとして指定します。これらのリクエストは、ユーザーとロールにアタッチする IAM アクセス許可ポリシーによって制御されます。これらのポリシーでは、リクエストされたリソースにアタッチされているタグを比較し、それらのタグのキーと値に応じてアクセスを許可または拒否できます。

リソースにアタッチされているタグを確認するには、タグキー名の前に aws:ResourceTag/ という文字列を付けて、Condition 要素内のタグを参照します。

例えば、以下のポリシー例では、リソースにキー department と値 security のタグがアタッチされない限り、ユーザーまたはロールはすべての AWS Organizations オペレーションを実行することができます。そのキーと値が存在する場合、ポリシーによって UntagResource オペレーションが明示的に拒否されます。

JSON

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

        },
        {
            "Effect" : "Deny",
            "Action" : "organizations:UntagResource",
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "aws:ResourceTag/department" : "security"
                }
            }
        }
    ]
}
```

この要素の使用方法の詳細については、IAM ユーザーガイドの「リソースへのアクセスのコントロール」および「aws:ResourceTag」を参照してください。

リクエストを行う IAM ユーザーまたはロールにアタッチされているタグを確認する

リクエストを行うユーザー (プリンシパル) が実行できるオペレーションを、そのユーザーの IAM ユーザーまたはロールにアタッチされたタグに応じて制御できます。これを行うには、`aws:PrincipalTag/`*`key-name`* 条件キーを使用して、呼び出し元のユーザーまたはロールにアタッチする必要のあるタグと値を指定します。

次の例では、指定されたタグ (`cost-center`) が、オペレーションを呼び出すプリンシパルと、オペレーションによってアクセスされるリソースの両方に同じ値が含まれる場合にのみ、アクションを許可する方法について説明します。この例では、呼び出し元ユーザーは、インスタンスにユーザーと同じ `cost-center` 値がタグ付けされている場合にのみ、Amazon EC2 インスタンスを開始および停止できます。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "ec2:startInstances",
            "ec2:stopInstances"
        ],
        "Resource": "*",
        "Condition": {"StringEquals":
            {"ec2:ResourceTag/cost-center": "${aws:PrincipalTag/cost-center}"}}
    }
}
```

この要素の使用方法の詳細については、IAM ユーザーガイドの「IAM プリンシパルのアクセスのコントロール」および「aws:PrincipalTag」を参照してください。

リクエストのパラメータとして含まれているタグをチェックする

いくつかのオペレーションでは、リクエストの一部としてタグを指定できます。例えば、リソースを作成する際に、新しいリソースにアタッチされるタグを指定できます。aws:TagKeys を使用する Condition 要素を指定し、特定のタグキーまたはキーのセットがリクエストに含まれているかどうかによって、オペレーションを許可または拒否できます。この比較演算子では、タグにどのような値が含まれていても問題ありません。指定されたキーのタグが存在するかどうかだけがチェックされます。

タグキーまたはキーのリストを確認するには、次の構文で Condition 要素を指定します。

```
"aws:TagKeys": [ "tag-key-1", "tag-key-2", ... , "tag-key-n" ]
```

比較演算子の前に ForAllValues: を使用することで、リクエストに含まれるすべてのキーが、ポリシーで指定されたキーの 1 つと確実に一致しているかどうかを確認できます。例えば次のポリシー例では、リクエストに存在するすべてのタグがこのポリシー内の 3 つのタグのサブセットである場合にのみ、Organizations のすべてのオペレーションが許可されます。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAllValues:StringEquals": {
                "aws:TagKeys": [
                    "department",
                    "costcenter",
                    "manager"
                ]
            }
        }
    }
}
```

あるいは、ForAnyValue: を比較演算子の前に記述して使用し、リクエスト内の少なくとも 1 つのキーが、ポリシーで指定されたキーの 1 つと確実に一致しているかどうかを確認できます。例えば、次のポリシーでは、指定されたタグキーの少なくとも 1 つがリクエスト内に存在する場合にのみ、Organizations のオペレーションを許可します。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "stage",
                    "region",
                    "domain"
                ]
```

```
            }
        }
    }
}
```

複数のオペレーションによって、リクエストのタグを指定できます。例えば、リソースを作成する際に、新しいリソースにアタッチされるタグを指定できます。ポリシー内のタグキーと値のペアと、リクエストに含まれるキーと値のペアを比較できます。これを行うには、タグのキー名の前に aws:RequestTag/*key-name* という文字列を付けて Condition 要素内のタグを参照し、含まれるべきタグの値を指定します。

たとえば、次のサンプルポリシーは、ユーザーまたはロールによるリクエストを拒否して、リクエスト AWS アカウント に costcenter タグが欠落している を作成するか、そのタグに 1、、2または以外の値を提供します3。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/costcenter": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/costcenter": [
                        "1",
                        "2",
                        "3"
                    ]
```

```
                }
            }
        }
    ]
}
```

これらの要素を使用する方法の詳細については、IAM ユーザーガイドの「aws:TagKeys」および「aws:RequestTag」を参照してください。

AWS Organizations ID とアクセスのトラブルシューティング

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

トピック

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

Organizations でアクションを実行する権限がない

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、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要なorganizations:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 organizations:GetWidget on resource: my-example-widget
```

この場合、organizations:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新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。

iam:PassRole を実行する権限がありません

`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 Organizations にロールを渡せ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 Organizations 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。サインイン資格情報を提供した担当者が管理者です。

自分の 以外のユーザーに Organizations リソース 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:

- Organizations がこれらの機能をサポートしているかどうかについては、「が IAM と AWS Organizations 連携する方法」を参照してください。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、「IAM ユーザーガイド」の「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。

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

でのログ記録とモニタリング AWS Organizations

ベストプラクティスとして、変更がログに記録されることを確実にするために組織を監視する必要があります。これにより、予期しない変更を調査でき、不要な変更をロールバックできます。 AWS Organizations は現在、組織とその内部で発生するアクティビティをモニタリング AWS のサービスできる 2 つの をサポートしています。

トピック

- for での API コール AWS CloudTrail のログ記録 AWS Organizations
- Amazon EventBridge と AWS Organizations

for での API コール AWS CloudTrail のログ記録 AWS Organizations

AWS Organizations は、ユーザー AWS CloudTrail、ロール、または のサービスによって実行されたアクションを記録する AWS サービスである と統合されています AWS Organizations。CloudTrail は、 AWS Organizations コンソールからの呼び出しや API へのコード呼び出しを含む、 のすべての API コールをイベント AWS Organizations としてキャプチャします。 AWS Organizations APIs 証跡を作成する場合は、イベントを含む Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます AWS Organizations。証跡を設定しない場合でも、CloudTrail コンソールの [イベント履歴] で最新のイベントを表示できます。CloudTrail によって収集された情報を使用して、リクエスト、リクエスト元の AWS Organizations IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

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

> **Important**
>
> のすべての CloudTrail 情報は、米国東部 (バージニア北部) リージョン AWS Organizations でのみ表示できます。CloudTrail コンソールに AWS Organizations アクティビティが表示されない場合は、右上隅のメニューを使用してコンソールを米国東部 (バージニア北部) に設定します。 AWS CLI または SDK ツールを使用して CloudTrail にクエリを実行する場合は、クエリを米国東部 (バージニア北部) エンドポイントに転送します。

AWS Organizations CloudTrail の情報

CloudTrail は、アカウントの作成 AWS アカウント 時に で有効になります。アクティビティが発生すると AWS Organizations、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。で最近のイベントを表示、検索、ダウンロードできます AWS アカウント。詳細については、CloudTrail イベント履歴でのイベントの表示を参照してください。

AWS Organizationsのイベントなど、 AWS アカウントのイベントの継続的な記録に対して、追跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。で CloudTrail ログ記録が有効になっている場合 AWS アカウント、 AWS Organizations アクションに対して行われた API コールは CloudTrail ログファイルで追跡され、他の AWS サービスレコードとともに書き込まれます。CloudTrail ログで収集されたイベントデータをさらに分析して処理 AWS のサービス するように他の を設定できます。詳細については、次を参照してください:

- 証跡の作成のための概要
- CloudTrail がサポートするサービスと統合
- CloudTrail 用 Amazon SNS 通知の構成

すべての AWS Organizations アクションは CloudTrail によってログに記録され、AWS Organizations API リファレンスに記載されています。例えば、`CreateAccount` (`CreateAccountResult` イベントを含む)、`ListHandshakesForAccount`、`CreatePolicy`、および `InviteAccountToOrganization` に対する呼び出しにより、CloudTrail ログファイルにエントリが生成されます。

各ログエントリには、リクエストの生成者に関する情報が含まれます。ログエントリのユーザーアイデンティティ情報は、次のことを確認するのに役立ちます。

- リクエストが、ルートユーザーまたは IAM ユーザーのどちらの認証情報を使用して送信されたかどうか
- リクエストが、IAM ロールの一時的なセキュリティ認証情報またはフェデレーティッドユーザーによって行われたかどうか
- リクエストが別の AWS サービスによって行われたかどうか

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

AWS Organizations ログファイルエントリについて

「トレイル」は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは任意ソースからの単一リクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどの情報を含みます。CloudTrail ログファイルは、パブリック API 呼び出しの順序付けられたスタックトレースではないため、特定の順序では表示されません。

ログエントリの例: CloseAccount

次の例は、API が呼び出され、アカウントを閉鎖するワークフローがバックグラウンドで処理を開始する際に生成されるサンプルの `CloseAccount` 呼び出しの CloudTrail ログエントリを示しています。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
            },
            "webIdFederationData": {},
            "attributes": {
```

```
                "mfaAuthenticated": "false",
                "creationDate": "2022-03-18T18:17:06Z"
            }
        }
    },
    "eventTime": "2022-03-18T18:17:06Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CloseAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)...",
    "requestParameters": {
        "accountId": "555555555555"
    },
    "responseElements": null,
    "requestID": "e28932f8-d5da-4d7a-8238-ef74f3d5c09a",
    "eventID": "19fe4c10-f57e-4cb7-a2bc-6b5c30233592",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

次の例は、アカウントを閉鎖するためのバックグラウンドワークフローが正常に完了した後の CloseAccountResult 呼び出しの CloudTrail ログエントリを示しています。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "organizations.amazonaws.com"
  },
  "eventTime": "2022-03-18T18:17:06Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CloseAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "organizations.amazonaws.com",
  "userAgent": "organizations.amazonaws.com",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
```

```
  "eventType": "AwsServiceEvent",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "closeAccountStatus": {
      "accountId": "555555555555",
      "state": "SUCCEEDED",
      "requestedTimestamp": "Mar 18, 2022 6:16:58 PM",
      "completedTimestamp": "Mar 18, 2022 6:16:58 PM"
    }
   },
   "eventCategory": "Management"
}
```

ログエントリの例: CreateAccount

次の例は、API が呼び出され、アカウントを作成するワークフローがバックグラウンドで処理を開始する際に生成されるサンプルの CreateAccount 呼び出しの CloudTrail ログエントリを示しています。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-09-16T21:16:45Z"
            }
```

```
        }
    },
    "eventTime": "2018-06-21T22:06:27Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Windows NT 10.0; Win64; x64)...",
    "requestParameters": {
        "tags": [],
        "email": "****",
        "accountName": "****"
    },
    "responseElements": {
        "createAccountStatus": {
            "accountName": "****",
            "state": "IN_PROGRESS",
            "id": "car-examplecreateaccountrequestid111",
            "requestedTimestamp": "Sep 16, 2020 9:20:50 PM"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

次の例は、アカウントを作成するためのバックグラウンドワークフローが正常に完了した後の CreateAccount 呼び出しの CloudTrail ログエントリを示しています。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "..."
  },
  "eventTime": "2020-09-16T21:20:53Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "....",
  "requestParameters": null,
```

```
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "SUCCEEDED",
      "accountName": "****",
      "accountId": "444455556666",
      "requestedTimestamp": "Sep 16, 2020 9:20:50 PM",
      "completedTimestamp": "Sep 16, 2020 9:20:53 PM"
    }
  }
}
```

次の例は、CreateAccount バックグラウンドワークフローがアカウントの作成に失敗した後に生成される CloudTrail ログエントリを示しています。

```
  {
  "eventVersion": "1.06",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2018-06-21T22:06:27Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "FAILED",
```

```
      "accountName": "****",
      "failureReason": "EMAIL_ALREADY_EXISTS",
      "requestedTimestamp": Jun 21, 2018 10:06:27 PM,
      "completedTimestamp": Jun 21, 2018 10:07:15 PM
    }
  }
}
```

ログエントリの例: CreateOrganizationalUnit

サンプルの `CreateOrganizationalUnit` 呼び出しの CloudTrail ログエントリの例を以下に示します。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:40:11Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateOrganizationalUnit",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "name": "OU-Developers-1",
        "parentId": "r-a1b2"
    },
    "responseElements": {
        "organizationalUnit": {
            "arn": "arn:aws:organizations::111111111111:ou/o-aa111bb222/ou-
examplerootid111-exampleouid111",
            "id": "ou-examplerootid111-exampleouid111",
            "name": "test-cloud-trail"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
```

```
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

ログエントリの例: InviteAccountToOrganization

サンプルの `InviteAccountToOrganization` 呼び出しの CloudTrail ログエントリの例を以下に示します。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:41:17Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "InviteAccountToOrganization",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "notes": "This is a request for Mary's account to join Diego's organization.",
        "target": {
            "type": "ACCOUNT",
            "id": "111111111111"
        }
    },
    "responseElements": {
        "handshake": {
            "requestedTimestamp": "Jan 18, 2017 9:41:16 PM",
            "state": "OPEN",
            "arn": "arn:aws:organizations::111111111111:handshake/o-aa111bb222/invite/
h-examplehandshakeid111",
            "id": "h-examplehandshakeid111",
            "parties": [
                {
```

```
                    "type": "ORGANIZATION",
                    "id": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "id": "222222222222"
                }
            ],
            "action": "invite",
            "expirationTimestamp": "Feb 2, 2017 9:41:16 PM",
            "resources": [
                {
                    "resources": [
                        {
                            "type": "MASTER_EMAIL",
                            "value": "diego@example.com"
                        },
                        {
                            "type": "MASTER_NAME",
                            "value": "Management account for organization"
                        },
                        {
                            "type": "ORGANIZATION_FEATURE_SET",
                            "value": "ALL"
                        }
                    ],
                    "type": "ORGANIZATION",
                    "value": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "value": "222222222222"
                },
                {
                    "type": "NOTES",
                    "value": "This is a request for Mary's account to join Diego's
organization."
                }
            ]
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
```

```
    "recipientAccountId": "111111111111"
}
```

ログエントリの例: AttachPolicy

サンプルの AttachPolicy 呼び出しの CloudTrail ログエントリの例を以下に示します。このレスポンスは、リクエストされたポリシータイプが、アタッチが試行された root で有効でないため、呼び出しが失敗したことを示します。

```
{
    "eventVersion": "1.06",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:42:44Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "AttachPolicy",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "errorCode": "PolicyTypeNotEnabledException",
    "errorMessage": "The given policy type ServiceControlPolicy is not enabled on the
 current view",
    "requestParameters": {
        "policyId": "p-examplepolicyid111",
        "targetId": "ou-examplerootid111-exampleouid111"
    },
    "responseElements": null,
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

ログエントリの例: 無効な有効なポリシー

次の例は、サンプルEffectivePolicyValidationイベントの CloudTrail ログエントリを示しています。このイベントは、組織内の更新によっていずれかのアカウントに無効な有効なポリシーが作成されるたびに、組織の管理アカウントに発行されます。


```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-07-17T14:53:40Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "EffectivePolicyValidation",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "readOnly": true,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "serviceEventDetails": {
        "accountId": "111111111111",
        "policyType": "BACKUP_POLICY",
        "state": "INVALID",
        "requestTimestamp": "Jul 17, 2025, 2:53:40 PM",
        "info": "All validation errors listed",
        "validationErrors": [
            {
                "accountPath": "o-aa111bb222/r-a1b2/111111111111/",
                "evaluationTimestamp": "Jul 17, 2025, 2:53:40 PM",
                "errorCode": "ELEMENTS_TOO_MANY",
                "errorMessage": "'hourly_rule' exceeds the allowed maximum limit 10",
                "pathToError": "plans/hourly-backup/rules/hourly_rule",
                "contributingPolicies": [
                    "p-examplepolicyid111"
                ]
            }
        ]
```

```
    },
    "eventCategory": "Management"
}
```

ログエントリの例: 有効な有効なポリシー

次の例は、サンプルEffectivePolicyValidationイベントの CloudTrail ログエントリを示しています。このイベントは、組織の更新によって以前に無効だったアカウントの有効なポリシーが修正されるたびに、組織の管理アカウントに発行されます。

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "111111111111",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-07-17T14:54:40Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "EffectivePolicyValidation",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "readOnly": true,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "serviceEventDetails": {
        "accountId": "111111111111",
        "policyType": "BACKUP_POLICY",
        "state": "VALID",
        "requestTimestamp": "Jul 17, 2025, 2:54:40 PM",
        "info": "Previous effective policy validation error(s) resolved for this
 account/policyType"
    },
    "eventCategory": "Management"
}
```

Amazon EventBridge と AWS Organizations

AWS Organizations は、以前の Amazon CloudWatch Events である Amazon EventBridge と連携して、組織内で管理者指定のアクションが発生したときにイベントを発生させることができます。例えば、アクションの重要性のため、ほとんどの管理者は、組織内に誰かが新しいアカウントを作成するたびに、またはメンバーアカウントの管理者が組織を離れようとするたびに警告を受けたいと考えています。これらのアクションを探す EventBridge ルールを設定し、生成されたイベントを管理者が定義したターゲットに送信できます。受信者に E メールまたはテキストメッセージを送信する Amazon SNS トピックをターゲットに指定できます。また、後で確認するためにアクションの詳細をログに記録する AWS Lambda 関数を作成することもできます。

組織内の主要なアクティビティをモニタリングするために EventBridge を有効にする方法を紹介しているチュートリアルについては、「チュートリアル: Amazon EventBridge を使用して、組織の重要な変更をモニタリングする」を参照してください。

> **Important**
>
> 現在、 AWS Organizations は米国東部 (バージニア北部) リージョンでのみホストされています (グローバルに利用可能ですが) 。このチュートリアルのステップを実行するには、そのリージョンを使用する AWS Management Console ように を設定する必要があります。

設定や有効化の方法などを含めた EventBridge の詳細については、「Amazon EventBridge ユーザーガイド」を参照してください。

AWS Organizationsのコンプライアンス検証

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスAWS のサービス プログラムによる対象範囲内コンプライアンス を参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「 Compliance ProgramsAssurance」を参照してください。

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

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

- セキュリティのコンプライアンスとガバナンス – これらのソリューション実装ガイドでは、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の機能をデプロイする手順を示します。
- HIPAA 対応サービスのリファレンス – HIPAA 対応サービスの一覧が提供されています。すべてが HIPAA 対応 AWS のサービス であるわけではありません。
- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界と場所に適用される場合があります。
- AWS カスタマーコンプライアンスガイド – コンプライアンスの観点から責任共有モデルを理解します。このガイドは、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールを保護し、そのガイダンスに AWS のサービス マッピングするためのベストプラクティスをまとめたものです。
- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に把握できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールの一覧については、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty – 環境をモニタリングして AWS アカウント不審なアクティビティや悪意のあるアクティビティがないか調べることで、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。GuardDuty を使用すると、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件に対応できます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

の耐障害性 AWS Organizations

AWS グローバルインフラストラクチャは、 AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。 は、低レイテンシー、高スループット、および高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティーゾーン AWS リージョンを提供します。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。ア

ベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、およびスケーラビリティが優れています。

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

のインフラストラクチャセキュリティ AWS Organizations

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

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

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

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

コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

トラブルシューティング AWS Organizations

の使用中に問題が発生した場合は AWS Organizations、このセクションのトピックを参照してください。

一般的な問題のトラブルシューティング

この情報を使用して、アクセスが拒否された問題や、作業中に発生する可能性があるその他の一般的な問題を診断して修正できます AWS Organizations。

トピック

- へのリクエスト時に「アクセス拒否」メッセージが表示される AWS Organizations
- 一時的なセキュリティ認証情報を使用してリクエストを送信すると「アクセスが拒否されました」というメッセージが表示される
- 組織をメンバーアカウントとして残したり、メンバーアカウントを管理アカウントとして削除しようとすると、「アクセスが拒否されました」というメッセージが表示されます。
- 組織にアカウントを追加しようとすると「クォータを超えました」というメッセージが表示される
- アカウントを追加または削除するときに「このオペレーションでは待機期間が必要です」というメッセージが表示される
- 組織にアカウントを追加しようとすると「組織がまだ初期化中です」というメッセージが表示される
- 組織にアカウントを招待しようとすると、「招待は無効になっています」というメッセージが表示される。
- 変更がすぐに表示されない
- 既に組織の一部であるアカウントにアクセスしようとすると、「サインアップの完了」というメッセージが表示される

へのリクエスト時に「アクセス拒否」メッセージが表示される AWS Organizations

- 要求したアクションとリソースを呼び出す権限を持っているかを確認します。管理者は、ユーザー、グループ、ロールに IAM ポリシーをアタッチし、許可を付与する必要があります。ポリシーが時間帯または IP アドレス制限などの条件を含む権限を付与する記述をしている場合は、リクエストを送信する際にそれらの条件を満たす必要もあります。ユーザー、グループ、ロールの

ポリシーの表示または修正に関する詳細については、「IAM ユーザーガイド」の「ポリシーの使用」を参照してください。

- 手動で API リクエストに署名する (AWS SDK を使用しない) 場合は、正確にリクエストに署名していることを確認します。

一時的なセキュリティ認証情報を使用してリクエストを送信すると「アクセスが拒否されました」というメッセージが表示される

- リクエストの作成に使用している ユーザーまたはロールに適切なアクセス権限があることを確認します。一時的なセキュリティ認証情報のアクセス権限は ユーザーまたはロールから生じるものであるため、 ユーザーまたはロールに付与されたアクセス権限に制限されます。一時的なセキュリティ認証情報のアクセス権限がどのように決定されるかについては、「IAM ユーザーガイド」の「Controlling Permissions for Temporary Security Credentials」を参照してください。
- リクエストが正しく署名されており、そのリクエストの形式が正しいことを確認します。詳細については、「IAM ユーザーガイド」の「選択した SDK のツールキットドキュメント」または「一時的なセキュリティ認証情報を使用して AWS リソースへのアクセスをリクエストする」を参照してください。
- 一時的な認証情報が失効していないことを確認します。詳細については、「IAM ユーザーガイド」の「Requesting Temporary Security Credentials」を参照してください。

組織をメンバーアカウントとして残したり、メンバーアカウントを管理アカウントとして削除しようとすると、「アクセスが拒否されました」というメッセージが表示されます。

- メンバーアカウントを削除できるのは、メンバーアカウントでの請求を IAM ユーザーアクセスで有効にした後のみです。詳細については、AWS Billing ユーザーガイドの「Billing and Cost Management コンソールへのアクセスを有効にする」を参照してください。
- アカウントがスタンドアロンアカウントとして動作するために必要な情報を持っている場合にのみ、組織からアカウントを削除できます。 AWS Organizations コンソール、API、または AWS CLI コマンドを使用して組織内にアカウントを作成すると、その情報は自動的に収集されません。スタンドアロンにするアカウントの場合、 AWS カスタマーアグリーメントを承諾し、サポートプランを選択し、必要な連絡先情報を指定して検証し、現在の支払い方法を指定する必要があります。 は、アカウントが組織にアタッチされていない間に発生する課金対象 (AWS 無料利用枠ではない) AWS アクティビティに対して課金するために支払い方法 AWS を使用します。詳細について

は、「を使用してメンバーアカウントから組織を退出する AWS Organizations」を参照してください。

組織にアカウントを追加しようとすると「クォータを超えました」というメッセージが表示される

組織内で保持できるアカウントの数には上限があります。削除したアカウントや閉じたアカウントは、引き続きこのクォータに対してカウントされます。

参加の招待は、組織内のアカウントの上限数に対してカウントされます。招待されたアカウントが拒否された場合、管理アカウントが招待をキャンセルした場合、または招待状の有効期限が切れた場合は、カウントが返されます。

- を閉鎖または削除する前に AWS アカウント、クォータに対して引き続きカウントされないように、組織から削除します。
- クォータ引き上げのリクエストの詳細については、「最大値および最小値」を参照してください。

アカウントを追加または削除するときに「このオペレーションでは待機期間が必要です」というメッセージが表示される

一部のアクションでは、アカウントクォータのために待機期間が必要です。たとえば、作成したばかりのアカウントをすぐに削除することはできません。数日後にアクションを再試行してください。

アカウントの追加に関する問題については、「デフォルトのアカウントの最大数」を参照してください。アカウントの削除に関する問題については、30 日以内に閉鎖できるアカウントのクォータ数を参照してください。

組織にアカウントを追加しようとすると「組織がまだ初期化中です」というメッセージが表示される

このエラーが表示され、組織を作成してから 1 時間以上が経過している場合は、AWS サポート までお問い合わせください。

組織にアカウントを招待しようとすると、「招待は無効になっています」というメッセージが表示される。

これは、組織内のすべての機能を有効にする場合に発生します。このオペレーションには時間がかかり、すべてのメンバーアカウントが応答する必要があります。オペレーションが完了するまで、新しいアカウントを組織サイトに加入するよう招待することはできません。

変更がすぐに表示されない

世界中のデータセンター内のコンピューターを介してアクセスされるサービスとして、 AWS Organizations は、結果整合性と呼ばれる分散コンピューティングモデルを採用しています。で行った変更は、可能なすべてのエンドポイントから表示されるまでに時間が AWS Organizations かかります。一部の遅延は、サーバーからサーバー、またはレプリケーションゾーンからレプリケーションゾーンにデータを送信するのにかかる時間から発生します。 AWS Organizations また、 はキャッシュを使用してパフォーマンスを向上させますが、場合によっては時間が増えることがあります。変更は、以前にキャッシュされたデータがタイムアウトになるまで反映されない場合があります。

発生する可能性のあるこれらの遅延を考慮して、グローバルなアプリケーションを設計します。ある場所で行われた変更が別の場所にすぐに表示されない場合でも、適切に動作することを確認します。

この AWS のサービス 影響を受ける他の の詳細については、次のリソースを参照してください。

- Amazon Redshift データベースデベロッパーガイドの「データの整合性の管理」
- 「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 Data Consistency Model」
- AWS ビッグデータブログの「ETL ワークフローに Amazon S3 と Amazon Elastic MapReduce を使用する場合の整合性の確保」
- Amazon EC2 API リファレンスの「EC2 の結果整合性」

既に組織の一部であるアカウントにアクセスしようとすると、「サインアップの完了」というメッセージが表示される

- メンバーアカウントが管理アカウントの請求詳細を継承するまでに最大 48 時間かかる場合があります。
- 問題が 48 時間後に解決しない場合は、アカウントおよび請求サポートチームにサポートケースを開くことができます。詳細については、「サポートケースの作成」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

このセクションには、 クエリ API の使用に関する一般的な情報が含まれています AWS Organizations。API オペレーションとエラーの詳細については、「AWS Organizations API リファレンス」を参照してください。

> **Note**
>
> クエリ API AWS Organizations を直接呼び出す代わりに、いずれかの AWS SDKsを使用できます。 AWS SDKsは、さまざまなプログラミング言語とプラットフォーム (Java、Ruby、.NET、iOS、Android など) 用のライブラリとサンプルコードで構成されています。SDKs は、 AWS Organizations および へのプログラムによるアクセスを作成するのに便利な方法を提供します AWS。例えば、SDK は要求への暗号を使用した署名、エラーの管理、要求の自動的な再試行などのタスクを処理します。 AWS SDKs「アマゾン ウェブ サービスのツール」を参照してください。

の Query API AWS Organizations を使用すると、サービスアクションを呼び出すことができます。クエリ API リクエストは HTTPS リクエストであり、実行するオペレーションを示す `Action`パラメータを含める必要があります。 は、すべてのオペレーションに対して GET リクエストと POST リクエスト AWS Organizations をサポートします。つまり、この API では、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。この制限はブラウザによって異なり、通常は 2048 バイトです。したがって、大きなサイズを必要とする Query API リクエストにおいては、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、「AWS Organizations API リファレンス」の個別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 Organizations API リクエストの署名

エンドポイント

AWS Organizations には、米国東部 (バージニア北部) リージョンでホストされている単一のグローバル API エンドポイントがあります。

すべてのサービスの AWS エンドポイントとリージョンの詳細については、「」の「リージョンエンドポイント」を参照してくださいAWS 全般のリファレンス。

HTTPS の必要性

Query API は、セキュリティ認証情報などの機密情報を返すため、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 Organizations API リクエストの署名

リクエストには、アクセスキー ID およびシークレットアクセスキーによる署名が必要です。での日常的な作業には AWS アカウントのルートユーザー 認証情報を使用しないことを強くお勧めします AWS Organizations。ユーザーまたはロールに認証情報を使用できます。

API リクエストに署名するには、 AWS 署名バージョン 4 を使用する必要があります。署名バージョン 4 の使用の詳細については、IAM ユーザーガイドの AWS API リクエストの署名を参照してください。

AWS Organizations は、署名バージョン 2 などの以前のバージョンをサポートしていません。

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 – アクセスに使用できる認証情報のタイプに関する一般的な情報を提供します AWS。
- IAM におけるセキュリティのベストプラクティス – IAM サービスを使用して、 のリソースを含む AWS リソースをセキュリティで保護するための提案を提供します AWS Organizations。
- 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 SDKsコード例

次のコード例は、 AWS Software Development Kit (SDK) で Organizations を使用する方法を示しています。

アクションはより大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。アクションは個々のサービス機能を呼び出す方法を示していますが、コンテキスト内のアクションは、関連するシナリオで確認できます。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Organizations での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

コードの例

- AWS SDKs基本的な例
  - AWS SDKsアクション
    - AWS SDK または CLI AttachPolicyで を使用する
    - AWS SDK または CLI CreateAccountで を使用する
    - AWS SDK または CLI CreateOrganizationで を使用する
    - AWS SDK または CLI CreateOrganizationalUnitで を使用する
    - AWS SDK または CLI CreatePolicyで を使用する
    - AWS SDK または CLI DeleteOrganizationで を使用する
    - AWS SDK または CLI DeleteOrganizationalUnitで を使用する
    - AWS SDK または CLI DeletePolicyで を使用する
    - AWS SDK または CLI DescribePolicyで を使用する
    - AWS SDK または CLI DetachPolicyで を使用する
    - AWS SDK または CLI ListAccountsで を使用する
    - AWS SDK または CLI ListOrganizationalUnitsForParentで を使用する
    - AWS SDK または CLI ListPoliciesで を使用する

AWS SDKs基本的な例

次のコード例は、 SDKs AWS Organizations で AWS の基本を使用する方法を示しています。

例

- AWS SDKsアクション
  - AWS SDK または CLI AttachPolicyで を使用する
  - AWS SDK または CLI CreateAccountで を使用する
  - AWS SDK または CLI CreateOrganizationで を使用する
  - AWS SDK または CLI CreateOrganizationalUnitで を使用する
  - AWS SDK または CLI CreatePolicyで を使用する
  - AWS SDK または CLI DeleteOrganizationで を使用する
  - AWS SDK または CLI DeleteOrganizationalUnitで を使用する
  - AWS SDK または CLI DeletePolicyで を使用する
  - AWS SDK または CLI DescribePolicyで を使用する
  - AWS SDK または CLI DetachPolicyで を使用する
  - AWS SDK または CLI ListAccountsで を使用する
  - AWS SDK または CLI ListOrganizationalUnitsForParentで を使用する
  - AWS SDK または CLI ListPoliciesで を使用する

AWS SDKsアクション

次のコード例は、 AWS SDKs を使用して個々の Organizations アクションを実行する方法を示しています。それぞれの例には、GitHub へのリンクがあり、そこにはコードの設定と実行に関する説明が記載されています。

以下の例には、最も一般的に使用されるアクションのみ含まれています。詳細な一覧については、「AWS Organizations API リファレンス」を参照してください。

例

- AWS SDK または CLI AttachPolicyで を使用する
- AWS SDK または CLI CreateAccountで を使用する
- AWS SDK または CLI CreateOrganizationで を使用する
- AWS SDK または CLI CreateOrganizationalUnitで を使用する
- AWS SDK または CLI CreatePolicyで を使用する
- AWS SDK または CLI DeleteOrganizationで を使用する
- AWS SDK または CLI DeleteOrganizationalUnitで を使用する

- AWS SDK または CLI DeletePolicyで を使用する
- AWS SDK または CLI DescribePolicyで を使用する
- AWS SDK または CLI DetachPolicyで を使用する
- AWS SDK または CLI ListAccountsで を使用する
- AWS SDK または CLI ListOrganizationalUnitsForParentで を使用する
- AWS SDK または CLI ListPoliciesで を使用する

AWS SDK または CLI **AttachPolicy**で を使用する

以下のコード例は、AttachPolicy の使用方法を示しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to attach an AWS Organizations policy to an organization,
/// an organizational unit, or an account.
/// </summary>
public class AttachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then calls the
    /// AttachPolicyAsync method to attach the policy to the root
    /// organization.
    /// </summary>
    public static async Task Main()
    {
```

```
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var policyId = "p-00000000";
            var targetId = "r-0000";

            var request = new AttachPolicyRequest
            {
                PolicyId = policyId,
                TargetId = targetId,
            };

            var response = await client.AttachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully attached Policy ID {policyId} to
 Target ID: {targetId}.");
            }
            else
            {
                Console.WriteLine("Was not successful in attaching the policy.");
            }
        }
    }
```

- API の詳細については、AWS SDK for .NET API リファレンスの「AttachPolicy」を参照してください。

CLI

AWS CLI

root、OU、またはアカウントにポリシーをアタッチするには

例 1

次の例は、サービスコントロールポリシーを OU にアタッチする方法を示しています。

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id ou-examplerootid111-exampleouid111
```

例 2

次の例は、サービスコントロールポリシーをアカウントに直接アタッチする方法を示しています。

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id 333333333333
```

- API の詳細については、AWS CLI コマンドリファレンスの「AttachPolicy」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
def attach_policy(policy_id, target_id, orgs_client):
    """
    Attaches a policy to a target. The target is an organization root, account,
 or
    organizational unit.

    :param policy_id: The ID of the policy to attach.
    :param target_id: The ID of the resources to attach the policy to.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.attach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Attached policy %s to target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't attach policy %s to target %s.", policy_id, target_id
        )
        raise
```

- API の詳細については、AWS SDK for Python (Boto3) API リファレンスの「AttachPolicy」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Organizations での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI `CreateAccount`で を使用する

以下のコード例は、`CreateAccount` の使用方法を示しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new AWS Organizations account.
/// </summary>
public class CreateAccount
{
    /// <summary>
    /// Initializes an Organizations client object and uses it to create
    /// the new account with the name specified in accountName.
    /// </summary>
    public static async Task Main()
    {
```

```
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var accountName = "ExampleAccount";
            var email = "someone@example.com";

            var request = new CreateAccountRequest
            {
                AccountName = accountName,
                Email = email,
            };

            var response = await client.CreateAccountAsync(request);
            var status = response.CreateAccountStatus;

            Console.WriteLine($"The staus of {status.AccountName} is
{status.State}.");
        }
    }
```

- API の詳細については、AWS SDK for .NET API リファレンスの「CreateAccount」を参照してください。

CLI

AWS CLI

自動的に組織の一部となるメンバーアカウントを作成するには

次の例は、組織のメンバーアカウントを作成する方法を示しています。メンバーアカウントは、「プロダクションアカウント」という名前と E メールアドレス (susan@example.com) で構成されます。roleName パラメータが指定されていないため、Organizations では OrganizationAccountAccessRole というデフォルト名を使用して IAM ロールが自動的に作成されます。また、IamUserAccessToBilling パラメータが指定されていないため、必要な権限を持つ IAM ユーザーまたはロールにアカウントの請求データへのアクセスを許可する設定には、デフォルト値 ALLOW が使用されます。Organizations は、スーザンに「ようこそ AWS」という E メールを自動的に送信します。

```
aws organizations create-account --email susan@example.com --account-
name "Production Account"
```

出力には、ステータスが現在の IN_PROGRESS 状態であることを示すリクエストオブジェクトが含まれます。

```
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
}
```

describe-create-account-status コマンドに Id レスポンス値を create-account-request-id parameter の値として指定することで、後でリクエストの現在のステータスをクエリすることができます。

詳細については、「 Organizations ユーザーガイド」の「組織での AWS アカウントの作成」を参照してください。 AWS

- API の詳細については、AWS CLI コマンドリファレンスの「CreateAccount」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Organizations での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **CreateOrganization**で を使用する

以下のコード例は、CreateOrganization の使用方法を示しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
using System;
using System.Threading.Tasks;
```

```
    using Amazon.Organizations;
    using Amazon.Organizations.Model;

    /// <summary>
    /// Creates an organization in AWS Organizations.
    /// </summary>
    public class CreateOrganization
    {
        /// <summary>
        /// Creates an Organizations client object and then uses it to create
        /// a new organization with the default user as the administrator, and
        /// then displays information about the new organization.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var response = await client.CreateOrganizationAsync(new
CreateOrganizationRequest
            {
                FeatureSet = "ALL",
            });

            Organization newOrg = response.Organization;

            Console.WriteLine($"Organization: {newOrg.Id} Main Accoount:
{newOrg.MasterAccountId}");
        }
    }
```

- API の詳細については、AWS SDK for .NET API リファレンスの「CreateOrganization」を参照してください。

CLI

AWS CLI

例 1: 新しい組織を作成するには

Bill は、アカウント 111111111111 の認証情報を使用して組織を作成したいと考えています。次の例は、このアカウントが新しい組織のマスターアカウントになることを示していま

す。Bill は機能セットを指定していないため、新しい組織ではデフォルトですべての機能が有効になり、サービスコントロールポリシーがルート上で有効になります。

```
aws organizations create-organization
```

出力には、新しい組織に関する詳細を含む組織オブジェクトが含まれます。

```
{
        "Organization": {
                "AvailablePolicyTypes": [
                        {
                                "Status": "ENABLED",
                                "Type": "SERVICE_CONTROL_POLICY"
                        }
                ],
                "MasterAccountId": "111111111111",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "FeatureSet": "ALL",
                "Id": "o-exampleorgid",
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid"
        }
}
```

例 2: 一括決済機能のみを有効にした新しい組織を作成するには

次の例では、一括決済機能のみをサポートする組織を作成します。

```
aws organizations create-organization --feature-set CONSOLIDATED_BILLING
```

出力には、新しい組織に関する詳細を含む組織オブジェクトが含まれます。

```
{
        "Organization": {
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
                "AvailablePolicyTypes": [],
                "Id": "o-exampleorgid",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
```

```
                "MasterAccountEmail": "bill@example.com",
                "MasterAccountId": "111111111111",
                "FeatureSet": "CONSOLIDATED_BILLING"
        }
}
```

詳細については、「AWS Organizations ユーザーガイド」の「Creating an Organization」を参照してください。

- API の詳細については、AWS CLI コマンドリファレンスの「CreateOrganization」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Organizations での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **CreateOrganizationalUnit**で を使用する

以下のコード例は、CreateOrganizationalUnit の使用方法を示しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new organizational unit in AWS Organizations.
/// </summary>
public class CreateOrganizationalUnit
{
    /// <summary>
```

```
        /// Initializes an Organizations client object and then uses it to call
        /// the CreateOrganizationalUnit method. If the call succeeds, it
        /// displays information about the new organizational unit.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var orgUnitName = "ProductDevelopmentUnit";

            var request = new CreateOrganizationalUnitRequest
            {
                Name = orgUnitName,
                ParentId = "r-0000",
            };

            var response = await client.CreateOrganizationalUnitAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully created organizational unit:
{orgUnitName}.");
                Console.WriteLine($"Organizational unit {orgUnitName} Details");
                Console.WriteLine($"ARN: {response.OrganizationalUnit.Arn} Id:
{response.OrganizationalUnit.Id}");
            }
            else
            {
                Console.WriteLine("Could not create new organizational unit.");
            }
        }
    }
```

- API の詳細については、AWS SDK for .NET API リファレンスの「CreateOrganizationalUnit」を参照してください。

CLI

AWS CLI

ルート OU または親 OU に OU を作成するには

次の例は、AccountingOU という名前の OU を作成する方法を示しています。

```
aws organizations create-organizational-unit --parent-id r-examplerootid111 --
name AccountingOU
```

出力には、新しい OU に関する詳細を含む organizationalUnit オブジェクトが含まれます。

```
{
        "OrganizationalUnit": {
                "Id": "ou-examplerootid111-exampleouid111",
                "Arn": "arn:aws:organizations::111111111111:ou/o-exampleorgid/ou-
examplerootid111-exampleouid111",
                "Name": "AccountingOU"
        }
}
```

- API の詳細については、AWS CLI コマンドリファレンスの「CreateOrganizationalUnit」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Organizations での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **CreatePolicy**で を使用する

以下のコード例は、`CreatePolicy` の使用方法を示しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
   using System;
   using System.Threading.Tasks;
   using Amazon.Organizations;
   using Amazon.Organizations.Model;

   /// <summary>
   /// Creates a new AWS Organizations Policy.
   /// </summary>
   public class CreatePolicy
   {
       /// <summary>
       /// Initializes the AWS Organizations client object, uses it to
       /// create a new Organizations Policy, and then displays information
       /// about the newly created Policy.
       /// </summary>
       public static async Task Main()
       {
           IAmazonOrganizations client = new AmazonOrganizationsClient();
           var policyContent = "{" +
               "   \"Version\": \"2012-10-17\"," +
               " \"Statement\" : [{" +
                   " \"Action\" : [\"s3:*\"]," +
                   " \"Effect\" : \"Allow\"," +
                   " \"Resource\" : \"*\"" +
               "}]" +
           "}";

           try
           {
               var response = await client.CreatePolicyAsync(new
CreatePolicyRequest
               {
                   Content = policyContent,
                   Description = "Enables admins of attached accounts to
delegate all Amazon S3 permissions",
                   Name = "AllowAllS3Actions",
                   Type = "SERVICE_CONTROL_POLICY",
               });

               Policy policy = response.Policy;
               Console.WriteLine($"{policy.PolicySummary.Name} has the following
content: {policy.Content}");
           }
```

```
            catch (Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
        }
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「CreatePolicy」を参照してください。

CLI

AWS CLI

例 1: JSON ポリシーのテキストソースファイルを使用してポリシーを作成するには

次の例は、AllowAllS3Actions という名前のサービスコントロールポリシーを作成する方法を示しています。ポリシーの内容は、policy.json というローカルコンピューター上のファイルから取得されます。

```
aws organizations create-policy --content file://policy.json --
name AllowAllS3Actions, --type SERVICE_CONTROL_POLICY --description "Allows
 delegation of all S3 actions"
```

出力には、新しいポリシーの詳細を含むポリシーオブジェクトが含まれます。

```
{
        "Policy": {
                "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Action\":[\"s3:*\"],\"Resource\":[\"*\"]}]}",
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::o-exampleorgid:policy/
service_control_policy/p-examplepolicyid111",
                        "Description": "Allows delegation of all S3 actions",
                        "Name": "AllowAllS3Actions",
                        "Type":"SERVICE_CONTROL_POLICY"
                }
        }
}
```

例 2: JSON ポリシーをパラメータとしてポリシーを作成するには

次の例は、ポリシーの内容を JSON 文字列としてパラメータに埋め込むことで、同じ SCP を作成する方法を示しています。文字列は、パラメータ内でリテラルとして扱われるように、二重引用符の前にバックスラッシュを付けてエスケープする必要があります。パラメータ自体も二重引用符で囲みます。

```
aws organizations create-policy --content "{\"Version\":\"2012-10-17\",
\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"s3:*\"],\"Resource
\":[\"*\"]}]}" --name AllowAllS3Actions --type SERVICE_CONTROL_POLICY --
description "Allows delegation of all S3 actions"
```

Organizations でのポリシーの作成と使用の詳細については、「AWS Organizations ユーザーガイド」の「Organizations のポリシーの管理」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「CreatePolicy」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
def create_policy(name, description, content, policy_type, orgs_client):
    """
    Creates a policy.

    :param name: The name of the policy.
    :param description: The description of the policy.
    :param content: The policy content as a dict. This is converted to JSON
 before
                    it is sent to AWS. The specific format depends on the policy
 type.
    :param policy_type: The type of the policy.
    :param orgs_client: The Boto3 Organizations client.
    :return: The newly created policy.
```

```
    """
    try:
        response = orgs_client.create_policy(
            Name=name,
            Description=description,
            Content=json.dumps(content),
            Type=policy_type,
        )
        policy = response["Policy"]
        logger.info("Created policy %s.", name)
    except ClientError:
        logger.exception("Couldn't create policy %s.", name)
        raise
    else:
        return policy
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「CreatePolicy」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Organizations での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **DeleteOrganization**で を使用する

以下のコード例は、DeleteOrganization の使用方法を示しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    using System;
```

```
    using System.Threading.Tasks;
    using Amazon.Organizations;
    using Amazon.Organizations.Model;

    /// <summary>
    /// Shows how to delete an existing organization using the AWS
    /// Organizations Service.
    /// </summary>
    public class DeleteOrganization
    {
        /// <summary>
        /// Initializes the Organizations client and then calls
        /// DeleteOrganizationAsync to delete the organization.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var response = await client.DeleteOrganizationAsync(new
DeleteOrganizationRequest());

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine("Successfully deleted organization.");
            }
            else
            {
                Console.WriteLine("Could not delete organization.");
            }
        }
    }
```

- API の詳細については、AWS SDK for .NET API リファレンスの「DeleteOrganization」を参照してください。

CLI

AWS CLI

組織を削除するには

次の例は、組織を削除する方法を示しています。この操作を実行するには、組織のマスターアカウントの管理者である必要があります。この例では、組織からメンバーアカウント、OU、ポリシーをすべて削除済みであることを前提としています。

```
aws organizations delete-organization
```

- API の詳細については、AWS CLI コマンドリファレンスの「DeleteOrganization」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Organizations での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **DeleteOrganizationalUnit**で を使用する

以下のコード例は、DeleteOrganizationalUnit の使用方法を示しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing AWS Organizations organizational unit.
/// </summary>
public class DeleteOrganizationalUnit
{
    /// <summary>
    /// Initializes the Organizations client object and calls
    /// DeleteOrganizationalUnitAsync to delete the organizational unit
```

```
        /// with the selected ID.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var orgUnitId = "ou-0000-00000000";

            var request = new DeleteOrganizationalUnitRequest
            {
                OrganizationalUnitId = orgUnitId,
            };

            var response = await client.DeleteOrganizationalUnitAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully deleted the organizational unit
with ID: {orgUnitId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete the organizational unit with
ID: {orgUnitId}.");
            }
        }
    }
```

- API の詳細については、AWS SDK for .NET API リファレンスの「DeleteOrganizationalUnit」を参照してください。

CLI

AWS CLI

OU を削除するには

次の例は、OU を削除する方法を示しています。この例では、OU からすべてのアカウントと他の OU を削除済みであることを前提としています。

```
aws organizations delete-organizational-unit --organizational-unit-id ou-
examplerootid111-exampleouid111
```

- API の詳細については、AWS CLI コマンドリファレンスの「DeleteOrganizationalUnit」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Organizations での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **DeletePolicy**で を使用する

以下のコード例は、DeletePolicy の使用方法を示しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Deletes an existing AWS Organizations policy.
/// </summary>
public class DeletePolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// delete the policy with the specified policyId.
    /// </summary>
    public static async Task Main()
    {
```

```
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var policyId = "p-00000000";

            var request = new DeletePolicyRequest
            {
                PolicyId = policyId,
            };

            var response = await client.DeletePolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully deleted Policy: {policyId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete Policy: {policyId}.");
            }
        }
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「DeletePolicy」を参照してください。

CLI

AWS CLI

ポリシーを削除するには

次の例は、組織からポリシーを削除する方法を示しています。この例では、ポリシーをすべてのエンティティから事前にデタッチしたことを前提としています。

```
aws organizations delete-policy --policy-id p-examplepolicyid111
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「DeletePolicy」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
def delete_policy(policy_id, orgs_client):
    """
    Deletes a policy.

    :param policy_id: The ID of the policy to delete.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.delete_policy(PolicyId=policy_id)
        logger.info("Deleted policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't delete policy %s.", policy_id)
        raise
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「DeletePolicy」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Organizations での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **DescribePolicy**で を使用する

以下のコード例は、DescribePolicy の使用方法を示しています。

CLI

AWS CLI

ポリシーに関する情報を取得するには

次の例は、ポリシーに関する情報をリクエストする方法を示しています。

```
aws organizations describe-policy --policy-id p-examplepolicyid111
```

出力には、ポリシーの詳細を含むポリシーオブジェクトが含まれます。

```
{
        "Policy": {
                "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement
\": [\n    {\n      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n
 \"Resource\": \"*\"\n    }\n  ]\n}",
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::111111111111:policy/o-
exampleorgid/service_control_policy/p-examplepolicyid111",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-examplepolicyid111",
                        "AwsManaged": false,
                        "Name": "AllowAllS3Actions",
                        "Description": "Enables admins to delegate S3
 permissions"
                }
        }
}
```

- API の詳細については、AWS CLI コマンドリファレンスの「DescribePolicy」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
def describe_policy(policy_id, orgs_client):
    """
    Describes a policy.

    :param policy_id: The ID of the policy to describe.
    :param orgs_client: The Boto3 Organizations client.
    :return: The description of the policy.
    """
    try:
        response = orgs_client.describe_policy(PolicyId=policy_id)
        policy = response["Policy"]
        logger.info("Got policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't get policy %s.", policy_id)
        raise
    else:
        return policy
```

- API の詳細については、AWS SDK for Python (Boto3) API リファレンスの「DescribePolicy」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Organizations での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **DetachPolicy**で を使用する

以下のコード例は、DetachPolicy の使用方法を示しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    using System;
    using System.Threading.Tasks;
    using Amazon.Organizations;
    using Amazon.Organizations.Model;

    /// <summary>
    /// Shows how to detach a policy from an AWS Organizations organization,
    /// organizational unit, or account.
    /// </summary>
    public class DetachPolicy
    {
        /// <summary>
        /// Initializes the Organizations client object and uses it to call
        /// DetachPolicyAsync to detach the policy.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var policyId = "p-00000000";
            var targetId = "r-0000";

            var request = new DetachPolicyRequest
            {
                PolicyId = policyId,
                TargetId = targetId,
            };

            var response = await client.DetachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully detached policy with Policy Id:
{policyId}.");
            }
            else
            {
                Console.WriteLine("Could not detach the policy.");
            }
        }
    }
```

- API の詳細については、AWS SDK for .NET API リファレンス の「DetachPolicy」を参照してください。

CLI

AWS CLI

root、OU、またはアカウントからポリシーをデタッチするには

次のコード例は、OU からポリシーをデタッチする方法を示しています。

```
aws organizations  detach-policy  --target-id ou-examplerootid111-exampleouid111
 --policy-id p-examplepolicyid111
```

- API の詳細については、AWS CLI コマンドリファレンスの「DetachPolicy」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
def detach_policy(policy_id, target_id, orgs_client):
    """
    Detaches a policy from a target.

    :param policy_id: The ID of the policy to detach.
    :param target_id: The ID of the resource where the policy is currently
 attached.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.detach_policy(PolicyId=policy_id, TargetId=target_id)
```

```
        logger.info("Detached policy %s from target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't detach policy %s from target %s.", policy_id, target_id
        )
        raise
```

- API の詳細については、AWS SDK for Python (Boto3) API リファレンス の「DetachPolicy」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Organizations での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **ListAccounts**で を使用する

以下のコード例は、ListAccounts の使用方法を示しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Uses the AWS Organizations service to list the accounts associated
/// with the default account.
/// </summary>
public class ListAccounts
```

```
    {
        /// <summary>
        /// Creates the Organizations client and then calls its
        /// ListAccountsAsync method.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var request = new ListAccountsRequest
            {
                MaxResults = 5,
            };

            var response = new ListAccountsResponse();
            try
            {
                do
                {
                    response = await client.ListAccountsAsync(request);
                    response.Accounts.ForEach(a => DisplayAccounts(a));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (AWSOrganizationsNotInUseException ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about an Organizations account.
        /// </summary>
        /// <param name="account">An Organizations account for which to display
        /// information on the console.</param>
        private static void DisplayAccounts(Account account)
        {
            string accountInfo = $"{account.Id}
{account.Name}\t{account.Status}";
```

```
            Console.WriteLine(accountInfo);
        }
    }
```

- API の詳細については、AWS SDK for .NET API リファレンスの「ListAccounts」を参照してください。

CLI

AWS CLI

組織内のすべてのアカウントのリストを取得するには

次の例は、組織内のアカウントのリストをリクエストする方法を示しています。

```
aws organizations list-accounts
```

出力には、アカウントサマリーオブジェクトのリストが含まれます。

```
{
        "Accounts": [
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/111111111111",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481830215.45,
                        "Id": "111111111111",
                        "Name": "Master Account",
                        "Email": "bill@example.com",
                        "Status": "ACTIVE"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/222222222222",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835741.044,
                        "Id": "222222222222",
                        "Name": "Production Account",
                        "Email": "alice@example.com",
```

```
                        "Status": "ACTIVE"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/333333333333",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835795.536,
                        "Id": "333333333333",
                        "Name": "Development Account",
                        "Email": "juan@example.com",
                        "Status": "ACTIVE"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/444444444444",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835812.143,
                        "Id": "444444444444",
                        "Name": "Test Account",
                        "Email": "anika@example.com",
                        "Status": "ACTIVE"
                }
        ]
}
```

- API の詳細については、AWS CLI コマンドリファレンスの「ListAccounts」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Organizations での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **ListOrganizationalUnitsForParent**で を使用する

以下のコード例は、ListOrganizationalUnitsForParent の使用方法を示しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Lists the AWS Organizations organizational units that belong to an
/// organization.
/// </summary>
public class ListOrganizationalUnitsForParent
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// call the ListOrganizationalUnitsForParentAsync method to retrieve
    /// the list of organizational units.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var parentId = "r-0000";

        var request = new ListOrganizationalUnitsForParentRequest
        {
            ParentId = parentId,
            MaxResults = 5,
        };

        var response = new ListOrganizationalUnitsForParentResponse();
        try
        {
```

```
                do
                {
                    response = await
client.ListOrganizationalUnitsForParentAsync(request);
                    response.OrganizationalUnits.ForEach(u =>
DisplayOrganizationalUnit(u));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about an Organizations organizational unit.
        /// </summary>
        /// <param name="unit">The OrganizationalUnit for which to display
        /// information.</param>
        public static void DisplayOrganizationalUnit(OrganizationalUnit unit)
        {
            string accountInfo = $"{unit.Id} {unit.Name}\t{unit.Arn}";

            Console.WriteLine(accountInfo);
        }
    }
```

- API の詳細については、AWS SDK for .NET API リファレンスの「ListOrganizationalUnitsForParent」を参照してください。

CLI

AWS CLI

親 OU またはルートの OU のリストを取得するには

次の例は、指定されたルート内の OU のリストを取得する方法を示しています。

```
aws organizations list-organizational-units-for-parent --parent-id r-
examplerootid111
```

出力は、指定されたルートに 2 つの OU が含まれていることを示し、それぞれの詳細を示します。

```
{
        "OrganizationalUnits": [
                {
                        "Name": "AccountingDepartment",
                        "Arn": "arn:aws:organizations::o-exampleorgid:ou/r-
examplerootid111/ou-examplerootid111-exampleouid111"
                },
                {
                        "Name": "ProductionDepartment",
                        "Arn": "arn:aws:organizations::o-exampleorgid:ou/r-
examplerootid111/ou-examplerootid111-exampleouid222"
                }
        ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「ListOrganizationalUnitsForParent」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Organizations での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **ListPolicies**で を使用する

以下のコード例は、ListPolicies の使用方法を示しています。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to list the AWS Organizations policies associated with an
/// organization.
/// </summary>
public class ListPolicies
{
    /// <summary>
    /// Initializes an Organizations client object, and then calls its
    /// ListPoliciesAsync method.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        // The value for the Filter parameter is required and must must be
        // one of the following:
        //     AISERVICES_OPT_OUT_POLICY
        //     BACKUP_POLICY
        //     SERVICE_CONTROL_POLICY
        //     TAG_POLICY
        var request = new ListPoliciesRequest
        {
            Filter = "SERVICE_CONTROL_POLICY",
            MaxResults = 5,
        };
```

```
            var response = new ListPoliciesResponse();
            try
            {
                do
                {
                    response = await client.ListPoliciesAsync(request);
                    response.Policies.ForEach(p => DisplayPolicies(p));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (AWSOrganizationsNotInUseException ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about the Organizations policies associated
        /// with an organization.
        /// </summary>
        /// <param name="policy">An Organizations policy summary to display
        /// information on the console.</param>
        private static void DisplayPolicies(PolicySummary policy)
        {
            string policyInfo = $"{policy.Id}
{policy.Name}\t{policy.Description}";

            Console.WriteLine(policyInfo);
        }
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「ListPolicies」を参照してください。

CLI

AWS CLI

特定のタイプの組織のすべてのポリシーのリストを取得するには

次の例は、フィルターパラメータで指定された SCP のリストを取得する方法を示しています。

```
aws organizations list-policies --filter SERVICE_CONTROL_POLICY
```

出力には、ポリシーのリストと概要情報が含まれます。

```
{
        "Policies": [
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllS3Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid111",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid111",
                        "Description": "Enables account admins to delegate
 permissions for any S3 actions to users and roles in their accounts."
                },
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllEC2Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid222",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid222",
                        "Description": "Enables account admins to delegate
 permissions for any EC2 actions to users and roles in their accounts."
                },
                {
                        "AwsManaged": true,
                        "Description": "Allows access to every operation",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-FullAWSAccess",
                        "Arn": "arn:aws:organizations::aws:policy/
service_control_policy/p-FullAWSAccess",
                        "Name": "FullAWSAccess"
```

```
                }
        ]
}
```

- API の詳細については、「AWS CLI Command Reference」の「ListPolicies」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
def list_policies(policy_filter, orgs_client):
    """
    Lists the policies for the account, limited to the specified filter.

    :param policy_filter: The kind of policies to return.
    :param orgs_client: The Boto3 Organizations client.
    :return: The list of policies found.
    """
    try:
        response = orgs_client.list_policies(Filter=policy_filter)
        policies = response["Policies"]
        logger.info("Found %s %s policies.", len(policies), policy_filter)
    except ClientError:
        logger.exception("Couldn't get %s policies.", policy_filter)
        raise
    else:
        return policies
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「ListPolicies」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS Organizations での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

のドキュメント履歴 AWS Organizations

次の表は、 AWS Organizationsのドキュメントの主な更新をまとめたものです。

- API バージョン: 2016-11-28
- ドキュメントの最終更新日: 2025 年 6 月 17 日

変更	説明	日付
Security Hub ポリシーを追加	Security Hub ポリシーを使用して、 全体の Security Hub 設定を一元管理できます AWS Organizations。これらのポリシーは、機能を有効にし、組織内の複数のアカウントにわたって一貫したセキュリティコントロールを維持するのに役立ちます。	2025 年 6 月 17 日
AWSOrganizationsFullAccess マネージドポリシーを更新しました	組織内の任意のアカウントのアカウント名を表示するアクセス`account:GetAccount Information` を有効にするアクションと、組織内の任意のアカウント名を変更するアクセスを有効にする`account:PutAccount Name` アクションを追加しました。	2025 年 4 月 22 日
Organizations と の統合 AWS User Notifications	User Notifications と統合 AWS Organizations して、組織内のアカウント間で通知を一元的に設定および表示できます。	2025 年 1 月 24 日

Organizations と AWS Managed Services (AMS) セルフサービスレポート (SSR) の統合	AMS SSR を と統合 AWS Organizations して、集約セルフサービスレポート (SSR) を有効にできます。これは、Advanced および Accelerate のお客様が組織レベルで集計された既存のセルフサービスレポートをクロスアカウントで表示できるようにする AMS 機能です。	2025 年 1 月 21 日
宣言ポリシーを追加	宣言ポリシーを使用して、組織全体 AWS のサービス の大規模な特定の に必要な設定を一元的に宣言して適用できます。一度接続すると、サービスに新しい機能や API が追加されても、設定は常に維持されます。	2024 年 12 月 1 日
新しい AWS 管理ポリシー	declarative-policies-ec2.amazonaws.com サービスにリンクされたロールの機能を有効にするDeclarativePoliciesEC2Report ポリシーを追加しました。	2024 年 11 月 22 日
バックアップポリシーを更新	AWS Backup ポリシーはselections ポリシーキーを更新してconditions ポリシーキーを含め、スキーマに新しいresources ポリシーキーを追加しました。新しいスキーマを使用すると、バックアップポリシーのリソース選択がより柔軟になります。	2024 年 11 月 14 日

メンバーアカウントのルートアクセスを一元管理	一元化されたルートアクセスを使用して、 AWS Organizations のメンバーアカウント間で特権ルートユーザー認証情報を管理できるようになりました。を使用して AWS アカウント マネージドのルートユーザー認証情報を一元的に保護 AWS Organizations し、ルートユーザー認証情報の復旧と大規模なアクセスを削除して防止します。	2024 年 11 月 14 日
リソースコントロールポリシー (RCPsを追加	リソースコントロールポリシー (RCPs) を使用して、組織内のリソースに対して使用可能なアクセス許可の最大数を制御できます。	2024 年 11 月 13 日
チャットアプリケーションポリシーを追加	チャットアプリケーションポリシーを使用して、Slack や Microsoft Teams などのチャットアプリケーションから組織のアカウントへのアクセスを制御できます。	2024 年 9 月 26 日
シナリオ駆動型コンテンツの更新	AWS Organizations ドキュメントはガイド全体でよりシナリオ駆動型に更新され、読みやすさと検出性を向上させるためにコンテンツが再編成されました。これらの変更に関するフィードバックがある場合は、ページの下部にある [フィードバックを提供する] ボタンを使用します。	2024 年 9 月 4 日

すべての AI サービスからの新しいオプトアウトに関するトピック	サポートされているすべての AWS AI サービスをオプトアウトする方法に関するドキュメントを追加しました。	2024 年 8 月 16 日
Organizations が組織内で 10,000 アカウントをサポートするようになりました	組織内で最大 10,000 個のメンバーアカウントを管理できるようになりました。これは、以前の 5,000 アカウントの 2 倍になります。有効な要件とビジネスニーズがある場合は、Organizations またはその他の統合された AWS のサービスのサービス制限チェックなしで、10,000 アカウントクォータをリクエストして承認できます。	2024 年 8 月 14 日
新しいアカウント移行に関するトピック	ある組織から別の組織へアカウントを移行する方法に関するドキュメントを追加しました。	2024 年 8 月 1 日
バックアップポリシーを更新	AWS Backup ポリシーが Amazon Elastic Block Store (Amazon EBS) スナップショットアーカイブをサポートするようになりました。更新された例については、「Updating a backup policy」と「Backup policy syntax and examples」を参照してください。	2024 年 7 月 9 日

AWSOrganizationsReadOnlyAccess マネージドポリシーを更新	AWSOrganizationsReadOnlyAccess ポリシーに account:GetPrimaryEmail アクションを追加しました。これにより、組織内の任意のメンバーアカウントのルートユーザーの E メールアドレスを表示するアクセスが可能になり、組織内の任意のメンバーアカウントの有効なリージョンを表示するアクセスを有効にする account:GetRegionOptStatus アクションが追加されました。	2024 年 6 月 6 日
新しいルートユーザーの E メールアドレスの更新トピック	Organizations では、組織内のメンバーアカウントのルートユーザーの E メールアドレスを一元的に更新できるようになりました。	2024 年 6 月 6 日
ポリシーステートメントを更新	AWS Organizations マネージドポリシーステートメントに新しいSid要素を追加しました。	2024 年 2 月 6 日
新しい管理アカウントの閉鎖に関するトピック	管理アカウントを閉鎖する方法を説明する考慮事項と詳細なステップへのリンクを追加しました。	2024 年 2 月 1 日
ベストプラクティスの更新	IAM のベストプラクティスとの整合に役立つ新しい情報をベストプラクティスのセクションに追加しました。	2023 年 6 月 12 日

AWSOrganizationsFullAccess と AWSOrganizationsReadOnlyAccess マネージドポリシーを更新しました	両方の管理ポリシーが更新され、アカウントの連絡先への書き込みまたは読み取りアクセスが可能になりました。	2022 年 10 月 21 日
AWSOrganizationsFullAccess マネージドポリシーを更新しました	マネージドポリシーが更新されました。これにより、新しい組織に必要なサービスにリンクされたロールを作成するためのアクセス許可を追加することで、組織の作成ができるようになりました。	2022 年 8 月 24 日
Organizations が AWS Organizations コンソールからアカウント機能を閉じる	管理アカウントのプリンシパルは、 AWS Organizations コンソールからメンバーアカウントを閉鎖することができ、IAM ポリシーを使用して、メンバーアカウントが誤って閉鎖されないように保護できます。	2022 年 3 月 29 日
AWS Organizations コンソールで別の連絡先を更新するためのお知らせを更新しました	Organizations では、 AWS Organizations コンソールを使用して、組織内のアカウントの代替連絡先を更新できるようになりました。新しい機能と手順の「Account Management リファレンス」を追記しました。	2022 年 2 月 8 日

Organizations 管理ポリシーの更新 – 既存のポリシーへの更新	AWSOrganizationsFullAccess および AWSOrganizationsReadOnlyAccess 管理ポリシーを更新し、 AWS Organizations コンソールを介してアカウントの代替連絡先を更新または表示するために必要なアカウント API アクセス許可を付与しました。	2022 年 2 月 7 日
Amazon DevOps Guru との組織の統合	Amazon DevOpsGuru を と統合 AWS Organizations することで、すべての組織アカウントでアプリケーションのヘルスを包括的にモニタリングし、インサイトを得ることができます。	2022 年 1 月 3 日
Amazon Detective との組織の統合	Amazon Detective を と統合 AWS Organizations して、Detective 動作グラフがすべての組織アカウントのアクティビティを可視化できるようにします。	2021 年 12 月 16 日
Organizations と の統合で、マルチアカウントのマルチリージョンデータ集約がサポートされ AWS Config るようになりました。	代理管理者アカウントを使用し、組織のすべてのメンバーアカウントを対象に、リソース構成とコンプライアンスデータを集約できます。詳しくは、AWS Config デベロッパーガイドの Multi-account multi-region data aggregation を参照してください。	2021年6月16日

Organizations と の統合に委任管理者のサポートが追加され AWS Firewall Manager ました	組織内のメンバーアカウントを、組織全体の Firewall Manager 管理者として指定できるようになりました。これにより、組織の管理アカウントからアクセス許可をより適切に分離できます。	2021 年 4 月 30 日
組織のバックアップ ポリシーで継続的なバックアップがサポートされるようになりました	AWS Backup 継続的バックアップ機能は、組織のバックアップポリシーで使用できます。	2021 年 3 月 10 日
Organizations と AWS CloudFormation StackSets の統合に、委任された管理者のサポートが含まれるようになりました	今後は、組織内のメンバーアカウントに、組織全体の AWS CloudFormation StackSets 管理者を委任できます。これにより、組織の管理アカウントからアクセス許可をより適切に分離できます。	2021 年 2 月 18 日
すべての機能を有効にしつつアカウントの招待を継続する	AWS は、組織内のすべての機能を有効にするプロセスを更新しました。既存のアカウントが招待に応答するのを待っている間も、引き続き新しいアカウントを組織に参加するよう招待できるようになりました。	2021 年 2 月 3 日
AWS Organizations コンソールのバージョン 2.0 を導入	AWS は、 AWS コンソールの新しいバージョンを導入しました。すべてのドキュメントが更新され、タスクの実行に新しい方法が適用されます。	2021 年 1 月 21 日

Organizations が との統合をサポートするようになりました AWS Marketplace	を有効に AWS Marketplace して、組織内のすべてのアカウント間でソフトウェアライセンスをより簡単に共有できるようになりました。	2020 年 12 月 3 日
Organizations が Amazon S3 Lens との統合のサポートを開始	Amazon S3 Lens は、Organizations の信頼されたアクセスと代理管理者の両方をサポートしています。詳しくは、Amazon Simple Storage Service ユーザーガイドの「Amazon S3 Storage Lens」を参照してください。	2020 年 11 月 18 日
クロスアカウントバックアップコピー	バックアップポリシーを使用して組織内のリソースをバックアップする場合、バックアップのコピーを組織 AWS アカウント 内の他の に保存できるようになりました。	2020 年 11 月 18 日
AWS リージョン 中国の が Organizations の信頼されたサービス AWS Resource Access Manager として をサポートするようになりました	Organizations および 中国 AWS RAM で Organizations を使用する場合、信頼できるサービスとして Organizations と統合する AWS RAM 機能を使用できるようになりました。	2020 年 11 月 18 日
Organizations が との統合をサポートするようになりました AWS Security Hub	組織内のすべてのアカウントで Security Hub を有効にし、組織のメンバーアカウント 1 つを Security Hub の委任管理者アカウントとして指定できます。	2020 年 11 月 12 日

マスターアカウントの名称の変更	AWS Organizations は、「マスターアカウント」の名前を「管理アカウント」に変更しました。変更されたのは名称だけです。機能に変更はありません。	2020 年 10 月 20 日
ベストプラクティスに関する新しいセクションとトピック	AWS Organizationsに関するベストプラクティスの新しいセクションを追加しました。この新しいセクションには、管理アカウント、メンバーアカウントのルートユーザー、パスワード管理のベストプラクティスについて説明するトピックが含まれています。	2020 年 10 月 6 日
ベストプラクティスのセクションを新設し、最初の 2 ページを追加	AWS Organizationsに関するベストプラクティスを説明するトピックの新しいセクションができました。今回の追加には、組織の管理アカウントのベストプラクティスのトピックと、メンバーアカウントのベストプラクティスのトピックが含まれています。	2020 年 10 月 2 日

組織のバックアップポリシーは、VSS (ボリュームシャドウコピーサービス) を使用して、Windows EC2 インスタンスでのアプリケーションコンシステントバックアップをサポートするようになりました	バックアップポリシーのサポートに、「advanced_backup_settings 」セクションが新たに追加されます。この新しいセクションに最初に追加されるのは、ユーザーによる有効と無効の切り替えが可能な WindowsVSS と呼ばれる ec2 設定です。詳しくは、AWS Backup デベロッパーガイドの Creating a VSS-Enabled Windows Backup を参照してください。	2020 年 9 月 24 日
Organizations が作成時のタグ付けとタグベースのアクセスコントロールをサポート	Organizations リソースを作成するときにリソースにタグを追加できます。タグポリシーを使用して、Organizations リソースでのタグの使用を標準化できます。特定のタグのキーと値があるリソースだけにアクセスを制限する IAM ポリシーを使用できます。	2020 年 9 月 15 日
信頼されたサービス AWS Health として を追加	組織内のアカウント間で AWS Health イベントを集約できます。	2020 年 8 月 4 日
人工知能 (AI) サービスのオプトアウトポリシー	AI サービスオプトアウトポリシーを使用して、 AWS AI サービスが AI サービスや AWS テクノロジーの開発と継続的な改善のために、それらのサービスによって処理された顧客コンテンツ (AI コンテンツ) を保存して使用できるかどうかを制御できます。	2020 年 7 月 8 日

バックアップポリシーと との統合を追加 AWS Backup	バックアップポリシーを使用して、バックアップポリシーを作成し、組織内のすべてのアカウントに適用できます。	2020 年 6 月 24 日
IAM Access Analyzer の委任管理をサポート	組織内のアクセスアナライザーの管理アクセスを、指定したメンバーアカウントに委任できます。	2020 年 3 月 30 日
AWS CloudFormation StackSets との統合	サービス管理スタックセットを作成して、 AWS Organizationsによって管理されるアカウントにスタックインスタンスをデプロイできます。	2020 年 2 月 11 日
Compute Optimizer との統合	組織のアカウントで操作できるサービスとして Compute Optimizer が追加されました。	2020 年 2 月 4 日
タグポリシー	タグポリシーを使用すると、組織のアカウント内のリソース間でタグを標準化できます。	2019 年 11 月 26 日
Systems Manager との統合	Systems Manager Explorer では、組織内のすべての AWS アカウント でオペレーションデータを同期できます。	2019 年 11 月 26 日
aws:PrincipalOrgPaths	新しいグローバル条件キーは、リクエストを行う IAM ユーザー、IAM ロール、または AWS アカウント ルートユーザーの AWS Organizations パスをチェックします。	2019 年 11 月 20 日

AWS Config ルールとの統合	AWS Config API オペレーションを使用して、組織内のすべての AWS アカウント で AWS Config ルールを管理できます。	2019 年 7 月 8 日
信頼されたアクセスに対応した新しいサービス	組織のアカウントで操作できるサービスとして Service Quotas を追加しました。	2019 年 6 月 24 日
AWS Control Tower との統合	AWS Control Tower が、組織内のアカウントを操作できるサービスとして追加されました。	2019 年 6 月 24 日
との統合 AWS Identity and Access Management	IAM は、組織のエンティティ (組織のルート、OU、アカウント) に対してサービスの最終アクセスデータを提供します。このデータを使用して、AWS のサービス 必要な のみにアクセスを制限できます。	2019 年 6 月 20 日
アカウントへのタグ付け	組織内のアカウントへのタグ付けとタグ解除を行い、組織内のアカウントのタグを表示できます。	2019 年 6 月 6 日
リソース、条件、サービスコントロールポリシー (SCP) 内の NotAction 要素	リソース、条件および SPC 内の NotAction 要素を指定して、組織や組織単位 (OU) 内のアカウント間のアクセスを拒否できるようになりました。	2019 年 3 月 25 日
信頼されたアクセスに対応した新しいサービス	AWS License Manager と Service Catalog が、組織内のアカウントと連携できるサービスとして追加されました。	2018 年 12 月 21 日

信頼されたアクセスに対応した新しいサービス	AWS CloudTrail および は、組織内のアカウントと連携できるサービスとして AWS RAM 追加されました。	2018 年 12 月 4 日
信頼されたアクセスに対応した新しいサービス	AWS Directory Service は、組織内のアカウントと連携できるサービスとして追加されました。	2018 年 9 月 25 日
E メールアドレスの検証	組織に既存のアカウントを招待する前に、管理アカウントに関連付けられた E メールアカウントを所有していることを確認する必要があります。	2018 年 9 月 20 日
CreateAccount 通知	`CreateAccount` 通知は、管理アカウントの CloudTrail 口グに発行されます。	2018 年 6 月 28 日
信頼されたアクセスに対応した新しいサービス	AWS Artifact 組織内のアカウントを操作できるサービスとして が追加されました。	2018 年 6 月 20 日
信頼されたアクセスに対応した新しいサービス	AWS Config および は、組織内のアカウントと連携できるサービスとして AWS Firewall Manager 追加されました。	2018 年 4 月 18 日
信頼されたサービスへのアクセス	Select が組織内のアカウントで動作する AWS のサービス ように、アクセスを有効または無効にできるようになりました。IAM Identity Center は、最初にサポートされている信頼されたサービスです。	2018 年 3 月 29 日

アカウントの削除がセルフサービスになりました	これで、 に連絡 AWS Organizations することなく、内から作成されたアカウントを削除できるようになりました AWS サポート。	2017 年 12 月 19 日
新しいサービスのサポートを追加 AWS IAM Identity Center	AWS Organizations は AWS IAM Identity Center (IAM Identity Center) との統合をサポートするようになりました。	2017 年 12 月 7 日
AWS がすべての組織アカウントにサービスにリンクされたロールを追加しました	という名前のサービスにリンクされたロール`AWSServiceRoleForOrganizations` が組織内のすべてのアカウントに追加され、 AWS Organizations と他の の統合が可能になります AWS のサービス。	2017 年 10 月 11 日
作成したアカウントを削除できるようになりました	作成したアカウントを組織から削除するには、 AWS サポートまでお問い合わせください。	2017 年 6 月 15 日
サービスの起動	新しいサービスの起動に伴う AWS Organizations ドキュメントの初版。	2017 年 2 月 17 日

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