aws

ユーザーガイド

AWS IAM アイデンティティセンター



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS IAM アイデンティティセンター: ユーザーガイド

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

IAM Identity Center とは何ですか? 1
IAM アイデンティティセンターを使用するメリット 1
IAM Identity Center の名称変更 3
レガシー名前空間は変わりません。 3
開始方法 4
IAM アイデンティティセンターに関する前提条件と考慮事項 6
AWS リージョンの選択 7
IAM アイデンティティセンターをアプリケーションのみに使用する 14
IAM アイデンティティセンターによって作成される IAM ロール 15
IAM アイデンティティセンターおよび AWS Organizations 16
IAM アイデンティティセンターのインスタンス 17
AWS アカウントIAM アイデンティティセンターを有効にできる タイプ 17
IAM アイデンティティセンターの組織インスタンス 19
IAM アイデンティティセンターのアカウントインスタンス 22
IAM アイデンティティセンターインスタンスを削除する 27
IAM Identity Center を有効にする 29
IAM アイデンティティセンターのインスタンスを有効にするには 30
ID ソースを確認する 34
ファイアウォールとゲートウェイを更新する 36
ドメインと URL エンドポイントの許可リストに関する考慮事項 39
ID ソースのチュートリアル 40
Active Directory 41
CyberArk 43
前提条件 44
SCIM に関する注意事項 44
ステップ 1: IAM Identity Center でプロビジョニングを有効にする 45
ステップ 2: CyberArk でプロビジョニングを設定する 46
(オプション) ステップ 3: IAM Identity Center でのアクセスコントロール (ABAC) のために CyberArk でユーザー属性を設定する 47
(オプション) アクセスコントロールの属性を渡す 48
Google Workspace 48
考慮事項 50
ステップ 1: Google Workspace: SAML アプリケーションを設定する 50

ステップ 2: IAM アイデンティティセンターおよび Google Workspace : IAM アイデンティティセンターの ID ソースを変更し、Google Workspace を SAML ID プロバイダーとして設定する ... 51
ステップ 3: Google Workspace: アプリを有効にする ... 53
ステップ 4: IAM Identity Center: IAM アイデンティティセンターの自動プロビジョニングを設定する ... 53
ステップ 5: Google Workspace: 自動プロビジョニングを設定する ... 54
アクセスコントロールの属性を渡す - オプション ... 56
AWS アカウントにアクセスを割り当てる ... 56
次のステップ ... 59
トラブルシューティング ... 60
JumpCloud ... 60
前提条件 ... 61
SCIM に関する注意事項 ... 62
ステップ 1: IAM Identity Center でプロビジョニングを有効にする ... 62
ステップ 2: JumpCloud でプロビジョニングを設定する ... 63
(オプション) ステップ 3: IAM Identity Center でのアクセスコントロールのために JumpCloud でユーザー属性を設定する ... 64
(オプション) アクセスコントロールの属性を渡す ... 65
Microsoft Entra ID ... 65
前提条件 ... 66
考慮事項 ... 66
ステップ 1: Microsoft テナントを準備する ... 68
ステップ 2: AWS アカウントを準備する ... 70
ステップ 3: SAML 接続を設定してテストする ... 73
ステップ 4: SCIM 同期を設定してテストする ... 77
ステップ 5: ABAC を設定する - オプション ... 81
AWS アカウントにアクセスを割り当てる ... 83
追加リージョンにアクセスするための Microsoft Entra ID の設定 ... 85
トラブルシューティング ... 85
Okta ... 88
考慮事項 ... 90
ステップ 1: Okta: Okta アカウントから SAML メタデータを取得する ... 90
ステップ 2: IAM Identity Center: Okta を IAM アイデンティティセンターの ID ソースとして設定する ... 91

ステップ 3: IAM アイデンティティセンターと Okta: Okta ユーザーをプロビジョニングする 93
ステップ 4: Okta: Okta から IAM アイデンティティセンターとユーザーを同期する 94
アクセスコントロールの属性を渡す - オプション 96
AWS アカウントにアクセスを割り当てる 97
追加リージョンにアクセスするための Okta の設定 99
次のステップ 100
トラブルシューティング 100
OneLogin 102
前提条件 103
ステップ 1: IAM Identity Center でプロビジョニングを有効にする 104
ステップ 2: OneLogin でプロビジョニングを設定する 105
(オプション) ステップ 3: IAM Identity Center でのアクセスコントロールのために OneLogin でユーザー属性を設定する 106
(オプション) アクセスコントロールの属性を渡す 107
トラブルシューティング 107
Ping Identity 108
PingFederate 108
PingOne 116
Identity Center ディレクトリ 122
ビデオチュートリアル 129
ワークフォースのセットアップ 130
ユーザー、グループ、プロビジョニング 130
ユーザー名と E メールアドレスの一意性 130
グループ 131
ユーザーおよびグループのプロビジョニング 131
ユーザーおよびグループのプロビジョニング解除 131
ID ソースを管理する 132
ID ソースの変更に関する注意事項 133
アイデンティティソースを変更する 138
IAM アイデンティティセンターのユーザー属性とグループ属性 140
外部 ID プロバイダー 141
Microsoft AD ディレクトリ 161
アイデンティティセンターディレクトリでユーザーを管理する 181
IAM Identity Center にいるユーザーのプロビジョニング 182
ID ソースの変更 182

ユーザーの追加 182
グループの追加 185
グループにユーザーを追加 186
グループの削除 187
ユーザーの削除 189
グループからユーザーを削除する 190
ユーザーのプロパティの編集 191
ワークフォースアクセス 193
認証セッションの理解 193
認証セッションのタイプ 194
エンドユーザーセッションの方法 196
セッションを終了するとユーザーアクセスがどうなるか 196
シングルログアウト 200
セッション管理のベストプラクティス 201
セッション期間を設定する 201
ユーザーインタラクティブセッション 201
ユーザーバックグラウンドセッション 202
Kiro の延長セッション 204
ワークフォースユーザーのアクティブなセッションを終了する 205
ID ソース、AWS CLI、および AWS SDK に関する考慮事項 207
ユーザーアクセスを無効にする 210
ユーザーアクセスを拒否する 211
IAM アイデンティティセンターユーザーのアクセス権を管理する 213
パスワード管理 213
MFA 213
ユーザーパスワードの設定 214
多要素認証 217
アプリケーションアクセス 231
AWS マネージドアプリケーション 232
アプリケーションへのアクセスの制御 232
ID 情報の共有 233
AWS マネージドアプリケーションの使用の制限 234
IAM アイデンティティセンターで使用できるアプリケーション 235
AWS マネージドアプリケーションをテストするための IAM アイデンティティセンターのセットアップ 240
アプリケーションの詳細の表示と変更 246

AWS マネージドアプリケーションの無効化 247
ID 拡張コンソールセッションの有効化 248
カスタマーマネージドアプリケーション 251
SAML 2.0 および OAuth 2.0 アプリケーション 252
SAML 2.0 アプリケーションのセットアップ 257
アカウントアクセスを有効にする 261
信頼できる ID の伝播 265
信頼できる ID の伝播の利点 265
信頼できる ID の伝播の有効化 265
信頼できる ID の伝播の仕組み 266
前提条件と考慮事項 267
ユースケース 269
認可サービス 295
独自の OAuth 2.0 アプリケーションを設定するには 305
カスタマー管理アプリケーションの設定 306
信頼されたアプリケーションを指定する 310
信頼できるトークン発行者 311
証明書をローテーションする 326
証明書をローテーションする前の注意事項 327
IAM Identity Center 証明書の交代 327
証明書の有効期限切れステータスインジケーター 330
アプリケーションプロパティを理解する 330
アプリケーション開始 URL 330
リレーステート 331
セッション期間 332
アプリケーションへのユーザーアクセスを割り当てる 333
アプリケーションへのユーザーアクセスを削除する 334
マップ属性 334
AWS アカウント アクセス 336
AWS アカウント タイプ 338
AWS アカウント アクセスの割り当て 340
エンドユーザーエクスペリエンス 340
アクセスの強制と制限 341
アクセス権の委任と強制 341
メンバーアカウントからのアイデンティティストアへのアクセスを制限する 342
委任された管理 343

ベストプラクティス 343
前提条件 348
メンバーアカウントを作成する 349
メンバーアカウントを登録解除する 350
委任管理者アカウントを確認する 351
一時的な昇格アクセス 351
AWS アカウント へのシングルサインオン・ アクセス 352
AWS アカウント にユーザーまたはグループアクセスを割り当てる 353
AWS アカウントへのユーザーおよびグループのアクセスを削除する 356
ユーザーアクセス権の取り消し 357
シングルサインオンアクセスを割り当てる権限を委任する 359
権限セット 360
最小特権権のアクセス許可を適用するアクセス許可セットを作成する 361
事前定義済み権限 363
カスタム権限 364
アクセス許可セットの作成、管理と削除 367
アクセス権限セットのプロパティを構成する 380
権限セットを参照する 386
アクセスが中断されないようにするための推奨事項 388
カスタム信頼ポリシーの例 389
属性ベースのアクセス制御 390
利点 391
チェックリスト: IAM Identity Center を使用して AWS で ABAC を設定する 392
アクセスコントロールの属性 394
サービスリンクロール 402
AWS アクセスポータル 403
AWS アクセスポータルの開始方法 403
AWS アクセスポータルを設定する 404
設定できる内容 404
AWS アクセスポータルの有効化 404
AWS アクセスポータル URL のカスタマイズ 405
ユーザーが AWS アクセスポータルにサインインできることを確認する 406
AWS アクセスポータルを使用する 407
AWS アクセスポータルの使用方法 408
AWS アクセスポータルにサインインします。 408
ユーザーパスワードのリセット 411

AWS CLI と AWS SDK アクセス ... 412
ショートカットリンクの作成 ... 418
MFA 用デバイスの登録 ... 420
アクティブなセッションの終了 ... 423
複数の 間で IAM アイデンティティセンターを使用するAWS リージョン ... 425
マルチリージョンサポートの利点 ... 425
前提条件と考慮事項 ... 425
追加のリージョンの選択 ... 426
IAM Identity Center を追加のリージョンにレプリケートする ... 427
ステップ 1: レプリカキーを作成する ... 427
手順 2: リージョンを追加する ... 428
手順 3 (外部 ID プロバイダーのみ): 外部 IdP 設定を更新する ... 429
手順 4: ファイアウォールとゲートウェイの許可リストを確認する ... 430
ステップ 5: ユーザーに情報を提供する ... 430
最初のリージョンの追加後のリージョン変更 ... 430
レプリケーション対象のデータ ... 430
追加のリージョンを介したワークフォースアクセス ... 432
複数の AWS リージョンにまたがるユーザーセッション ... 432
プライマリおよび追加の AWS リージョンの AWS アクセスポータルエンドポイント ... 433
プライマリおよび追加の AWS リージョンの ACS エンドポイント ... 434
複数の ACS URL なしで AWS マネージドアプリケーションを使用する ... 436
AWS アカウントアクセスのための追加リージョンへのフェイルオーバー ... 437
複数の ACS URL を使用しない AWS アカウントアクセス回復性 ... 438
複数の AWS リージョンにまたがるアプリケーションのデプロイと管理 ... 439
複数の AWS リージョンにまたがる AWS マネージドアプリケーションのデプロイと管理 . 439
複数の AWS リージョンにまたがるカスタマーマネージドアプリケーションのデプロイと管理 ... 441
IAM Identity Center からリージョンを削除する ... 441
手順 1: 外部 IdP 設定を更新する (該当する場合) ... 441
手順 2: リージョンを削除する ... 441
手順 3: レプリカキーを削除する ... 443
追加の AWS リージョンでサポートされているサービス API ... 443
プライマリリージョンと追加のリージョンの CloudTrail イベント ... 444
プライマリリージョンと追加のリージョンでの IAM Identity Center のユースケース ... 444
復元力設計とリージョンごとの動作 ... 448
可用性を考慮した設計 ... 449

AWS マネジメントコンソール への緊急アクセスを設定する 449
緊急アクセス設定の概要 450
重要な運用上の役割を設計する方法 451
アクセスモデルを計画する方法 452
緊急時のロール、アカウント、グループのマッピングを設計する方法 453
緊急アクセス設定の作成方法 453
緊急事態に備えたタスク 455
緊急フェイルオーバープロセス 455
通常の運用に戻る 456
Okta でダイレクト IAM フェデレーションアプリケーションの 1 回限りの設定を行う 456
ADFS でダイレクト IAM フェデレーションアプリケーションの 1 回限りの設定を行う 459
セキュリティ 466
IAM Identity Center の ID とアクセス管理 467
認証 467
アクセスコントロール 467
アクセス管理の概要 468
アイデンティティベースのポリシーの例 472
リソースベースのポリシーの例 480
AWS マネージドポリシー 483
サービスリンクロールの使用 504
IAM Identity Center コンソールと API 認可 512
2023 年 11 月以降の API アクション 512
2020 年 10 月以降の API アクション 514
AWS STSIAM アイデンティティセンターの 条件キー 515
UserId 517
IdentityStoreArn 517
ApplicationArn 517
CredentialId 518
InstanceArn 518
ログ記録とモニタリング 518
AWS CloudTrail を使用した IAM Identity Center API コールのログ記録 519
AWS CloudTrail を使用した IAM アイデンティティセンター SCIM のログ記録 559
Amazon EventBridge 566
設定可能な AD 同期エラーのログ記録 566
コンプライアンス検証 569
サポートされるコンプライアンス標準 570

レジリエンス 571
インフラストラクチャセキュリティ 572
データ保護 573
転送中の暗号化 573
データプライバシー 574
データ保持 574
保管中の暗号化 574
IAM アイデンティティセンターの暗号化コンテキスト 576
暗号化コンテキストを使用して顧客マネージドキーへのアクセスを制御する 576
IAM アイデンティティセンターの暗号化キーのモニタリング 577
AWS マネージドアプリケーションの IAM アイデンティティセンター ID 属性のストレージ、暗号化、削除 577
カスタマーマネージド KMS キーの実装 578
ベースライン KMS キーポリシー 588
高度な KMS キーポリシーステートメント 593
リソースのタグ付け 602
タグの制限 603
コンソールでタグを管理する 603
AWS CLI の例 604
タグの割り当て 604
タグの表示 605
タグの削除 605
権限セット作成時のタグの適用 605
API アクション 606
AWS CLI と IAM Identity Center の統合 607
AWS CLI と IAM Identity Center の統合方法 607
プライベートアクセスに関する注意事項 608
クォータ 609
アプリケーションクォータ 609
AWS アカウント のクォータ 610
Active Directory のクォータ 611
IAM Identity Center Identity Store クォータ 611
IAM Identity Center のスロットル制限 611
OIDC サービスリクエストのクォータ 612
追加のクォータ 614
トラブルシューティング 616

IAM アイデンティティセンターのアカウントインスタンスの作成に関する問題 616
IAM アイデンティティセンターと連携するように事前設定されているクラウドアプリケーションのリストを表示しようとすると、エラーが表示されます。 616
IAM Identity Center によって作成された SAML アサーションの内容に関する問題 618
特定のユーザーが、外部の SCIM プロバイダーからの IAM Identity Center に同期できません . 618
外部 ID プロバイダーを使用してユーザーまたはグループをプロビジョニングする際の重複ユーザーまたはグループのエラー 620
ユーザー名が UPN 形式の場合、ユーザーはサインインできません 621
IAM ロールを変更すると、「Cannot perform the operation on the protected role」(保護されたロールでオペレーションを実行できません) というエラーが発生する 621
ディレクトリユーザーが、パスワードをリセットできません 622
ユーザーはアクセス権限セットを参照しているが、割り当てられたアカウントやアプリケーションにアクセスできません 622
アプリケーションカタログからアプリケーションを正しく設定できない 623
ユーザーが外部の ID プロバイダーを使用してサインインしようとすると、「予期しないエラーが発生しました」というエラーが発生します 623
エラー「アクセスコントロールのための属性の有効化に失敗しました」 625
MFA にデバイスを登録しようとすると、「Browser not supported」(サポートされていないブラウザ) というメッセージが表示されます。 625
アクティブディレクトリの「ドメインユーザー」グループが IAM Identity Center に正しく同期しない 625
無効な MFA 認証情報エラー 625
認証アプリケーションを使って登録やサインインをしようとすると、「予期しないエラーが発生しました」というメッセージが表示されます 626
IAM アイデンティティセンターへのサインインを試行すると、「ご迷惑をおかけしています」と表示されます 626
ユーザーが IAM Identity Center からのメールを受信できません 627
エラー: 管理アカウントにプロビジョニングされたアクセス権限セットを削除/変更/削除/割り当てることはできません 627
エラー: セッショントークンが見つからない、または無効です 627
信頼できるドメインのグループメンバーが IAM Identity Center と同期しない 627
AWS IAM アイデンティティセンター でのカスタマーマネージドキーのトラブルシューティング 628
アクセス拒否: KMS 復号アクセス許可の問題 628
IAM Identity Center でカスタマーマネージドキーを有効にした AWS マネージドアプリケーションのログインに失敗する 629

IAM Identity Center でカスタマーマネージドキーを有効にした AWS マネージドアプリケーションのインストールおよび/またはユーザー割り当てが失敗する 629
KMS アクセス許可の問題: AWS IAM アイデンティティセンター でカスタマーマネージドキーを設定する 629
IAM Identity Center でカスタマーマネージドキーを有効にした場合に、AWS アクセスポータルのログインに失敗する 630
AWS IAM アイデンティティセンター でのマルチリージョンセットアップをトラブルシューティングする 630
IAM Identity Center インスタンスのレプリケート先にしたいリージョンが、IAM Identity Center コンソールで使用できない 630
追加リージョンで AWS マネージドアプリケーションのサインインに失敗する 631
IAM Identity Center のマルチリージョンインスタンスを有効にする際の問題 631
キーの作成に失敗する 631
キーのレプリケーションに失敗する 631
インスタンスの作成に失敗する 632
ドキュメント履歴 633
AWS 用語集 646

IAM Identity Center とは何ですか?

AWS IAM アイデンティティセンター は、ワークフォースユーザーを Kiro や Amazon Quick などの AWS マネージドアプリケーションやその他の AWS リソースに接続するための AWS ソリューションです。既存の ID プロバイダーを接続してお手持ちのディレクトリとの間でユーザーやグループを同期したり、あるいは IAM アイデンティティセンター内でユーザーを直接作成して管理することができます。これにより、IAM アイデンティティセンターを次のいずれかまたは両方に使用できます。

- アプリケーションへのユーザーアクセス
- AWS アカウントへのユーザーアクセス

へのアクセスに IAM を既に使用していますか?AWS アカウント

IAM アイデンティティセンターを使用して AWS マネージドアプリケーションにアクセスするのに現在の AWS アカウントワークフローを変更する必要はありません。AWS アカウント へのアクセスに IAM とのフェデレーションを使用している場合、各ユーザーはこれまでと同じ方法で AWS アカウント にアクセスし、既存のワークフローを使用してアクセスを管理することができます。

IAM アイデンティティセンターを使用するメリット

IAM アイデンティティセンターは、主に以下の機能を通じて、ワークフォースユーザーによるアプリケーションまたは AWS アカウント、またはその両方へのアクセスを合理化しシンプルにします。

AWS 管理アプリケーションとの 統合

Kiro や Amazon Redshift などの AWS マネージドアプリケーションは、IAM Identity Center と統合されます。IAM アイデンティティセンターは、ユーザーやグループの共通ビューを AWS マネージドアプリケーションに提供します。

アプリケーション間での信頼できる ID の伝播

信頼できる ID の伝播により、Amazon Quick などの AWS マネージドアプリケーションは、ユーザー ID を Amazon Redshift などの他の AWS マネージドアプリケーションと安全に共有し、ユーザー ID に基づいて AWS リソースへのアクセスを許可することができます。CloudTrail イベントはユーザーとユーザーが開始したアクションに基づいてログ記録されるため、ユーザーアクティビティをより簡単に監査できます。これにより、誰が何にアクセスしたかを一目で把握でき

ます。エンドツーエンドの構成ガイダンスなど、サポートされているユースケースについては、「信頼できる ID の伝播のユースケース」を参照してください。

1 つのフェデレーションポイントで へのユーザーアクセスを簡素化するAWS

単一のフェデレーションポイントを提供することで、IAM アイデンティティセンターは 複数の AWS マネージドアプリケーションや AWS アカウントの使用に必要な管理作業の量を減らします。例えば SAML 2.0 ID プロバイダーを使用する場合、IAM アイデンティティセンターでは必要なフェデレーションは 1 回のみで、管理する証明書は 1 つだけです。IAM アイデンティティセンターは、信頼できる ID の伝播のユースケースや、ユーザーが他のユーザーと AWS リソースへのアクセスを共有する場合に、AWS マネージドアプリケーションにユーザーおよびグループの共通のビューを提供します。

一般的な ID プロバイダーを IAM アイデンティティセンターと連携するための設定方法については、「IAM アイデンティティセンターの ID ソースに関するチュートリアル」を参照してください。すでに使用している ID プロバイダーがない場合は、IAM アイデンティティセンターでユーザーを直接作成および管理できます。

ワークフォースから複数の AWS アカウント へのアクセスを管理する機能

IAM Identity Center では、ワークフォースから AWS アカウント へのアクセスを一元管理するオプションが提供されています。

- チームは、AWS アカウント に IAM ロールを作成し、IAM アカウントアクセスマネージャー機能を使用して IAM Identity Center ユーザーとグループへのロール割り当てを一元管理できます。詳細については、「IAM ユーザーガイド」の「アカウントアクセスマネージャーを使用する理由」を参照してください。
- また、IAM Identity Center のアクセス許可セットを使用すると、admin などの一般的なジョブ機能に対するアクセス許可を一元的に作成し、AWS アカウント 全体にプロビジョニングして、ユーザーとグループに割り当てることもできます。このオプション機能は、IAM アイデンティティセンターの組織インスタンスでのみ使用できます。

2 つのインスタンスタイプ

IAM アイデンティティセンターは、組織インスタンスとアカウントインスタンスの 2 種類のインスタンスをサポートします。組織インスタンスはベストプラクティスです。AWS アカウント へのアクセスを管理できる唯一のインスタンスであり、アプリケーションを本番環境で使用するすべての場合に推奨されます。組織インスタンスは AWS Organizations 管理アカウントにデプロイされ、AWS 全体のユーザーアクセスを一元的に管理できます。

アカウントインスタンスは、有効化されている AWS アカウント へバインドされます。IAM アイデンティティセンターのアカウントインスタンスは、特定の AWS マネージドアプリケーション

の個別のデプロイをサポートする場合にのみ使用してください。詳細については、「IAM アイデンティティセンターの組織インスタンスとアカウントインスタンス」を参照してください。

ユーザー向けの使いやすい Web ポータルアクセス

AWS アクセスポータルは、ユーザーに割り当てられたすべてのアプリケーション、AWS アカウント、またはその両方へのシームレスなアクセスを提供する、使いやすい Web ポータルです。

AWS アカウント およびアプリケーションへのマルチリージョンアクセス

IAM Identity Center インスタンスを追加リージョンにレプリケートすると、ワークフォースは有効なすべてのリージョンを介して割り当てられた AWS アカウント およびアプリケーションにアクセスでき、有効な各リージョンに AWS マネージドアプリケーションをデプロイできます。

IAM Identity Center の名称変更

2022 年 7 月 26 日、AWSシングルサインオン は AWS IAM アイデンティティセンター に名称が変更されました。

レガシー名前空間は変わりません。

`sso` および `identitystore` API 名前空間、および以下の関連名前空間は、下位互換性を保つため変更されていません。

- CLI コマンド
  - `aws configure sso`
  - `identitystore`
  - `sso`
  - `sso-admin`
  - `sso-oidc`
- `AWSSSO` と `AWSIdentitySync` プレフィックスを含む管理ポリシー
- `sso` と `identitystore` を含むサービスエンドポイント
- `AWS::SSO` プレフィックスを含む CloudFormation リソース
- `AWSServiceRoleForSSO` を含むサービスにリンクされたロール
- `sso` と `singlesignon` を含むコンソール URL
- `singlesignon` を含むドキュメンテーション URL

IAM アイデンティティセンターを使用した開始方法

以下は、IAM アイデンティティセンターの使用を開始する方法の概要です。

1. IAM アイデンティティセンターを有効にします。

   IAM アイデンティティセンターを有効にするときは、2 種類の IAM アイデンティティセンターインスタンスから選択します。これらのタイプは、組織インスタンス (推奨) とアカウントインスタンスです。これらのインスタンスタイプのさまざまな機能の詳細については、「IAM アイデンティティセンターの組織インスタンスとアカウントインスタンス」を参照してください。

   > **Note**
   >
   > IAM アイデンティティセンターを有効にすると、次のいずれかを実行してサインインし、IAM アイデンティティセンターコンソールを開くことができます。
   >
   > - 組織インスタンス - 管理アカウントの管理権限を持つ認証情報を使用して AWS にサインインします。
   > - アカウントインスタンス - IAM アイデンティティセンターが有効になっている AWS アカウント で、管理者権限を持つ認証情報を使用して AWS にサインインします。

2. ID ソースを IAM アイデンティティセンターに接続するには

   IAM アイデンティティセンターコンソールで、使用する ID ソースを確認します。ID ソースについては、以下を参照してください。

   - 外部 ID プロバイダー - ワークフォースユーザーを管理する既存の ID プロバイダーがある場合は、IAM アイデンティティセンターに接続できます。一般的な ID プロバイダーを IAM アイデンティティセンターと連携するための設定方法の詳細については、「IAM アイデンティティセンターの ID ソースに関するチュートリアル」を参照してください。
   - Active Directory - Active Directory を使用してワークフォースユーザーを管理している場合は、IAM アイデンティティセンターに接続できます。詳細については、「Active Directory を ID ソースとして使用する」を参照してください。
   - IAM アイデンティティセンター - または、IAM アイデンティティセンターでユーザーとグループを直接作成および管理できます。

> **Note**
>
> マルチリージョンセットアップを利用するには、IAM Identity Center の ID ソースとして、外部 ID プロバイダーまたはアイデンティティセンターディレクトリを使用する必要があります。マルチリージョンのサポートは Active Directory では使用できません。詳細については、「複数の 間で IAM アイデンティティセンターを使用するAWS リージョン」を参照してください。

3. AWS アカウント へのユーザーアクセスを設定する (組織インスタンスのみ)

   IAM アイデンティティセンターの組織インスタンスを使用している場合は、アクセス許可セットを使用して AWS アカウント および リソースへのアクセス権をユーザーに付与し、AWS アカウント への ユーザーまたはグループアクセスに割り当てることができます。

4. アプリケーションへの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を使用すると、次の 2 種類のアプリケーションへのアクセス権をユーザーに付与できます。

   a. AWS マネージドアプリケーション

   - IAM アイデンティティセンターは、Amazon Q Business、AWS CLI、Amazon Redshift などの AWS マネージドアプリケーションで使用できます。詳細については、「AWS マネージドアプリケーション」および「AWS CLI と IAM Identity Center の統合」を参照してください。

   b. カスタマーマネージドアプリケーション

   - 次のいずれかのタイプのカスタマーマネージドアプリケーションを IAM アイデンティティセンターと統合できます。
     - IAM アイデンティティセンターにリストされているアプリケーション
     - カスタムアプリケーション
   - アプリケーションを設定したら、ユーザーにアプリケーションへのアクセスを割り当てることができます。

5. AWS アクセスポータルのサインイン手順をユーザーに提供する

   AWS アクセスポータルは、ユーザーに割り当てられたすべてのアプリケーション、AWS アカウント、またはその両方へのシームレスなアクセスを提供する Web ポータルです。IAM アイデンティティセンターの新しいユーザーは、AWS アクセスポータルにサインインする前にユーザー認証情報をアクティベートする必要があります。

AWS アクセスポータルについてサインイン方法については、「AWS サインイン ユーザーガイド」の「AWS アクセスポータルへのサインイン」を参照してください。AWS アクセスポータルのサインインプロセスの詳細については、「AWS アクセスポータルへのサインイン」を参照してください。

IAM アイデンティティセンターに関する前提条件と考慮事項

IAM アイデンティティセンターでは、AWS マネージドアプリケーションのみ、AWS アカウント のみ、またはその両方へのアクセスを管理できます。IAM フェデレーションを使用して AWS アカウント へのアクセスを管理している場合は、アプリケーションアクセスに IAM アイデンティティセンターを使用している間も引き続きアクセスできます。

IAM アイデンティティセンターを有効にする前に次の点を考慮します。

- AWS リージョン

  IAM Identity Center のインスタンスごとに、サポートされている単一のリージョンで IAM Identity Center をまず有効にします。AWS アカウントへのシングルサインオンアクセスに IAM アイデンティティセンターを使用する場合は、組織内のすべてのユーザーがリージョンにアクセスできる必要があります。アプリケーションアクセスに IAM アイデンティティセンターを使用する場合は、Amazon SageMaker AI などの一部の AWS マネージドアプリケーションは、サポートするリージョンでのみ動作できることに注意してください。また、ほとんどの AWS マネージドアプリケーションでは、そのアプリケーションと同じリージョンで IAM Identity Center を使用できるようにする必要があります。これを実現するためには、同じリージョンにそれらを共存させるか、サポートされている場合には IAM Identity Center インスタンスを AWS マネージドアプリケーションの目的のデプロイリージョンにレプリケートします。詳細については、「AWS リージョンを選択するための考慮事項」を参照してください。
- アプリケーションアクセスのみ

  IAM Identity Center は、既存の ID プロバイダーを使用して、Kiro などのアプリケーションへのユーザーアクセスにのみ使用できます。詳細については、「アプリケーションへのユーザーアクセスのみに IAM アイデンティティセンターを使用する」を参照してください。

> **Note**
>
> アプリケーションリソースへのアクセスは、アプリケーション所有者によって個別に管理されます。

- IAM ロールのクォータ

  IAM アイデンティティセンターは、IAM ロールを作成して、ユーザーにアカウントリソースへのアクセス許可を付与します。詳細については、「IAM アイデンティティセンターによって作成される IAM ロール」を参照してください。

- IAM アイデンティティセンターおよび AWS Organizations

  AWS Organizations は IAM アイデンティティセンターと併用することをお勧めしますが、必須ではありません。組織をまだ設定していない場合は、設定する必要はありません。すでに AWS Organizations をセットアップしていて、IAM アイデンティティセンターを組織に追加する場合は、すべての AWS Organizations 機能が有効になっていることを確認してください。詳細については、「IAM アイデンティティセンターおよび AWS Organizations」を参照してください。

アクセスポータルや IAM Identity Center コンソールなど、IAM Identity Center ウェブインターフェイスは、サポート対象のウェブブラウザから人間がアクセスすることを目的としています。互換性のあるブラウザには、Microsoft Edge、Mozilla Firefox、Google Chrome、Apple Safari の最新の 3 つのバージョンが含まれます。これらのエンドポイントにブラウザベース以外のパスを使用してアクセスすることはサポートされていません。IAM Identity Center サービスにプログラムでアクセスする場合は、IAM Identity Center および Identity Store API のリファレンスガイドに文書化された API を使用することをお勧めします。

AWS リージョンを選択するための考慮事項

IAM アイデンティティセンターは、選択した 1 つのサポートされている AWS リージョン で有効にでき、世界中のユーザーが利用できます。全世界で利用可能なため、複数の AWS アカウントやアプリケーションへのユーザーアクセスを簡単に設定することができます。以下は、AWS リージョン を選択する際の主な考慮事項です。

- ユーザーの地理的位置 – 対象となるエンドユーザーの大部分に地理的にもっとも近いリージョンを選択することで、AWS アクセスポータルや Amazon SageMaker AI などの AWS マネージドアプリケーションへのアクセスのレイテンシーを低くすることができます。

- オプトインリージョン (デフォルトで無効になっているリージョン) – オプトインリージョンは、デフォルトで無効になっている AWS リージョン です。オプトインリージョンで使用するには、それを有効にする必要があります。詳細については、「オプトインリージョンでの IAM アイデンティティセンターの管理」を参照してください。
- IAM Identity Center を追加リージョンにレプリケートする – IAM Identity Center を追加の AWS リージョンにレプリケートする場合は、デフォルトで有効になっているリージョンを選択する必要があります。詳細については、「複数の 間で IAM アイデンティティセンターを使用するAWS リージョン」を参照してください。
- AWS マネージドアプリケーションのデプロイリージョンの選択 – AWS マネージドアプリケーションは、利用可能な AWS リージョン でのみ動作できます。また、多くの AWS マネージドアプリケーションは、IAM Identity Center が有効化またはレプリケートされているリージョン (プライマリリージョンまたは追加リージョン) でのみ動作できます。IAM Identity Center インスタンスが追加リージョンへのレプリケーションをサポートしているかどうかを確認するには、「複数の 間で IAM アイデンティティセンターを使用するAWS リージョン」を参照してください。レプリケーションが選択肢にない場合は、AWS マネージドアプリケーションを使用する予定のリージョンで IAM Identity Center を有効にすることを検討してください。
- デジタル主権 – デジタル主権の法規制または組織ポリシーによっては、特定の AWS リージョンの使用が義務付けられる場合があります。組織の法務部に相談してください。
- ID ソース – AWS Managed Microsoft AD またはセルフマネージドディレクトリを ID ソースとして Active Directory (AD) で使用している場合、そのホームリージョンは、IAM アイデンティティセンターを有効にしている AWS リージョン と一致する必要があります。
- Amazon Simple Email Service を使用したクロスリージョン E メール – 一部のリージョンでは、IAM アイデンティティセンターが別のリージョンの Amazon Simple Email Service (Amazon SES) を呼び出して E メールを送信する場合があります。これらのクロスリージョン呼び出しでは、IAM アイデンティティセンターは特定のユーザー属性を他のリージョンに送信します。詳細については、「Amazon SES を使用したクロスリージョン E メール」を参照してください。
- AWS Control Tower – AWS Control Tower から IAM Identity Center の組織インスタンスを有効にする場合、インスタンスは AWS Control Tower ランディングゾーンと同じリージョンに作成されます。

トピック

- IAM アイデンティティセンターリージョンのデータストレージとオペレーション
- AWS リージョンの切り替え
- IAM アイデンティティセンターが有効になっている AWS リージョンを無効にする

IAM アイデンティティセンターリージョンのデータストレージとオペレーション

IAM アイデンティティセンターが AWS リージョン 全体でデータストレージとオペレーションを処理する方法について説明します。

IAM アイデンティティセンターがデータを保存する方法を理解する

IAM Identity Center を有効にすると、IAM Identity Center で設定したすべてのデータが、有効にしたリージョンに保存されます。このデータには、ディレクトリ構成、アクセス権限セット、アプリケーションインスタンス、AWS アカウント アプリケーションへのユーザー割り当てが含まれます。IAM Identity Center の ID ストアを使用している場合、IAM Identity Center で作成したすべてのユーザーとグループも同じリージョンに保存されます。IAM Identity Center インスタンスを追加リージョンにレプリケートすると、IAM Identity Center はそれらのリージョンにユーザー、グループ、アクセス許可セットとその割り当て、およびその他のメタデータと設定を自動的にレプリケートします。

Amazon SES を使用したクロスリージョン E メール

IAM アイデンティティセンターは、エンドユーザーがワンタイムパスワード (OTP) を第 2 認証要素として使用してサインインしようとすると、Amazon Simple Email Service (Amazon SES) を使用して E メールを送信します。これらの E メールは、ユーザーが初期パスワードの設定、E メールアドレスの検証、パスワードのリセットを依頼されたときなど、特定の ID および認証情報の管理イベントでも送信されます。Amazon SES は IAM Identity Center がサポートするAWS リージョンのサブセットで利用できます。

IAM Identity Center は、Amazon SES がAWS リージョンでローカルで利用可能な場合に Amazon SES ローカルエンドポイントを呼び出します。Amazon SES がローカルで利用できない場合、IAM Identity Center は次の表に示すように、別のAWS リージョンで Amazon SES エンドポイントを呼び出します。

IAM Identity Center リージョンコード	IAM Identity Center リージョン名	Amazon SES リージョンコード	Amazon SES リージョン名
ap-east-1	アジアパシフィック (香港)	ap-northeast-2	アジアパシフィック (ソウル)
ap-east-2	アジアパシフィック (台北)	ap-northeast-1	アジアパシフィック (東京)
ap-south-2	アジアパシフィック (ハイデラバード)	ap-south-1	アジアパシフィック (ムンバイ)

IAM Identity Center リージョンコード	IAM Identity Center リージョン名	Amazon SES リージョンコード	Amazon SES リージョン名
ap-southeast-4	アジアパシフィック (メルボルン)	ap-southeast-2	アジアパシフィック (シドニー)
ap-southeast-5	アジアパシフィック (マレーシア)	ap-southeast-1	アジアパシフィック (シンガポール)
ap-southeast-6	アジアパシフィック (ニュージーランド)	ap-southeast-2	アジアパシフィック (シドニー)
ap-southeast-7	アジアパシフィック (タイ)	ap-northeast-3	アジアパシフィック (大阪)
ca-west-1	カナダ西部 (カルガリー)	ca-central-1	カナダ (中部)
eu-south-2	欧州 (スペイン)	eu-west-3	欧州 (パリ)
eu-central-2	欧州 (チューリッヒ)	eu-central-1	欧州 (フランクフルト)
mx-central-1	メキシコ (中部)	us-east-2	米国東部 (オハイオ)
me-central-1	中東 (アラブ首長国連邦)	eu-central-1	欧州 (フランクフルト)
us-gov-east-1	AWS GovCloud (米国東部)	us-gov-west-1	AWS GovCloud (米国西部)

これらのクロスリージョン呼び出しでは、IAM Identity Center は次のユーザー属性を送信する場合があります。

- E メールアドレス
- 名
- 姓
- AWS Organizations のアカウント
- AWS アクセスポータル URL

- ユーザー名
- ディレクトリ ID
- ユーザー ID

オプトインリージョン (デフォルトで無効になっているリージョン) での IAM アイデンティティセンターの管理

ほとんどの AWS リージョン はデフォルトですべての AWS サービスのオペレーションで有効になっていますが、IAM アイデンティティセンターを使用する場合は、次のオプトインリージョンを有効にする必要があります。

- アフリカ (ケープタウン)
- アジアパシフィック (香港)
- アジアパシフィック (台北)
- アジアパシフィック (ハイデラバード)
- アジアパシフィック (ジャカルタ)
- アジアパシフィック (メルボルン)
- アジアパシフィック (マレーシア)
- アジアパシフィック (ニュージーランド)
- アジアパシフィック (タイ)
- カナダ西部 (カルガリー)
- 欧州 (ミラノ)
- 欧州 (スペイン)
- 欧州 (チューリッヒ)
- イスラエル (テルアビブ)
- メキシコ (中部)
- 中東 (バーレーン)
- 中東 (アラブ首長国連邦)

オプトインリージョンに IAM アイデンティティセンターをデプロイする場合は、IAM アイデンティティセンターへのアクセスを管理するすべてのアカウントでこのリージョンを有効にする必要があります。すべてのアカウントで、そのリージョンにリソースを作成するかどうかにかかわらず、こ

の設定が必要です。組織内の現在のアカウントで特定のリージョンを有効にできます。新しいアカウントを追加する場合は、このアクションを繰り返す必要があります。手順については、「AWS Organizations ユーザーガイド」の「組織内のリージョンを有効または無効にする」を参照してください。これらの追加ステップの繰り返しを回避するため、デフォルトで有効になっているリージョンに対して IAM アイデンティティセンターをデプロイするよう選択できます。

> **Note**
>
> AWS メンバーアカウントは、AWS アクセスポータルから AWS メンバーアカウントにアクセスできるように、IAM アイデンティティセンターインスタンスが配置されているオプトインリージョンと同じリージョンにオプトインする必要があります。

オプトインリージョンに保存されているメタデータ

オプトイン AWS リージョンで、管理アカウントの IAM アイデンティティセンターを有効にすると、すべてのメンバーアカウントの次の IAM アイデンティティセンターメタデータがリージョンに保存されます。

- アカウント ID
- アカウント名
- 連絡先 E メール
- IAM Identity Center がメンバーアカウントに作成する IAM ロールの Amazon リソースネーム (ARN)

AWS リージョンデフォルトで有効になっている

以下のリージョンはデフォルトで有効になっており、これらのリージョンで IAM アイデンティティセンターを有効にできます。

- 米国東部(オハイオ)
- 米国東部 (バージニア北部)
- 米国西部 (オレゴン)
- 米国西部 (北カリフォルニア)
- 欧州 (パリ)
- 南米 (サンパウロ)

- アジアパシフィック (ムンバイ)
- 欧州 (ストックホルム)
- アジアパシフィック (ソウル)
- アジアパシフィック (東京)
- 欧州 (アイルランド)
- 欧州 (フランクフルト)
- 欧州 (ロンドン)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- カナダ (中部)
- アジアパシフィック (大阪)

AWS リージョンの切り替え

IAM Identity Center は、無効にする必要のあるリージョンではなく、ユーザーが利用できるようにしておきたいリージョンにインストールすることをお勧めします。詳細については、「AWS リージョンを選択するための考慮事項」を参照してください。

IAM アイデンティティセンターリージョンの切り替えは、現在の IAM アイデンティティセンターインスタンスを削除し、別のリージョンに新しいインスタンスを作成することによってのみ可能です。既存のインスタンスで AWS マネージドアプリケーションを既に有効にしている場合は、IAM アイデンティティセンターを削除する前に、そのアプリケーションを削除する必要があります。AWS マネージドアプリケーションを無効にする手順については、「AWS マネージドアプリケーションの無効化」を参照してください。

> **Note**
>
> 別のリージョンに AWS マネージドアプリケーションをデプロイできるように IAM Identity Center リージョンを切り替えることを検討している場合は、代わりに IAM Identity Center インスタンスをそのリージョンにレプリケートすることを検討してください。詳細については、「複数の 間で IAM アイデンティティセンターを使用するAWS リージョン」を参照してください。

新しいリージョンの設定に関する考慮事項

ユーザー、グループ、アクセス許可セット、アプリケーション、割り当てを新しい IAM アイデンティティセンターインスタンスで再作成する必要があります。IAM アイデンティティセンターアカウントとアプリケーション割り当て API を使用して現在の設定のスナップショットを取得し、そのスナップショットを使用して新しいリージョンで設定を再構築できます。別のリージョンに切り替えると、 AWS アクセスポータルの URL も変更されます。これにより、ユーザーは AWS アカウントおよび アプリケーションへのシングルサインオンアクセスが可能になります。あるいは、新しいインスタンスの管理コンソールを使用して、一部の IAM アイデンティティセンター設定を再作成する必要がある場合もあります。

IAM アイデンティティセンターが有効になっている AWS リージョンを無効にする

IAM アイデンティティセンターがインストールされている AWS リージョンを無効にすると、IAM アイデンティティセンターも無効になります。IAM アイデンティティセンターをリージョンで無効にすると、そのリージョンのユーザーは AWS アカウント とアプリケーションにシングルサインオンアクセスできなくなります。

オプトイン AWS リージョンで IAM アイデンティティセンターを再度有効にするには、そのリージョンを再度有効にする必要があります。IAM アイデンティティセンターでは一時停止中のイベントをすべて再処理する必要があるため、IAM アイデンティティセンターを再度有効にするとしばらく時間がかかる場合があります。

> **Note**
>
> IAM アイデンティティセンターは、AWS リージョンで使用が有効になっている AWS アカウントへのアクセスのみを管理できます。組織内のすべてのアカウントへのアクセスを管理するには、IAM アイデンティティセンターで使用できるよう自動的にアクティブ化された AWS リージョン の管理アカウントで IAM アイデンティティセンターを有効にします。

AWS リージョン の有効化と無効化の詳細については、「AWS 全般のリファレンス」の「AWS リージョン の管理」を参照してください。

アプリケーションへのユーザーアクセスのみに IAM アイデンティティセンターを使用する

IAM Identity Center は、Kiro、AWS アカウント、またはその両方などのアプリケーションへのユーザーアクセスに使用できます。既存の ID プロバイダーを接続し、ディレクトリからユーザーとグループを同期することも、IAM アイデンティティセンターで直接ユーザーを作成・管理することも

できます。既存の ID プロバイダーを IAM アイデンティティセンターに接続する方法については、「IAM アイデンティティセンターの ID ソースに関するチュートリアル」を参照してください。

へのアクセスに IAM を既に使用していますか?AWS アカウント

IAM アイデンティティセンターを使用して AWS マネージドアプリケーションにアクセスするのに現在の AWS アカウントワークフローを変更する必要はありません。AWS アカウント へのアクセスに IAM とのフェデレーションを使用している場合、各ユーザーはこれまでと同じ方法で AWS アカウント にアクセスし、既存のワークフローを使用してアクセスを管理することができます。

IAM アイデンティティセンターによって作成される IAM ロール

ユーザーを AWS アカウントに割り当てると、IAM アイデンティティセンターは、IAM ロールを作成して、ユーザーにリソースへのアクセス許可を付与します。

権限セットを割り当てると、IAM アイデンティティセンターは、IAM アイデンティティセンターでコントロールされる対応する IAM ロールを各アカウントに作成し、権限セットで指定されたポリシーをそれらのロールにアタッチします。IAM アイデンティティセンターはロールを管理し、AWS アクセスポータルまたは AWS CLI を使用して、定義した承認済みユーザーがロールを引き受けることを許可します。アクセス権限セットを変更すると、IAM Identity Center は、対応する IAM ポリシーとロールがそれに応じて更新されることを保証します。IAM Identity Center インスタンスを追加リージョンにレプリケートしても、既存の IAM ロールには影響せず、新しい IAM ロールも作成されません。

> **Note**
>
> アクセス許可セットは、アプリケーションにアクセス許可を付与するために使用されません。

AWS アカウント で IAM ロールをすでに設定している場合は、アカウントが IAM ロールのクォータに近づいているかどうかを確認することをお勧めします。アカウントあたりの IAM ロールのデフォルトクォータは 1000 ロールです。詳細については、「IAM オブジェクトクォータ」を参照してください。

クォータに近づいている場合は、クォータの増額をリクエストすることを検討してください。そうしないと、IAM ロールクォータを超えたアカウントにアクセス権限セットをプロビジョニングする際に、IAM Identity Center の問題が発生する可能性があります。クォータ引き上げのリクエストの詳細情報については、「Service Quotas ユーザーガイド」の「クォータ引き上げリクエスト」を参照してください。

> **Note**
>
> すでに IAM アイデンティティセンターを使用しているアカウントの IAM ロールを確認している場合は、ロール名が “AWSReservedSSO_” で始まることに気づくかもしれません。これらは、IAM Identity Center サービスがアカウントに作成したロールであり、アカウントにアクセス権限セットを割り当てたものです。

IAM アイデンティティセンターおよび AWS Organizations

AWS Organizations は IAM アイデンティティセンターと併用することをお勧めしますが、必須ではありません。組織をまだ設定していない場合は、設定する必要はありません。IAM アイデンティティセンターを有効にする場合は、AWS Organizations でサービスを有効にするかどうかを選択します。組織をセットアップすると、組織をセットアップした AWS アカウント が組織の管理アカウントになります。AWS アカウント のルートユーザーが組織管理アカウントの所有者になりました。組織に追加で招待したすべて AWS アカウント は、メンバーアカウントです。管理アカウントは、メンバーアカウントを管理する組織リソース、組織単位、およびポリシーを作成します。アクセス許可は管理アカウントによってメンバーアカウントに委任されます。

> **Note**
>
> AWS Organizations を使用して IAM アイデンティティセンターを有効にすることをお勧めします。これにより IAM アイデンティティセンターの組織インスタンスが作成されます。組織インスタンスは IAM アイデンティティセンターのすべての機能をサポートし、一元管理機能を提供するため、おすすめのベストプラクティスです。詳細については、「IAM アイデンティティセンターの組織インスタンス」を参照してください。

すでに AWS Organizations をセットアップしていて、IAM アイデンティティセンターを組織に追加する場合は、すべての AWS Organizations 機能が有効になっていることを確認してください。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。詳細については、「AWS Organizations ユーザーガイド」の「組織内のすべての機能の有効化」を参照してください。

IAM アイデンティティセンターの組織インスタンスを有効にするには、管理者認証情報を持つユーザーまたはルートユーザーとして AWS Organizations 管理アカウントにサインインして、AWS マネジメントコンソール にサインインする必要があります (他の管理ユーザーが存在しない場合を除き、ルートユーザーとしてのサインインは推奨されません)。詳細については、「AWS Organizations ユーザーガイド」の「AWS 組織の作成と管理」を参照してください。

AWS Organizations メンバーアカウントの管理認証情報を使用してサインインすると、IAM アイデンティティセンターのアカウントインスタンスを有効化できます。アカウントインスタンスの機能は限られており、1 つの AWS アカウントにバインドされます。

IAM アイデンティティセンターの組織インスタンスとアカウントインスタンス

インスタンスは IAM アイデンティティセンターの単一デプロイです。IAM アイデンティティセンターで使用できるインスタンスには、組織インスタンスとアカウントインスタンスの 2 種類があります。

- 組織インスタンス (推奨)

  AWS Organizations 管理アカウントで有効にする IAM アイデンティティセンターのインスタンス。組織インスタンスは、IAM アイデンティティセンターのすべての機能をサポートしています。管理ポイントの数を最小限に抑えるには、アカウントインスタンスではなく組織インスタンスをデプロイすることをお勧めします。
- アカウントインスタンス

  単一の AWS アカウント にバインドされ、有効になっている AWS アカウント および AWS リージョン内でのみ表示される IAM アイデンティティセンターのインスタンス。よりシンプルな単一アカウントのシナリオでは、 アカウントインスタンスを使用します。以下のいずれかからアカウントインスタンスを有効にできます。
  - AWS Organizations によって管理されていない AWS アカウント
  - AWS Organizations のメンバーアカウント

AWS アカウントIAM アイデンティティセンターを有効にできる タイプ

IAM アイデンティティセンターを有効にするには、作成するインスタンスタイプに応じて、次のいずれかの認証情報を使用して AWS マネジメントコンソールにサインインします。

- AWS Organizations 管理アカウント (推奨) — IAM アイデンティティセンターの組織インスタンスを作成するために必要です。組織全体でのマルチアカウント権限とアプリケーションの割り当てには、組織インスタンスを使用してください。
- AWS Organizations メンバーアカウント — IAM アイデンティティセンターのアカウントインスタンスを作成し、そのメンバーアカウント内でのアプリケーション割り当てを有効にするのに使用し

ます。メンバーレベルのインスタンスを持つ 1 つ以上のアカウントを組織内に持つことができます。

- スタンドアロン AWS アカウント — IAM アイデンティティセンターの組織インスタンスまたはアカウントインスタンスを作成する場合に使用します。スタンドアロン AWS アカウント は、AWS Organizations によって管理されません。スタンドアロン AWS アカウント に関連付けることができるのは IAM アイデンティティセンターのインスタンス 1 つだけであり、そのインスタンスはスタンドアロン AWS アカウント 内のアプリケーション割り当てに使用できます。

次の表を使用して、インスタンスタイプによって提供される機能を比較します。

機能	AWS Organizations 管理アカウント内のインスタンス (推奨)	メンバーアカウント内のインスタンス	スタンドアロン AWS アカウント 内のインスタンス
ユーザーの管理	✓はい	✓はい	✓はい
AWS マネージドアプリケーションにシングルサインオンでアクセスできる AWS アクセスポータル	✓はい	✓はい	✓はい
OAuth 2.0 (OIDC) カスタマーマネージドアプリケーション	✓はい	✓はい	✓はい
マルチアカウント権限	✓はい	✗いいえ	✗いいえ
AWS へのシングルサインオン用 アクセスポータルAWS アカウント	✓はい	✗いいえ	✗いいえ
SAML 2.0 カスタマーマネージドアプリケーション	✓はい	✗いいえ	✗いいえ

機能	AWS Organizations 管理アカウント内のインスタンス (推奨)	メンバーアカウント内のインスタンス	スタンドアロン AWS アカウント 内のインスタンス
委任管理者がインスタンスを管理できる	✓はい	✗いいえ	✗いいえ
カスタマーマネージド KMS キーを使用した保管中の暗号化	✓はい	✗いいえ	✗いいえ
IAM Identity Center を追加リージョンにレプリケートする	✓はい	✗いいえ	✗いいえ

AWS マネージドアプリケーションと IAM アイデンティティセンターの詳細については「AWSIAM アイデンティティセンターで使用できる マネージドアプリケーション」を参照してください。

トピック

- IAM アイデンティティセンターの組織インスタンス
- IAM アイデンティティセンターのアカウントインスタンス
- IAM アイデンティティセンターインスタンスを削除する

IAM アイデンティティセンターの組織インスタンス

IAM アイデンティティセンターを AWS Organizations と組み合わせて有効にすると、IAM アイデンティティセンターの組織インスタンスが作成されます。ユーザーとグループのアクセスを 1 つの組織インスタンスで一元管理するには、組織インスタンスは管理アカウントで有効化されている必要があります。AWS Organizations では、各管理アカウントにつき 1 つの組織インスタンスしか作成できません。

2023 年 11 月 15 日より前に IAM アイデンティティセンターを有効にした場合は、IAM アイデンティティセンターの組織インスタンスがあります。

IAM アイデンティティセンターの組織インスタンスを有効にするには、「IAM アイデンティティセンターのインスタンスを有効にするには」を参照してください。

組織インスタンスを使用するタイミング

組織インスタンスは IAM アイデンティティセンターを有効にする主要な方法であり、通常は組織インスタンスが推奨されます。組織インスタンスには、次のような利点があります。

- IAM Identity Center のすべての機能のサポート — 組織内の複数の AWS アカウント の権限管理、カスタマーマネージドアプリケーションへのアクセス権の割り当て、マルチリージョンレプリケーションなどが含まれます。
- 管理ポイントの削減 — 組織インスタンスには単一の管理ポイント、つまり管理アカウントがあります。管理ポイントの数を減らすには、アカウントインスタンスではなく組織インスタンスを有効にすることをお勧めします。
- アカウントインスタンスの作成の集中管理 — オプトインリージョン (デフォルトでは無効の AWS リージョン) の組織に IAM アイデンティティセンターのインスタンスをデプロイしていない限り、組織内のメンバーアカウントがアカウントインスタンスを作成できるかどうかをコントロールできます。

IAM アイデンティティセンターの組織インスタンスを有効にする手順については、「IAM アイデンティティセンターのインスタンスを有効にするには」を参照してください。

インスタンス設定オプション

デフォルトで有効になっている AWS リージョンで組織インスタンスを有効にする場合は、インスタンス設定を選択します。他のリージョンでは、インスタンスはデフォルト設定で作成されます。

> **Note**
>
> [マルチリージョンインスタンス] オプションと [カスタムインスタンス] (新しいキーの作成) オプションは、`CreatedBy: IAM Identity Center` でタグ付けされたカスタマーマネージド KMS キーを作成して、ユーザーに代わって追加リージョンにレプリケートします。IAM プリンシパルに、IAM Identity Center を有効にするために必要なアクセス許可に加えて、`kms:CreateKey`、`kms:TagResource`、`kms:ReplicateKey` の各アクセス許可があることを確認します。

シングルリージョンインスタンス

インスタンスは現在のリージョンに作成されます。

- 保管中の暗号化 – データは AWS 所有キーで暗号化されます。後で設定ページからカスタマーマネージドキーに切り替えることができます。
- 許可セット – デフォルトで有効になっており、ユーザーとグループの AWS アカウント アクセスを管理できます。一度有効にすると、無効にすることはできません。
- プライマリリージョン – インスタンスは現在のリージョンに作成されます。作成後に変更することはできません。
- 追加リージョン – 追加リージョンは設定されていません。後で設定ページからリージョンを追加できます。

マルチリージョンインスタンス

インスタンスは現在のリージョンに作成され、AWS アカウント とアプリケーションアクセスを回復できるように追加リージョンにレプリケートされます。

- 保管中の暗号化 – データは、レプリケーションをサポートするキーポリシーを持つアカウントで作成されたカスタマーマネージドマルチリージョンキーで暗号化されます。キーには `CreatedBy: IAM Identity Center` というタグが付いているため、アカウント内で簡単に識別できます。キーは後で変更できます。AWS KMS 料金が適用されます。
- 許可セット – デフォルトで有効になっており、ユーザーとグループの AWS アカウント アクセスを管理できます。一度有効にすると、無効にすることはできません。
- プライマリリージョン – インスタンスは現在のリージョンに作成されます。作成後に変更することはできません。
- 追加リージョン – インスタンスは現在のリージョンに作成され、AWS アカウント とアプリケーションアクセスを回復できるように追加リージョンにレプリケートされます。リージョンは後で変更または追加することができます。

カスタムインスタンス

インスタンス設定を個別に行います。

保管中の暗号化

次のいずれかを選択します。追加リージョンを追加するには、カスタマーマネージドキーが必要です。

- AWS 所有キーを使用する – データは、AWS が所有および管理するキーで暗号化されます。追加料金はかかりません。

- 新しいカスタマーマネージドキーを作成する – マルチリージョンキーは、レプリケーションをサポートするベースラインキーポリシーを使用してアカウントに作成されます。AWS KMS 料金が適用されます。
- 既存のカスタマーマネージドキーを選択する – アカウントに既にあるキーを使用します。キーポリシーがインスタンスの要件を満たしていることを確認します。AWS KMS 料金が適用されます。

権限セット

アクセス許可セットを有効にして、ユーザーとグループの AWS アカウント アクセスを管理できます。一度有効にすると、無効にすることはできません。

追加リージョン

AWS アカウント とアプリケーションアクセスを回復できるようにリージョンを追加します。選択したリージョンでも、カスタマーマネージド AWS KMS キーを利用できる必要があります。

組織インスタンスを有効にする手順については、「IAM Identity Center を有効にする」を参照してください。マルチリージョンのサポートの詳細については、「複数の 間で IAM アイデンティティセンターを使用するAWS リージョン」を参照してください。

IAM アイデンティティセンターのアカウントインスタンス

IAM アイデンティティセンターのアカウントインスタンスでは、サポートされている AWS マネージドアプリケーションと OIDC ベースのカスタマーマネージドアプリケーションをデプロイできます。アカウントインスタンスは、IAM アイデンティティセンターのワークフォース ID 機能とアクセスポータル機能を活用して、アプリケーションを個別に単一の AWS アカウント にデプロイすることをサポートします。

アカウントインスタンスは単一の AWS アカウント にバインドされ、同じアカウントと AWS リージョン 内のサポート対象アプリケーションへのユーザーとグループのアクセスを管理するためにのみ使用されます。AWS アカウント ごとに、アカウントインスタンスは 1 つに制限されています。アカウントインスタンスは、AWS Organizations のメンバーアカウントまたは AWS Organizations によって管理されていないスタンドアロン AWS アカウント のいずれかから作成できます。

IAM アイデンティティセンターのアカウントインスタンスを有効にする手順については、「IAM アイデンティティセンターのインスタンスを有効にするには」を参照して[アカウント] タブを選択します。

アカウントインスタンスを使用するタイミング

ほとんどの場合には、組織インスタンスをお勧めします。アカウントインスタンスは、以下のシナリオのいずれかに当てはまる場合にのみ使用します。

- サポート対象の AWS マネージドアプリケーションを一時的に試用して、そのアプリケーションがビジネスニーズに合っているかどうかを判断したい。
- 組織全体に IAM アイデンティティセンターを導入する予定はないが、1 つ以上の AWS マネージドアプリケーションをサポートしたいと考えている。
- IAM アイデンティティセンターの組織インスタンスはあるが、サポートされている AWS マネージドアプリケーションを、組織インスタンス内のユーザーとは異なる、分離されたユーザーグループにデプロイしたいと考えている。
- 運用している AWS 組織を管理していない。例えば、サードパーティーが AWS アカウント を管理する AWS 組織をコントロールしている。

> **Important**
>
> IAM アイデンティティセンターを使用して複数のアカウントのアプリケーションをサポートする予定がある場合は、組織インスタンスを使用してください。アカウントインスタンスはこのユースケースをサポートしていません。

AWSアカウントインスタンスをサポートする マネージドアプリケーション

どの AWS マネージドアプリケーションが IAM アイデンティティセンターのアカウントインスタンスをサポートしているかについては、「AWSIAM アイデンティティセンターで使用できる マネージドアプリケーション」を参照してください。AWS マネージドアプリケーションでアカウントインスタンスを作成できるかどうかを確認してください。

メンバーアカウントの可用性制約

IAM アイデンティティセンターのアカウントインスタンスを AWS Organizations メンバーアカウントにデプロイするには、次のいずれかの条件が満たされている必要があります。

- 組織内に IAM アイデンティティセンターの組織インスタンスがないこと。
- 組織内に IAM アイデンティティセンターの組織インスタンスがあるが、インスタンス管理者が IAM アイデンティティセンターのアカウントインスタンス作成を許可している (2023 年 11 月 15 日以降に作成された組織インスタンスの場合)。

- 組織内に IAM アイデンティティセンターの組織インスタンスがあるが、インスタンス管理者が組織内のメンバーアカウント によるアカウントインスタンス作成を手動で有効化している (2023 年 11 月 15 日以前に作成された組織インスタンスの場合)。手順については、「メンバーアカウントでアカウントインスタンスの作成を許可する」を参照してください。

上記の条件のいずれかを満たしていることを前提として、さらに以下の条件がすべて満たされている必要があります。

- 管理者が、メンバーアカウントによるアカウントインスタンスの作成を禁止するサービスコントロールポリシーを作成していないこと。
- AWS リージョン にかかわらず、同じアカウントに IAM アイデンティティセンターのインスタンスがまだない。
- その AWS リージョンで IAM アイデンティティセンターが利用可能であること。リージョンの詳細については、「IAM アイデンティティセンターリージョンのデータストレージとオペレーション」を参照してください。

アカウントインスタンスに関する考慮事項

アカウントインスタンスは特殊なユースケース向けに設計されており、組織インスタンスで使用できる機能のサブセットを提供します。アカウントインスタンスを作成する前に、以下を考慮してください。

- アカウントインスタンスはアクセス許可セットをサポートしていないため、AWS アカウント へのアクセスはサポートしていません。
- アカウントインスタンスを組織インスタンスに変換またはマージすることはできません。
- アカウントインスタンスは、一部の AWS マネージドアプリケーションのみでサポートされています。
- アカウントインスタンスは、1 つのアカウントでのみアプリケーションを使用する孤立したユーザーで、使用するアプリケーションの存続期間中だけ使用してください。
- アカウントインスタンスにアタッチされたアプリケーションは、アプリケーションとそのリソースを削除するまでアカウントインスタンスにアタッチされたままにしておく必要があります。
- アカウントインスタンスは、作成された AWS アカウント に置く必要があります。

メンバーアカウントでアカウントインスタンスの作成を許可する

2023 年 11 月 15 日より前に IAM アイデンティティセンターを有効にしている場合は、IAM アイデンティティセンターの組織インスタンスが存在しており、メンバーアカウントがアカウントインスタンスを作成する機能はデフォルトで無効になっています。IAM アイデンティティセンターコンソールでアカウントインスタンス機能を有効にすると、メンバーアカウントでアカウントインスタンスを作成できるかどうかを選択できるようになります。

組織内のメンバーアカウントによるアカウントインスタンスの作成を有効にするには

> **Important**
>
> メンバーアカウントに対して IAM アイデンティティセンターのアカウントインスタンスを有効にする操作は、1 回しか実行できません。つまり、いったん実行すると元に戻すことができません。アカウントインスタンスを有効にしてからサービスコントロールポリシー (SCP) を作成すれば、アカウントインスタンスの作成を制限できます。手順については、「Control account instance creation with Services Control Policies」を参照してください。

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択し、[管理] タブを選択します。
3. [IAM アイデンティティセンターのアカウントインスタンス] セクションで、[IAM アイデンティティセンターのアカウントインスタンスを有効にする] を選択します。
4. [IAM アイデンティティセンターのアカウントインスタンスを有効にする] ダイアログボックスで、[有効にする] を選択して、組織内のメンバーアカウントにアカウントインスタンスの作成を許可することを確認します。

サービスコントロールポリシーを使用してアカウントインスタンスの作成をコントロールする

メンバーアカウントがアカウントインスタンスを作成できるかどうかは、IAM アイデンティティセンターを有効にした時期によって異なります。

- 2023 年 11 月より前 – メンバーアカウントでアカウントインスタンスの作成を許可する必要があります。これは元に戻すことができないアクションです。
- 2023 年 11 月 15 日以降 – メンバーアカウントは、デフォルトでアカウントインスタンスを作成できます。

いずれの場合も、サービスコントロールポリシー (SCP) を使用して以下を行うことができます。

- すべてのメンバーアカウントがアカウントインスタンスを作成できないようにします。
- 特定のメンバーアカウントのみがアカウントインスタンスを作成できるようにします。

アカウントインスタンス作成の防止

以下の手順を使用して、メンバーアカウントが IAM アイデンティティセンターのアカウントインスタンスを作成できないようにする SCP を生成します。

1. IAM Identity Center コンソールを開きます。
2. [ダッシュボード] の [中央管理] セクションで、[アカウントインスタンスの抑制] ボタンを選択します。
3. [SCP をアタッチして新しいアカウントインスタンスが作成されないようにする] ダイアログボックスに SCP が表示されます。SCP をコピーし、[SCP ダッシュボードに移動] ボタンを選択します。AWS Organizations コンソールに移動し、SCP を作成するか、既存の SCP にステートメントとしてアタッチします。SCP は AWS Organizations の機能です。SCP をアタッチする手順については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシーのアタッチとデタッチ」を参照してください。

アカウントインスタンスの制限

すべてのアカウントインスタンスの作成を妨げる代わりに、このポリシーは、「*<ALLOWED-ACCOUNT-ID>*」プレースホルダーに明示的にリストされているものを除くすべての AWS アカウント に対して、IAM アイデンティティセンターのアカウントインスタンスを作成する試みを拒否します。

Example: アカウントインスタンスの作成を制限するポリシーを拒否する

JSON

```
{

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

```
            "Action": "sso:CreateInstance",
            "Resource": "*",
            "Condition": {
                 "StringNotEquals": {
                    "aws:PrincipalAccount": ["<ALLOWED-ACCOUNT-ID>"]
                }
            }
        }
    ]
}
```

- ["<ALLOWED-ACCOUNT-ID>"] を、IAM アイデンティティセンターのアカウントインスタンスの作成を許可する実際の AWS アカウント ID (複数可) に置き換えます。
- 複数の許可されたアカウント ID を配列形式で一覧表示できます: ["111122223333", "444455556666"]。
- このポリシーを組織 SCP にアタッチして、IAM アイデンティティセンターアカウントインスタンスの作成を一元管理します。

  SCP をアタッチする手順については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシーのアタッチとデタッチ」を参照してください。

IAM アイデンティティセンターインスタンスを削除する

IAM アイデンティティセンターインスタンスを削除すると、そのインスタンス内のすべてのデータが削除され、復元することはできません。以下の表は、IAM アイデンティティセンターで設定されているディレクトリタイプに基づいて、どのようなデータが削除されるかを示したものです。

削除されるデータについて	接続済みディレクトリ - AWS Managed Microsoft AD、AD Connector、または外部 ID プロバイダー	IAM Identity Center Identity Store	
AWS アカウント に設定したすべてのアクセス権限セット	✓はい	✓はい	

削除されるデータについて	接続済みディレクトリ - AWS Managed Microsoft AD、AD Connector、または外部 ID プロバイダー	IAM Identity Center Identity Store	
IAM Identity Center で設定したすべてのアプリケーション	⊘はい	⊘はい	
AWS アカウント とアプリケーションに設定したすべてのユーザー割り当て	⊘はい	⊘はい	
ディレクトリまたはストア内のすべてのユーザーとグループ	: 該当なし	⊘はい	

IAM Identity Center インスタンスを追加リージョンにレプリケートした場合は、インスタンスを削除する前に、それらのリージョンを削除する必要があります。

IAM アイデンティティセンターインスタンスを削除するには、次の手順に従います。

IAM アイデンティティセンターインスタンスを削除するには

1. IAM Identity Center コンソールを開きます。
2. 左のナビゲーションペインの [設定] を選択します。
3. [設定] ページで、[管理] タブをクリックします。
4. [IAM Identity Center 設定の削除] セクションで、[削除] を選択します。
5. [IAM アイデンティティセンター設定の削除] ダイアログで、データが削除されることを理解したことを示す各チェックボックスを選択します。テキストボックスに IAM Identity Center インスタンスを入力し、[確認] を選択します。

IAM Identity Center を有効にする

IAM アイデンティティセンターを有効にするときは、有効にする AWS IAM アイデンティティセンター インスタンスタイプを選択します。サービスのインスタンスは、 AWS 環境内のサービスの単一のデプロイです。IAM アイデンティティセンターで使用できるインスタンスには、組織インスタンスとアカウントインスタンスの 2 種類があります。有効にできるインスタンスタイプは、サインインしているアカウントタイプによって異なります。

次のリストは、AWS アカウント のタイプごとに有効にできる IAM アイデンティティセンターインスタンスのタイプを示しています。

- AWS Organizations 管理アカウント (推奨) — IAM アイデンティティセンターの組織インスタンスを作成するために必要です。組織全体でのマルチアカウント権限とアプリケーションの割り当てには、組織インスタンスを使用してください。このインスタンスタイプを追加リージョンにレプリケートすると、アカウントアクセスの回復力を高め、AWS アプリケーションデプロイリージョンを柔軟に選択できるようになります。
- AWS Organizations メンバーアカウント — IAM アイデンティティセンターのアカウントインスタンスを作成し、そのメンバーアカウント内でのアプリケーション割り当てを有効にするのに使用します。メンバーレベルのインスタンスを持つ 1 つ以上のアカウントを組織内に持つことができます。
- スタンドアロン AWS アカウント — IAM アイデンティティセンターの組織インスタンスまたはアカウントインスタンスを作成する場合に使用します。スタンドアロン AWS アカウント は、AWS Organizations によって管理されません。スタンドアロン AWS アカウント に関連付けることができるのは IAM アイデンティティセンターのインスタンス 1 つだけであり、そのインスタンスはスタンドアロン AWS アカウント 内のアプリケーション割り当てに使用できます。

> **Important**
>
> 組織管理アカウントは、サービスコントロールポリシーを使用して、組織メンバーアカウントが IAM アイデンティティセンターのアカウントインスタンスを作成できるかどうかをコントロールできます。
> 無料利用枠アカウントを使用する場合に、AWS 組織を作成すると、従量制料金の有料プランにアカウントが自動的にアップグレードされます。無料利用枠クレジットはすぐに期限切れになります。詳細については、「AWS 無料利用枠に関するよくある質問」を参照してください。

さまざまなインスタンスタイプによって提供されるさまざまな機能の比較については、「IAM アイデンティティセンターの組織インスタンスとアカウントインスタンス」を参照してください。

IAM Identity Center を有効にする前に、IAM アイデンティティセンターに関する前提条件と考慮事項を確認することをお勧めします。

IAM アイデンティティセンターのインスタンスを有効にするには

有効にする IAM アイデンティティセンターインスタンスのタイプについて、組織インスタンスまたはアカウントインスタンスのタブを選択します。

Organization (recommended)

1. 以下のいずれかを行って、AWS マネジメントコンソール にサインインします。

   - AWS[新規の (ルートユーザー)] – [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、アカウント所有者としてサインインします。次のページでパスワードを入力します。
   - [既にスタンドアロンの AWS アカウント (IAM 認証情報) を使って AWS を利用している場合] — 管理者権限を持つ IAM 認証情報を使用してサインインします。
   - 既に使用している AWS Organizations (IAM 認証情報) – 管理アカウントの認証情報を使用してサインインします。
2. IAM Identity Center コンソールを開きます。
3. この手順は、デフォルトで有効になっている AWS リージョンにのみ適用されます。別のリージョンで IAM Identity Center を有効にする場合は、手順 4 に進みます。

   [インスタンス設定] で、次のいずれかのオプションを選択します。

   - シングルリージョンインスタンス – インスタンスは現在のリージョンに作成されます。
   - マルチリージョンインスタンス – インスタンスは現在のリージョンに作成され、AWS アカウント とアプリケーションアクセスを回復できるように追加リージョンにレプリケートされます。カスタマーマネージドマルチリージョン KMS キーは、マルチリージョンをサポートするために自動的に作成されます。AWS KMS の料金が適用されます。
   - カスタムインスタンス – インスタンス設定を個別に行います。

   各オプションの詳細については、「インスタンス設定オプション」を参照してください。

   [有効] を選択してインスタンスを作成します。

4. (オプション) デフォルトの マネージドキーではなく、カスタマー AWS マネージド KMS キーを保管時の暗号化に使用する場合は、[IAM アイデンティティセンターの保管中のデータを暗号化するためのキー] セクションでカスタマーマネージドキーを設定します。詳細については、AWS IAM アイデンティティセンター でのカスタマーマネージド KMS キーの実装を参照してください。

> **Important**
>
> KMS カスタマーマネージドキーを使用するために必要なアクセス許可を設定している場合にのみ、このステップを実行します。適切なアクセス許可がないと、このステップが失敗したり、IAM アイデンティティセンターの管理アプリケーションや AWS マネージドアプリケーションが中断されたりする可能性があります。

5. (オプション) インスタンスでは、マルチアカウントのアクセス許可がデフォルトで有効になっています。IAM Identity Center をアプリケーションの認証とユーザーの管理にのみ使用する場合は、[マルチアカウントのアクセス許可を有効にする] トグルをオフにします。

   マルチアカウントのアクセス許可を今すぐに有効にしないと、AWS アカウント セクションは IAM Identity Center コンソールに表示されません。IAM Identity Center は、サービスリンクロールをメンバーアカウントにデプロイしません。マルチアカウントのアクセス許可は、後で [設定] ページの [管理] タブから有効にできます。

6. [IAM Identity Center を有効にする] で、[有効にする] を選択します。

   - 既存の組織の管理アカウントにサインインしている場合、IAM Identity Center の有効化が始まります。環境のセットアップに進みます。
   - スタンドアロン AWS アカウント (組織の一部ではない) を使用している場合は、[AWS Organizations で IAM Identity Center を有効にする] ページが表示されます。このオプションでは、アカウントを管理アカウントとして新しい組織を作成します。情報を確認し、[有効] を選択してプロセスを完了します。

> **Note**
>
> AWS Organizations では、IAM アイデンティティセンターを 1 つの AWS リージョンでのみ有効にできます。IAM アイデンティティセンターを有効にした後、IAM アイデンティティセンターが有効になっているリージョンを変更する必要がある場合は、

現在のインスタンスを削除し、他のリージョンにインスタンスを作成する必要があります。

> **Tip**
>
> スタンドアロンアカウントがあり、組織インスタンスではなくアカウントインスタンスを作成する場合は、[アカウント] タブを参照してください。

組織インスタンスを有効にしたら、次の手順を実行して環境の設定を完了することをお勧めします。

- 選択した ID ソースを使用していることを確認します。ID ソースが既に割り当てられている場合は、引き続き使用できます。詳細については、「IAM アイデンティティセンターの ID ソースを確認する」を参照してください。
- 委任された管理者としてのメンバーアカウントの登録。詳細については、「委任された管理」を参照してください。
- IAM アイデンティティセンターは、AWS リソースへのアクセスポータルを提供します。次世代ファイアウォール (NGFW) や セキュア Web ゲートウェイ (SWG) などの Web コンテンツフィルタリングソリューションを使用して、特定の AWS ドメインや URL エンドポイントへのアクセスをフィルタリングする場合は、ファイアウォールとゲートウェイを更新して AWS アクセスポータル へのアクセスを許可する を参照してください。

Account

1. 以下のいずれかを行って、AWS マネジメントコンソール にサインインします。
   - AWS[新規の (ルートユーザー)] – [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、アカウント所有者としてサインインします。次のページでパスワードを入力します。
   - すでに使用している AWS (IAM 認証情報) — 管理者権限を持つ IAM 認証情報を使用してサインインします。
   - 既に使用している AWS Organizations (IAM 認証情報) — メンバーアカウントの管理者認証情報を使用してサインインします。
2. IAM Identity Center コンソールを開きます。

3. AWS を初めて使用する場合、またはスタンドアロンの AWS アカウント がある場合は、[IAM アイデンティティセンターを有効にする] で [有効化] を選択します。

   [AWS Organizations で IAM アイデンティティセンターを有効にする] ページが表示されます。これにより、組織インスタンスが作成されます。この方法をお勧めします。ただし、代わりにアカウントインスタンスを使用する場合は、「IAM Identity Center のアカウントインスタンスを有効にする」のリンクを選択します。

4. AWS Organizations メンバーアカウントの管理者の場合は、[IAM アイデンティティセンターのアカウントインスタンスを有効にする] で、[アカウントインスタンスを有効にする]を選択します。

5. [IAM アイデンティティセンターのアカウントインスタンスを有効にする] ページで情報を確認し、必要に応じてこのアカウントインスタンスに関連付けるタグを追加します。次に、[有効化] を選択してプロセスを完了します。

> **Note**
>
> AWS アカウントが組織のメンバーである場合、IAM アイデンティティセンターのアカウントインスタンスを有効にする機能に制限がある場合があります。
>
> - 組織が 2023 年 11 月 15 日より前に IAM アイデンティティセンターを有効にしている場合、メンバーアカウントがアカウントインスタンスを作成する機能はデフォルトで無効になっており、組織の管理アカウントで有効にする必要があります。
> - 組織が 2023 年 11 月 15 日より後に IAM アイデンティティセンターを有効にしている場合は、メンバーアカウントがアカウントインスタンスを作成する機能はデフォルトで無効になっています。ただし、サービスコントロールポリシーを使用して、組織内での IAM アイデンティティセンターのアカウントインスタンスの作成を防ぐことができます。
>
> 詳細については、「the section called “メンバーアカウントでアカウントインスタンスの作成を許可する”」および「the section called “アカウントインスタンス作成用の SCP”」を参照してください。

IAM アイデンティティセンターの ID ソースを確認する

IAM Identity Center の ID ソースは、ユーザーやグループがどこで管理されているかを定義します。IAM アイデンティティセンターを有効にしたら、選択した ID ソースを使用していることを確認します。ID ソースが既に割り当てられている場合は、引き続き使用できます。

Active Directory または外部 IdP ですでにユーザーとグループを管理している場合は、IAM アイデンティティセンターを有効にして ID ソースを選択するときに、この ID ソースの接続を検討することをお勧めします。これは、ユーザーやグループをデフォルトの Identity Center ディレクトリに作成して割り当てを行う前に行う必要があります。

すでに IAM Identity Center の 1 つの ID ソースでユーザーとグループを管理している場合、別の ID ソースに変更すると、IAM Identity Center で設定したユーザーとグループの割り当てがすべて削除される可能性があります。この場合、IAM Identity Center の管理ユーザーを含むすべてのユーザーが、AWS アカウント およびアプリケーショ ンへのシングルサインオンアクセスを失います。詳細については、「ID ソースの変更に関する注意事項」を参照してください。

ID ソースを確認するには

1. IAM Identity Center コンソールを開きます。
2. [ダッシュボード] ページで、[推奨セットアップステップ] セクションの下にある [ID ソースの確認] を選択します。[設定] を選択し、[ID ソース] タブを選択してもこのページにアクセスできます。
3. 割り当てられた ID ソースを維持したい場合はアクションはありません。変更したい場合は、[アクション] を選択し、[ID ソースの変更] を選択します。

ID ソースとして以下のいずれかを選択できます。

Identity Center ディレクトリ

IAM Identity Center を初めて有効にすると、IAM Identity Center ディレクトリがデフォルトの ID ソースとして自動的に構成されます。別の外部 ID プロバイダーをまだ使用していない場合は、ユーザーとグループの作成を開始し、それらのアクセスレベルを AWS アカウント およびアプリケーションに割り当てることができます。この ID ソースの使用に関するチュートリアルについては、「デフォルトの IAM アイデンティティセンターディレクトリを使用してユーザーアクセスを設定する」を参照してください。

Active Directory

Directory Service を使用して AWS Managed Microsoft AD ディレクトリまたは Active Directory (AD) のセルフマネージドディレクトリのいずれかでユーザーとグループをすでに管理している場合は、IAM アイデンティティセンターを有効にするときにそのディレクトリに接続することをお勧めします。デフォルトの Identity Center ディレクトリにはユーザーとグループを作成しないでください。IAM Identity Center は、AWS Directory Service によって提供された接続を使用して、Active Directory のソースディレクトリにあるユーザー、グループ、メンバーシップ情報を IAM ID センターアイデンティティストアに同期します。詳細については、「Microsoft AD ディレクトリ」を参照してください。

> **Note**
>
> IAM アイデンティティセンターは SAMBA4 ベースの Simple AD を ID ソースとしてサポートしていません。

外部 ID プロバイダー

Okta や Microsoft Entra ID などの外部 ID プロバイダー (IdP) の場合、IAM アイデンティティセンターを使用して、Security Assertion Markup Language (SAML) 2.0 標準を通じて IdP からの ID を認証できます。SAML プロトコルは、ユーザーやグループについての情報を得るために IdP へクエリする方法は提供していません。IAM アイデンティティセンターがこれらのユーザーやグループを IAM アイデンティティセンターにプロビジョニングして認識する必要があります。IdP が SCIM をサポートしている場合は、System for Cross-domain Identity Management (SCIM) v2.0 プロトコルを使用して、IdP から IAM アイデンティティセンターへのユーザーおよびグループの情報の自動プロビジョニング (同期) を実行できます。それ以外の場合は、ユーザー名、E メールアドレス、グループを IAM アイデンティティセンターに手動で入力して、ユーザーとグループを手動でプロビジョニングできます。

ID ソースの設定方法の詳細については、「IAM アイデンティティセンターの ID ソースに関するチュートリアル」を参照してください。

> **Note**
>
> 外部 ID プロバイダーを使用する予定の場合は、IAM アイデンティティセンターではなく外部 IdP が多要素認証 (MFA) 設定を管理することに注意してください。IAM アイデン

ティティセンターの MFA では、外部 ID プロバイダーによる使用はサポートされていません。詳細については、「ユーザーに MFA を求める」を参照してください。

> **Note**
>
> IAM Identity Center を追加リージョンにレプリケートする場合は、外部 ID プロバイダーまたはアイデンティティセンターディレクトリを ID ソースとして使用する必要があります。マルチリージョンのサポートは Active Directory では使用できません。前提条件などの詳細については、「複数の 間で IAM アイデンティティセンターを使用するAWS リージョン」を参照してください。

ファイアウォールとゲートウェイを更新して AWS アクセスポータル へのアクセスを許可する

AWS アクセスポータルは、すべての AWS アカウントおよび Office 365、Concur、Salesforce などのよく使用されるクラウドアプリケーションへのシングルサインオンアクセスをユーザーに提供します。ポータル内から、AWS アカウント またはアプリケーションのアイコンを選択するだけで、複数のアプリケーションをすばやく起動できます。

> **Note**
>
> AWS マネージドアプリケーションは IAM アイデンティティセンターと統合され、認証およびディレクトリサービスに使用されますが、アプリケーションアクセスに AWS アクセスポータルを使用しない場合があります。

次世代ファイアウォール (NGFW) や セキュア Web ゲートウェイ (SWG) などの Web コンテンツフィルタリングソリューションを使用して、特定の AWS ドメインや URL エンドポイントへのアクセスをフィルタリングする場合は、AWS アクセスポータルに関連付けられているドメインや URL エンドポイントを許可リストに追加する必要があります。

次のリストには、ウェブコンテンツフィルタリングソリューションの許可リストに追加する IPv4 ドメイン、デュアルスタックドメイン、および URL エンドポイントが示されています。

IPv4 許可リスト

- *[Directory ID or alias]*.awsapps.com
- *[Identity Center instance ID]*.*[Region]*.portal.amazonaws.com
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- *.sso-portal.*[Region]*.amazonaws.com
- *[Region]*.prod.pr.panorama.console.api.aws/panoramaroute
- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

デュアルスタック許可リスト

- *[Identity Center instance ID]*.portal.*[Region]*.app.aws
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.api.aws
- sso.*[Region]*.api.aws
- portal.sso.*[Region]*.api.aws
- *[Region]*.sso.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com

- *.cloudfront.net
- cdn.us-east-1.threat-mitigation.aws.amazon.com
- us-east-1.threat-mitigation.aws.amazon.com
- amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com

結合許可リスト (IPv4 + 下位互換性のあるデュアルスタック)

- *[Directory ID or alias]*.awsapps.com
- *[Identity Center instance ID]*.*[Region]*.portal.amazonaws.com
- *[Identity Centers instance ID]*.portal.*[Region]*.app.aws
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- oidc.*[Region]*.api.aws
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- sso.*[Region]*.api.aws
- *.sso-portal.*[Region]*.amazonaws.com
- portal.sso.*[Region]*.api.aws
- *[Region]*.prod.pr.panorama.console.api.aws/panoramaroute
- *[Region]*.signin.aws
- *[Region]*.sso.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com
- cdn.us-east-1.threat-mitigation.aws.amazon.com
- us-east-1.threat-mitigation.aws.amazon.com
- amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com

ドメインと URL エンドポイントの許可リストに関する考慮事項

AWS アクセスポータルの許可リスト要件に加えて、使用する他のサービスやアプリケーションでは、ドメインの許可リストが必要になる場合があります。

- AWS アクセスポータルから AWS アカウント、AWS マネジメントコンソール、および IAM アイデンティティセンターコンソールにアクセスするには、追加のドメインの許可リストを作成する必要があります。AWS マネジメントコンソールドメインのリストについては、「AWS マネジメントコンソール Getting Started Guide」の「Troubleshooting」を参照してください。
- AWS アクセスポータルから AWS マネージドアプリケーションにアクセスするには、それぞれのドメインを許可リストに登録する必要があります。ガイダンスについては、各サービスドキュメントを参照してください。
- 外部 IdPs (例えば、Okta や Microsoft Entra ID) などの外部ソフトウェアを使用する場合は、それらのドメインを許可リストに含める必要があります。

IAM アイデンティティセンターの ID ソースに関するチュートリアル

AWS Organizations 管理アカウント内の既存の ID ソースを IAM アイデンティティセンターの組織インスタンスに接続できます。すでに使用している ID プロバイダーがない場合は、デフォルトの IAM アイデンティティセンターディレクトリで直接ユーザーを作成・管理できます。ID ソースは、組織ごとに 1 つ持つことができます。

このセクションのチュートリアルでは、一般的に使用される ID ソースを使用して IAM アイデンティティセンターの組織インスタンスをセットアップする方法、管理ユーザーを作成する方法、および AWS アカウントへのアクセスを管理するために IAM アイデンティティセンターを使用する場合は、アクセス許可セットを作成して設定する方法について説明します。IAM アイデンティティセンターをアプリケーションへのアクセスのみに使用する場合は、権限セットを使用する必要はありません。

これらのチュートリアルでは、IAM アイデンティティセンターのアカウントインスタンスを設定する方法については説明していません。アカウントインスタンスを使用してアプリケーションにユーザーとグループを割り当てることはできますが、このインスタンスタイプを使用して AWS アカウントへのユーザーアクセスを管理することはできません。詳細については、「IAM アイデンティティセンターのアカウントインスタンス」を参照してください。

> **Note**
>
> これらのチュートリアルを開始する前に、IAM アイデンティティセンターを有効にしてください。詳細については、「IAM Identity Center を有効にする」を参照してください。

トピック

- Active Directory を ID ソースとして使用する
- Setting up SCIM provisioning between CyberArk and IAM Identity Center
- Google Workspace および IAM アイデンティティセンターによる SAML と SCIM の設定
- IAM アイデンティティセンターを使用して JumpCloud ディレクトリプラットフォームに接続する
- Microsoft Entra ID および IAM アイデンティティセンターによる SAML と SCIM の設定
- Okta および IAM アイデンティティセンターによる SAML と SCIM の設定
- OneLogin と IAM アイデンティティセンター間の SCIM プロビジョニングのセットアップ
- IAM アイデンティティセンターで Ping Identity 製品を使用する

- デフォルトの IAM アイデンティティセンターディレクトリを使用してユーザーアクセスを設定する
- ビデオチュートリアル

Active Directory を ID ソースとして使用する

Active Directory (AD) で Directory Service を使用する AWS Managed Microsoft AD ディレクトリまたは自己管理型ディレクトリのいずれかでユーザーを管理している場合は、それらのユーザーと連携するように IAM アイデンティティセンターの ID ソースを変更できます。IAM アイデンティティセンターを有効にして ID ソースを選択するときは、この ID ソースを接続することを検討することをお勧めします。ユーザーやグループをデフォルトの Identity Center ディレクトリに作成する前に接続しておくと、後で ID ソースを変更する場合に必要となる追加の設定を避けることができます。

Active Directory を ID ソースとして使用するには、設定は次の前提条件を満たす必要があります。

- AWS Managed Microsoft AD を使用している場合は、AWS Managed Microsoft AD ディレクトリが設定されている場所と同じ AWS リージョン で IAM アイデンティティセンターを有効にする必要があります。IAM Identity Center では、割り当てデータに関するディレクトリと同じリージョンに保存されます。IAM Identity Center を管理するには、IAM Identity Center が設定されているリージョンに切り替える必要がある場合があります。また、AWS のアクセスポータルでは、ディレクトリと同じアクセス URL が使用されます。
- 管理アカウントにある Active Directory を使用してください。

  既存の AD コネクタまたは AWS Managed Microsoft AD ディレクトリが AWS Directory Service に設定されており、AWS Organizations 管理アカウント内に存在する必要があります。一度に接続できる AD Connector ディレクトリは 1 つか、ディレクトリは AWS Managed Microsoft AD 1 つだけです。複数のドメインやフォレストをサポートする必要がある場合は、AWS Managed Microsoft AD を使用してください。詳細については、以下を参照してください。

  - AWS Managed Microsoft AD のディレクトリを IAM Identity Center に接続する
  - Active Directory の自己管理型ディレクトリを IAM Identity Center に接続する
- 委任された管理者アカウントにある Active Directory を使用してください。

  IAM アイデンティティセンター委任管理者を有効にし、IAM アイデンティティセンターの ID ソースとして Active Directory を使用する予定の場合は、委任された管理者アカウントにある AWS ディレクトリに設定された既存の AD Connector または AWS Managed Microsoft AD ディレクトリを使用できます。

IAM Identity Center ID ソースを他のソースから Active Directory に変更するか、Active Directory から他のソースに変更する場合、そのディレクトリは IAM Identity Center 委任管理者メンバーアカウント (存在する場合) に存在する (所有されている) 必要があります。それ以外の場合は、管理アカウントに含まれている必要があります。

このチュートリアルでは、Active Directory を IAM アイデンティティセンターの ID ソースとして使用するための基本設定について説明します。

ステップ 1: Active Directory に接続し、ユーザーを指定する

すでに Active Directory を使用している場合は、以下のトピックがディレクトリを IAM アイデンティティセンターに接続する準備に役立ちます。

> **Note**
>
> Active Directory 内の AWS Managed Microsoft AD ディレクトリまたは自己管理型ディレクトリを接続する予定で、RADIUS MFA を AWS Directory Service と一緒に使用していない場合は、IAM アイデンティティセンターで MFA を有効にします。

AWS Managed Microsoft AD

1. Microsoft AD ディレクトリ のガイダンスを確認してください。
2. 「AWS Managed Microsoft AD のディレクトリを IAM Identity Center に接続する」のステップを実行してください。
3. 管理者権限を付与したいユーザーを IAM Identity Center と同期するように Active Directory を設定します。詳細については、「管理ユーザーを IAM Identity Center と同期する」を参照してください。

Active Directory 内の自己管理型ディレクトリ

1. Microsoft AD ディレクトリ のガイダンスを確認してください。
2. 「Active Directory の自己管理型ディレクトリを IAM Identity Center に接続する」のステップを実行してください。

3. 管理者権限を付与したいユーザーを IAM Identity Center と同期するように Active Directory を設定します。詳細については、「管理ユーザーを IAM Identity Center と同期する」を参照してください。

ステップ 2: 管理ユーザーを IAM アイデンティティセンターと同期する

ディレクトリを IAM Identity Center に接続したら、管理権限を付与するユーザーを指定し、そのユーザーをディレクトリから IAM Identity Center に同期できます。

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [設定]ページで[ID ソース]タブを選択し、[アクション]を選択し、[同期を管理] を選択します。
4. [同期の管理] ページで、[ユーザー] タブを選択し、[ユーザーとグループの追加] を選択します。
5. [ユーザー] タブの [ユーザー] に正確なユーザー名を入力し、[追加] を選択します。
6. [追加されたユーザーとグループ] で、次の操作を行います。
   a. 管理者権限を付与するユーザーが指定されていることを確認します。
   b. ユーザー名の左側にあるチェックボックスをオンにします。
   c. [Submit] を選択してください。
7. [同期の管理] ページで、指定したユーザーが同期対象のユーザーリストに表示されます。
8. ナビゲーションペインで [ユーザー] を選択します。
9. [ユーザー] ページでは、指定したユーザーがリストに表示されるまでに時間がかかる場合があります。ユーザーリストを更新するには、[更新] アイコンをクリックします。

この時点では、ユーザーは管理アカウントにアクセスできません。このアカウントへの管理アクセスを設定するには、管理アクセス権限セットを作成し、そのアクセス権限セットにユーザを割り当てます。詳細については、「アクセス権限セットを作成します。」を参照してください。

Setting up SCIM provisioning between CyberArk and IAM Identity Center

IAM Identity Center は、CyberArk Directory Platform から IAM Identity Center へのユーザ情報の自動プロビジョニン グ (同期) をサポートしています。このプロビジョニングでは、クロスドメインア

イデンティティ管理システム (SCIM) v2.0 プロトコルを使用します。詳細については、「外部 ID プロバイダーで SAML および SCIM ID フェデレーションを使用する」を参照してください。

SCIM のデプロイを開始する前に、まず 自動プロビジョニングを使用する際の注意事項 を確認することをお勧めします。そして、次のセクションで残りの注意事項を確認します。

トピック

- 前提条件
- SCIM に関する注意事項
- ステップ 1: IAM Identity Center でプロビジョニングを有効にする
- ステップ 2: CyberArk でプロビジョニングを設定する
- (オプション) ステップ 3: IAM Identity Center でのアクセスコントロール (ABAC) のために CyberArk でユーザー属性を設定する
- (オプション) アクセスコントロールの属性を渡す

前提条件

開始する前に、以下の準備が必要です。

- CyberArk のサブスクリプションまたは無料トライアル。無料トライアルにサインアップするには、CyberArk にアクセスしてください。
- IAM Identity Center 対応アカウント (無料)。詳細については、「IAM Identity Center の有効化」を参照してください。
- 「CyberArkIAM ID Centerのドキュメント」で説明されている、CyberArk アカウントから IAM Identity Center への SAML 接続。
- IAM Identity Center コネクターを、AWS アカウント へのアクセスを許可したいロール、ユーザー、組織に関連付けます。

SCIM に関する注意事項

IAM Identity Center に CyberArk のフェデレーションを使用する場合の注意事項を以下に示します。

- アプリケーションプロビジョニングセクションでマッピングされたロールだけが IAM Identity Center に同期されます。
- プロビジョニングスクリプトはデフォルトの状態でのみサポートされており、変更すると SCIM のプロビジョニングに失敗する可能性があります。

  - 同期できる電話番号属性は 1 つだけです。デフォルトは「仕事用の電話」です。
- CyberArk IAM Identity Center アプリケーションのロールマッピングを変更すると、以下のような動作になります。
  - ロール名を変更しても、IAM Identity Center のグループ名は変更されません。
  - グループ名が変更された場合、IAM Identity Center では新しいグループが作成されます。古いグループは残りますが、メンバーはいません。
- ユーザーの同期とプロビジョニング解除の動作は、CyberArk IAM Identity Center アプリケーションから設定できますので、組織に合った動作を設定してください。オプションは次の通りです。
  - Identity Center ディレクトリ内の同じプリンシパル名のユーザーを上書きする (しない)。
  - ユーザーが CyberArk のロールから削除されたときに、IAM Identity Center からユーザーを非プロビジョニングします。
  - ユーザー動作のプロビジョニングの解除 - 無効化または削除。

ステップ 1: IAM Identity Center でプロビジョニングを有効にする

この最初のステップでは、IAM Identity Center コンソールを使用して、自動プロビジョニングを有効にします。

IAM アイデンティティセンターで自動プロビジョニングを有効にするには

1. 前提条件が整ったら、IAM アイデンティティセンターコンソールを開きます。
2. 左側のナビゲーションペインの [設定] を選択します。
3. [設定] ページで、[自動プロビジョニング] 情報ボックスを探し、[有効化] を選択します。これにより、すぐに IAM アイデンティティセンターの自動プロビジョニングが有効になり、必要なエンドポイントとアクセストークンの情報が表示されます。
4. [インバウンド自動プロビジョニング] ダイアログボックスで、SCIM エンドポイントとアクセストークンをコピーします。これらは、後で IdP でプロビジョニングを設定する際に貼り付ける必要があります。

   a. [SCIM エンドポイント] - 例えば https://scim.*us-east-2*.amazonaws.com/*11111111111-2222-3333-4444-555555555555*/scim/v2

   b. [アクセストークン] - [トークンを表示] を選択して値をコピーします。

> **Warning**
>
> SCIM エンドポイントとアクセストークンを取得できるタイミングは、この時のみです。先に進む前に、これらの値をコピーしておいてください。このチュートリアルの後半で、お使いの IdP 上でこれらの値を入力して自動プロビジョニングを設定します。

5. [閉じる] を選択します。

IAM Identity Center でプロビジョニングを設定したので、CyberArk IAM Identity Center アプリケーションを使用して残りのタスクを完了する必要があります。これらのステップについて、次の手順で説明します。

ステップ 2: CyberArk でプロビジョニングを設定する

CyberArk IAM Identity Center アプリケーションで以下の手順を使用して、IAM Identity Center によるプロビジョニングを有効にします。この手順では、CyberArk IAM Identity Center アプリケーションが Web Apps (ウェブアプリケーション)で CyberArk 管理コンソールに追加されていることを前提としています。まだ実行していない場合は、「前提条件」を参照してから、この手順を実行して SCIM プロビジョニングを設定してください。

CyberArk でプロビジョニングを設定するには

1. CyberArk の SAML 構成の一部として追加した CyberArk IAM Identity Center アプリケーションを開きます（アプリ>ウェブアプリ）。「前提条件」を参照してください。
2. [IAM Identity Center] アプリケーションを選択し、[プロビジョニング] セクションに移動します。
3. [Enable provisioning for this application] (このアプリケーションのプロビジョニングを有効にする) にチェックを入れ、[Live Mode] (ライブモード) を選択します。
4. 前の手順で、IAM Identity Center から [SCIM エンドポイント] の値をコピーしました。CyberArk IAM アイデンティティセンターアプリケーションの [SCIM Service URL] フィールドにその値を貼り付け、[認証タイプ] を [認証ヘッダー] に設定します。
5. [Header Type] (ヘッダータイプ) を [Bearer Token] (ベアラートークン) に設定します。
6. 前の手順で、IAM Identity Center の [アクセストークン] の値をコピーしました。その値を CyberArk IAM Identity Center アプリケーションの[ベアラートークン] フィールドに貼り付けます。

7. [Verify] (検証) をクリックすると、設定をテストして、適用します。
8. [同期オプション] で、CyberArk からのアウトバウンドプロビジョニングを動作させるための正しい動作を選択します。似たようなプリンシパル名を持つ既存の IAM Identity Center ユーザーを上書きする (または上書きしない) かどうか、プロビジョニング解除の動作を選択できます。
9. [ロールマッピング] では、[名前] フィールドにある CyberArk ロールから [送信先グループ] にある IAM Identity Center グループへのマッピングを設定します。
10. 完了したら、下部の [Save] (保存) をクリックします。
11. ユーザーが IAM Identity Center に正常に同期されたことを確認するには、IAM Identity Center コンソールに戻り、[ユーザー] を選択します。CyberArk から同期されたユーザーは、[ユーザー] ページに表示されます。これらのユーザーは、アカウントに割り当てられ、IAM Identity Center で接続できるようになりました。

(オプション) ステップ 3: IAM Identity Center でのアクセスコントロール (ABAC) のために CyberArk でユーザー属性を設定する

これは、AWS リソースへのアクセスを管理するために IAM Identity Center の属性設定を選択した場合の CyberArk のオプション手順です。CyberArk で定義した属性は、SAML アサーションで IAM Identity Center に渡されます。その後、IAM Identity Center でアクセス権限セットを作成し、CyberArk から渡された属性に基づいてアクセスを管理します。

この手順を始める前に、最初に アクセスコントロールの属性 機能を有効にしておく必要があります。これを行う方法については、「アクセスコントロールのための属性の有効化と設定」を参照してください。

IAM Identity Center でのアクセスコントロールに使用される CyberArk の属性の有効化と設定

1. CyberArk の SAML 構成の一部としてインストールした CyberArk IAM Identity Center アプリケーションを開きます（ アプリ>ウェブアプリ ）。
2. [SAML Response] (SAML レスポンス) オプションに移動します。
3. [Attributes] (属性) では、以下のようなロジックでテーブルに関連する属性を追加します。
   a. [属性名] は、CyberArk のオリジナルの属性名です。
   b. [属性値] は、IAM Identity Center への SAML アサーションで送信される属性名です。
4. [保存] を選択します。

(オプション) アクセスコントロールの属性を渡す

IAM Identity Center の アクセスコントロールの属性 機能をオプションで使用して、Name 属性を `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` に設定した Attribute 要素を渡すことができます。この要素を使用すると、SAML アサーションでセッションタグとして属性を渡すことができます。セッションタグの詳細については、「IAM ユーザーガイド」の「AWS STS でのタグ付けの規則 」を参照してください。

属性をセッションタグとして渡すには、タグの値を指定する AttributeValue 要素を含めます。例えば、タグのキーバリューのペア `CostCenter = blue` を渡すには、次のような属性を使用します。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

複数の属性を追加する必要がある場合は、各タグに個別の Attribute 要素を含めます。

Google Workspace および IAM アイデンティティセンターによる SAML と SCIM の設定

組織が Google Workspace を使用している場合は、Google Workspace から IAM アイデンティティセンターにユーザーを統合して、AWS リソースへのアクセスを許可できます。この統合を実現するには、IAM アイデンティティセンターID ソースをデフォルトの IAM アイデンティティセンターID ソースから Google Workspace に変更します。

> **Note**
>
> Google Workspace は現在、AWS IAM アイデンティティセンター アプリケーションで SAML マルチアサーションコンシューマーサービス (ACS) URL をサポートしていません。この SAML 機能は、IAM Identity Center のマルチリージョンサポートを最大限に活用するために必要です。IAM Identity Center を追加リージョンにレプリケートする場合に、単一の ACS URL を使用すると、それらの追加リージョンでのユーザーエクスペリエンスに影響が出る可能性があることに注意してください。プライマリリージョンは、引き続き正常に

機能します。IdP ベンダーと協力して、この機能を有効にすることをお勧めします。単一の ACS URL による追加リージョンでのユーザーエクスペリエンスの詳細については、「the section called “複数の ACS URL なしで AWS マネージドアプリケーションを使用する”」および「the section called “複数の ACS URL を使用しない AWS アカウントアクセス回復性”」を参照してください。

Google Workspace のユーザー情報は、クロスドメイン ID 管理システム (SCIM) v2.0 プロトコルを使用して IAM アイデンティティセンターに同期されます。詳細については、「外部 ID プロバイダーで SAML および SCIM ID フェデレーションを使用する」を参照してください。

Google Workspace で、この接続を IAM アイデンティティセンター用 SCIM エンドポイントと IAM アイデンティティセンターのベアラートークンを使用して設定します。SCIM 同期を設定すると、Google Workspace のユーザー属性と IAM Identity Center の名前付き属性のマッピングが作成されます。このマッピングは、IAM アイデンティティセンターと Google Workspace の間で、期待されるユーザー属性を照合します。そのためには、Google Workspace を ID プロバイダーとして設定し、IAM アイデンティティセンター ID プロバイダーに接続する必要があります。

目的

このチュートリアルの手順に従うと、Google Workspace と AWS の間の SAML 接続を確立する手順がわかります。後で、SCIM を使用して Google Workspace のユーザーを同期します。すべてが正しく設定されていることを確認するには、設定手順を完了した後に、Google Workspace ユーザーとしてサインインし、AWS リソースへのアクセスを確認します。このチュートリアルは小規模 Google Workspace ディレクトリのテスト環境に基づいていることに注意してください。グループや組織単位などのディレクトリ構造はこのチュートリアルには含まれていません。このチュートリアルを完了すると、ユーザーは Google Workspace 認証情報を使用して AWS アクセスポータルにアクセスできるようになります。

> **Note**
>
> Google Workspace の無料トライアルにサインアップするには、Google's Web サイトの Google Workspace にアクセスしてください。
> IAM アイデンティティセンターをまだ有効にしていない場合は、「IAM Identity Center を有効にする」を参照してください。

考慮事項

- Google Workspace と IAM アイデンティティセンター間で SCIM プロビジョニングを設定する前に、まず「自動プロビジョニングを使用する際の注意事項」を確認することをお勧めします。
- Google Workspace からの SCIM 自動同期は、現在、ユーザープロビジョニングに限定されています。現在、自動グループプロビジョニングはサポートされていません。グループは、AWS CLI ID ストアの [create-group] コマンドを使用して、または AWS Identity and Access Management (IAM) API の [CreateGroup] を使用して手動で作成できます。または、ssosync を使用して Google Workspace ユーザーとグループを IAM アイデンティティセンターに同期することもできます。
- すべての Google Workspace ユーザーにおいて、[名]、[姓]、[ユーザー名]、[表示名] の値を指定する必要があります。
- 各 Google Workspace ユーザーには、E メールアドレスや電話番号などのデータ属性ごとに 1 つの値のみが割り当てられます。複数の値を持つユーザーは同期に失敗します。属性に複数の値を持つユーザーがいる場合は、IAM アイデンティティセンターでユーザーをプロビジョニングする前に、重複する属性を削除してください。例えば、同期できる電話番号属性は 1 つだけです。デフォルトの電話番号属性は「勤務先の電話」なので、ユーザーの電話番号が自宅の電話でも携帯電話でも、「勤務先の電話」属性を使用してユーザーの電話番号を保存します。
- ユーザーが IAM Identity Center で無効化されていても、Google Workspace で有効化されていれば、属性は引き続き同期されます。
- アイデンティティセンターディレクトリに同じユーザーネームと E メールアドレスを持つ既存のユーザーがいる場合、そのユーザーは上書きされ、Google Workspace から SCIM を介して同期されます。
- ID ソースを変更する場合は、追加の考慮事項があります。詳細については、「the section called “IAM アイデンティティセンターから外部 IdP への変更”」を参照してください。

ステップ 1: Google Workspace: SAML アプリケーションを設定する

1. スーパー管理者権限を持つアカウントを使用して [Google 管理コンソール] にサインインします。
2. [Google 管理コンソール] の左側のナビゲーションパネルで、[アプリ] を選択してから、[ウェブとモバイルアプリ] を選択します。
3. [アプリの追加] ドロップダウンリストで、[アプリの検索] を選択します。
4. 検索ボックスに [Amazon Web Services] と入力し、リストから [Amazon Web Services (SAML)] アプリを選択します。

5. [Google Identity Provider の詳細 - Amazon Web Services] ページで、次のいずれかを実行できます。

   a. IdP メタデータをダウンロードします。

   b. SSO URL、エンティティ ID URL、および証明書情報をコピーします。

   ステップ 2 では、XML ファイルまたは URL 情報が必要です。

6. Google 管理者コンソールの次のステップに進む前に、このページを開いたままにして、IAM アイデンティティセンターコンソールに移動します。

ステップ 2: IAM アイデンティティセンターおよび Google Workspace : IAM アイデンティティセンターの ID ソースを変更し、Google Workspace を SAML ID プロバイダーとして設定する

1. 管理者権限を持つロールを使用して IAM アイデンティティセンターコンソールにサインインします。
2. 左側のナビゲーションペインの [設定] を選択します。
3. [設定] ページで [アクション] タブを選択し、[ID ソースを変更] を選択します。

   - IAM アイデンティティセンターをまだ有効化していない場合、詳細については「IAM Identity Center を有効にする」を参照してください。IAM アイデンティティセンターを初めて有効にしてアクセスすると、[ダッシュボード] が表示され、[ID ソースを選択] を選択できます。

4. [ID ソースを選択] ページで [外部 ID プロバイダー] を選択したら、[次へ] を選択します。
5. [外部 ID プロバイダーの設定] ページが開きます。このページとステップ 1 の Google Workspace ページを完了するには、以下を完了する必要があります。

   - IAM アイデンティティセンターコンソールの [Identity Provider メタデータ]セクションで、次のいずれかを実行する必要があります。

     i. IAM アイデンティティセンターコンソールで [IdP SAML メタデータ] として [Google SAML メタデータ] をアップロードします。

     ii. [Google SSO URL] をコピーして [IdP サインイン URL] フィールドに貼り付け、[Google 発行者 URL] を [IdP 発行者 URL] フィールドに貼り付け、Google 証明書を [IdP 証明書] としてアップロードします。

6. [IAM Identity Center] コンソールの [ID プロバイダーメタデータ] セクションで Google メタデータを指定した後、[サービスプロバイダーのメタデータ] で [デフォルト IPv4] または [デュアルスタック] を選択します。AWS アクセスポータル URL をカスタマイズした場合は、[デフォルト IPv4] を選択します。[IAM アイデンティティアサーションコンシューマーサービス (ACS) URL] と [IAM Identity Center 発行者 URL] をコピーします。次の手順で Google 管理者コンソールの設定を完了するには、これらの URL が必要です。ACS URL の詳細については、「プライマリおよび追加の AWS リージョンの ACS エンドポイント」を参照してください。
7. IAM アイデンティティセンターコンソールでページを開いたままにして、Google 管理者コンソールに戻ります。[Amazon Web Services - サービスプロバイダーの詳細] ページが開いているはずです。[Continue] (続行) をクリックします。
8. [サービスプロバイダーの詳細] ページで、[ACS URL] と [エンティティ ID] の値を入力します。これらの値は前のステップでメモしたもので、IAM アイデンティティセンターコンソールで確認できます。
   - [IAM アイデンティティセンターAssertion Consumer Service (ACS) URL] を [ACS URL] フィールドに貼り付けます。
   - [IAM アイデンティティセンター発行者 URL] を[エンティティ ID] フィールドに貼り付けます。
9. [サービスプロバイダーの詳細] ページで、[名前 ID] のフィールドに次のように入力します。
   - [名前 ID 形式] で、[E メール] を選択します。
   - [名前 ID] で、[基本情報] > [プライマリ E メールアドレス] を選択します。
10. [続行] をクリックしてください。
11. [属性マッピング] ページの [属性] で、[マッピングの追加] を選択後、[Google Directory 属性] で次のフィールドを設定します。
    - `https://aws.amazon.com/SAML/Attributes/RoleSessionName` [アプリ属性] については、[Google Directory 属性] から[基本情報、プライマリ E メール] フィールドを選択します。
    - `https://aws.amazon.com/SAML/Attributes/Role` [アプリ属性] については、任意の[Google Directory 属性] を選択します。Google Directory 属性は、[部門] である可能性があります。
12. [終了] を選択します

13. IAM アイデンティティセンターコンソールに戻り、[次へ] を選択します。[レビューと確定] ページで情報を確認し、表示されたスペースに [ACCEPT] と入力します。[IDソースの変更] を選択します。

これで、Google Workspace で Amazon Web Services アプリを有効化して、ユーザーを IAM アイデンティティセンターにプロビジョニングする準備ができました。

ステップ 3: Google Workspace: アプリを有効にする

1. Google 管理者コンソールに戻り、[アプリ] と [Web およびモバイルアプリ] の下にある AWS IAM アイデンティティセンター アプリケーションを確認します。
2. [ユーザーアクセス] の横にある [ユーザーアクセス] パネルで、下矢印を選択して [ユーザーアクセス] を展開し、[サービスのステータス] パネルを表示します。
3. [サービスのステータス] パネルで [全員オン] を選択し、次に [保存] を選択します。

> **Note**
>
> 最小特権の原則を維持するために、このチュートリアルの完了後、[サービスのステータス] を [全員オフ] に変更することをお勧めします。AWS にアクセスする必要のあるユーザーのみに対して、このサービスを有効にしてください。Google Workspace グループまたは組織単位を使用して、ユーザーの特定のサブセットへのアクセス権をユーザーに付与できます。

ステップ 4: IAM Identity Center: IAM アイデンティティセンターの自動プロビジョニングを設定する

1. IAM アイデンティティセンターコンソールに戻ります。
2. [設定] ページで、[自動プロビジョニング] 情報ボックスを探し、[有効化] を選択します。これにより、すぐに IAM アイデンティティセンターの自動プロビジョニングが有効になり、必要なエンドポイントとアクセストークンの情報が表示されます。
3. [インバウンド自動プロビジョニング] ダイアログボックスで、以下のオプションの値をそれぞれコピーします。このチュートリアルのステップ 5 では、Google Workspace でこれらの値を入力して自動プロビジョニングを設定します。

    a. SCIM エンドポイント — 例:

- IPv4https://scim.*Region*.amazonaws.com/*11111111111-2222-3333-4444-555555555555*/scim/v2
- デュアルスタックhttps://scim.*Region*.api.aws/*11111111111-2222-3333-4444-555555555555*/scim/v2

b. [アクセストークン] - [トークンを表示] を選択して値をコピーします。

> **Warning**
>
> SCIM エンドポイントとアクセストークンを取得できるタイミングは、この時のみです。先に進む前に、これらの値をコピーしておいてください。

4. [閉じる] を選択してください。

IAM アイデンティティセンターコンソールでプロビジョニングを設定したので、次のステップでは、Google Workspace で自動プロビジョニングを設定します。

ステップ 5: Google Workspace: 自動プロビジョニングを設定する

1. Google 管理者コンソールに戻り、[アプリ] と [Web およびモバイルアプリ] の下にある AWS IAM アイデンティティセンター アプリケーションを確認します。[自動プロビジョニング] セクションで、[自動プロビジョニングの設定] を選択します。
2. 前の手順で、IAM アイデンティティセンターコンソールで [アクセストークン] の値をコピーしました。その値を [アクセストークン] フィールドに貼り付け、[続行] を選択します。また、前の手順で、IAM アイデンティティセンターコンソールで [SCIM エンドポイント] の値をコピーしました。その値を [エンドポイント URL] フィールドに貼り付け、[続行] を選択します。
3. すべての必須の IAM アイデンティティセンター属性 (* の付いた属性) が Google Cloud Directory 属性にマップされていることを確認します。そうでない場合は、下矢印を選択して適切な属性にマップします。[続行] をクリックしてください。
4. [プロビジョニング範囲] セクションでは、Amazon Web Services アプリへのアクセスを付与する Google Workspace ディレクトリを含むグループを選択できます。このステップをスキップして [続行] を選択します。

5. [プロビジョニング解除] セクションでは、ユーザーのアクセス権取り消しにつながるさまざまなイベントへの対応方法を選択できます。状況ごとに、プロビジョニング解除を開始するまでの時間を指定できます。

   - 24 時間以内
   - 1 日後
   - 7 日後
   - 30 日後

   それぞれの状況には、アカウントのアクセスを一時停止するタイミングとアカウントを削除するタイミングがあります。

   > **Tip**
   >
   > ユーザーのアカウントを削除するまでの時間は、必ずユーザーのアカウントを停止するよりも長く設定してください。

6. [Finish] を選択してください。Amazon Web Services アプリページに戻ります。
7. [自動プロビジョニング] セクションで、トグルスイッチを操作して [非アクティブ] から [アクティブ] に変更します。

   > **Note**
   >
   > IAM Identity Center がユーザーに対して有効になっていない場合、アクティベーションスライダーは無効になります。[ユーザーアクセス] を選択し、アプリをオンにしてスライダーを有効にします。

8. 確認ダイアログボックスで [オンにする] をクリックします。
9. ユーザーが IAM Identity Center と正常に同期されたことを確認するには、IAM Identity Center コンソールに戻り、[ユーザー] を選択します。[ユーザー] ページには、SCIM によって作成された Google Workspace ディレクトリのユーザーが一覧表示されます。ユーザーがまだリストに表示されていない場合は、プロビジョニングがまだ進行中である可能性があります。プロビジョニングには最長で 24 時間かかることがありますが、ほとんどの場合、数分以内に完了します。ブラウザウィンドウは数分おきに更新してください。

   ユーザーを選択し、その詳細を確認します。表示される情報が Google Workspace ディレクトリ内の情報と一致しているか確認すること。

お疲れ様でした。

Google Workspace と AWS の間の SAML 接続が正常にセットアップされ、自動プロビジョニングが機能していることが確認できました。[IAM Identity Center] でこれらのユーザーをアカウントおよびアプリケーションに割り当てることができるようになりました。このチュートリアルでは、次のステップで、管理アカウントへの管理アクセス許可を付与して、ユーザーの 1 人を IAM アイデンティティセンター管理者として指定しましょう。

アクセスコントロールの属性を渡す - オプション

IAM Identity Center の アクセスコントロールの属性 機能をオプションで使用して、Name 属性を `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` に設定した `Attribute` 要素を渡すことができます。この要素を使用すると、SAML アサーションでセッションタグとして属性を渡すことができます。セッションタグの詳細については、「IAM ユーザーガイド」の「AWS STS でのタグ付けの規則 」を参照してください。

属性をセッションタグとして渡すには、タグの値を指定する `AttributeValue` 要素を含めます。例えば、タグのキーバリューのペア `CostCenter = blue` を渡すには、次のような属性を使用します。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

複数の属性を追加する必要がある場合は、各タグに個別の `Attribute` 要素を含めます。

AWS アカウントにアクセスを割り当てる

以下の手順は、AWS アカウントへのアクセスのみを許可する場合にのみ必要となります。これらのステップは、AWS アプリケーションへのアクセスを許可する場合には必要ありません。

> **Note**
>
> このステップを完了するには、IAM アイデンティティセンターの組織インスタンスが必要です。詳細については、「IAM アイデンティティセンターの組織インスタンスとアカウントインスタンス」を参照してください。

ステップ 1: IAM アイデンティティセンター: Google Workspace ユーザーにアカウントへのアクセスを付与する

1. IAM アイデンティティセンターコンソールに戻ります。IAM アイデンティティセンターのナビゲーションペインの [マルチアカウントのアクセス許可] で、[AWS アカウント] を選択します。
2. AWS アカウント ページの [組織構造] には、組織のルートと、その下にあるアカウントが階層内で表示されます。管理アカウントのチェックボックスをオンにし、[ユーザーまたはグループを割り当て] を選択します。
3. [ユーザーとグループを割り当てる] のワークフローが表示されます。これは、3 つのステップから構成されています。

   a. [ステップ 1: ユーザーとグループの選択] では、管理者の職務を実行するユーザーを選択します。次に、[次へ] を選択します。

   b. [ステップ 2: アクセス許可セットの選択] では、[許可セットを作成] を選択します。新しいタブが開き、アクセス許可セットを作成するための 3 つのサブステップが順を追って表示されます。

      i. [ステップ 1: 許可セットタイプを選択] では、以下を完了します。

         - [許可セットのタイプ] で、[事前定義された許可セット] を選択します。
         - [事前定義された許可セットのポリシー] で [AdministratorAccess] を選択します。

         [次へ] を選択します。

      ii. [ステップ 2: 許可セットの詳細を指定] では、デフォルト設定のままで、[次へ] を選択します。

         デフォルト設定では、*AdministratorAccess* という名前の許可セットが作成され、セッション期間は 1 時間に設定されます。

iii. [ステップ 3: 確認して作成] では、[許可セットのタイプ] が AWS 管理ポリシー [AdministratorAccess] を使用していることを確認します。[作成] を選択します。[アクセス許可セット] ページに、アクセス許可セットが作成されたことを知らせる通知が表示されます。この時点で、ウェブブラウザでこのタブを閉じてもかまいません。

iv. [ユーザーとグループを割り当てる] ブラウザタブでは、[ステップ 2: 許可セットを選択] でアクセス許可セットの作成ワークフローを開始した状態のままになっています。

v. [アクセス許可セット] 領域で、[更新] ボタンを選択します。作成した *AdministratorAccess* 許可セットがリストに表示されます。そのアクセス許可セットのチェックボックスを選択したら、[次へ] を選択します。

c. [ステップ 3: 確認と送信] では、選択したユーザーとアクセス許可セットを確認し、[送信] を選択します。

ページが更新され、AWS アカウント が設定中であることを示すメッセージが表示されます。プロセスが完了するまで待ちます。

AWS アカウント ページに戻ります。AWS アカウント が再プロビジョニングされ、更新されたアクセス許可セットが適用されたことを知らせる通知メッセージが表示されます。ユーザーはサインインすると、*[AdministratorAccess]* ロールを選択できます。

> **Note**
>
> Google Workspace からの SCIM 自動同期は、ユーザーのプロビジョニングのみをサポートしています。現在、自動グループプロビジョニングはサポートされていません。AWS マネジメントコンソール を使用して Google Workspace ユーザーのグループを作成することはできません。ユーザーをプロビジョニングした後、AWS CLI ID ストアの [create-group] コマンドまたは IAM API の [CreateGroup] を使用してグループを作成できます。

ステップ 2: Google Workspace: Google Workspace ユーザーの AWS リソースへのアクセスを確認する

1. テストユーザーアカウントを使用して Google にサインインします。Google Workspace にユーザーを追加する方法については、「Google Workspace ドキュメント」を参照してください。
2. Google apps ランチャー (ワッフル) アイコンを選択します。

3. カスタム Google Workspace アプリが置かれているアプリケーションリストの下部にスクロールします。Amazon Web Services アプリが表示されます。
4. Amazon Web Services アプリを選択します。AWS アクセスポータルにサインインすると、AWS アカウントアイコンが表示されます。そのアイコンを展開すると、ユーザーがアクセスできる AWS アカウント のリストが表示されます。このチュートリアルでは 1 つのアカウントしか使用していなかったため、アイコンを展開しても 1 つのアカウントしか表示されません。
5. アカウントを選択すると、そのユーザーが利用可能なアクセス許可セットが表示されます。このチュートリアルでは、AdministratorAccess 許可セットを作成しました。
6. アクセス許可セットの横には、その許可セットで利用できるアクセスの種類を示すリンクがあります。アクセス許可セットを作成したときに、管理コンソールとプログラムによるアクセスの両方を有効にするように指定したので、これら 2 つのオプションが表示されます。[管理コンソール] を選択して AWS マネジメントコンソールを開きます。
7. ユーザーはコンソールにサインインしています。

次のステップ

Google Workspace を ID プロバイダーとして設定し、IAM アイデンティティセンターにユーザーをプロビジョニングしたので、次のことが可能になります。

- AWS CLI ID ストアの [create-group] コマンドまたは、IAM API の [CreateGroup] を使用してユーザー用のグループを作成します。

  グループは、AWS アカウント やアプリケーションへのアクセスを割り当てる際に便利です。各ユーザーを個別に割り当てるのではなく、グループに権限を与えます。その後、グループにユーザーを追加したり削除したりすると、そのユーザーはグループに割り当てられたアカウントやアプリケーションへのアクセス権を動的に得たり、失ったりします。
- 職務に基づいてアクセス許可を設定します。「アクセス許可セットの作成」を参照してください。

  アクセス権限セットは、ユーザーおよびグループが持つこの AWS アカウント アカウントに対するアクセスのレベルを定義します。権限セットは IAM Identity Center に保存され、1 つまたは複数の AWS アカウント にプロビジョニングできます。複数のアクセス権限セットを 1 人のユーザーに割り当てることができます。

> **Note**
>
> IAM アイデンティティセンターの管理者として、古い IdP 証明書を新しい証明書に置き換える必要がある場合があります。例えば、IdP 証明書の有効期限が近づいている場合は、証明書を交換する必要があります。古い証明書を新しい証明書に置き換えるプロセスは、証明書のローテーションと呼ばれています。Google Workspace については、SAML 証明書の管理方法を必ず確認してください。

トラブルシューティング

Google Workspace を使用した一般的な SCIM および SAML のトラブルシューティングについては、以下のセクションを参照してください。

- 特定のユーザーが、外部の SCIM プロバイダーからの IAM Identity Center に同期できません
- IAM Identity Center によって作成された SAML アサーションの内容に関する問題
- 外部 ID プロバイダーを使用してユーザーまたはグループをプロビジョニングする際の重複ユーザーまたはグループのエラー
- Google Workspace に関するトラブルシューティングについては、Google Workspace ドキュメントを参照してください。

AWS を使用する際のトラブルシューティングに役立つリソースを以下に示します。

- AWS re:Post — 問題のトラブルシューティングに役立つ FAQ やその他のリソースへのリンクを検索できます。
- AWS サポート - テクニカルサポートを受ける

IAM アイデンティティセンターを使用して JumpCloud ディレクトリプラットフォームに接続する

IAM Identity Center は、 JumpCloud ディレクトリプラットフォームから IAM Identity Center へのユーザー情報の自動プロビジョニング (同期) をサポートします。このプロビジョニングでは、Security Assertion Markup Language (SAML) 2.0 プロトコルを使用します。詳細については、「外部 ID プロバイダーで SAML および SCIM ID フェデレーションを使用する」を参照してください。

この接続を JumpCloud で設定するには、IAM Identity Center SCIM エンドポイントとアクセストークンを使用します。SCIM 同期を設定すると、JumpCloud のユーザー属性と IAM Identity Center の名前付き属性のマッピングが作成されます。これにより、IAM Identity Center と JumpCloud の間で、期待される属性が一致します。

このガイドは、2021 年 6 月時点の JumpCloud に基づきます。新しいバージョンでは、手順が異なる場合があります。このガイドには、SAML によるユーザー認証の設定に関するいくつかの注意事項が記載されています。

次のステップでは、SCIM プロトコルを使用して、JumpCloud から IAM Identity Center へのユーザーとグループの自動プロビジョニングを有効にする方法を説明します。

> **Note**
>
> SCIM のデプロイを開始する前に、まず 自動プロビジョニングを使用する際の注意事項 を確認することをお勧めします。そして、次のセクションで残りの注意事項を確認します。

トピック

- 前提条件
- SCIM に関する注意事項
- ステップ 1: IAM Identity Center でプロビジョニングを有効にする
- ステップ 2: JumpCloud でプロビジョニングを設定する
- (オプション) ステップ 3: IAM Identity Center でのアクセスコントロールのために JumpCloud でユーザー属性を設定する
- (オプション) アクセスコントロールの属性を渡す

前提条件

開始する前に、以下の準備が必要です。

- JumpCloud のサブスクリプションまたは無料トライアル。無料トライアルにサインアップするには、JumpCloud にアクセスしてください。
- IAM Identity Center 対応アカウント (無料)。詳細については、「IAM Identity Center の有効化」を参照してください。
- 「JumpCloudIAM ID Centerのドキュメント」で説明されている、JumpCloud アカウントから IAM アイデンティティセンターへの SAML 接続。

- IAM Identity Center を追加リージョンにレプリケートした場合は、ID プロバイダーの設定を更新して、AWS マネージドアプリケーションへのアクセスと、それらのリージョンから AWS アカウント へのアクセスを有効にする必要があります。詳細については、以下を参照してください。the section called “手順 3 (外部 ID プロバイダーのみ): 外部 IdP 設定を更新する”詳細については、JumpCloud のドキュメントを参照してください。
- IAM Identity Center コネクターを、AWS アカウントへのアクセスを許可するグループに関連付けます。

SCIM に関する注意事項

IAM Identity Center に JumpCloud のフェデレーションを使用する場合の注意事項を以下に示します。

- JumpCloud の AWS シングルサインオンコネクターに関連するグループのみが SCIM を介して同期されます。
- 同期できる電話番号属性は 1 つだけです。デフォルトは「仕事用の電話」です。
- JumpCloud ディレクトリのユーザーは、SCIM 経由で IAM Identity Center に同期されるように姓名が設定されている必要があります。
- ユーザーが IAM Identity Center で無効化されていても、JumpCloud で有効化されていれば、属性は引き続き同期されます。
- コネクターの [Enable management of User Groups and Group membership] (ユーザーグループおよびグループメンバーシップの管理を有効にする) のチェックを外すことで、ユーザー情報だけの SCIM 同期を有効にすることができます。

ステップ 1: IAM Identity Center でプロビジョニングを有効にする

この最初のステップでは、IAM Identity Center コンソールを使用して、自動プロビジョニングを有効にします。

IAM アイデンティティセンターで自動プロビジョニングを有効にするには

1. 前提条件が整ったら、IAM アイデンティティセンターコンソールを開きます。
2. 左側のナビゲーションペインの [設定] を選択します。
3. [設定] ページで、[自動プロビジョニング] 情報ボックスを探し、[有効化] を選択します。これにより、すぐに IAM アイデンティティセンターの自動プロビジョニングが有効になり、必要なエンドポイントとアクセストークンの情報が表示されます。

4. [インバウンド自動プロビジョニング] ダイアログボックスで、SCIM エンドポイントとアクセストークンをコピーします。これらは、後で IdP でプロビジョニングを設定する際に貼り付ける必要があります。

   a. [SCIM エンドポイント] - 例えば https://scim.*us-east-2*.amazonaws.com/*11111111111-2222-3333-4444-555555555555*/scim/v2

   b. [アクセストークン] - [トークンを表示] を選択して値をコピーします。

   > **Warning**
   >
   > SCIM エンドポイントとアクセストークンを取得できるタイミングは、この時のみです。先に進む前に、これらの値をコピーしておいてください。このチュートリアルの後半で、お使いの IdP 上でこれらの値を入力して自動プロビジョニングを設定します。

5. [閉じる] を選択してください。

IAM Identity Center でプロビジョニングを設定したので、JumpCloud IAM Identity Center を使用して残りのタスクを完了する必要があります。これらのステップについて、次の手順で説明します。

ステップ 2: JumpCloud でプロビジョニングを設定する

JumpCloud IAM ID センターコネクタで以下の手順を実行して、IAM ID センターによるプロビジョニングを有効にします。この手順では、 JumpCloud IAM Identity Center が既に JumpCloud 管理者ポータルとグループに追加されていることを前提としています。まだ実行していない場合は、「前提条件」を参照してから、この手順を実行して SCIM プロビジョニングを設定してください。

JumpCloud でプロビジョニングを設定するには

1. JumpCloud 用 SAML 設定の一部としてインストールした JumpCloud IAM Identity Center コネクタを開きます([ユーザー認証] > [IAM Identity Center])。「前提条件」を参照してください。
2. [IAM ID センター] コネクタを選択し、3 つ目のタブ [ID 管理] を選択します。
3. グループを SCIM 同期させたい場合は、[Enable management of User Groups and Group membership in this application] (このアプリケーションでのユーザーグループとグループメンバーシップの管理を有効にする) にチェックを入れます。
4. [Configure] (構成) をクリックします。
5. 前の手順で、IAM Identity Center から [SCIM エンドポイント] の値をコピーしました。その値を JumpCloud IAM Identity Center コネクターの [ベース URL] フィールドに貼り付けます。

6. 前の手順で、IAM Identity Center の [アクセストークン] の値をコピーしました。その値を JumpCloud IAM Identity Center コネクターの [トークンキー] フィールドに貼り付けます。
7. [Activate] (有効化) をクリックすると、設定が適用されます。
8. [Single Sign-On] (Single Sign-On) の横にある緑色のインジケータが有効になっていることを確認してください。
9. 4 つ目のタブ [ユーザーグループ] に移動し、SCIM でプロビジョニングしたいグループにチェックを入れます。
10. 完了したら、下部の [Save] (保存) をクリックします。
11. ユーザーが IAM Identity Center に正常に同期されたことを確認するには、IAM Identity Center コンソールに戻り、[ユーザー] を選択します。 JumpCloud から同期されたユーザーは、[ユーザー] ページに表示されます。これらのユーザーは、IAM Identity Center でアカウントに割り当てられるようになりました。

(オプション) ステップ 3: IAM Identity Center でのアクセスコントロールのために JumpCloud でユーザー属性を設定する

これは、AWS リソースへのアクセスを管理するために IAM Identity Center の属性設定を選択した場合の JumpCloud のオプション手順です。JumpCloud で定義した属性は、SAML アサーションで IAM Identity Center に渡されます。その後、IAM Identity Center でアクセス権限セットを作成し、JumpCloud から渡された属性に基づいてアクセスを管理します。

この手順を始める前に、最初に [Attributes for access control] (アクセスコントロールのための属性) 機能を有効にしておく必要があります。これを行う方法については、「Enable and configure attributes for access control」(アクセスコントロールの属性を有効にし、設定する) を参照してください。

IAM Identity Center でのアクセスコントロールに使用される JumpCloud の属性の有効化と設定

1. JumpCloud 用 SAML 設定の一部としてインストールした JumpCloud IAM Identity Center コネクタを開きます([ユーザー認証] > [IAM Identity Center])。
2. IAM Identity Center コネクターを選択します。次に、2 つ目のタブ [IAM Identity Center] を選択します。
3. このタブの下部には、[ユーザー属性マッピング] があり、[A新規属性の追加] を選択して、以下の操作を行います。これらの手順は、IAM Identity Center でのアクセスコントロールに使用するために追加する各属性に行う必要があります。

a. [サービス提供属性] フィールドには `https://aws.amazon.com/SAML/Attributes/AccessControl:` **`AttributeName`**`.` を入力し、 **`AttributeName`** は IAM Identity Center で想定している属性名に置き換えます。例えば、 `https://aws.amazon.com/SAML/Attributes/AccessControl:` **`Email`** です。

b. [JumpCloud 属性名] フィールドで、JumpCloud ディレクトリからユーザー属性を選択します。例えば、E メール (仕事用)などです。

4. [保存] を選択します。

(オプション) アクセスコントロールの属性を渡す

IAM Identity Center の アクセスコントロールの属性 機能をオプションで使用して、`Name` 属性を `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`** に設定した `Attribute` 要素を渡すことができます。この要素を使用すると、SAML アサーションでセッションタグとして属性を渡すことができます。セッションタグの詳細については、「IAM ユーザーガイド」の「AWS STS でのタグ付けの規則 」を参照してください。

属性をセッションタグとして渡すには、タグの値を指定する `AttributeValue` 要素を含めます。例えば、タグのキーバリューのペア `CostCenter = blue` を渡すには、次のような属性を使用します。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

複数の属性を追加する必要がある場合は、各タグに個別の `Attribute` 要素を含めます。

Microsoft Entra ID および IAM アイデンティティセンターによる SAML と SCIM の設定

AWS IAM アイデンティティセンター は、Security Assertion Markup Language (SAML) 2.0 との統合および、クロスドメイン ID 管理システム (SCIM) 2.0 プロトコルによる Microsoft Entra ID (旧称 Azure Active Directory または Azure AD) から IAM アイデンティティセンターへのユーザーとグルー

プの情報の自動プロビジョニング (同期) をサポートしています。詳細については、「外部 ID プロバイダーで SAML および SCIM ID フェデレーションを使用する」を参照してください。

目的

このチュートリアルでは、テストラボをセットアップし、Microsoft Entra ID と IAM アイデンティティセンター間の SAML 接続と SCIM プロビジョニングを設定します。最初の準備ステップでは、両方向の SAML 接続をテストするのに使用する Microsoft Entra ID と IAM アイデンティティセンターの両方にテストユーザー (Nikki Wolf) を作成します。後で SCIM の手順の一環として、別のテストユーザー (Richard Roe) を作成して、Microsoft Entra ID の新しい属性が想定どおりに IAM アイデンティティセンターと同期されていることを確認します。

前提条件

このチュートリアルを開始する前に、まず以下を設定する必要があります。

- Microsoft Entra ID テナント。詳細については、Microsoft ドキュメントの「Quickstart: Set up a tenant」を参照してください。
- AWS IAM アイデンティティセンター が有効なアカウント。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「 IAM アイデンティティセンターを有効にする」を参照してください。

考慮事項

以下は、SCIM v2 プロトコルを使用して、本番環境内で IAM アイデンティティセンターを使用した自動プロビジョニングを実装するための計画に影響を与える場合がある Microsoft Entra ID に関する重要な考慮事項です。

自動プロビジョニング

SCIM のデプロイを開始する前に、まず 自動プロビジョニングを使用する際の注意事項 を確認することをお勧めします。

アクセスコントロールの属性

アクセス制御の属性は、ID ソース内の誰が AWS リソースにアクセスできるかを決定するアクセス許可ポリシーで使用されます。Microsoft Entra ID のユーザーから属性を削除しても、IAM アイデンティティセンターの対応するユーザーからはその属性は削除されません。これは、Microsoft Entra ID の既知の制限事項です。ユーザーの属性が異なる (空でない) 値に変更された場合、その変更は IAM Identity Center に同期されます。

ネストされたグループ

Microsoft Entra ID ユーザープロビジョニングサービスは、ネストされたグループのユーザーを読み取ったりプロビジョニングしたりすることはできません。明示的に割り当てられたグループの直接のメンバであるユーザーのみが、読み取りとプロビジョニングを行うことができます。Microsoft Entra ID は、間接的に割り当てられたユーザまたはグループ (直接割り当てられたグループのメンバであるユーザまたはグループ) のグループ・メンバシップを再帰的に解凍することはありません。詳細については、「Microsoft ドキュメント」の「割り当てベースのスコープ」を参照してください。または、IAM アイデンティティセンターで設定可能な AD Sync を使用して、Active Directory グループを IAM アイデンティティセンターと統合できます。

動的グループ

Microsoft Entra ID ユーザープロビジョニングサービスは、「動的グループ」のユーザーを読み取ってプロビジョニングできます。動的グループを使用する場合のユーザーとグループの構造と IAM Identity Center での表示方法を示す例については、以下を参照してください。これらのユーザーとグループは SCIM 経由で Microsoft Entra ID から IAM Identity Center にプロビジョニングされました。

たとえば、動的グループの Microsoft Entra ID 構造が以下のような場合：

1. メンバー ua1、ua2 を持つグループ A
2. メンバー ub1 を持つグループ B
3. メンバー uc1 を持つグループ C
4. グループ K (グループ A、B、C のメンバーを含むルールを持つ)
5. グループ L (グループ B と C のメンバーを含むルールを持つ)

ユーザとグループ情報が Microsoft Entra ID から SCIM を介して IAM Identity Center にプロビジョニングされた後、構造は以下のようになります。

1. メンバー ua1、ua2 を持つグループ A
2. メンバー ub1 を持つグループ B
3. メンバー uc1 を持つグループ C
4. メンバー ua1、ua2、ub1、uc1 を含むグループ K
5. メンバー ub1、uc1 を持つグループ L

動的グループを使用して自動プロビジョニングを設定する場合、次の考慮事項に留意してください。

- 動的グループにはネストされたグループを含めることができます。ただし、Microsoft Entra ID プロビジョニングサービスはネストされたグループをフラット化しません。たとえば、Microsoft Entra ID 動的グループの構造が以下のような場合：
  - グループ A はグループ B の親です。
  - グループ A には ua1 がメンバーとしています。
  - グループ B には ub1 がメンバーとしています。

グループ A を含む動的グループには、グループ A の直接のメンバー (つまり ua1) のみが含まれます。グループ B のメンバーは再帰的に含まれません。

- 動的グループには他の動的グループを含めることはできません。詳細については、Microsoft ドキュメントの「プレビューに関する制限」を参照してください。

ステップ 1: Microsoft テナントを準備する

このステップでは、AWS IAM アイデンティティセンター エンタープライズアプリケーションをインストールして構成し、新しく作成した Microsoft Entra ID テストユーザーにアクセス権を割り当てる方法について説明します。

Step 1.1 >

ステップ 1.1: Microsoft Entra ID で AWS IAM アイデンティティセンター エンタープライズアプリケーションを設定する

この手順では、AWS IAM アイデンティティセンター エンタープライズアプリケーションを Microsoft Entra ID にインストールします。このアプリケーションは、後で AWS との SAML 接続を設定する際に必要になります。

1. クラウドアプリケーション管理者以上の権限で、Microsoft Entra 管理センターにサインインします。
2. [ID] > [アプリケーション] > [エンタープライズアプリケーション] に移動し、[新しいアプリケーション] を選択します。
3. [Microsoft Entra ギャラリーの参照] ページで、検索ボックスに **`AWS IAM ############`** を入力します。
4. 検索結果から AWS IAM アイデンティティセンター を選択します。
5. [作成] を選択します。

Step 1.2 >

ステップ 1.2: Microsoft Entra ID でテストユーザーを作成する

Nikki Wolf は、この手順で作成する Microsoft Entra ID テストユーザーの名前です。

1. Microsoft Entra 管理センターコンソールで、[ID] > [ユーザー] > [すべてのユーザー] に移動します。
2. [新しいユーザー] を選択し、画面上部の [新しいユーザーの作成] を選択します。
3. [ユーザープリンシパル名] に **NikkiWolf** と入力し、目的のドメインと拡張子を選択します。例えば、NikkiWolf@*example.org* と入力します。
4. [表示名] に **NikkiWolf** と入力します。
5. [パスワード] に、強力なパスワードを入力するか、目のアイコンを選択して自動生成されたパスワードを表示し、表示された値をコピーするか書き留めてください。
6. [プロパティ] を選択し、[名] に **Nikki** と入力します。[姓] に、**Wolf** と入力します。
7. [レビューと作成] を選択したら、[作成] を選択します。

Step 1.3

ステップ 1.3: Nikki に AWS IAM アイデンティティセンター へのアクセス権を割り当てる前に、Nikki のエクスペリエンスをテストする

この手順では、Nikki が Microsoft マイアカウントポータルに正常にサインインできることを確認します。

1. 同じブラウザで新しいタブを開き、[マイアカウントポータル] サインインページに移動して、Nikki 向けの完全なメールアドレスを入力します。例えば、NikkiWolf@*example.org* と入力します。
2. プロンプトが表示されたら、Nikki のパスワードを入力し、[サインイン] を選択します。これが自動生成されたパスワードの場合は、パスワードを変更するように求められます。
3. [アクションが必要] ページで [後で確認する] を選択すると、追加のセキュリティメソッドの入力を求めるプロンプトは表示されなくなります。
4. [マイアカウント] ページの左側のナビゲーションペインで、[マイアプリ] を選択します。現時点では、アドイン以外のアプリが表示されていないことに注意してください。後のステップでここに表示される AWS IAM アイデンティティセンター アプリを追加します。

Step 1.4

ステップ 1.4: Microsoft Entra ID で Nikki に権限を割り当てる

Nikki が [マイアカウントポータル] に正常にアクセスできることを確認したので、次の手順に従って Nikki のユーザーを AWS IAM アイデンティティセンター アプリに割り当てます。

1. Microsoft Entra 管理センターコンソールで、[ID] > [アプリケーション] > [エンタープライズアプリケーション] に移動し、リストから AWS IAM アイデンティティセンター を選択します。
2. 左側で [ユーザーとグループ] を選択します。
3. [Add user/group] (ユーザーとグループを追加) を選択します。グループを割り当てることができないというメッセージは無視してかまいません。このチュートリアルでは、割り当てにグループを使用しません。
4. [割り当てを追加] ページの [ユーザー] で、[何も選択されていません] を選択します。
5. [NikkiWolf] を選択し、次に [選択] を選択します。
6. [Add Assignment] (割り当てを追加) ページで、[Assign] (割り当て) を選択します。これで、AWS IAM アイデンティティセンター アプリに割り当てられたユーザーのリストに NikkiWolf が表示されるようになりました。

ステップ 2: AWS アカウントを準備する

このステップでは、IAM Identity Center を使用して (許可セットにより) アクセス許可を設定する方法、対応する Nikki Wolf ユーザを手動で作成する方法、および AWS のリソースを管理するために必要な権限をそのユーザに割り当てる方法について説明します。

Step 2.1 >

ステップ 2.1: IAM Identity Center で RegionalAdmin 許可セットを作成する

このアクセス許可セットを使用して、AWS マネジメントコンソール内の [アカウント] ページからリージョンを管理するのに必要な AWS アカウント許可を Nikki に付与します。Nikki のアカウントのその他の情報を閲覧または管理するその他の権限は、デフォルトではすべて拒否されています。

1. IAM アイデンティティセンターコンソールを開きます。
2. [マルチアカウント権限] で、[権限セット] を選択します。

3. [Create permission set] (アクセス許可セットの作成) を選択します。
4. [許可セットタイプを選択] ページで [カスタム許可セット] を選択し、[次へ] を選択します。
5. [インラインポリシー] を選択して展開し、次の手順を使用してアクセス許可セットのポリシーを作成します。

   a. [新しいステートメントを追加] を選択してポリシーステートメントを作成します。

   b. [ステートメントの編集] で、リストから [アカウント] を選択し、次のチェックボックスを選択します。

      - **ListRegions**
      - **GetRegionOptStatus**
      - **DisableRegion**
      - **EnableRegion**

   c. [リソースの追加] の横にある [追加] を選択します。

   d. [リソースを追加] ページの [リソースタイプ] で、[すべてのリソース] を選択し、[リソースを追加] を選択します。ポリシーが次のようになっていることを確認します。

```
{
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "account:ListRegions",
                "account:DisableRegion",
                "account:EnableRegion",
                "account:GetRegionOptStatus"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. [次へ] を選択します。
7. [許可セットの詳細を指定] ページの [許可セット名] に **RegionalAdmin** と入力し、[次へ] を選択します。

8. [確認して作成] ページで、[作成] をクリックします。アクセス許可セットのリストに RegionalAdmin が表示されます。

Step 2.2 >

ステップ 2.2: IAM Identity Center で対応する NikkiWolf ユーザーを作成する

SAML プロトコルには IdP (Microsoft Entra ID) をクエリして IAM アイデンティティセンターで自動的にユーザーを作成するメカニズムがないため、次の手順に従って、Microsoft Entra ID の Nikki Wolfs ユーザーのコア属性をミラーリングするユーザーを IAM アイデンティティセンターに手動で作成します。

1. IAM Identity Center コンソールを開きます。
2. [ユーザー] を選択し、[ユーザーを追加] を選択して、次の情報を入力します。
   a. [ユーザー名] と [メールアドレス] の両方に、Microsoft Entra ID ユーザーの作成時に使用したのと同じ **NikkiWolf@*yourcompanydomain.extension*** を入力します。例えば、NikkiWolf@*example.org* と入力します。
   b. [メールアドレスの確認] — 前のステップで使用したメールアドレスを再入力します。
   c. [名] — **Nikki** と入力します。
   d. [姓] — **Wolf** と入力します。
   e. [表示名] — **Nikki Wolf** と入力します。
3. [次へ] を 2 回選択後、[ユーザーの追加] を選択します。
4. [Close] を選択します。

Step 2.3

ステップ 2.3: IAM Identity Center で RegionalAdmin 許可セットに Nikki を割り当てる

ここで、Nikki がリージョンを管理する AWS アカウント を特定し、AWS アクセスポータルに正常にアクセスするために必要なアクセス許可を割り当てます。

1. IAM Identity Center コンソール を開きます。
2. [マルチアカウント権限] で、[AWS アカウント] を選択します。
3. Nikki にリージョンを管理するためのアクセス権を付与するアカウント名 (例えば、*Sandbox*) の横のチェックボックスを選択し、[ユーザーとグループを割り当てる] を選択します。

4. [ユーザーとグループを割り当てる] ページで [ユーザー] タブを選択し、Nikki の横にあるボックスを探してオンにし、[次へ] を選択します。
5. Example

   <caption>On the アクセス許可セットを選択する page, choose the RegionalAdmin permission set created in Step 2.1, and then choose 次.</caption>
6. [確認と送信] ページで選択内容を確認し、[送信] を選択します。

ステップ 3: SAML 接続を設定してテストする

このステップでは、Microsoft Entra ID の AWS IAM アイデンティティセンター エンタープライズアプリケーションと IAM アイデンティティセンターの外部 IdP 設定を使用して SAML 接続を設定します。

Step 3.1 >

ステップ 3.1: IAM アイデンティティセンターから必要なサービスプロバイダーのメタデータを収集する

このステップでは、IAM アイデンティティセンターコンソール内から [ID ソースを変更] ウィザードを起動し、メタデータファイルと、次のステップで Microsoft Entra ID との接続を設定するときに入力する必要のある AWS 固有のサインイン URL を取得します。

1. [IAM アイデンティティセンターコンソール] で [設定] を選択します。
2. [設定] ページで [ID ソース] タブを選択し、[アクション] > [ID ソースを変更] を選択します。
3. [ID ソースを選択] ページで [外部 ID プロバイダー] を選択したら、[次へ] を選択します。
4. [外部 ID プロバイダーを設定] ページの [サービスプロバイダーのメタデータ] で、[デフォルト IPv4] または [デュアルスタック] を選択します。ID ソースの変更が完了したら、サービスプロバイダーのメタデータファイルをダウンロードできます。
5. 同じセクションで、[AWS アクセスポータルのサインイン URL] 値を見つけてコピーします。この値は、次のステップで求められたときに入力します。
6. このページは開いたままにして、次のステップ (**Step 3.2**) に進み、Microsoft Entra ID の AWS IAM アイデンティティセンター エンタープライズアプリケーションを設定します。後でこのページに戻り、プロセスを完了します。

Step 3.2 >

ステップ 3.2: Microsoft Entra ID の AWS IAM アイデンティティセンター エンタープライズアプリケーションを設定する

この手順では、前のステップで取得したメタデータファイルの値とサインオン URL を使用して、Microsoft 側の SAML 接続の半分を確立します。

1. Microsoft Entra 管理センターコンソールで、[ID] > [アプリケーション] > [エンタープライズアプリケーション] に移動し、[AWS IAM アイデンティティセンター] を選択します。
2. 左側で、2 を選択します。シングルサインオンをセットアップします。
3. [SAML でシングルサインオンを設定] のページで、[SAML] を選択します。更に、[メタデータファイルのアップロード] を選択し、フォルダアイコンを選択し、前のステップでダウンロードしたサービスプロバイダーのメタデータファイルを選択して、[追加] を選択します。
4. [基本的な SAML 設定] ページで、[識別子] と [返信 URL (アサーションコンシューマーサービスの URL)] の値の両方が、AWS のエンドポイントを指していることを確認します。

   - 識別子 - これは IAM Identity Center の発行者 URL です。IPv4 専用エンドポイントとデュアルスタックエンドポイントのどちらを使用するかに関係なく、同じ値が適用されます。
   - 返信 URL (アサーションコンシューマーサービス URL) - この値には、IAM Identity Center の有効なすべてのリージョンの IPv4 専用エンドポイントとデュアルスタックエンドポイントの両方が含まれます。プライマリリージョンの ACS URL をデフォルトとして使用すると、ユーザーが Microsoft Entra ID から Amazon Web Services アプリケーションを起動するときにプライマリリージョンにリダイレクトされるようになります。ACS URL の詳細については、「プライマリおよび追加の AWS リージョンの ACS エンドポイント」を参照してください。
   - (オプション) IAM Identity Center を追加リージョンにレプリケートした場合は、追加リージョンごとに Microsoft Entra ID で AWS アクセスポータルのブックマークアプリを作成することもできます。これにより、ユーザーは Microsoft Entra ID から追加リージョンの AWS アクセスポータルにアクセスできます。Microsoft Entra ID でブックマークアプリにアクセスするためのアクセス許可をユーザーに付与します。詳細については、「Microsoft Entra ID 関連ドキュメント」を参照してください。後で IAM Identity Center を追加リージョンにレプリケートする場合は、「追加リージョンにアクセスするための Microsoft Entra ID の設定」を参照して、この初期セットアップ後に追加リージョンへのアクセスを有効にする方法を確認してください。

5. [サインオン URL (オプション)] に、前のステップでコピーした AWS アクセスポータルのサインイン URL の値 (**Step 3.1**) を貼り付け、[保存] を選択したら、[X] を選択してウィンドウを閉じます。
6. AWS IAM アイデンティティセンター でシングルサインオンをテストするよう求められたら、[いいえ、後でテストします] を選択します。この検証は、後のステップで行います。
7. [SAML によるシングルサインオンの設定] ページの [SAML 証明書] セクションで、[フェデレーションメタデータ XML] の横にある [ダウンロード] を選択し、メタデータファイルをシステムに保存します。次のステップでプロンプトが表示されたら、このファイルをアップロードする必要があります。

Step 3.3 >

ステップ 3.3: AWS IAM アイデンティティセンター で Microsoft Entra ID の外部 IdP を設定する

ここで、IAM アイデンティティセンターコンソールの [ID ソースを変更] ウィザードに戻り、AWS の SAML 接続の後半を完了します。

1. IAM アイデンティティセンターコンソールで、**Step 3.1** で開いたままにしたブラウザセッションに戻ります。
2. [外部 ID プロバイダーの設定] ページの [ID プロバイダーのメタデータ] セクションの [IdP SAML メタデータ] で、[ファイルを選択] ボタンを選択し、前のステップで Microsoft Entra ID からダウンロードした ID プロバイダーのメタデータファイルを選択して、[開く] を選択します。
3. [次へ] を選択します。
4. 免責事項を読み、次に進む準備ができたら、**ACCEPT** と入力してください。
5. [ID ソースを変更] を選択して変更を適用します。

Step 3.4 >

ステップ 3.4: Nikki が AWS アクセスポータルにリダイレクトされることをテストする

この手順では、Nikki の認証情報を使用して Microsoft の [マイアカウントポータル] にサインインして SAML 接続をテストします。認証されたら、Nikki を AWS アクセスポータルにリダイレクトする AWS IAM アイデンティティセンター アプリケーションを選択します。

1. マイアカウントポータルのサインインページに移動し、Nikki の完全なメールアドレスを入力します。例えば、***NikkiWolf***@*example.org* と入力します。

2. プロンプトが表示されたら、Nikki のパスワードを入力し、[サインイン] を選択します。
3. [マイアカウント] ページの左側のナビゲーションペインで、[マイアプリ] を選択します。
4. [マイアプリ] ページで、AWS IAM アイデンティティセンター という名前のアプリを選択します。これにより、追加の認証を求めるプロンプトが表示されます。
5. Microsoft のサインインページで、NikkiWolf の認証情報を選択します。2 度目に認証を求められたら、NikkiWolf の認証情報をもう一度選択してください。これにより、AWS アクセスポータルに自動的にリダイレクトされます。

> **Tip**
>
> 正常にリダイレクトされない場合は、[**Step 3.2**] に入力した AWS アクセスポータルのサインイン URL の値がコピー元 **Step 3.1** の値と一致することを確認してください。

6. AWS アカウントディスプレイを確認します。

> **Tip**
>
> ページが空で、AWS アカウントが表示されない場合は、Nikki が [RegionalAdmin] 許可セットに正常に割り当てられているかどうかを確認してください (**Step 2.3** を参照)。

Step 3.5

ステップ 3.5: Nikki が AWS アカウント を管理するためのアクセスレベルをテストする

このステップでは、Nikki が AWS アカウント のリージョン設定を管理するためのアクセスレベルを確認します。Nikki には、[アカウント] ページからリージョンを管理するための十分な管理者権限のみを持つことが期待されています。

1. AWS アクセスポータルで、[アカウント] タブを選択してアカウントのリストを表示します。アクセス許可セットを定義したアカウントに関連付けられているアカウント名、アカウント ID、メールアドレスが表示されます。
2. アクセス許可セットを適用したアカウント名 (*Sandbox* など) を選択します (**Step 2.3** をご覧ください)。これにより、Nikki が自分のアカウントを管理するために選択できるアクセス許可セットのリストが展開されます。

3. RegionalAdmin の横にある [管理コンソール] を選択し、RegionalAdmin 許可セットで定義したロールを引き継ぎます。これにより、AWS マネジメントコンソールホームページにリダイレクトされます。
4. コンソールの右上で、アカウント名を選択してから [アカウント] を選択します。これにより、[アカウント] ページに移動します。このページの他のすべてのセクションには、これらの設定を表示または変更するのに必要なアクセス許可がないことを示すメッセージが表示されます。
5. [アカウント] ページで、 [AWS リージョン] までスクロールダウンします。テーブル内の使用可能なリージョンのチェックボックスをオンにします。Nikki には、自分のアカウントのリージョンのリストを意図したとおりに [有効化] または [無効化] するために必要なアクセス許可が付与されています。

> よくできました!
>
> ステップ 1 ~ 3 は、SAML 接続の実装とテストを正常に実行するのに役立ちました。チュートリアルを完了するには、ステップ 4 に進んで自動プロビジョニングを実装することをお勧めします。

ステップ 4: SCIM 同期を設定してテストする

このステップでは、SCIM v2.0 プロトコルを使用して Microsoft Entra ID から IAM アイデンティティセンターへのユーザー情報の自動プロビジョニング (同期) を設定します。この接続を Microsoft Entra ID IAM アイデンティティセンター用の SCIM エンドポイントと IAM アイデンティティセンターで自動作成されたベアラートークンを使用して設定します。

SCIM 同期を設定すると、Microsoft Entra ID のユーザー属性と IAM Identity Center の名前付き属性のマッピングが作成されます。これにより、IAM アイデンティティセンターと Microsoft Entra ID の間で、期待される属性が一致します。

次のステップでは、Microsoft Entra ID の IAM アイデンティティセンターアプリを使って、主に Microsoft Entra ID に設置されたユーザーの IAM アイデンティティセンターへの自動プロビジョニングを有効にする方法を説明します。

Step 4.1 >

ステップ 4.1: Microsoft Entra ID で 2 人目のテストユーザーを作成する

テスト用に、Microsoft Entra ID で新しいユーザー (Richard Roe) を作成します。後で SCIM 同期を設定したら、このユーザーとすべての関連属性が IAM アイデンティティセンターと正常に同期されたことをテストします。

1. Microsoft Entra 管理センターコンソールで、[ID] > [ユーザー] > [すべてのユーザー] に移動します。
2. [新しいユーザー] を選択し、画面上部の [新しいユーザーの作成] を選択します。
3. [ユーザープリンシパル名] に **RichRoe** と入力し、目的のドメインと拡張子を選択します。例えば、RichRoe@*example.org* と入力します。
4. [表示名] に **RichRoe** と入力します。
5. [パスワード] に、強力なパスワードを入力するか、目のアイコンを選択して自動生成されたパスワードを表示し、表示された値をコピーするか書き留めてください。
6. [プロパティ] を選択し、以下の値を指定します。
   - [名] - **Richard** と入力します。
   - [姓] - **Roe** と入力します。
   - [役職名] - **Marketing Lead** と入力します。
   - [部門] - **Sales** と入力します。
   - [従業員 ID] - **12345** と入力します。
7. [レビューと作成] を選択したら、[作成] を選択します。

Step 4.2 >

ステップ 4.2: IAM アイデンティティセンターで自動プロビジョニングを有効にする

この手順では、IAM アイデンティティセンターコンソールを使用して、ユーザーとグループの Microsoft Entra ID から IAM アイデンティティセンターへの自動プロビジョニングを有効にします。

1. [IAM アイデンティティセンターコンソール] で、左のナビゲーションペインの [設定] を選択します。
2. [設定] ページの [ID ソース] タブで、[プロビジョニング方法] が [手動] に設定されていることに注目してください。
3. [自動プロビジョニング] 情報ボックスを見つけ、[有効にする] を選択します。これにより、すぐに IAM アイデンティティセンターの自動プロビジョニングが有効になり、必要な SCIM エンドポイントとアクセストークンの情報が表示されます。

4. [インバウンド自動プロビジョニング] ダイアログボックスで、以下のオプションの値をそれぞれコピーします。これらは、次のステップで Microsoft Entra ID でプロビジョニングを設定する際に貼り付ける必要があります。

   a. SCIM エンドポイント — 例:

      - IPv4:`https://scim.aws-region.amazonaws.com/11111111111-2222-3333-4444-555555555555/scim/v2`
      - デュアルスタック: `https://scim.aws-region.api.aws/11111111111-2222-3333-4444-555555555555/scim/v2`

   b. [アクセストークン] - [トークンを表示] を選択して値をコピーします。

> **Warning**
>
> SCIM エンドポイントとアクセストークンを取得できるタイミングは、この時のみです。先に進む前に、これらの値をコピーしておいてください。

5. [閉じる] を選択してください。
6. [ID ソース] タブで、[プロビジョニング方法] が [SCIM] に設定されていることに注目してください。

Step 4.3 >

ステップ 4.3: Microsoft Entra ID の自動プロビジョニングを設定する

RichRoe テストユーザーが用意され、IAM アイデンティティセンターで SCIM を有効にしたので、Microsoft Entra ID で SCIM 同期設定の設定に進むことができます。

1. Microsoft Entra 管理センターコンソールで、[ID] > [アプリケーション] > [エンタープライズアプリケーション] に移動し、[AWS IAM アイデンティティセンター] を選択します。
2. [プロビジョニング] を選択し、[管理] で [プロビジョニング] をもう一度選択します。
3. [プロビジョニングモード] で [自動] を選択します。
4. [管理者認証情報] の [テナント URL] に、**Step 4.2** で先ほどコピーした [SCIM エンドポイント] URL 値を貼り付けます。[シークレットトークン] にアクセストークンの値を貼り付けます。

5. 接続のテストを選択します。テストした認証情報が正常に認証され、プロビジョニングが可能になったことを示すメッセージが表示されます。
6. [保存] を選択します。
7. [管理] で [ユーザーとグループ] を選択し、[ユーザー/グループの追加] を選択します。
8. [割り当てを追加] ページの [ユーザー] で、[何も選択されていません] を選択します。
9. [RichRoe] を選択後、[選択] を選択します。
10. [Add Assignment] (割り当てを追加) ページで、[Assign] (割り当て) を選択します。
11. [概要] を選択したら、[プロビジョニングの開始] を選択します。

Step 4.4

ステップ 4.4: 同期が行われたことを確認する

このセクションでは、Richard のユーザーが正常にプロビジョニングされ、すべての属性が IAM アイデンティティセンターに表示されていることを確認します。

1. IAM アイデンティティセンターコンソールで [ユーザー] をクリックします。
2. [ユーザー] ページに [RichRoe] ユーザーが表示されているはずです。[作成者] 列の値が [SCIM] に設定されていることに注意してください。
3. [RichRoe] を選択し、[プロファイル] で以下の属性が Microsoft Entra ID からコピーされていることを確認します。

   - [名]**Richard** -
   - [姓]**Roe** -
   - [部門]**Sales** -
   - 役職 - **Marketing Lead**
   - [従業員番号]**12345** -

   これで Richard のユーザーが IAM アイデンティティセンターで作成されたので、そのユーザーを任意のアクセス許可セットに割り当てて、AWS リソースに対する Richard のアクセスレベルを制御できます。例えば、以前に Nikki にリージョンを管理するためのアクセス許可 (**Step 2.3** をご覧ください) を付与するために使用した **RegionalAdmin** 許可セットを [RichRoe] に割り当てた後、**Step 3.5** で RichRoe のアクセスレベルをテストできます。

お疲れ様でした。

Microsoft と AWS 間の SAML 接続が正常に設定され、自動プロビジョニングがすべてを同期させるために機能していることが確認できました。これで、学習した内容を応用して、本番環境をよりスムーズに設定できます。

ステップ 5: ABAC を設定する - オプション

SAML と SCIM を正常に設定したので、属性ベースのアクセス制御 (ABAC) を任意で設定することができます。ABAC は、属性に基づいて権限を定義する認可戦略です。

Microsoft Entra ID では、次の 2 つの方法のいずれかを使用して、IAM アイデンティティセンターで使用するために ABAC を構成できます。

Configure user attributes in Microsoft Entra ID for access control in IAM Identity Center

IAM アイデンティティセンターでのアクセスコントロール用に Microsoft Entra ID でユーザー属性を設定する

以下の手順では、AWS リソースへのアクセスを管理するために IAM アイデンティティセンターが Microsoft Entra ID のどの属性を使用すべきかを決定します。定義されると、Microsoft Entra ID は SAML アサーションを通じてこれらの属性を IAM アイデンティティセンターに送信します。その後、IAM Identity Center で アクセス権限セットを作成します。 を行い、Microsoft Entra ID から渡された属性に基づいてアクセスを管理する必要があります。

この手順を始める前に、まず アクセスコントロールの属性 機能を有効にしておく必要があります。これを行う方法については、「アクセスコントロールのための属性の有効化と設定」を参照してください。

1. Microsoft Entra 管理センターコンソールで、[ID] > [アプリケーション] > [エンタープライズアプリケーション] に移動し、[AWS IAM アイデンティティセンター] を選択します。
2. [Single Sign-On] を選択します。
3. [属性とクレーム] セクションで、[編集] を選択します。
4. [属性とクレーム] ページで、以下を実行します。

    a. [Add new claim] (新しいクレームを追加する) を選択します。

b. [Name] (名前) に AccessControl:*AttributeName* を入力します。*AttributeName* を IAM アイデンティティセンターで想定している属性名に置き換えます。例えば、AccessControl:**Department**。

c. [名前空間] に **https://aws.amazon.com/SAML/Attributes** と入力します。

d. [出典] で、[属性] を選択します。

e. [ソースの属性] で、ドロップダウンリストを使用して、[Microsoft Entra ID ユーザー属性] を選択します。例えば、user.**department**。

5. SAML アサーションで IAM Identity Center に送信する必要のある各属性について、前のステップを繰り返します。

6. [保存] を選択します。

Configure ABAC using IAM Identity Center

IAM アイデンティティセンターを使用して ABAC を構成する

この方法では、IAM アイデンティティセンターの アクセスコントロールの属性 機能を使って、Name 属性を https://aws.amazon.com/SAML/Attributes/AccessControl:**{TagKey}** に設定した Attribute 要素を渡します。この要素を使用すると、SAML アサーションで属性をセッションタグとして渡すことができます。セッションタグの詳細については、「IAM ユーザーガイド」の「AWS STS でのタグ付けの規則 」を参照してください。

属性をセッションタグとして渡すには、タグの値を指定する AttributeValue 要素を含めます。例えば、タグのキーバリューのペア Department=billing を渡すには、次の属性を使用します。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/
AccessControl:Department">
<saml:AttributeValue>billing
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

複数の属性を追加する必要がある場合は、各タグに個別の Attribute 要素を含めます。

AWS アカウントにアクセスを割り当てる

以下の手順は、AWS アカウントへのアクセスのみを許可する場合にのみ必要となります。これらのステップは、AWS アプリケーションへのアクセスを許可する場合には必要ありません。

> **Note**
>
> このステップを完了するには、IAM アイデンティティセンターの組織インスタンスが必要です。詳細については、「IAM アイデンティティセンターの組織インスタンスとアカウントインスタンス」を参照してください。

ステップ 1: IAM アイデンティティセンター: Microsoft Entra ID ユーザーにアカウントへのアクセスを付与する

1. IAM アイデンティティセンターコンソールに戻ります。IAM アイデンティティセンターのナビゲーションペインの [マルチアカウントのアクセス許可] で、[AWS アカウント] を選択します。
2. AWS アカウント ページの [組織構造] には、組織のルートと、その下にあるアカウントが階層内で表示されます。管理アカウントのチェックボックスをオンにし、[ユーザーまたはグループを割り当て] を選択します。
3. [ユーザーとグループを割り当てる] のワークフローが表示されます。これは、3 つのステップから構成されています。

   a. [ステップ 1: ユーザーとグループの選択] では、管理者の職務を実行するユーザーを選択します。次に、[次へ] を選択します。

   b. [ステップ 2: アクセス許可セットの選択] では、[許可セットを作成] を選択します。新しいタブが開き、アクセス許可セットを作成するための 3 つのサブステップが順を追って表示されます。

      i. [ステップ 1: 許可セットタイプを選択] では、以下を完了します。

         - [許可セットのタイプ] で、[事前定義された許可セット] を選択します。
         - [事前定義された許可セットのポリシー] で [AdministratorAccess] を選択します。

         [次へ] を選択します。

      ii. [ステップ 2: 許可セットの詳細を指定] では、デフォルト設定のままで、[次へ] を選択します。

デフォルト設定では、*AdministratorAccess* という名前の許可セットが作成され、セッション期間は 1 時間に設定されます。

iii. [ステップ 3: 確認して作成] では、[許可セットのタイプ] が AWS 管理ポリシー [AdministratorAccess] を使用していることを確認します。[作成] を選択します。[アクセス許可セット] ページに、アクセス許可セットが作成されたことを知らせる通知が表示されます。この時点で、ウェブブラウザでこのタブを閉じてもかまいません。

iv. [ユーザーとグループを割り当てる] ブラウザタブでは、[ステップ 2: 許可セットを選択] でアクセス許可セットの作成ワークフローを開始した状態のままになっています。

v. [アクセス許可セット] 領域で、[更新] ボタンを選択します。作成した *AdministratorAccess* 許可セットがリストに表示されます。そのアクセス許可セットのチェックボックスを選択したら、[次へ] を選択します。

c. [ステップ 3: 確認と送信] では、選択したユーザーとアクセス許可セットを確認し、[送信] を選択します。

ページが更新され、AWS アカウント が設定中であることを示すメッセージが表示されます。プロセスが完了するまで待ちます。

AWS アカウント ページに戻ります。AWS アカウント が再プロビジョニングされ、更新されたアクセス許可セットが適用されたことを知らせる通知メッセージが表示されます。ユーザーはサインインすると、*[AdministratorAccess]* ロールを選択できます。

ステップ 2: Microsoft Entra ID: Microsoft Entra ID ユーザーの AWS リソースへのアクセスを確認する

1. Microsoft Entra ID コンソールに戻り、IAM アイデンティティセンターの SAML ベースのサインオンアプリケーションに移動します。
2. [ユーザーとグループ] を選択し、[ユーザーまたはグループの追加] を選択します。このチュートリアルで作成したユーザーをステップ 4 で Microsoft Entra ID アプリケーションに追加します。ユーザーを追加することで、ユーザーに AWS へのサインインを許可します。ステップ 4 で作成したユーザーを検索します。このステップに従った場合、**RichardRoe** になります。

- デモについては、「既存の IAM アイデンティティセンターインスタンスを Microsoft Entra ID とフェデレーションさせる」を参照してください。

IAM Identity Center の追加リージョンにアクセスするための Microsoft Entra ID の設定 - オプション

IAM Identity Center を追加リージョンにレプリケートした場合は、ID プロバイダーの設定を更新して、AWS マネージドアプリケーションへのアクセスと、追加リージョンから AWS アカウント へのアクセスを有効にする必要があります。以下のステップでは、この手順について説明します。前提条件などこのトピックの詳細については、「複数の 間で IAM アイデンティティセンターを使用する AWS リージョン」を参照してください。

1. プライマリおよび追加の AWS リージョンの ACS エンドポイント に記載されている手順に従って、IAM Identity Center コンソールから追加リージョンの ACS URL を取得します。
2. Microsoft Entra 管理センターコンソールで、[ID] > [アプリケーション] > [エンタープライズアプリケーション] に移動し、[AWS IAM アイデンティティセンター] を選択します。
3. 左側で、2 を選択します。シングルサインオンをセットアップします。
4. [SAML の基本的な設定] ページの [返信 URL (アサーションコンシューマーサービス URL)] セクションで、追加リージョンの ACS URL ごとに [返信 URL を追加] を選択します。プライマリリージョンの ACS URL をデフォルトのままにしておくと、ユーザーが Microsoft Entra ID から AWS IAM アイデンティティセンター アプリケーションを起動するときに、引き続きプライマリリージョンにリダイレクトされます。
5. ACS URL の追加が完了したら、AWS IAM アイデンティティセンター アプリケーションを保存します。
6. 追加リージョンごとに、Microsoft Entra ID で AWS アクセスポータルのブックマークアプリを作成できます。これにより、ユーザーは Microsoft Entra ID から追加リージョンの AWS アクセスポータルにアクセスできます。Microsoft Entra ID でブックマークアプリにアクセスするためのアクセス許可をユーザーに付与します。詳細については、「Microsoft Entra ID 関連ドキュメント」を参照してください。
7. 追加リージョンごとに、AWS アクセスポータルにサインインできることを確認します。AWS アクセスポータル URL に移動するか、Microsoft Entra ID からブックマークアプリを起動します。

トラブルシューティング

Microsoft Entra ID を使用した一般的な SCIM および SAML のトラブルシューティングについては、以下のセクションを参照してください。

- Microsoft Entra ID と IAM アイデンティティセンターの同期に関する問題

- 特定のユーザーが、外部の SCIM プロバイダーからの IAM Identity Center に同期できません
- IAM Identity Center によって作成された SAML アサーションの内容に関する問題
- 外部 ID プロバイダーを使用してユーザーまたはグループをプロビジョニングする際の重複ユーザーまたはグループのエラー
- その他のリソース

Microsoft Entra ID と IAM アイデンティティセンターの同期に関する問題

Microsoft Entra ID ユーザーが IAM アイデンティティセンターと同期しないという問題が発生している場合は、IAM アイデンティティセンターに新しいユーザーを追加する際に IAM アイデンティティセンターがフラグを立てた構文の問題が原因である可能性があります。これは、`'Export'` などの失敗したイベントに関する Microsoft Entra ID 監査ログで確認できます。このイベントの Status Reason (ステータス理由) には、次のように記述されます。

```
{"schema":["urn:ietf:params:scim:api:messages:2.0:Error"],"detail":"Request is
 unparsable, syntactically incorrect, or violates schema.","status":"400"}
```

また、失敗したイベントの AWS CloudTrail を確認することもできます。これは、CloudTrail の Event History (イベントの履歴) コンソールで以下のフィルターを使って検索できます。

```
"eventName":"CreateUser"
```

CloudTrail イベントのエラーには以下のように記載されます。

```
"errorCode": "ValidationException",
        "errorMessage": "Currently list attributes only allow single item“
```

最終的に、この例外は、Microsoft Entra ID から渡された値の中に予想よりも多い値が含まれていたことを示しています。問題を解決するには、Microsoft Entra ID のユーザー属性を再確認し、重複した値が含まれていないかをチェックしてください。重複した値の一般的な例の一つは、携帯電話、仕事、FAX などの連絡先に複数の値が存在することです。別々の値ではありますが、これらはすべて 1 つの親属性 phoneNumbers として IAM Identity Center に渡されます。

一般的な SCIM のトラブルシューティングのヒントについては、「Troubleshooting」を参照してください。

Microsoft Entra ID ゲストアカウントの同期

Microsoft Entra ID ゲストユーザーを IAM アイデンティティセンターに同期する場合は、次の手順を参照してください。

Microsoft Entra ID ゲストユーザーの E メールは Microsoft Entra ID ユーザーとは異なります。この差異によって、Microsoft Entra ID ゲストユーザーを IAM アイデンティティセンターと同期しようとすると問題が発生します。例えば、ゲストユーザーの場合は、次の E メールアドレスを参照してください。

`exampleuser_domain.com#EXT#@domain.onmicrosoft.com.`

IAM アイデンティティセンターは、ユーザーのメールアドレスに *#EXT#@####* 形式が含まれないことを想定しています。

1. Microsoft Entra 管理センターにサインインし、[ID] > [アプリケーション] > [エンタープライズアプリケーション] に移動し、[AWS IAM アイデンティティセンター] を選択します。
2. 左側ペインの [シングルサインオン] タブに移動します。
3. [ユーザー属性とクレーム] の横にある [編集] を選択します。
4. [必須クレーム] に続く [一意のユーザー識別子 (名前 ID)] を選択します。
5. Microsoft Entra ID ユーザーとゲストユーザーに 2 つのクレーム条件を作成します。
    a. Microsoft Entra ID ユーザーの場合、ソース属性が `user.userprincipalname` に設定されているメンバーのユーザータイプを作成します。
    b. Microsoft Entra ID ゲストユーザーの場合、ソース属性を `user.mail` に設定して、外部ゲストのユーザータイプを作成します。
    c. [保存] を選択し、Microsoft Entra ID ゲストユーザーとしてサインインを再試行します。

その他のリソース

- 一般的な SCIM のトラブルシューティングについては、「IAM Identity Center の問題のトラブルシューティング」をご覧ください。
- Microsoft Entra ID に関するトラブルシューティングについては、Microsoft ドキュメントを参照してください。
- 複数の AWS アカウント間のフェデレーションの詳細については、「Securing AWS アカウント with Azure Active Directory Federation」を参照してください。

AWS を使用する際のトラブルシューティングに役立つリソースを以下に示します。

- AWS re:Post — 問題のトラブルシューティングに役立つ FAQ やその他のリソースへのリンクを検索できます。
- AWS サポート - テクニカルサポートを受ける

Okta および IAM アイデンティティセンターによる SAML と SCIM の設定

System for Cross-domain Identity Management (SCIM) v2.0 プロトコルを使用して、Okta からのユーザーとグループの情報を IAM アイデンティティセンターに自動的にプロビジョニングまたは同期できます。詳細については、「外部 ID プロバイダーで SAML および SCIM ID フェデレーションを使用する」を参照してください。

この接続を Okta で設定するには、IAM Identity Center 用の SCIM エンドポイントと、IAM Identity Center で自動的に作成されるベアラートークンを使用します。SCIM 同期を設定すると、Okta のユーザー属性と IAM Identity Center の名前付き属性のマッピングが作成されます。これにより、想定されるユーザー属性を IAM アイデンティティセンターと Okta アカウントの間でマッチングします。

SCIM を介して IAM アイデンティティセンターに接続した場合、Okta は以下のプロビジョニング機能をサポートします。

- ユーザーの作成 — Okta で IAM Identity Center アプリケーションに割り当てられたユーザーは IAM ID センターでプロビジョニングされます。
- ユーザー属性の更新 — Okta で IAM Identity Center に割り当てられているユーザーの属性変更は、IAM Identity Center で更新されます。
- ユーザーの無効化 — Okta で IAM Identity Center から割り当てられていないユーザーは、IAM Identity Center では無効になります。
- グループプッシュ — Okta のグループ (およびそのメンバー) は、IAM Identity Center に同期されます。

> **Note**
>
> Okta と IAM アイデンティティセンターの両方で管理上のオーバーヘッドを最小限に抑えるために、個々のユーザーではなくグループを割り当てを行い、プッシュすることをお勧めします。

- ユーザーをインポートする – ユーザーは IAM Identity Center から Okta にインポートできます。

目的

このチュートリアルでは、Okta IAM アイデンティティセンターとの SAML 接続をセットアップする手順を順を追って説明します。後で、SCIM を使用して Okta からのユーザーを同期します。このシナリオでは、Okta 内のすべてのユーザーとグループを管理します。ユーザーは Okta ポータルを通じてサインインします。すべてが正しく設定されていることを確認するため、設定手順を完了した後に、Okta ユーザーとしてサインインし、AWS リソースへのアクセスを確認してください。

SAML 経由で Okta を IAM Identity Center に接続する場合、次の機能がサポートされています。

- IdP が開始した SAML サインイン – ユーザーは Okta ポータルからサインインし、IAM Identity Center にアクセスします。
- SP が開始した SAML サインイン – ユーザーは AWS アクセスポータルにアクセスし、Okta ポータルからサインインするようにリダイレクトされます。

> **Note**
>
> Okta's IAM アイデンティティセンターアプリケーションがインストールされている Okta アカウント (無料トライアル) にサインアップできます。有料の Okta 製品の場合は、Okta のライセンスがライフサイクル管理やアウトバウンドプロビジョニングを可能にする同様の機能をサポートしているかどうかを確認する必要があるかもしれません。これらの機能は、Okta から IAM Identity Center に SCIM を設定する際に必要となる場合があります。
> IAM アイデンティティセンターをまだ有効にしていない場合は、「IAM Identity Center を有効にする」を参照してください。

考慮事項

- Okta と IAM アイデンティティセンター間で SCIM プロビジョニングを設定する前に、まず「自動プロビジョニングを使用する際の注意事項」を確認することをお勧めします。
- すべての Okta ユーザーにおいて、[名]、[姓]、[ユーザー名]、[表示名] の値を指定する必要があります。
- 各 Okta ユーザーには、E メールアドレスや電話番号などのデータ属性ごとに 1 つの値のみが割り当てられます。複数の値を持つユーザーは同期に失敗します。属性に複数の値を持つユーザーがいる場合は、IAM アイデンティティセンターでユーザーをプロビジョニングする前に、重複する属性を削除してください。例えば、同期できる電話番号属性は 1 つだけです。デフォルトの電話番号属性は「勤務先の電話」なので、ユーザーの電話番号が自宅の電話でも携帯電話でも、「勤務先の電話」属性を使用してユーザーの電話番号を保存します。
- IAM アイデンティティセンターで Okta を使用する場合、IAM アイデンティティセンターは一般的に Okta のアプリケーションとして設定されます。これにより、Okta の単一のインスタンス内で複数の AWS Organizations へのアクセスをサポートする複数のアプリケーションとして、IAM アイデンティティセンターの複数のインスタンスを設定できます。
- 資格とロール属性はサポートされていないため、IAM アイデンティティセンターと同期できません。
- 同じ Okta グループを割り当てとグループプッシュの両方に使用することは、現在サポートされていません。Okta と IAM アイデンティティセンターの間で一貫したグループメンバーシップを維持するためには、別のグループを作成し、IAM アイデンティティセンターにグループをプッシュするように設定する必要があります。
- IAM Identity Center を追加リージョンにレプリケートした場合は、ID プロバイダーの設定を更新して、AWS マネージドアプリケーションへのアクセスと、追加リージョンから AWS アカウントへのアクセスを有効にする必要があります。前提条件などの詳細については、「複数の 間で IAM アイデンティティセンターを使用するAWS リージョン」を参照してください。Okta 固有の手順については、「追加リージョンにアクセスするための Okta の設定」を参照してください。

ステップ 1: Okta: Okta アカウントから SAML メタデータを取得する

1. Okta admin dashboard にログインして [アプリケーション] を展開し、[アプリケーション] を選択します。
2. [Applications] (アプリケーション) ページで、[Browse App Catalog] (アプリケーションカタログを参照) を選択します。

3. 検索ボックスに、[AWS IAM アイデンティティセンター] を入力して、IAM アイデンティティセンターアプリを追加するアプリを選択します。
4. [サインオン] タブを選択します。
5. [SAML 署名証明書] で、[アクション] を選択し、[IdP メタデータの表示] を選択します。新しいブラウザタブが開き、XML ファイルのドキュメントツリーが表示されます。`<md:EntityDescriptor>` から `</md:EntityDescriptor>` まで XML をすべて選択し、テキストファイルにコピーします。
6. `metadata.xml` としてテキストファイルを保存します。

Okta admin dashboard は開いたままにしておき、後のステップでもそのコンソールを引き続き使用します。

ステップ 2: IAM Identity Center: Okta を IAM アイデンティティセンターの ID ソースとして設定する

1. 管理者権限を持つユーザーとして IAM アイデンティティセンターコンソールを開きます。
2. 左側のナビゲーションペインの [設定] を選択します。
3. [設定] ページで [アクション] タブを選択し、[ID ソースを変更] を選択します。
4. [ID ソースの選択] で [外部 ID プロバイダー] を選択し、[次へ] を選択します。
5. [外部 ID プロバイダーの設定] で、次の操作を行います。

   a. [サービスプロバイダーのメタデータ] で、以下の項目をテキストファイルにコピーすると、簡単にアクセスできるようになります。

      - [IAM Identity Center アサーションコンシューマーサービス (ACS) URL] – IPv4 専用とデュアルスタックの ACS URL のいずれかを選択できます。また、IAM Identity Center インスタンスが複数のリージョンで有効になっている場合、追加リージョンごとに独自の IPv4 専用およびデュアルスタックの ACS URL があります。ACS URL の詳細については、「プライマリおよび追加の AWS リージョンの ACS エンドポイント」を参照してください。
      - IAM アイデンティティセンター発行者 URL

      これらの値は、このチュートリアルの後半で必要になります。

   b. [ID プロバイダーからのメタデータ] の [IdP SAML メタデータ] で [ファイルの選択] を選択し、前の手順で作成した `metadata.xml` ファイルを選択します。

c. [次へ] を選択します。

6. 免責事項を読み、次に進む準備ができたら、[ACCEPT] (許諾) を押してください。
7. [Change identity source] (ID ソースの変更) を選択します。

   AWS コンソールは開いたままにしておき、次の手順でもこのコンソールを引き続き使用します。
8. Okta admin dashboard に戻り、AWS IAM アイデンティティセンター アプリの [サインオン] タブを選択し、[編集] を選択します。
9. [詳細なサインオン設定] で、次のように入力します。

   - ACS URL には、IAM Identity Center アサーションコンシューマーサービス (ACS) URL でメモしておいた値を入力します。プライマリリージョンの ACS URL をデフォルトとして使用すると、ユーザーが Okta から Amazon Web Services アプリケーションを起動するときにプライマリリージョンにリダイレクトされるようになります。
   - (オプション) IAM Identity Center を追加リージョンにレプリケートした場合は、追加リージョンごとに Okta で AWS アクセスポータルのブックマークアプリを作成することもできます。これにより、ユーザーは Okta から追加リージョンの AWS アクセスポータルにアクセスできます。Okta でブックマークアプリにアクセスするためのアクセス許可をユーザーに付与します。詳細については、「Okta 関連ドキュメント」を参照してください。後で IAM Identity Center を追加リージョンにレプリケートする場合は、「追加リージョンにアクセスするための Okta の設定」を参照して、この初期セットアップ後に追加リージョンへのアクセスを有効にする方法を確認してください。
   - [発行者 URL] には、[IAM アイデンティティセンターの発行者 URL] でメモしておいた値を入力します。
   - [アプリケーションのユーザー名形式] で、メニューからいずれかのオプションを選択します。

     選択する値が各ユーザーに固有となることを確認します。このチュートリアルでは、[Okta ユーザー名] を選択します。
10. [保存] を選択します。

これで、Okta から IAM アイデンティティセンターにユーザーをプロビジョニングする準備が整いました。Okta admin dashboard を開いたままにして、IAM アイデンティティセンターコンソールに戻って次の手順に進みます。

ステップ 3: IAM アイデンティティセンターと Okta: Okta ユーザーをプロビジョニングする

1. IAM アイデンティティセンターコンソールの [設定] ページで、[自動プロビジョニング] 情報ボックスを見つけて、[有効にする] を選択します。これにより、IAM アイデンティティセンターの自動プロビジョニングが有効になり、必要な SCIM エンドポイントとアクセストークンの情報が表示されます。
2. [インバウンド自動プロビジョニング] ダイアログボックスで、以下のオプションの値をそれぞれコピーします。

   a. SCIM エンドポイント - エンドポイントの形式は、設定によって異なります。

      - IPv4: https://scim.*us-east-2*.amazonaws.com/*11111111111-2222-3333-4444-555555555555*/scim/v2
      - Dual-stack: https://scim.*us-east-2*.api.aws/*11111111111-2222-3333-4444-555555555555*/scim/v2

   b. [アクセストークン] - [トークンを表示] を選択して値をコピーします。

   > ⚠ Warning
   >
   > SCIM エンドポイントとアクセストークンを取得できるタイミングは、この時のみです。先に進む前に、これらの値をコピーしておいてください。このチュートリアルの後半で、Okta でこれらの値を入力してプロビジョニングを設定します。

3. [閉じる] を選択してください。
4. Okta admin dashboard に戻り、IAM アイデンティティセンターアプリに移動します。
5. [IAM アイデンティティセンターアプリ] ページで、[プロビジョニング] タブを選択し、左側のナビゲーションペインにある [設定] の下で [統合] を選択します。
6. [編集] を選択し、[API 統合を有効にする] の横にあるチェックボックスを選択して自動プロビジョニングを有効にします。
7. ここで、先ほどメモしておいた AWS IAM アイデンティティセンター からの SCIM プロビジョニング値を使用して Okta を設定します。

   a. [ベース URL] フィールドに [SCIM エンドポイント] の値を入力します。

   b. [API トークン] フィールドに、[アクセストークン] の値を入力します。

8. [Test API Credentials] (API 認証情報をテストする) を選択して、入力された認証情報が有効であることを確認します。

   [AWS IAM アイデンティティセンター は正常に検証されました] というメッセージが表示されます。
9. [保存] を選択します。引き続き [統合] が選択されている状態で、[設定] セクションに移動します。
10. [設定] の下で [アプリへ] を選択し、[アプリへのプロビジョニング] の有効にしたい各項目について [有効にする] チェックボックスをオンにします。このチュートリアルでは、すべてのオプションを選択します。
11. [保存] を選択します。

これで、IAM アイデンティティセンターでユーザーを Okta から同期する準備が整いました。

ステップ 4: Okta: Okta から IAM アイデンティティセンターとユーザーを同期する

デフォルトでは、Okta IAM アイデンティティセンターアプリにはグループやユーザーは割り当てられていません。プロビジョニンググループは、グループのメンバーであるユーザーをプロビジョニングします。グループとユーザーを AWS IAM アイデンティティセンター と同期するには、以下の手順を実行します。

1. [Okta IAM アイデンティティセンターアプリ] ページで [割り当て] タブを選択します。IAM アイデンティティセンターアプリにはユーザーとグループの両方を割り当てることができます。

   a. ユーザーを割り当てるには:

      - [割り当て] ページで、[割り当てる] を選択し、[人に割り当てる] を選択します。
      - IAM アイデンティティセンターアプリへのアクセスを付与する Okta ユーザーを選択します。[Assign] (割り当て)、[Save and Go Back] (保存して戻る)、[Done] (完了) の順に選択します。

      これにより、IAM アイデンティティセンターへのユーザーのプロビジョニングプロセスが開始されます。

   b. グループを割り当てるには:

      - [割り当て] ページで、[割り当てる] を選択し、[グループに割り当てる] を選択します。

- IAM アイデンティティセンターアプリへのアクセスを付与する Okta グループを選択します。[Assign] (割り当て)、[Save and Go Back] (保存して戻る)、[Done] (完了) の順に選択します。

これにより、IAM Identity Center へのグループ内のユーザーのプロビジョニングプロセスが開始されます。

> **Note**
>
> グループに追加の属性がすべてのユーザーレコードに含まれていない場合は、その属性を指定する必要がある場合があります。グループに指定された属性は、個々の属性値よりも優先されます。

2. [Push Groups] (プッシュグループ) タブを選択します。IAM アイデンティティセンターと同期する Okta グループを選択します。[保存] を選択します。

   グループとそのメンバーが IAM アイデンティティセンターに正常にプッシュされると、グループのステータスが [アクティブ] に変わります。

3. [割り当て] タブに戻ります。
4. IAM アイデンティティセンターに個別の Okta ユーザーを追加するには、次の手順を実行します。

   a. [Assignments] (割り当て) ページで、[Assign] (割り当て) を選択し、[Assign to People] (人に割り当てる) を選択します。

   b. IAM アイデンティティセンターアプリへのアクセスを付与する Okta ユーザーを選択します。[Assign] (割り当て)、[Save and Go Back] (保存して戻る)、[Done] (完了) の順に選択します。

   これにより、IAM アイデンティティセンターへの個人ユーザーのプロビジョニングプロセスが開始されます。

> **Note**
>
> Okta admin dashboard の [アプリケーション] ページから、ユーザーとグループを AWS IAM アイデンティティセンター アプリケーションに割り当てることもできま

す。これを行うには、[設定] アイコンを選択し、[ユーザーに割り当てる] または [グループに割り当てる] を選択し、ユーザーまたはグループを指定します。

5. IAM アイデンティティセンターコンソールに戻ります。左側のナビゲーションで [ユーザー] を選択すると、Okta ユーザーが入力したユーザーリストが表示されます。

お疲れ様でした。

Okta と AWS の間の SAML 接続が正常にセットアップされ、自動プロビジョニングが機能していることが確認できました。[IAM Identity Center] でこれらのユーザーをアカウントおよびアプリケーションに割り当てることができるようになりました。このチュートリアルでは、次のステップで、管理アカウントへの管理アクセス許可を付与して、ユーザーの 1 人を IAM アイデンティティセンター管理者として指定しましょう。

アクセスコントロールの属性を渡す - オプション

IAM Identity Center の アクセスコントロールの属性 機能をオプションで使用して、Name 属性を `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` に設定した `Attribute` 要素を渡すことができます。この要素を使用すると、SAML アサーションでセッションタグとして属性を渡すことができます。セッションタグの詳細については、「IAM ユーザーガイド」の「AWS STS でのタグ付けの規則 」を参照してください。

属性をセッションタグとして渡すには、タグの値を指定する `AttributeValue` 要素を含めます。例えば、タグのキーバリューのペア `CostCenter = blue` を渡すには、次のような属性を使用します。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

複数の属性を追加する必要がある場合は、各タグに個別の `Attribute` 要素を含めます。

AWS アカウントにアクセスを割り当てる

以下の手順は、AWS アカウントへのアクセスのみを許可する場合にのみ必要となります。これらのステップは、AWS アプリケーションへのアクセスを許可する場合には必要ありません。

> **Note**
>
> このステップを完了するには、IAM アイデンティティセンターの組織インスタンスが必要です。詳細については、「IAM アイデンティティセンターの組織インスタンスとアカウントインスタンス」を参照してください。

ステップ 1: IAM アイデンティティセンター: Okta ユーザーにアカウントへのアクセスを付与する

1. IAM アイデンティティセンターのナビゲーションペインの [マルチアカウントのアクセス許可] で、[AWS アカウント] を選択します。
2. AWS アカウント ページの [組織構造] には、組織のルートと、その下にあるアカウントが階層内で表示されます。管理アカウントのチェックボックスをオンにし、[ユーザーまたはグループを割り当て] を選択します。
3. [ユーザーとグループを割り当てる] のワークフローが表示されます。これは、3 つのステップから構成されています。

   a. [ステップ 1: ユーザーとグループの選択] では、管理者の職務を実行するユーザーを選択します。次に、[次へ] を選択します。

   b. [ステップ 2: 許可セットの選択] で、[許可セットを作成する] を選択します。新しいタブが開き、許可セットを作成するための 3 つの手順が順に表示されます。

      i. [ステップ 1: 許可セットタイプを選択] では、以下を完了します。

      - [許可セットのタイプ] で、[事前定義された許可セット] を選択します。
      - [事前定義された許可セットのポリシー] で [AdministratorAccess] を選択します。

      [次へ] を選択します。

      ii. [ステップ 2: 許可セットの詳細を指定] では、デフォルト設定のままで、[次へ] を選択します。

デフォルト設定では、*AdministratorAccess* という名前の許可セットが作成され、セッション期間は 1 時間に設定されます。

iii. [ステップ 3: 確認して作成] では、[許可セットのタイプ] が AWS 管理ポリシー [AdministratorAccess] を使用していることを確認します。[作成] を選択します。[許可セット] ページに、許可セットが作成されたことを知らせる通知が表示されます。この時点で、ウェブブラウザでこのタブを閉じてもかまいません。

[ユーザーとグループを割り当てる] ブラウザタブでは、[ステップ 2: 許可セットを選択] でアクセス許可セットの作成ワークフローを開始した状態のままになっています。

[アクセス許可セット] 領域で、[更新] ボタンを選択します。作成した *AdministratorAccess* 許可セットがリストに表示されます。そのアクセス許可セットのチェックボックスを選択したら、[次へ] を選択します。

c. [ステップ 3: 確認と送信] では、選択されているユーザと許可セットを確認して、[送信] を選択します。

ページが更新され、AWS アカウント が設定中であることを示すメッセージが表示されます。プロセスが完了するまで待ちます。

AWS アカウント ページに戻ります。AWS アカウント が再プロビジョニングされ、更新されたアクセス許可セットが適用されたことを知らせる通知メッセージが表示されます。ユーザーがサインインすると、*AdministratorAccess* ロールを選択できます。

ステップ 2: Okta: Okta ユーザーの AWS リソースへのアクセスを確認する

1. テストアカウントを使用して Okta dashboard にサインインします。
2. [マイアプリ] で、AWS IAM アイデンティティセンター アイコンを選択します。
3. AWS アカウントアイコンが表示されます。そのアイコンを展開すると、ユーザーがアクセスできる AWS アカウント のリストが表示されます。このチュートリアルでは 1 つのアカウントしか使用していなかったため、アイコンを展開しても 1 つのアカウントしか表示されません。
4. アカウントを選択すると、そのユーザーが利用可能なアクセス許可セットが表示されます。このチュートリアルでは、AdministratorAccess 許可セットを作成しました。
5. アクセス許可セットの横には、その許可セットで利用できるアクセスの種類を示すリンクがあります。許可セットを作成することにより、AWS マネジメントコンソールよるアクセスとプログ

ラムによるアクセス両方についてのアクセス許可が指定されます。[管理コンソール] を選択して AWS マネジメントコンソールを開きます。

6. ユーザーは、AWS マネジメントコンソールにサインインされます。

AWS アクセスポータルを使用することもできます。これにより、AWS アクセスポータルに移動する前に、Okta ポータルからサインインするようにリダイレクトされます。このパスは、SP が開始した SAML サインインフローに従います。

IAM Identity Center の追加リージョンにアクセスするための Okta の設定 - オプション

IAM Identity Center を追加リージョンにレプリケートした場合は、ID プロバイダーの設定を更新して、AWS マネージドアプリケーションへのアクセスと、追加リージョンから AWS アカウント へのアクセスを有効にする必要があります。以下のステップでは、この手順について説明します。前提条件などこのトピックの詳細については、「複数の 間で IAM アイデンティティセンターを使用する AWS リージョン」を参照してください。

1. プライマリおよび追加の AWS リージョンの ACS エンドポイント に記載されている手順に従って、IAM Identity Center コンソールから追加リージョンの ACS URL を取得します。
2. Okta 管理ダッシュボードのナビゲーションペインで、[アプリケーション] を選択し、展開されたリストで [アプリケーション] を再度選択します。
3. AWS IAM アイデンティティセンター アプリケーションを選択します。
4. [Sign On] タブを選択します。
5. [詳細なサインオン設定] の [その他のリクエスト可能な SSO URL] で、追加リージョンの ACS URL ごとに [別のものを追加] を選択し、ACS URL をテキストフィールドに貼り付けます。
6. ACS URL の追加が完了したら、AWS IAM アイデンティティセンター アプリケーションを保存します。
7. 追加リージョンごとに、Okta で AWS アクセスポータルのブックマークアプリを作成できます。これにより、ユーザーは Okta から追加リージョンの AWS アクセスポータルにアクセスできます。Okta でブックマークアプリにアクセスするためのアクセス許可をユーザーに付与します。詳細については、「Okta 関連ドキュメント」を参照してください。
8. 追加リージョンごとに、AWS アクセスポータルにサインインできることを確認します。AWS アクセスポータル URL に移動するか、Okta からブックマークアプリを起動します。

次のステップ

Okta を ID プロバイダーとして設定し、IAM アイデンティティセンターにユーザーをプロビジョニングしたので、次のことが可能になります。

- AWS アカウント へのアクセスを許可し、「AWS アカウント にユーザーまたはグループアクセスを割り当てる」を参照してください。
- クラウドアプリケーションへのアクセスを許可し、「IAM Identity Center コンソールでアプリケーションへのユーザーアクセスを割り当てます。」を参照してください。
- 職務に基づいてアクセス許可を設定します。「許可セットの作成」を参照してください。

トラブルシューティング

Okta を使用した一般的な SCIM および SAML のトラブルシューティングについては、以下のセクションを参照してください。

- IAM アイデンティティセンターから削除されたユーザーとグループの再プロビジョニング
- Okta の自動プロビジョニングエラー
- 特定のユーザーが、外部の SCIM プロバイダーからの IAM Identity Center に同期できません
- IAM Identity Center によって作成された SAML アサーションの内容に関する問題
- 外部 ID プロバイダーを使用してユーザーまたはグループをプロビジョニングする際の重複ユーザーまたはグループのエラー
- その他のリソース

IAM アイデンティティセンターから削除されたユーザーとグループの再プロビジョニング

- 一旦同期した後に IAM アイデンティティセンターから削除された Okta のユーザーまたはグループを変更しようとすると、Okta コンソールに次のエラーメッセージが表示されることがあります。
  - Automatic profile push of user *`Jane Doe`* to app AWS IAM アイデンティティセンター failed: Error while trying to push profile update for *`jane_doe@example.com`*: No user returned for user *`xxxxx-xxxxxx-xxxxx-xxxxxxx`*
  - Linked group is missing in AWS IAM アイデンティティセンター. Change the linked group to resume pushing group memberships.

- また、同期後に削除された IAM アイデンティティセンターユーザーまたはグループについて、Okta のシステムログに次のエラーメッセージが表示される場合もあります。
  - Okta Error: Eventfailed application.provision.user.push_profile : No user returned for user *xxxxx-xxxxxx-xxxxx-xxxxxxx*
  - Okta Error: application.provision.group_push.mapping.update.or.delete.failed.with.error : Linked group is missing in AWS IAM アイデンティティセンター. リンク済みグループを変更して、グループメンバーシップのプッシュを再開します。

> **Warning**
>
> SCIM を使用して Okta と IAM アイデンティティセンターを同期している場合は、IAM アイデンティティセンターではなく Okta からユーザーとグループを削除する必要があります。

削除された IAM アイデンティティセンターユーザーに関するトラブルシューティング

削除された IAM アイデンティティセンターユーザーに関する問題に対処するには、そのユーザーをいったん Okta から削除する必要があります。その後、必要に応じてこれらのユーザーを Okta で再作成してください。ユーザーが Okta で再作成されると、SCIM を介して IAM アイデンティティセンターにも再プロビジョニングされます。ユーザ削除の詳細については、「Okta ドキュメント」を参照してください。

> **Note**
>
> IAM アイデンティティセンターへの Okta ユーザーのアクセスを削除する必要がある場合は、まずグループプッシュから削除してから、Okta で割り当てグループを削除する必要があります。これにより、ユーザーは IAM アイデンティティセンターの関連付けられたグループメンバーシップから削除されます。グループプッシュのトラブルシューティングの詳細については、「Okta ドキュメント」を参照してください。

削除された IAM アイデンティティセンターグループに関するトラブルシューティング

削除された IAM アイデンティティセンターグループに関する問題に対処するには、そのグループを Okta からいったん削除する必要があります。その後、必要に応じてグループプッシュを使用してそれらのグループを Okta で再作成してください。ユーザーが Okta で再作成されると、SCIM を介し

て IAM アイデンティティセンターにも再プロビジョニングされます。グループの削除の詳細については、Okta のドキュメントを参照してください。

Okta の自動プロビジョニングエラー

Okta で以下のエラーメッセージが表示された場合、次の操作を行います。

アプリ AWS IAM アイデンティティセンター へのユーザー Jane Doe の自動プロビジョニングに失敗しました: 一致するユーザーが見つかりません

詳細については、「Okta ドキュメント」を参照してください。

その他のリソース

- 一般的な SCIM のトラブルシューティングについては、「IAM Identity Center の問題のトラブルシューティング」をご覧ください。

AWS を使用する際のトラブルシューティングに役立つリソースを以下に示します。

- AWS re:Post — 問題のトラブルシューティングに役立つ FAQ やその他のリソースへのリンクを検索できます。
- AWS サポート - テクニカルサポートを受ける

OneLogin と IAM アイデンティティセンター間の SCIM プロビジョニングのセットアップ

IAM Identity Center は、クロスドメインアイデンティティ管理システム (SCIM) v2.0 プロトコルを使用して、OneLogin から IAM Identity Center へのユーザーおよびグループ情報の自動プロビジョニング (同期化) をサポートしています。詳細については、「外部 ID プロバイダーで SAML および SCIM ID フェデレーションを使用する」を参照してください。

> **Note**
>
> OneLogin は現在、AWS IAM アイデンティティセンター アプリケーションで SAML マルチアサーションコンシューマーサービス (ACS) URL をサポートしていません。この SAML 機能は、IAM Identity Center のマルチリージョンサポートを最大限に活用するために必要です。IAM Identity Center を追加リージョンにレプリケートする場合に、単一の ACS URL を使用すると、それらの追加リージョンでのユーザーエクスペリエンスに影響が出る可能性が

あることに注意してください。プライマリリージョンは、引き続き正常に機能します。IdP ベンダーと協力して、この機能を有効にすることをお勧めします。単一の ACS URL による追加リージョンでのユーザーエクスペリエンスの詳細については、「the section called “複数の ACS URL なしで AWS マネージドアプリケーションを使用する”」および「the section called “複数の ACS URL を使用しない AWS アカウントアクセス回復性”」を参照してください。

この接続を OneLogin で設定するには、IAM Identity Center 用の SCIM エンドポイントと IAM Identity Center で自動的に作成したベアラートークンを使用します。SCIM 同期を設定すると、OneLogin のユーザー属性と IAM Identity Center の名前付き属性のマッピングが作成されます。これにより、IAM Identity Center と OneLogin の間で、期待される属性が一致します。

次のステップでは、SCIM プロトコルを使用して、OneLogin から IAM Identity Center へのユーザーとグループの自動プロビジョニングを有効にする方法を説明します。

> **Note**
>
> SCIM のデプロイを開始する前に、まず 自動プロビジョニングを使用する際の注意事項 を確認することをお勧めします。

トピック

- 前提条件
- ステップ 1: IAM Identity Center でプロビジョニングを有効にする
- ステップ 2: OneLogin でプロビジョニングを設定する
- (オプション) ステップ 3: IAM Identity Center でのアクセスコントロールのために OneLogin でユーザー属性を設定する
- (オプション) アクセスコントロールの属性を渡す
- トラブルシューティング

前提条件

開始する前に、以下の準備が必要です。

- OneLogin アカウント。既存のアカウントをお持ちでない場合は、OneLogin のウェブサイトから無料トライアルまたはデベロッパーアカウントを取得できるかもしれません。

- IAM アイデンティティセンター対応アカウント (無料)。詳細については、「IAM Identity Center の有効化」を参照してください。
- OneLogin アカウントから IAM Identity Center への SAML 接続。詳細については、AWS パートナーネットワークブログの「OneLogin と AWS の間の有効化」 を参照してください。

ステップ 1: IAM Identity Center でプロビジョニングを有効にする

この最初のステップでは、IAM Identity Center コンソールを使用して、自動プロビジョニングを有効にします。

IAM アイデンティティセンターで自動プロビジョニングを有効にするには

1. 前提条件が整ったら、IAM アイデンティティセンターコンソールを開きます。
2. 左側のナビゲーションペインの [設定] を選択します。
3. [設定] ページで、[自動プロビジョニング] 情報ボックスを探し、[有効化] を選択します。これにより、すぐに IAM アイデンティティセンターの自動プロビジョニングが有効になり、必要なエンドポイントとアクセストークンの情報が表示されます。
4. [インバウンド自動プロビジョニング] ダイアログボックスで、SCIM エンドポイントとアクセストークンをコピーします。これらは、後で IdP でプロビジョニングを設定する際に貼り付ける必要があります。

   a. [SCIM エンドポイント] - 例えば https://scim.*us-east-2*.amazonaws.com/*11111111111-2222-3333-4444-555555555555*/scim/v2

   b. [アクセストークン] - [トークンを表示] を選択して値をコピーします。

   > **Warning**
   >
   > SCIM エンドポイントとアクセストークンを取得できるタイミングは、この時のみです。先に進む前に、これらの値をコピーしておいてください。このチュートリアルの後半で、お使いの IdP 上でこれらの値を入力して自動プロビジョニングを設定します。

5. [閉じる] を選択します。

IAM Identity Center コンソールでプロビジョニングを設定しています。あとは OneLogin 管理者コンソールのユーザーインターフェースに従い、以下の残りの手順を行う必要があります。

ステップ 2: OneLogin でプロビジョニングを設定する

OneLogin 管理コンソールで以下の手順を使用して、IAM Identity Center と IAM Identity Center アプリケーション間の統合を有効にします。この手順では、AWS の OneLogin シングルサインオンアプリケーションで SAML 認証が設定済みであることを前提としています。この SAML 接続をまだ作成していない場合は、先に進む前に SAML 接続を作成し、ここに戻って SCIM のプロビジョニングプロセスを完了してください。OneLogin での SAML の設定の詳細については、AWS パートナーネットワークブログの「Enabling Single Sign-On Between OneLogin and AWS」を参照してください。

OneLogin でプロビジョニングを設定するには

1. OneLogin にサインインして、[アプリケーション] > [アプリケーション] と進みます。
2. [アプリケーション] ページで、IAM Identity Center との SAML 接続を形成するために以前に作成したアプリケーションを検索します。それを選択して、左のナビゲーションバーから [設定] を選択します。
3. 前の手順で、IAM Identity Center から [SCIM エンドポイント] の値をコピーしました。その値を OneLogin の [ベース URL] フィールドに貼り付けます。また、前の手順で、IAM アイデンティティセンターの [アクセストークン] の値をコピーしました。その値を OneLogin の [SCIM ベアラートークン] フィールドに貼り付けます。
4. [API Connection] (API 接続) の隣にある [Enable] (有効化) をクリックし、[Save] (保存) をクリックして設定を完了します。
5. ナビゲーションペインで、[Provisioning] (プロビジョニング) を選択します。
6. [Enable provisioning] (プロビジョニングの有効化)、[Create user] (ユーザーの作成)、[Delete user] (ユーザーの削除)、[Update user] (ユーザーの更新) の各チェックボックスを選択し、[Save] (保存) を選択します。
7. ナビゲーションペインで [ユーザー] を選択します。
8. [More Actions] (その他のアクション) をクリックして、[Sync logins] (ログイン同期) を選択します。[Synchronizing users with AWS Single Sign-On を使用したユーザーの同期] というメッセージが表示されます。
9. もう一度 [More Actions] (その他のアクション) をクリックして、[Reapply entitlement mappings] (エンタイトルメントマッピングの再適用) を選択します。Mappings are being reapplied (マッピングが再適用されている) というメッセージが表示されます。
10. この時点で、プロビジョニングプロセスを開始する必要があります。これを確認するには、[Activity] (アクティビティ) > Events (イベント) をクリックして、進行状況をモニタリングします。プロビジョニングに成功したイベントやエラーがイベントストリームに表示されます。

11. ユーザーおよびグループが IAM Identity Center にすべて正常に同期されたことを確認するには、 IAM Identity Center コンソールに戻り、[ユーザー] を選択します。OneLogin から同期されたユーザーは、[ユーザー] ページに表示されます。また、同期したグループは [Groups] (グループ) ページで確認できます。
12. ユーザーの変更を IAM Identity Center に自動的に同期させるには、[プロビジョニング] ページに移動し、[この操作を実行する前に管理者の承認を要求する] セクションを見つけ、[ユーザーの作成]、[ユーザーの削除]、[ユーザーの更新] の選択を解除し、[保存] をクリックします。

(オプション) ステップ 3: IAM Identity Center でのアクセスコントロールのために OneLogin でユーザー属性を設定する

これは、AWS リソースへのアクセスを管理するために IAM Identity Center の属性設定を選択した場合の OneLogin のオプション手順です。OneLogin で定義した属性は、SAML アサーションで IAM Identity Center に渡されます。その後、IAM Identity Center でアクセス権限セットを作成し、OneLogin から渡された属性に基づいてアクセスを管理します。

この手順を始める前に、最初に アクセスコントロールの属性 機能を有効にしておく必要があります。これを行う方法については、「アクセスコントロールのための属性の有効化と設定」を参照してください。

IAM Identity Center でのアクセスコントロールに使用される OneLogin の属性の有効化と設定

1. OneLogin にサインインして、[アプリケーション] > [アプリケーション] と進みます。
2. [アプリケーション] ページで、IAM Identity Center との SAML 接続を形成するために以前に作成したアプリケーションを検索します。それを選択して、ナビゲーションバーから [パラメータ] を選択します。
3. [必須パラメータ] セクションでは、IAM Identity Center で使用する各属性について以下のように設定します。

    a. を選択します。。

    b. [名前] フィールドには `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`** を入力し、**`AttributeName`** は IAM Identity Center で想定している属性名に置き換えます。例えば、`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**。

    c. [Flags] (フラグ) で、[Include in SAML assertion] (SAML アサーションに含める) の横のボックスをチェックして、[Save] (保存) を選択します。

d. [値] フィールドでは、ドロップダウンリストを使って、OneLogin のユーザー属性を選択します。例えば、Department (部署) などです。

4. [保存] を選択します。

(オプション) アクセスコントロールの属性を渡す

IAM Identity Center の アクセスコントロールの属性 機能をオプションで使用して、Name 属性を `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` に設定した Attribute 要素を渡すことができます。この要素を使用すると、SAML アサーションでセッションタグとして属性を渡すことができます。セッションタグの詳細については、「IAM ユーザーガイド」の「AWS STS でのタグ付けの規則 」を参照してください。

属性をセッションタグとして渡すには、タグの値を指定する AttributeValue 要素を含めます。例えば、タグのキーバリューのペア `CostCenter = blue` を渡すには、次のような属性を使用します。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

複数の属性を追加する必要がある場合は、各タグに個別の Attribute 要素を含めます。

トラブルシューティング

以下は、OneLogin で自動プロビジョニングで発生する問題のトラブルシューティングに役立ちます。

グループは IAM Identity Center にプロビジョニングされない

デフォルトでは、グループは OneLogin から IAM Identity Center にプロビジョニングできません。OneLogin で IAM Identity Center アプリケーションのグループプロビジョニングが有効になっていることを確認します。これを行うには、OneLogin 管理コンソールにサインインし、IAM Identity Center アプリケーションのプロパティ (IAM Identity Center アプリケーション > パラメータ > グループ) で、[ユーザープロビジョニングに含める] オプションが選択されている必要があります。SCIM のグループとして OneLogin のロールを同期させる方法を含め、OneLogin でグループを作成する方法の詳細については、「OneLogin のウェブサイト」 を参照してください。

すべての設定が正しいにもかかわらず、OneLogin から IAM Identity Center へ何も同期されない

上記の管理者承認に関する注意事項に加えて、多くの設定変更を有効にするためには、エンタイトルメントマッピングを再適用する必要があります。これは、[アプリケーション] > [アプリケーション] > [IAM Identity Center アプリケーション] > [その他のアクション] で確認できます。同期イベントを含む OneLogin のほとんどのアクションの詳細と ログは、[Activity] (アクティビティ) > [Events] (イベント) で確認できます。

OneLogin でグループを削除または無効にしたが、IAM Identity Center でまだ表示されている

OneLogin は現在、グループに対する SCIM DELETE オペレーションをサポートしていないため、グループは IAM Identity Center で存在し続けます。そのため、IAM Identity Center からグループを直接削除して、そのグループに対応する IAM Identity Center 内のアクセス権限が削除されるようにする必要があります。

OneLogin からグループを削除せずに IAM Identity Center でグループを削除したら、ユーザー/グループの同期問題が発生した

この問題を解決するには、まず、OneLogin に冗長なグループプロビジョニングルールや構成がないことを確認してください。例えば、アプリケーションに直接割り当てられたグループと、同じグループに発行するルールなどです。次に、IAM Identity Center 内の不必要なグループを削除します。最後に OneLogin でエンタイトルメントを リフレッシュして ([IAM Identity Center アプリケーション] > [プロビジョニング] > [エンタイトルメント])、エンタイトルメントマッピングを再度適用します ([IAM Identity Center アプリケーション] > [その他のアクション])。今後この問題を回避するには、まず OneLogin でグループのプロビジョニングを停止するように変更し、その後 IAM Identity Center からグループを削除します。

IAM アイデンティティセンターで Ping Identity 製品を使用する

以下の Ping Identity 製品は、IAM Identity Center でテストされます。

トピック

- PingFederate
- PingOne

PingFederate

IAM Identity Center は、Ping Identity (以下、Ping) の PingFederate 製品から IAM Identity Center へのユーザーおよびグループ情報の自動プロビジョニング (同期化) をサポートしています。このプロ

ビジョニングでは、クロスドメインアイデンティティ管理システム (SCIM) v2.0 プロトコルを使用します。詳細については、「外部 ID プロバイダーで SAML および SCIM ID フェデレーションを使用する」を参照してください。

この接続を PingFederate で設定するには、IAM Identity Center SCIM エンドポイントとアクセストークンを使用します。SCIM 同期を設定すると、PingFederate のユーザー属性と IAM Identity Center の名前付き属性のマッピングが作成されます。これにより、IAM Identity Center と PingFederate の間で、期待される属性が一致します。

このガイドは、PingFederate バージョン 10.2 に基づいています。他のバージョンでは、手順が異なる場合があります。他のバージョンの Ping の IAM Identity Center へのプロビジョニングの設定方法の詳細については、PingFederate にお問い合わせください。

次のステップでは、SCIM プロトコルを使用して、PingFederate から IAM Identity Center へのユーザーとグループの自動プロビジョニングを有効にする方法を説明します。

> **Note**
>
> SCIM のデプロイを開始する前に、まず 自動プロビジョニングを使用する際の注意事項 を確認することをお勧めします。そして、次のセクションで残りの注意事項を確認します。

トピック

- 前提条件
- 考慮事項
- ステップ 1: IAM Identity Center でプロビジョニングを有効にする
- ステップ 2: PingFederate でプロビジョニングを設定する
- (オプション) ステップ 3: IAM Identity Center でのアクセスコントロールのために でユーザー属性を設定する
- (オプション) アクセスコントロールの属性を渡す
- トラブルシューティング

前提条件

開始する前に、以下の準備が必要です。

- 動作中の PingFederate サーバー。既存の PingFederate サーバーをお持ちでない場合は、Ping Identity のウェブサイトから無料トライアルまたはデベロッパーアカウントを取得できるかもしれません。無料トライアルには、ライセンスやソフトウェアのダウンロード、関連するドキュメントが含まれています。
- PingFederate サーバーにインストールされている PingFederate IAM Identity Center ソフトウェアのコピー。このソフトウェアの入手方法については、Ping Identity ウェブサイトの「IAM Identity Center Connector」を参照してください。
- IAM アイデンティティセンター対応アカウント (無料)。詳細については、「IAM Identity Center の有効化」を参照してください。
- PingFederate インスタンスから IAM Identity Center への SAML 接続。この接続を設定する手順については、PingFederate のドキュメントを参照してください。つまり推奨される方法は、IAM Identity Center コネクターを使用して PingFederate で「ブラウザ SSO」を構成し、両端のメタデータの「ダウンロード」および「インポート」機能を使用して、PingFederate と IAM Identity Center の間で SAML メタデータを交換します。
- IAM Identity Center を追加リージョンにレプリケートした場合は、ID プロバイダーの設定を更新して、AWS マネージドアプリケーションへのアクセスと、それらのリージョンから AWS アカウント へのアクセスを有効にする必要があります。詳細については、以下を参照してください。the section called “手順 3 (外部 ID プロバイダーのみ): 外部 IdP 設定を更新する”詳細については、PingFederate のドキュメントを参照してください。

考慮事項

以下は、IAM Identity Center によるプロビジョニングの実装方法に影響を与える可能性がある PingFederate に関する重要な注意事項です。

- PingFederate で設定したデータストアのユーザーから属性 (電話番号など) を削除しても、IAM Identity Center に対応するユーザーからはその属性は削除されません。これは、PingFederate’s のプロビジョナーの実装における既知の制限です。ユーザーの属性が異なる (空でない) 値に変更された場合、その変更は IAM Identity Center に同期されます。

ステップ 1: IAM Identity Center でプロビジョニングを有効にする

この最初のステップでは、IAM Identity Center コンソールを使用して、自動プロビジョニングを有効にします。

IAM アイデンティティセンターで自動プロビジョニングを有効にするには

1. 前提条件が整ったら、IAM アイデンティティセンターコンソールを開きます。
2. 左側のナビゲーションペインの [設定] を選択します。
3. [設定] ページで、[自動プロビジョニング] 情報ボックスを探し、[有効化] を選択します。これにより、すぐに IAM アイデンティティセンターの自動プロビジョニングが有効になり、必要なエンドポイントとアクセストークンの情報が表示されます。
4. [インバウンド自動プロビジョニング] ダイアログボックスで、SCIM エンドポイントとアクセストークンをコピーします。これらは、後で IdP でプロビジョニングを設定する際に貼り付ける必要があります。

   a. [SCIM エンドポイント] - 例えば https://scim.*us-east-2*.amazonaws.com/*11111111111-2222-3333-4444-555555555555*/scim/v2

   b. [アクセストークン] - [トークンを表示] を選択して値をコピーします。

   > **Warning**
   >
   > SCIM エンドポイントとアクセストークンを取得できるタイミングは、この時のみです。先に進む前に、これらの値をコピーしておいてください。このチュートリアルの後半で、お使いの IdP 上でこれらの値を入力して自動プロビジョニングを設定します。

5. [閉じる] を選択してください。

IAM Identity Center コンソールでプロビジョニングを設定した後、PingFederate 管理コンソールを使用して残りのタスクを完了する必要があります。

ステップ 2: PingFederate でプロビジョニングを設定する

PingFederate 管理コンソールで以下の手順を使用して、IAM Identity Center と IAM Identity Center コネクター間の統合を有効にします。この手順では、IAM Identity Center コネクターソフトウェアが既にインストールされていることを前提としています。まだ実行していない場合は、「前提条件」を参照してから、この手順を実行して SCIM プロビジョニングを設定してください。

> **Important**
>
> PingFederate サーバーが以前にアウトバウンド SCIM プロビジョニング用に設定されていない場合は、プロビジョニングを有効にするために設定ファイルの変更が必要になることが

あります。詳細については、Ping ドキュメントを参照してください。つまり、pingfederate-<version>/pingfederate/bin/run.properties ファイル内の `pf.provisioner.mode` 設定を `OFF` (デフォルト) 以外の値に変更して、現在稼働中のサーバーがあれば再起動する必要があります。例えば、PingFederate を使った高可用性の構成でない場合は `STANDALONE` を使用することができます。

PingFederate でプロビジョニングを設定するには

1. PingFederate 管理コンソールにサインオンします。
2. ページ上部の [Applications] (アプリケーション) を選択し、[SP Connections] (SP 接続) をクリックします。
3. IAM Identity Center との SAML 接続を形成するために前回作成したアプリケーションを検索して、接続名をクリックします。
4. ページの上部にある暗いナビゲーションの見出しから [Connection Type] (接続タイプ) を選択します。前回の SAML の設定で、Browser SSO が既に選択されているはずです。選択されていない場合は、先にその手順を完了させてから次に進みます。
5. [アウトバウンドプロビジョニング] チェックボックスを選択して、タイプとして [IAM Identity Center クラウドコネクター] を選択して、[保存] をクリックします。[IAM Identity Center Cloud Connector] がオプションとして表示されない場合は、IAM Identity Center がインストールされていることを確認して、PingFederate サーバーを再起動します。
6. [Outbound Provisioning] (アウトバウンドプロビジョニング) ページが表示されるまで、繰り返し [Next] (次へ) をしクリックします。ページが表示されたら、[Configure Provisioning] (プロビジョニングの設定) ボタンをクリックします。
7. 前の手順で、IAM Identity Center から [SCIM エンドポイント] の値をコピーしました。その値を PingFederate コンソールの [SCIM URL] フィールドに貼り付けます。また、前の手順で、IAM アイデンティティセンターの [アクセストークン] の値をコピーしました。その値を PingFederate コンソールの [アクセストークン] フィールドに貼り付けます。[Save] (保存) をクリックします。
8. [Channel Configuration (Configure Channels)] (チャンネル設定 (チャンネルの設定)) ページで [Create] (作成) をクリックします。
9. 新しいプロビジョニングチャネルのチャネル名 (**`AWSIAMIdentityCenterchannel`** など) を入力し、[Next] (次へ) をクリックします。
10. [ソース] ページでは、IAM Identity Center への接続に使用する [アクティブデータストア] を選択し、[次へ] をクリックします。

> **Note**
>
> データソースを設定していない場合は、すぐに設定する必要があります。Ping でのデータソースの選択と設定方法については、PingFederate 製品のドキュメントを参照してください。

11. [Source Settings] (ソースの設定) ページで、すべての値がインストールに対して正しいことを確認して、[Next] (次へ) をクリックします。
12. [Source Location] (ソースの場所) ページで、データソースに適した設定を入力して、[Next] (次へ) をクリックします。例えば、アクティブディレクトリを LDAP ディレクトリとして使用する場合などです。

    a. AD フォレストのベース DN を入力します (例: **`DC=myforest,DC=mydomain,DC=com`**)。

    b. [ユーザー] > [グループ DN] を選択して、IAM Identity Center にプロビジョニングしたいすべてのユーザーを含む単一のグループを指定します。単一のグループが存在しない場合は、AD にグループを作成してからこの設定に戻って、対応する DN を入力します。

    c. サブグループを検索するかどうか (ネスト検索) と、必要な LDAP フィルターを指定します。

    d. [グループ] > [グループ DN] を選択して、IAM Identity Center にプロビジョニングしたいすべてのグループを含む単一のグループを指定します。通常、これは [Users] (ユーザー) セクションで指定したのと同じ DN である可能性があります。必要に応じて ネスト検索とフィルターの値を入力します。

13. [Attribute Mapping] (属性マッピング) ページで以下の項目を確認し、[Next] (次へ) をクリックします。

    a. [userName] フィールドは、E メールとしてフォーマットされた属性にマッピングされている必要があります (user@domain.com)。また、ユーザーが Ping にログインする際に使用する値と一致していなければなりません。この値は、フェデレーション認証の際に SAML `nameId` クレームに入力され、IAM Identity Center でのユーザーとのマッチングに使用されます。例えば、アクティブディレクトリを使用している場合、userName に `UserPrincipalName` を指定することができます。

    b. サフィックスに * が付いているその他のフィールドは、ユーザーの NULL 以外の属性にマップする必要があります。

14. [Activation & Summary] (アクティベーションとサマリー) ページで、[Channel Status] (チャネルステータス) を Active (アクティブ) に設定すると、保存するとすぐに同期が開始されます。

15. ページ上の設定値がすべて正しいことを確認して、[Done] (完了) をクリックします。
16. [Manage Channels] (チャネルの管理) ページで [Save] (保存) をクリックします。
17. この時点で、プロビジョニングが開始します。アクティビティは、provisioner.log ファイルで確認できます。デフォルトでは PingFederate サーバーの pingfederate-<version>/pingfederate/log ディレクトリに保存されています。
18. ユーザーおよびグループが IAM Identity Center にすべて正常に同期されたことを確認するには、 IAM Identity Center コンソールに戻り、[Users] (ユーザー) を選択します。PingFederate から同期されたユーザーは、[ユーザー] ページに表示されます。また、同期したグループは [Groups] (グループ) ページで確認できます。

(オプション) ステップ 3: IAM Identity Center でのアクセスコントロールのために でユーザー属性を設定する

これは、AWS リソースへのアクセスを管理するために IAM Identity Center の属性設定を選択した場合の PingFederate のオプション手順です。PingFederate で定義した属性は、SAML アサーションで IAM Identity Center に渡されます。その後、IAM Identity Center でアクセス権限セットを作成し、PingFederate から渡された属性に基づいてアクセスを管理します。

この手順を始める前に、最初に アクセスコントロールの属性 機能を有効にしておく必要があります。これを行う方法については、「アクセスコントロールのための属性の有効化と設定」を参照してください。

IAM Identity Center でのアクセスコントロールに使用される PingFederate の属性の有効化と設定

1. PingFederate 管理コンソールにサインオンします。
2. ページ上部の [Applications] (アプリケーション) を選択し、[SP Connections] (SP 接続) をクリックします。
3. IAM Identity Center との SAML 接続を形成するために前回作成したアプリケーションを検索して、接続名をクリックします。
4. ページの上部にある暗いナビゲーションの見出しから [Browser SSO] (ブラウザ SSO) を選択します。次に [Configure Browser SSO] (ブラウザ SSO の設定) をクリックします。
5. [Configure Browser SSO] (ブラウザ SSO の設定) ページで、[Assertion Creation] (アサーションの作成) を選択し、[Configure Assertion Creation] (アサーション作成の設定) をクリックします。
6. [Configure Assertion Creation] (アサーション作成の設定) ページで、[Attribute Contract] (属性契約) を選択します。

7. [Attribute Contract] (属性の契約) ページの [Extend the Contract] (契約の拡張) セクションで、以下の手順で新しい属性を追加します。

   a. テキストボックスには `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`** を入力し、**`AttributeName`** は IAM Identity Center で想定している属性名に置き換えます。例えば、`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**。

   b. [属性名の形式] では、[urn:oasis:names:tc:SAML:2.0:attrname-format:uri] を選択します。

   c. [Add] (追加) を選択して、次に [Next] (次へ) を選択します。

8. [Authentication Source Mapping] (認証ソースマッピング) ページで、アプリケーションに設定されているアダプタインスタンスを選択します。

9. [Attribute Contract Fulfillment] (属性契約の履行) ページで、[Attribute Contract] (属性契約) `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`** の [Source] (ソース) (data store (データストア)) と [Value] (値) (data store attribute (データストア属性)) を選択します。

   > **Note**
   >
   > データソースを設定していない場合は、すぐに設定する必要があります。Ping でのデータソースの選択と設定方法については、PingFederate 製品のドキュメントを参照してください。

10. [Activation & Summary] (アクティベーションとサマリー) ページが表示されるまで、繰り返し [Next] (次へ) をクリックします。ページが表示されたら、[Save] (保存) をクリックします。

(オプション) アクセスコントロールの属性を渡す

IAM Identity Center の アクセスコントロールの属性 機能をオプションで使用して、Name 属性を `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`** に設定した `Attribute` 要素を渡すことができます。この要素を使用すると、SAML アサーションでセッションタグとして属性を渡すことができます。セッションタグの詳細については、「IAM ユーザーガイド」の「AWS STS でのタグ付けの規則 」を参照してください。

属性をセッションタグとして渡すには、タグの値を指定する `AttributeValue` 要素を含めます。例えば、タグのキーバリューのペア `CostCenter = blue` を渡すには、次のような属性を使用します。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

複数の属性を追加する必要がある場合は、各タグに個別の `Attribute` 要素を含めます。

トラブルシューティング

PingFederate を使用した一般的な SCIM および SAML のトラブルシューティングについては、以下のセクションを参照してください。

- 特定のユーザーが、外部の SCIM プロバイダーからの IAM Identity Center に同期できません
- IAM Identity Center によって作成された SAML アサーションの内容に関する問題
- 外部 ID プロバイダーを使用してユーザーまたはグループをプロビジョニングする際の重複ユーザーまたはグループのエラー
- PingFederate の詳細については、「PingFederate のドキュメント」を参照してください。

AWS を使用する際のトラブルシューティングに役立つリソースを以下に示します。

- AWS re:Post — 問題のトラブルシューティングに役立つ FAQ やその他のリソースへのリンクを検索できます。
- AWS サポート - テクニカルサポートを受ける

PingOne

IAM Identity Center は、Ping Identity(以下、Ping) の PingOne 製品から IAM Identity Center へのユーザー情報の自動プロビジョニング (同期化) をサポートしています。このプロビジョニングでは、クロスドメインアイデンティティ管理システム (SCIM) v2.0 プロトコルを使用します。この接続を PingOne で設定するには、IAM Identity Center SCIM エンドポイントとアクセストークンを使用します。SCIM 同期を設定すると、PingOne のユーザー属性と IAM Identity Center の名前付き属性のマッピングが作成されます。これにより、IAM Identity Center と PingOne の間で、期待される属性が一致します。

次のステップでは、SCIM プロトコルを使用して、PingOne から IAM Identity Center へのユーザーとグループの自動プロビジョニングを有効にする方法を説明します。

> **Note**
>
> SCIM のデプロイを開始する前に、まず 自動プロビジョニングを使用する際の注意事項 を確認することをお勧めします。そして、次のセクションで残りの注意事項を確認します。

トピック

- 前提条件
- 考慮事項
- ステップ 1: IAM Identity Center でプロビジョニングを有効にする
- ステップ 2: PingOne でプロビジョニングを設定する
- (オプション) ステップ 3: IAM Identity Center でのアクセスコントロールのために PingOne でユーザー属性を設定する
- (オプション) アクセスコントロールの属性を渡す
- トラブルシューティング

前提条件

開始する前に、以下の準備が必要です。

- フェデレーション認証とプロビジョニング機能の両方を備えた PingOne のサブスクリプションまたは無料トライアル。無料トライアルの取得方法の詳細については、Ping Identityウェブサイトを参照してください。
- IAM アイデンティティセンター対応アカウント (無料)。詳細については、「IAM Identity Center の有効化」を参照してください。
- PingOneIAM ID センターアプリケーションがPingOne管理ポータルに追加されました。PingOneIAM Identity Center アプリケーションはPingOneアプリケーションカタログから入手できます。一般的な情報については、Ping Identity ウェブサイトの「アプリケーションカタログからアプリケーションを追加する」を参照してください。
- PingOne インスタンスから IAM Identity Center への SAML 接続。PingOneIAM Identity Center アプリケーションが、PingOne管理者ポータルに追加されたら、そのアプリケーションを使用して、PingOneインスタンスから IAM Identity Center への SAML 接続を設定する必要があります。両端のメタデータの「ダウンロード」および「インポート」機能を使用して、PingOne と IAM Identity Center 間で SAML メタデータを交換します。この接続を設定する手順については、PingOne のドキュメントを参照してください。

- IAM Identity Center を追加リージョンにレプリケートした場合は、ID プロバイダーの設定を更新して、AWS マネージドアプリケーションへのアクセスと、それらのリージョンから AWS アカウント へのアクセスを有効にする必要があります。詳細については、以下を参照してください。the section called “手順 3 (外部 ID プロバイダーのみ): 外部 IdP 設定を更新する”詳細については、PingOne のドキュメントを参照してください。

考慮事項

以下は、IAM Identity Center によるプロビジョニングの実装方法に影響を与える可能性がある PingOne に関する重要な注意事項です。

- PingOne は SCIM によるグループのプロビジョニングをサポートしていません。Ping の SCIM のグループサポートに関する最新情報については、PingOne にお問い合わせください。
- PingOne 管理者ポータルでプロビジョニングを無効にしても、PingOne からユーザーのプロビジョニングが継続される場合があります。プロビジョニングをすぐに終了する必要がある場合は、該当する SCIM ベアラートークンを削除するか、IAM Identity Center の SCIM を使用して外部 ID プロバイダーからユーザーとグループをプロビジョニングする を無効にします。
- ユーザーの属性が PingOne で設定されたデータストアから削除されても、IAM Identity Center の対応するユーザーからはその属性は削除されません。これは、PingOne’s のプロビジョナーの実装における既知の制限です。属性が変更された場合、その変更は IAM Identity Center に同期されます。
- 以下は、PingOne での SAML 設定に関する重要な注意事項です。
  - IAM Identity Center は `NameId` 形式として `emailaddress` のみサポートします。これは、PingOne の SAML_SUBJECT マッピングのために、PingOne のディレクトリ内で一意であり、NULL 以外で、E メール/UPN としてフォーマットされた (例えば、user@domain.com) ユーザー属性を選択する必要があるということです。E メール (仕事用) は、 のPingOne内部ディレクトリを使ったテスト構成に使用するのに適した値です。
  - PingOne で + 文字を含むメールアドレスを使用しているユーザーが IAM Identity Center にサインインできず、`'SAML_215'` や `'Invalid input'` などのエラーが発生することがあります。この問題を解決するには、PingOne で、[属性マッピング] の [SAML_SUBJECT] マッピングで [詳細] オプションを選択します。次に、[SP に送信する名前 ID フォーマット:] をドロップダウンメニューで「urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress」に設定します。

ステップ 1: IAM Identity Center でプロビジョニングを有効にする

この最初のステップでは、IAM Identity Center コンソールを使用して、自動プロビジョニングを有効にします。

IAM アイデンティティセンターで自動プロビジョニングを有効にするには

1. 前提条件が整ったら、IAM アイデンティティセンターコンソールを開きます。
2. 左側のナビゲーションペインの [設定] を選択します。
3. [設定] ページで、[自動プロビジョニング] 情報ボックスを探し、[有効化] を選択します。これにより、すぐに IAM アイデンティティセンターの自動プロビジョニングが有効になり、必要なエンドポイントとアクセストークンの情報が表示されます。
4. [インバウンド自動プロビジョニング] ダイアログボックスで、SCIM エンドポイントとアクセストークンをコピーします。これらは、後で IdP でプロビジョニングを設定する際に貼り付ける必要があります。

   a. [SCIM エンドポイント] - 例えば https://scim.*us-east-2*.amazonaws.com/*11111111111-2222-3333-4444-555555555555*/scim/v2

   b. [アクセストークン] - [トークンを表示] を選択して値をコピーします。

   > **Warning**
   >
   > SCIM エンドポイントとアクセストークンを取得できるタイミングは、この時のみです。先に進む前に、これらの値をコピーしておいてください。このチュートリアルの後半で、お使いの IdP 上でこれらの値を入力して自動プロビジョニングを設定します。

5. [閉じる] を選択します。

IAM Identity Center でプロビジョニングを設定したので、PingOne IAM Identity Center アプリケーションを使用して残りのタスクを完了する必要があります。これらのステップについて、次の手順で説明します。

ステップ 2: PingOne でプロビジョニングを設定する

PingOne IAM Identity Center アプリケーションで以下の手順を使用して、IAM Identity Center によるプロビジョニングを有効にします。この手順では、PingOne IAM Identity Center アプリケーションが

PingOne管理ポータルに既に追加されていることを前提としています。まだ実行していない場合は、「前提条件」を参照してから、この手順を実行して SCIM プロビジョニングを設定してください。

PingOne でプロビジョニングを設定するには

1. PingOne の SAML 設定でインストールした PingOne IAM Identity Center アプリケーションを開きます ([アプリケーション] > [マイアプリケーション])。「前提条件」を参照してください。
2. ページの下部までスクロールします。[User Provisioning] (ユーザープロビジョニング) では、[Complete] (完了) リンクを選択して、接続のユーザープロビジョニング構成に移動します。
3. [Provisioning Instructions] (プロビジョニング手順) ページで、[Continue to Next Step] (次のステップに進む) を選択します。
4. 前の手順で、IAM Identity Center から [SCIM エンドポイント] の値をコピーしました。その値をPingOne IAM Identity Center アプリケーションの [SCIM URL] フィールドに貼り付けます。また、前の手順で、IAM アイデンティティセンターの [アクセストークン] の値をコピーしました。その値をPingOne IAM Identity Center アプリケーションの [ACCESS_TOKEN] フィールドに貼り付けます。
5. [REMOVE_ACTION] では、[Disabled] または [Delete] のいずれかを選択します (詳細はページの説明を参照してください)。
6. [Attribute Mapping] (属性マッピング) ページでは、このページで紹介した 考慮事項 のガイダンスに従って、SAML_SUBJECT (`NameId`) アサーションに使用する値を選択します。[Next] (次へ) を選択して続行します。
7. [PingOne アプリケーションのカスタマイズ - IAM Identity Center] ページで、必要なカスタマイズの変更を行い (オプション)、[次のステップに進む] をクリックします。
8. [グループアクセス] ページでは、プロビジョニングと IAM Identity Center へのシングルサインオンを有効にするユーザーを含むグループを選択します。[Continue to Next Step] (次のステップに進む) を選択します。
9. ページの下部までスクロールして、[Finish] (完了) を選択してプロビジョニングを開始します。
10. ユーザーが IAM Identity Center に正常に同期されたことを確認するには、IAM Identity Center コンソールに戻り、[ユーザー] を選択します。PingOne から同期されたユーザーは、[ユーザー] ページに表示されます。これらのユーザーは、IAM Identity Center 内のアカウントおよびアプリケーションに割り当てられるようになりました。

    PingOne は SCIM によるグループやグループメンバーシップのプロビジョニングをサポートしていないことに注意してください。詳細については、Ping にお問い合わせください。

(オプション) ステップ 3: IAM Identity Center でのアクセスコントロールのために PingOne でユーザー属性を設定する

これは、AWS リソースへのアクセスを管理するために IAM Identity Center の属性設定を選択した場合の PingOne のオプション手順です。PingOne で定義した属性は、SAML アサーションで IAM Identity Center に渡されます。その後、IAM Identity Center でアクセス権限セットを作成し、PingOne から渡された属性に基づいてアクセスを管理します。

この手順を始める前に、最初に アクセスコントロールの属性 機能を有効にしておく必要があります。これを行う方法については、「アクセスコントロールのための属性の有効化と設定」を参照してください。

IAM Identity Center でのアクセスコントロールに使用される PingOne の属性の有効化と設定

1. PingOne の SAML 設定でインストールした PingOne IAM Identity Center アプリケーションを開きます (アプリケーション > マイアプリケーション)。
2. [Edit] (編集) を選択し、[Continue to Next Step] (次のステップに進む) を選択すると、[Attribute Mappings] (属性マッピング) ページが表示されます。
3. [Attribute Mappings] (属性マッピング) ページで [Add new attribute] (新規属性の追加) を選択し、以下の操作を行います。これらの手順は、IAM Identity Center でのアクセスコントロールに使用するために追加する各属性について行う必要があります。

    a. [Application Attribute] (アプリケーション属性) フィールドに `https://aws.amazon.com/SAML/Attributes/AccessControl:`*`AttributeName`* と入力します。*`AttributeName`* を IAM Identity Center で想定している属性名に置き換えます。例えば、`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**。

    b. [ID ブリッジ属性またはリテラル値] フィールドで、PingOne ディレクトリからユーザー属性を選択します。例えば、E メール (仕事用)。
4. [Next] (次へ) を数回選択して、次に [Finish] (完了) を選択します。

(オプション) アクセスコントロールの属性を渡す

IAM Identity Center の アクセスコントロールの属性 機能をオプションで使用して、Name 属性を `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`** に設定した Attribute 要素を渡すことができます。この要素を使用すると、SAML アサーションでセッションタグとして属性を渡すことができます。セッションタグの詳細については、「IAM ユーザーガイド」の「AWS STS でのタグ付けの規則 」を参照してください。

属性をセッションタグとして渡すには、タグの値を指定する AttributeValue 要素を含めます。例えば、タグのキーバリューのペア CostCenter = blue を渡すには、次のような属性を使用します。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

複数の属性を追加する必要がある場合は、各タグに個別の Attribute 要素を含めます。

トラブルシューティング

PingOne を使用した一般的な SCIM および SAML のトラブルシューティングについては、以下のセクションを参照してください。

- 特定のユーザーが、外部の SCIM プロバイダーからの IAM Identity Center に同期できません
- IAM Identity Center によって作成された SAML アサーションの内容に関する問題
- 外部 ID プロバイダーを使用してユーザーまたはグループをプロビジョニングする際の重複ユーザーまたはグループのエラー
- PingOne の詳細については、「PingOne のドキュメント」を参照してください。

AWS を使用する際のトラブルシューティングに役立つリソースを以下に示します。

- AWS re:Post — 問題のトラブルシューティングに役立つ FAQ やその他のリソースへのリンクを検索できます。
- AWS サポート - テクニカルサポートを受ける

デフォルトの IAM アイデンティティセンターディレクトリ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を初めて有効にすると、アイデンティティセンターディレクトリがデフォルトの ID ソースとして自動的に構成されるため、ID ソースを選択する必要はありません。組織が、Microsoft Active Directory、Microsoft Entra ID または Okta などの別の ID プロバイダーを使用

している場合、デフォルト設定を使用する代わりに、その ID ソースを IAM アイデンティティセンターと統合することを検討してください。

目的

このチュートリアルでは、デフォルトのディレクトリを ID ソースとして使用し、IAM アイデンティティセンター組織インスタンスを使用して管理ユーザーをセットアップしてテストします。この管理ユーザーは、ユーザーとグループを作成および管理し、アクセス許可セットを使用して AWS アクセスを許可します。次のステップでは、以下を作成します。

- *Nikki Wolf* という名前の管理ユーザー
- ***#####*** という名前のグループ。
- *AdminAccess* という名前のアクセス許可セット

すべてが正しく作成されたことを確認するには、サインインして管理ユーザーのパスワードを設定します。このチュートリアルを完了すると、管理ユーザーを使用して IAM アイデンティティセンターにユーザーを追加したり、アクセス許可セットを追加したり、アプリケーションへの組織的なアクセスを設定したりできます。または、ユーザーにアプリケーションへのアクセスを許可する場合は、この手順のステップ 1 に従ってアプリケーションアクセスを設定できます。

前提条件

このチュートリアルを完了するには、以下の前提条件が必要です。

- IAM Identity Center を有効にする であり、IAM アイデンティティセンターの組織インスタンスを持っている。
  - IAM アイデンティティセンターのアカウントインスタンスを持っていれば、ユーザーとグループを作成し、アプリケーションへのアクセス権を付与できます。詳細については、「アプリケーションへのアクセス」を参照してください。
- AWS マネジメントコンソール にサインインし、IAM アイデンティティセンターコンソールを開きます。
  - 新規の AWS (ルートユーザー) – [AWS アカウント ルートユーザー] を選択し、AWS アカウント の E メールアドレスを入力して、アカウント所有者としてサインインします。次のページでパスワードを入力します。
  - すでに使用している AWS (IAM 認証情報) — 管理者権限を持つ IAM 認証情報を使用してサインインします。

  - AWS マネジメントコンソール へのサインインの詳細については、「AWS サインインガイド」を参照してください。
- IAM アイデンティティセンターユーザーの多要素認証を設定できます。詳細については、「IAM アイデンティティセンターでの MFA の設定」を参照してください。

ステップ 1: ユーザーを追加する

1. IAM Identity Center コンソールを開きます。
2. IAM アイデンティティセンターナビゲーションペインで、[ユーザー] を選択し、[ユーザーの追加] を選択します。
3. [ユーザーの詳細を指定] ページで、次の情報を入力します。
   - [ユーザー名] - このチュートリアルでは、*nikkiw* と入力します。

     ユーザーを作成するときは、覚えやすいユーザー名を選択してください。ユーザーは AWS アクセスポータルにサインインする際にユーザー名を覚えておく必要があり、後で変更することはできません。
   - [パスワード] - [このユーザーにパスワード設定の手順を記載した E メールを送信 (推奨)] を選択します。

     このオプションでは、Amazon Web Services からユーザーに「Invitation to join IAM Identity Center」という件名の E メールが送信されます。E メールは、`no-reply@signin.aws` または `no-reply@login.awsapps.com` から送信されます。これらの E メールアドレスを承認済み送信者リストに追加してください。
   - [E メールアドレス] - メールを受信できるユーザーの E メールアドレスを入力します。確認のため再入力します。各ユーザーは一意の E メールアドレスを持っている必要があります。
   - [名] - ユーザーの名を入力します。このチュートリアルでは、*Nikki* と入力します。
   - [姓] - ユーザーの姓を入力します。このチュートリアルでは、*Wolf* と入力します。
   - [表示名] - デフォルト値は、ユーザーの名と姓です。表示名を変更したい場合は、別の名前を入力できます。表示名はサインインポータルとユーザーリストに表示されます。
   - 必要に応じてオプション情報を入力します。このチュートリアルでは使用されないので、後で変更できます。
4. [次へ] を選択します。[ユーザーをグループに追加] ページが表示されます。*Nikki* に直接アクセス許可を与えるのではなく、管理者のアクセス許可を割り当てるグループを作成します。

[グループを作成] を選択する

新しいブラウザタブで [グループの作成] ページが開きます。

a. [グループの詳細] の [グループ名] に、グループの名前を入力します。グループのロールを識別するグループ名を使用することをおすすめします。このチュートリアルでは、*Admin team*と入力します。

b. [グループを作成] を選択する

c. [グループ] ブラウザータブを閉じて、[ユーザーを追加] ブラウザタブに戻ります。

5. [グループ] 領域で、[更新] ボタンを選択します。*#####*グループがリストに表示されます。

[#####] の横にあるチェックボックスをオンにし、[次へ] を選択します。

6. [ユーザーの確認と追加] ページで、次のことを確認します。

- 主要情報は意図したとおりに表示されます。
- グループには、作成したグループに追加されたユーザーが表示されます。

変更するには、[Edit] (編集) を選択します。すべての情報が正しければ、[ユーザーを追加] を選択します。

ユーザーが追加されたことを知らせる通知メッセージが表示されます。

次に、*#####*グループの管理アクセス許可を追加して、*Nikki* がリソースにアクセスできるようにします。

ステップ 2: 管理者アクセス許可を追加する

> **Important**
>
> IAM アイデンティティセンターの組織インスタンスを有効にした場合にのみ、以下の手順に従います。

1. IAM アイデンティティセンターのナビゲーションペインの [マルチアカウントのアクセス許可] で、[AWS アカウント] を選択します。

2. [AWS アカウント] ページの[組織構造] には、自分の組織とその下のアカウントが階層内で表示されます。管理アカウントのチェックボックスをオンにし、[ユーザーまたはグループを割り当て] を選択します。
3. [ユーザーとグループを割り当てる] のワークフローが表示されます。これは、3 つのステップから構成されています。

   a. [ステップ 1: ユーザーとグループの選択] では、作成した*#####*グループを選択します。次に、[次へ] を選択します。

   b. [ステップ 2: アクセス許可セットの選択] では、[許可セットを作成] を選択します。新しいタブが開き、アクセス許可セットを作成するための 3 つのサブステップが順を追って表示されます。

      i. [ステップ 1: 許可セットタイプを選択] では、以下を完了します。

         - [許可セットのタイプ] で、[事前定義された許可セット] を選択します。
         - [事前定義された許可セットのポリシー] で [AdministratorAccess] を選択します。

         [次へ] を選択します。

      ii. [ステップ 2: 許可セットの詳細を指定] では、デフォルト設定のままで、[次へ] を選択します。

         デフォルト設定では、*AdministratorAccess* という名前の許可セットが作成され、セッション期間は 1 時間に設定されます。アクセス許可セットの名前を変更するには、[許可セット名] フィールドに新しい名前を入力します。

      iii. [ステップ 3: 確認して作成] では、[許可セットのタイプ] が AWS 管理ポリシー [AdministratorAccess] を使用していることを確認します。[作成] を選択します。[アクセス許可セット] ページに、アクセス許可セットが作成されたことを知らせる通知が表示されます。この時点で、ウェブブラウザでこのタブを閉じてもかまいません。

   [ユーザーとグループを割り当てる] ブラウザタブでは、[ステップ 2: 許可セットを選択] でアクセス許可セットの作成ワークフローを開始した状態のままになっています。

   [アクセス許可セット] 領域で、[更新] ボタンを選択します。作成した *AdministratorAccess* 許可セットがリストに表示されます。そのアクセス許可セットのチェックボックスを選択して、[次へ] を選択します。

c. [ステップ 3: 割り当ての確認と送信] ページで、*[######]* グループが選択されていることと、*AdministratorAccess* 許可セットが選択されていることを確認し、[送信] を選択します。

ページが更新され、AWS アカウント が設定中であることを示すメッセージが表示されます。プロセスが完了するまで待ちます。

AWS アカウント ページに戻ります。AWS アカウント が再プロビジョニングされ、更新されたアクセス許可セットが適用されたことを知らせる通知メッセージが表示されます。

お疲れ様でした。

最初のユーザー、グループ、アクセス許可セットが正常に設定されました。

このチュートリアルの次の部分では、管理者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、パスワードを設定して *Nikki* のアクセスをテストします。すぐにコンソールからサインアウトします。

ステップ 3: ユーザーアクセスのテスト

これで *Nikki Wolf* は組織のユーザーになりました。Nikki Wolf は、サインインして、アクセス許可セットに従ってアクセス許可が付与されているリソースにアクセスできます。ユーザーが正しく設定されていることを確認するために、次のステップでは *Nikki* の認証情報を使用してサインインし、パスワードを設定します。ステップ 1 でユーザー *Nikki Wolf* を追加したときに、*Nikki* にパスワード設定手順が記載された E メールが送信されるように選択しました。この E メールを開いて、以下の操作を行います。

1. E メール内の [招待を承認] リンクを選択して招待を承諾します。

   Note

   E メールには、*Nikki* のユーザー名と、組織へのサインインに使用する AWS アクセスポータル URL も含まれています。将来使用するためにこの情報を記録します。

   Nikki のパスワードを設定し、MFA デバイスを登録できる [新規ユーザーのサインアップ] ページが表示されます。

2. *Nikki* のパスワードを設定すると、[サインイン] ページに移動します。*nikkiw* と入力して [次へ] を選択し、*Nikki* のパスワードを入力して [サインイン] を選択します。
3. AWS アクセスポータルが開き、アクセス可能な組織とアプリケーションが表示されます。

   組織を選択して AWS アカウント のリストを展開し、アカウントを選択すると、アカウント内のリソースへのアクセスに使用できるロールが表示されます。

   各アクセス許可セットには、ロール方式とアクセスキー方式の 2 つの管理方式があります。

   - ロール方式、例えば*AdministratorAccess*の場合、AWS Console Homeを開きます。
   - アクセスキー方式の場合、AWS CLI および/または AWS SDK で使用できる認証情報が提供されます。自動的に更新される短期認証情報または短期アクセスキーのいずれかを使用するための情報が含まれます。詳細については、「AWS CLI または AWS SDK の IAM Identity Center のユーザー認証情報を取得します。」を参照してください。
4. [ロール] のリンクを選択して AWS Console Homeにサインインします。

サインインし、AWS Console Home ページに移動しました。コンソールを表示して、期待どおりのアクセス許可があることを確認します。

次のステップ

IAM アイデンティティセンターで管理ユーザーを作成したため、次のことができるようになりました。

- アプリケーションを割り当てる
- 他のユーザーを追加する
- ユーザーをアカウントに割り当てる
- 追加のアクセス許可セットを設定する

> **Note**
>
> 同じユーザーに複数のアクセス許可セットを割り当てることもできます。最小権限の権限を適用するというベストプラクティスに従うには、管理ユーザーを作成した後に、より制限の厳しいアクセス権限セットを作成して同じユーザーに割り当てます。そうすれば、管理者権限ではなく、必要な権限のみで AWS アカウント にアクセスできるようになります。

ユーザがアカウントを有効化するための招待を受け入れ、AWS アクセスポータルにサインインすると、ポータルに表示されるのは、割り当てられている AWS アカウント、ロール、アプリケーションに関する項目だけです。

ビデオチュートリアル

追加のリソースとして、以下のビデオチュートリアルを使用して、外部 ID プロバイダーの設定について詳しく知ることができます。

- での外部 ID プロバイダー間の移行AWS IAM アイデンティティセンター
- Microsoft Entra ID を使用して既存の AWS IAM アイデンティティセンター インスタンスをフェデレーションする

IAM アイデンティティセンターでワークフォースを設定する

IAM Identity Center は、ワークフォースユーザーを Kiro や Amazon Quick などの AWS マネージドアプリケーションやその他の AWS リソースに接続するための AWS ソリューションです。既存の ID プロバイダーを接続してお手持ちのディレクトリとの間でユーザーやグループを同期したり、あるいは IAM アイデンティティセンター内でユーザーを直接作成して管理することができます。

へのアクセスに IAM を既に使用していますか?AWS アカウント

IAM アイデンティティセンターを使用して AWS マネージドアプリケーションにアクセスするのに現在の AWS アカウントワークフローを変更する必要はありません。AWS アカウント へのアクセスに IAM とのフェデレーションを使用している場合、各ユーザーはこれまでと同じ方法で AWS アカウント にアクセスし、既存のワークフローを使用してアクセスを管理することができます。

組織の ID 管理戦略と既存のインフラストラクチャに最適なアプローチを選択します。

トピック

- IAM アイデンティティセンターにおけるユーザー、グループ、およびプロビジョニング
- ID ソースを管理する
- アイデンティティセンターディレクトリでユーザーを管理する

IAM アイデンティティセンターにおけるユーザー、グループ、およびプロビジョニング

IAM アイデンティティセンターを使用すると、サインインできるユーザーとアクセスできるリソースをコントロールできます。サインインするには、ユーザーをプロビジョニングする必要があります。その後、プロビジョニングされたユーザーまたはグループにのみアクセスを割り当てることができます。IAM アイデンティティセンターにおけるユーザー、グループ、およびプロビジョニングについて説明します。

ユーザー名と E メールアドレスの一意性

IAM アイデンティティセンターでは、各ユーザーに一意のユーザー名が必要です。ユーザー名はユーザーのプライマリ識別子です。ユーザー名はユーザーの E メールアドレスと一致する必要はあ

りません。IAM アイデンティティセンターでは、ユーザーのすべてのユーザー名と E メールアドレスが、NULL ではない一意なものである必要があります。

グループ

グループは、定義するユーザーの論理的な組み合わせです。グループを作成し、グループにユーザーを追加できます。IAM アイデンティティセンターは、ネストされたグループ構成 (グループ内のグループ) をサポートしていません。グループは、AWS アカウント やアプリケーションへのアクセスを割り当てる際に便利です。各ユーザーを個別に割り当てるのではなく、グループに権限を与えます。その後、グループにユーザーを追加したり削除したりすると、そのユーザーはグループに割り当てられたアカウントやアプリケーションへのアクセス権を動的に得たり、失ったりします。

ユーザーおよびグループのプロビジョニング

プロビジョニングは、ユーザーおよびグループの情報を IAM アイデンティティセンターおよび AWS マネージドアプリケーションまたはカスタマーマネージドアプリケーションで使用できるようにするプロセスです。ユーザーとグループを IAM アイデンティティセンターで直接作成することも、アイデンティティソースを IAM アイデンティティセンターに接続することもできます。IAM アイデンティティセンターを使用すると、接続されたアプリケーションと AWS アカウント へのアクセスをユーザーとグループに割り当てることができます。

IAM Identity Center のプロビジョニングは、使用する ID ソースに応じて異なります。詳細については、「ID ソースを管理する」を参照してください。

ユーザーおよびグループのプロビジョニング解除

プロビジョニング解除は、IAM アイデンティティセンターからユーザーとグループ情報を削除するプロセスです。

IAM アイデンティティセンターで Active Directory または外部 ID プロバイダーを使用している場合は、IAM アイデンティティセンターではなく、これらの ID ソースからユーザーとグループを削除する必要があります。ID ソースが Active Directory または外部 ID プロバイダーである場合、IAM アイデンティティセンターユーザーとグループを削除しても、それらは完全に削除されません。

IAM アイデンティティセンターユーザーまたはグループのプロビジョニングを解除する必要がある場合は、まず、プロビジョニングを解除するユーザーまたはグループに対するアクセス許可セットまたはアプリケーションの割り当てをすべて削除する必要があります。それ以外の場合は、IAM アイデンティティセンターに未割り当てのアクセス許可セットとアプリケーション割り当てがあります。

ID ソースを管理する

IAM Identity Center の ID ソースは、ユーザーやグループがどこで管理されているかを定義します。ID ソースの設定が完了すると、ユーザーまたはグループを検索して、AWS アカウント、アプリケーション、またはその両方へのシングルサインオンアクセスを付与することができます。

ID ソースは AWS Organizations で組織あたり 1 つのみ持つことができます。ID ソースとして以下のいずれかを選択できます。

- 外部 ID プロバイダー – Okta や Microsoft Entra ID などの外部 ID プロバイダー (IdP) でユーザーを管理したい場合は、このオプションを選択します。
- オンプレミスまたは AWS マネージド Active Directory – Active Directory (AD) を接続する場合は、このオプションを選択します。
- アイデンティティセンターディレクトリ — IAM アイデンティティセンターを初めて有効にすると、別の ID ソースを選択しない限り、デフォルトの ID ソースとしてアイデンティティセンターディレクトリで自動的に設定されます。Identity Center ディレクトリを使用して、ユーザーとグループを作成し、AWS アカウントやアプリケーションへのアクセスレベルを割り当てることができます。

> **Note**
>
> IAM Identity Center は SAMBA4 ベースの Simple AD をアイデンティティソースとしてサポートしていません。

トピック

- ID ソースの変更に関する注意事項
- アイデンティティソースを変更する
- IAM アイデンティティセンターでサポートされるユーザー属性とグループ属性
- 外部 ID プロバイダー
- Microsoft AD ディレクトリ

ID ソースの変更に関する注意事項

アイデンティティソースはいつでも変更できますが、この変更が現在のデプロイにどのように影響するかを検討することをお勧めします。

あるアイデンティティソースですでにユーザーとグループを管理している場合、別のアイデンティティソースに変更すると、IAM アイデンティティセンターで設定したユーザーとグループの割り当てがすべて削除される可能性があります。この場合、IAM アイデンティティセンターの管理ユーザーを含むすべてのユーザーが、AWS アカウント およびアプリケーショ ンへのシングルサインオンアクセスを失います。

IAM アイデンティティセンターの ID ソースを変更する前に、以下の考慮事項を確認してください。ID ソースの変更を続行する場合は、詳細について アイデンティティソースを変更する を参照してください。

IAM アイデンティティセンターディレクトリと Active Directory 間の切り替え

すでに Active Directory でユーザーとグループを管理している場合は、IAM アイデンティティセンターを有効にして ID ソースを選択するときに、ディレクトリの接続を検討することをお勧めします。デフォルトの Identity Center ディレクトリにユーザーやグループを作成して割り当てを行う前に、この作業を行ってください。

> **Important**
>
> IAM アイデンティティセンターの ID ソースタイプを Active Directory との間で変更する場合は、ID ストア ID が変更されることに注意してください。これには、以下のような影響が考えられます。
>
> - デフォルトの AWS アクセスポータル URL が変更されます。新しい URL をワークフォースに伝え、ブックマーク、ゲートウォールまたはファイアウォールの許可リスト、およびこの URL が参照される設定を更新する必要があります。この変更は、ユーザーの中断を最小限に抑えるために、スケジュールされたメンテナンスウィンドウで実行することをお勧めします。
> - IAM アイデンティティセンターで保管時の暗号化にカスタマーマネージド KMS キーを使用していて、暗号化コンテキストで KMS キーポリシーを設定している場合は、ID ストアの暗号化コンテキストが変更されることに注意してください。例えば、ID ストア ARN の「arn:aws:identitystore::123456789012:identitystore/d-922763e9b3」では、「d-922763e9b3」は ID ストア ID です。この移行中のサービスの中断を防ぐには、ワイ

ルドカードパターン「arn:aws:identitystore::123456789012:identitystore/*」を使用するように KMS キーポリシーを一時的に変更します。

既に Identity Center のデフォルトディレクトリでユーザーとグループを管理している場合は、次の点を考慮してください。

- 割り当ての削除、ユーザーとグループの削除 — ID ソースを Active Directory に変更すると、ユーザーとグループが Identity Center ディレクトリから削除されます。この変更により、割り当ても削除されます。この場合、Active Directory に変更した後に、Active Directory のユーザーとグループを Identity Center ディレクトリに同期してから、それらの割り当てを再適用する必要があります。

  Active Directory を使用しない場合は、Identity Center のディレクトリにユーザーとグループを作成し、割り当てを行う必要があります。
- ID が削除されても割り当ては削除されない — アイデンティティセンターディレクトリで ID が削除されると、IAM アイデンティティセンターでも対応する割り当てが削除されます。しかし Active Directory では、(Active Directory または同期された ID のどちらかで) ID が削除されても、対応する割り当ては削除されません。
- API のアウトバウンド同期なし — Active Directory をアイデンティティソースとして使用する場合、「作成、更新、および削除」API は注意して使用することをお勧めします。IAM アイデンティティセンターはアウトバウンド同期をサポートしていないため、これらの API を使用してユーザーまたはグループに加えた変更によってアイデンティティソースが自動的に更新されることはありません。
- アクセスポータル URL が変更される — IAM Identity Center と Active Directory の間で ID ソースを変更すると、AWS アクセスポータルの URL も変更されます。
- IAM アイデンティティセンターコンソールで ID ストア API を使用してユーザーが削除または無効化された場合、アクティブなセッションを持つユーザーは、 統合されたアプリケーションおよびアカウントに引き続きアクセスできます。認証セッションの期間とユーザー動作については、「IAM アイデンティティセンターの認証セッションについて」を参照してください。
- マルチリージョンのサポート – IAM Identity Center を追加リージョンにレプリケートした場合や、今後レプリケートする予定がある場合は、外部 ID プロバイダーまたはアイデンティティセンターディレクトリを ID ソースとして使用する必要があります。マルチリージョンのサポートは Active Directory では使用できません。その他の前提条件などの詳細については、「複数の 間で IAM アイデンティティセンターを使用するAWS リージョン」を参照してください。

IAM アイデンティティセンターがユーザーとグループをどのようにプロビジョニングするかについては、「Microsoft AD ディレクトリ」を参照してください。

IAM アイデンティティセンターから外部 IdP への変更

ID ソースを IAM アイデンティティセンターから外部 ID プロバイダー (IdP) に変更する場合は、次の点を考慮してください。

- 割り当てとメンバーシップは正しいアサーションで機能する – 新しい IdP が正しいアサーション (SAML nameID など) を送信する限り、ユーザー割り当て、グループ割り当て、グループメンバーシップは引き続き機能します。これらのアサーションは、IAM アイデンティティセンターのユーザー名およびグループと一致する必要があります。
- アウトバウンド同期なし — IAM アイデンティティセンターはアウトバウンド同期をサポートしていないため、IAM アイデンティティセンターで行ったユーザーやグループの変更によって外部 IdP が自動的に更新されることはありません。
- SCIM プロビジョニング – SCIM プロビジョニングを使用している場合、ID プロバイダーのユーザーおよびグループに対する変更は、ID プロバイダーがそれらの変更を IAM アイデンティティセンターに送信した後にのみ IAM アイデンティティセンターに反映されます。「自動プロビジョニングを使用する際の注意事項」を参照してください。
- ロールバック – IAM アイデンティティセンターを使用して ID ソースをいつでも元に戻すことができます。「外部 IdP から IAM アイデンティティセンターへの変更」を参照してください。
- セッション期間の有効期限が切れると、既存のユーザーセッションを取り消し – ID ソースを外部 ID プロバイダーに変更すると、アクティブなユーザーセッションは、コンソールで設定された最大セッション期間の残りの間、継続します。例えば、AWS アクセスポータルセッションの期間が 8 時間に設定されていて、4 時間目に ID ソースを変更した場合、アクティブなユーザーセッションはさらに 4 時間継続されます。ユーザーセッションを取り消すには、「the section called “ワークフォースユーザーのアクティブなセッションを終了する”」を参照してください。

  IAM アイデンティティセンターコンソールで ID ストア API を使用してユーザーが削除または無効化された場合、アクティブなセッションを持つユーザーは、 統合されたアプリケーションおよびアカウントに引き続きアクセスできます。認証セッションの期間とユーザー動作については、「IAM アイデンティティセンターの認証セッションについて」を参照してください。

> **Note**
>
> ユーザーの削除後、IAM アイデンティティセンターコンソールからユーザーセッションを取り消すことはできません。

IAM アイデンティティセンターがユーザーとグループをどのようにプロビジョニングするかについては、「外部 ID プロバイダー」を参照してください。

外部 IdP から IAM アイデンティティセンターへの変更

ID ソースを外部 ID プロバイダー (IdP) から IAM アイデンティティセンターに変更する場合は、次の点を考慮してください。

- IAM アイデンティティセンターセンターではすべての割り当てが保持されます。
- パスワードリセットを強制する — IAM アイデンティティセンターでパスワードを持っていたユーザーは、以前のパスワードでサインインを続けることができます。外部 IdP にいて、IAM アイデンティティセンターにいなかったユーザーに対して、パスワードリセットを強制する必要があります。
- セッション期間の有効期限が切れると、既存のユーザーセッションが取り消される – ID ソースを IAM アイデンティティセンターに変更すると、アクティブなユーザーセッションは、コンソールで設定された最大セッション期間の残りの時間の間、継続されます。例えば、AWS アクセスポータルセッションの期間が 8 時間で、4 時間目に ID ソースを変更した場合、アクティブなユーザーセッションはさらに 4 時間継続して実行されます。ユーザーセッションを取り消すには、「the section called “ワークフォースユーザーのアクティブなセッションを終了する”」を参照してください。

  IAM アイデンティティセンターコンソールで ID ストア API を使用してユーザーが削除または無効化された場合、アクティブなセッションを持つユーザーは、 統合されたアプリケーションおよびアカウントに引き続きアクセスできます。認証セッションの期間とユーザー動作については、「IAM アイデンティティセンターの認証セッションについて」を参照してください。

  > **Note**
  >
  > ユーザーの削除後、IAM アイデンティティセンターコンソールからユーザーセッションを取り消すことはできなくなります。

IAM Identity Center がユーザーとグループをどのようにプロビジョニングするかについては、「アイデンティティセンターディレクトリでユーザーを管理する」を参照してください。

ある外部 IdP から別の外部 IdP への変更

IAM アイデンティティセンターの ID ソースとして既に外部 IdP を使用していて、別の外部 IdP に変更する場合は、次の点を考慮してください。

- アサインメントとメンバーシップは正しいアサーションで機能する – IAM アイデンティティセンターはアサインメントをすべて保持します。新しい IdP が正しいアサーション (SAML nameID など) を送信する限り、ユーザー割り当て、グループ割り当て、グループメンバーシップは引き続き機能します。

  これらのアサーションは、ユーザーが新しい外部 IdP を介して認証する際に、IAM アイデンティティセンターのユーザー名と一致する必要があります。

- SCIM プロビジョニング – IAM アイデンティティセンターへのプロビジョニングに SCIM を使用している場合は、本ガイドの IdP 固有の情報や IdP のドキュメントを確認して、SCIM を有効にしたときに新しいプロバイダーでユーザーやグループが正しく一致するかどうかを確認するようお勧めします。

- セッション期間の有効期限が切れると、既存のユーザーセッションが取り消される – ID ソースを別の外部 ID プロバイダーに変更すると、アクティブなユーザーセッションは、コンソールで設定された最大セッション期間の残り時間の間、継続します。例えば、AWS アクセスポータルセッションの期間が 8 時間で、4 時間目に ID ソースを変更した場合、アクティブなユーザーセッションはさらに 4 時間継続します。ユーザーセッションを取り消すには、「the section called “ワークフォースユーザーのアクティブなセッションを終了する”」を参照してください。

  IAM アイデンティティセンターコンソールで ID ストア API を使用してユーザーが削除または無効化された場合、アクティブなセッションを持つユーザーは、 統合されたアプリケーションおよびアカウントに引き続きアクセスできます。認証セッションの期間とユーザー動作については、「IAM アイデンティティセンターの認証セッションについて」を参照してください。

  > **Note**
  >
  > ユーザーの削除後、IAM アイデンティティセンターコンソールからユーザーセッションを取り消すことはできません。

IAM Identity Center がユーザーとグループをどのようにプロビジョニングするかについては、「外部 ID プロバイダー」を参照してください。

IAM アイデンティティセンターと Active Directory の切り替え

アイデンティティソースを外部 IdP から Active Directory に、または Active Directory から外部 IdP に変更する場合は、次の点を考慮してください。

- ユーザー、グループ、割り当てが削除される — すべてのユーザー、グループ、および割り当てが IAM アイデンティティセンターから削除されます。外部の IdP や Active Directory のユーザーやグループの情報は影響を受けません。
- ユーザーのプロビジョニング — 外部 IdP に変更した場合、ユーザーのプロビジョニングに IAM アイデンティティセンターを設定する必要があります。または、外部 IdP のユーザーやグループを手動でプロビジョニングしてから、割り当てを設定する必要があります。
- アサインメントとグループの作成 — Active Directory に変更する場合は、Active Directory 内のディレクトリにあるユーザーとグループを使用してアサインメントを作成する必要があります。
- IAM アイデンティティセンターコンソールで ID ストア API を使用してユーザーが削除または無効化された場合、アクティブなセッションを持つユーザーは、 統合されたアプリケーションおよびアカウントに引き続きアクセスできます。認証セッションの期間とユーザー動作については、「IAM アイデンティティセンターの認証セッションについて」を参照してください。
- マルチリージョンのサポート – IAM Identity Center を追加リージョンにレプリケートした場合や、今後レプリケートする予定がある場合は、外部 ID プロバイダーまたはアイデンティティセンターディレクトリを ID ソースとして使用する必要があります。マルチリージョンのサポートは Active Directory では使用できません。その他の前提条件などの詳細については、「複数の 間で IAM アイデンティティセンターを使用するAWS リージョン」を参照してください。

IAM Identity Center がユーザーとグループをどのようにプロビジョニングするかについては、「Microsoft AD ディレクトリ」を参照してください。

アイデンティティソースを変更する

以下の手順では、IAM アイデンティティセンターが提供するディレクトリ (デフォルトの ID センターディレクトリ) から Active Directory または外部 ID プロバイダ、またはその逆に変更する方法について説明します。次に進む前に、ID ソースの変更に関する注意事項の情報を確認してください。この手順を完了するには、IAM アイデンティティセンターの組織インスタンスが必要です。詳細については、「IAM アイデンティティセンターの組織インスタンスとアカウントインスタンス」を参照してください。

> **Warning**
>
> 現在のデプロイメントによっては、この変更により IAM アイデンティティセンターで設定したユーザーとグループの割り当てがすべて削除されます。この変更により、アクセス許可セットの IAM ロールも AWS アカウント から削除されます。その結果、リソースポリシーを更新する必要がある場合があります。これにより、AWS KMS キーと Amazon EKS クラス

ターへのアクセスが中断されないようにする必要があります。詳細については[リソースポリシー、Amazon EKS クラスター構成マップ、および AWS KMS キーポリシーでの権限セットを参照する]を参照してください。
この場合、IAM アイデンティティセンターの管理ユーザーを含むすべてのユーザーとグループが、AWS アカウント およびアプリケーショ ンへのシングルサインオンアクセスを失います。

アイデンティティソースを変更するには

1. [IAM アイデンティティセンターコンソール] を開きます。
2. [設定] を選択します。
3. [設定] ページの [ID ソース] タブを選択します。[アクション] を選択し、[ID ソースの変更] を選択します。
4. [ID ソースを変更] ページで、切り替え先のソースを選択し、[次へ] を選択します。

   Active Directory に変更する場合は、次のページのメニューから使用可能なディレクトリを選択します。

> **Important**
>
> ID ソースを Active Directory に変更したり、Active Directory から変更したりすると、ID センターのディレクトリからユーザーとグループが削除されます。この変更により、IAM アイデンティティセンターで設定した割り当てもすべて削除されます。

> **Note**
>
> IAM Identity Center を追加リージョンにレプリケートし、ID ソースを Active Directory に変更する場合は、まず追加リージョンをすべて削除する必要があります。マルチリージョンのサポートは、Active Directory を ID ソースとして使用するインスタンスでは使用できません。詳細については、[複数の 間で IAM アイデンティティセンターを使用するAWS リージョン]を参照してください。

外部 ID プロバイダーに切り替えるには、[外部 ID プロバイダに接続する方法]の手順を実施することをお勧めします。

5. 免責事項を読み、次に進む準備ができたら、[許諾] と入力してください。
6. [IDソースの変更] を選択します。アイデンティティソースを Active Directory に変更する場合は、次のステップに進んでください。
7. ID ソースを Active Directory に変更すると、[設定] ページが表示されます。[設定] ページでは、次のいずれかの操作を行います。

   - [ガイド付きセットアップ] を選択します。ガイド付きセットアッププロセスを完了する方法についての詳細は、ガイド付きセットアップを参照してください。
   - [アイデンティティソース] セクションで、[アクション] を選択し、[同期の管理] を選択して、[同期範囲]、つまり同期するユーザーとグループのリストを設定します。

IAM アイデンティティセンターでサポートされるユーザー属性とグループ属性

このガイドでは、IAM アイデンティティセンターでの SCIM 属性のサポートに関するリファレンスを提供します。SCIM 仕様のユーザー属性とグループ属性が IAM アイデンティティセンター ID ストアでサポートされていることをリストし、サポートされていない特定の属性とサブ属性を識別します。

属性とは、`name`、`email`、`members` など、個々のユーザーやグループのオブジェクトを定義し、識別するための情報のことです。IAM アイデンティティセンターは、手動入力と自動 SCIM プロビジョニングの両方を通じて、最も一般的に使用される属性をサポートします。

- System for Cross-Domain Identity Management (SCIM) 仕様の詳細については、https://tools.ietf.org/html/rfc7642 を参照してください。
- 手動および自動プロビジョニングの詳細については、「ユーザーが外部の IdP から来た場合のプロビジョニング」を参照してください。
- 属性のマッピングの詳細については、「IAM アイデンティティセンターと外部 ID プロバイダーディレクトリ間の属性マッピング」を参照してください。

IAM アイデンティティセンターは自動プロビジョニングのユースケースのために SCIM をサポートしているので、アイデンティティセンターは、いくつかの例外を除いて、SCIM 仕様に記載されているのと同じユーザーとグループの属性をすべてサポートしています。次のセクションでは、IAM アイデンティティセンターでサポートしていない属性について説明します。

サポートされていないユーザーオブジェクト

SCIM ユーザースキーマ (https://tools.ietf.org/html/rfc7643#section-8.3) のすべての属性は、IAM Identity Center ID ストアでサポートされていますが、以下を除きます。

- `password`
- `ims`
- `photos`
- `entitlements`
- `x509Certificates`

ユーザーのすべてのサブ属性がサポートされていますが、以下の項目はサポートされていません。

- 複数の値を持つ属性のうち、`'display'` の副属性 (例えば、`emails` や `phoneNumbers` など)
- `'meta'` 属性の `'version'` サブ属性

グループオブジェクトはサポートされていません

SCIM グループスキーマ (https://tools.ietf.org/html/rfc7643#section-8.4) のすべての属性がサポートされています。

グループのすべてのサブ属性は、以下を除いてサポートされています。

- `'display'`多値属性 (例: メンバー) の サブ属性。

外部 ID プロバイダー

IAM アイデンティティセンターでは、Security Assertion Markup Language (SAML) 2.0 および System for Cross-Domain Identity Management (SCIM) プロトコルを使用して、外部 ID プロバイダー (IdP) から既存のワークフォース ID を接続できます。これにより、ユーザーは AWS アクセスポータルにサインインできるようになります。そして、外部の IdP でホストされている、割り当てられたアカウント、ロール、アプリケーションにナビゲートすることができます。

例えば、Okta や Microsoft Entra ID などの外部 IdP を IAM アイデンティティセンターに接続できます。ユーザーは、既存の Okta や Microsoft Entra ID の認証情報を使って、AWS アクセスポータルにサインインすることができます。ユーザーがサインイン後にできることを制御するには、AWS 組織

内のすべてのアカウントとアプリケーションにわたってアクセス許可を一元的に割り当てることができます。さらに、開発者は既存の認証情報を使って AWS Command Line Interface (AWS CLI) にサインインするだけで、短期間の認証情報の自動生成やローテーションを利用することができます。

Active Directory または AWS Managed Microsoft AD で自己管理型ディレクトリを使用している場合は、Microsoft AD ディレクトリ を参照してください。

> **Note**
>
> SAML プロトコルは、ユーザーやグループについての情報を得るために IdP へクエリする方法は提供していません。そのため、IAM アイデンティティセンターがこれらのユーザーやグループを IAM アイデンティティセンターにプロビジョニングして認識する必要があります。

ユーザーが外部の IdP から来た場合のプロビジョニング

外部の IdP を使用する場合、AWS アカウント やアプリケーションへの割り当てを行う前に、すべての該当するユーザーとグループを IAM アイデンティティセンターにプロビジョニングする必要があります。これを行うには、ユーザーやグループに合わせて SCIM を使用して外部 ID プロバイダーからユーザーとグループをプロビジョニングする を設定するか、手動のプロビジョニング を使用します。ユーザーのプロビジョニング方法に関係なく、IAM アイデンティティセンターは AWS マネジメントコンソール、コマンドラインインターフェース、およびアプリケーション認証を外部の IdP にリダイレクトします。IAM アイデンティティセンターでは、IAM アイデンティティセンターセンターで作成したポリシーに基づいて、それらのリソースへのアクセス権を付与します。プロビジョニングの詳細については、「ユーザーおよびグループのプロビジョニング」を参照してください。

トピック

- 外部 ID プロバイダに接続する方法
- IAM アイデンティティセンターで外部 ID プロバイダーからのメタデータを変更するには
- 外部 ID プロバイダーで SAML および SCIM ID フェデレーションを使用する
- SCIM プロファイルおよび SAML 2.0 の実装

外部 ID プロバイダに接続する方法

サポートされている外部 IdP ごとに、さまざまな前提条件、考慮事項、プロビジョニング手順があります。複数の IdP 向けに、ステップバイステップのチュートリアルが用意されています。

- CyberArk
- Google Workspace
- JumpCloud
- Microsoft Entra ID
- Okta
- OneLogin
- Ping Identity

IAM アイデンティティセンターがサポートする外部 IdP に関する考慮事項については、「外部 ID プロバイダーで SAML および SCIM ID フェデレーションを使用する」を参照してください。

以下の手順は、すべての外部 ID プロバイダーで使用される手順の概要を示しています。

外部 ID プロバイダに接続する方法には

1. IAM アイデンティティセンターコンソールを開きます。
2. [設定] を選択します。
3. [設定] ページで [ID ソース] タブを選択し、[アクション] > [ID ソースを変更] を選択します。
4. [ID ソースの選択] で [外部 ID プロバイダー] を選択し、[次へ] を選択します。
5. [外部 ID プロバイダーの設定] で、次の操作を行います。

    a. [サービスプロバイダーメタデータ] で、[Download metadata file] (メタデータファイルのダウンロード) を選択すると、メタデータファイルがダウンロードされ、システムに保存されます。IAM アイデンティティセンター SAML メタデータファイルは、外部の ID プロバイダーに必要です。

    > **Note**
    >
    > ダウンロードする SAML メタデータファイルには、IPv4 専用とデュアルスタックの両方のアサーションコンシューマーサービス (ACS) URL が含まれています。さらに、IAM Identity Center が追加のリージョンにレプリケートされている場合、メタデータファイルには追加のリージョンごとに ACS URL が含まれます。外部 IdP に ACS URL の数に制限がある場合は、不要な ACS URL を削除する必要があります。例えば、組織でデュアルスタックエンドポイントが完全に採用されており、IPv4 専用エンドポイントを使用しなくなった場合は、後者を削除できます。別

の方法は、メタデータファイルを使用するのではなく、ACS URL をコピーして外部 IdP に貼り付けることです。

b. [ID プロバイダのメタデータ] で、[ファイルを参照] を選択し、外部の ID プロバイダからダウンロードしたメタデータファイルを検索します。次に、ファイルをアップロードします。このメタデータファイルには , IdP から送信されるメッセージを信頼を得るための公開 x509 証明書が含まれています。

c. [次へ] を選択します。

> **Important**
>
> ソースをアクティブディレクトリとの間で変更すると、既存のユーザーやグループの割り当てがすべて削除されます。ソースの変更が成功したら、手動で割り当てを再適用する必要があります。

6. 免責事項を読み、次に進む準備ができたら、[ACCEPT] (許諾) を押してください。
7. [Change identity source] (ID ソースの変更) を選択します。ID ソースを正常に変更したことを知らせるメッセージが表示されます。

IAM アイデンティティセンターで外部 ID プロバイダーからのメタデータを変更するには

IAM アイデンティティセンターに提供済みの外部 ID プロバイダーからのメタデータを変更することができます。これらのメタデータを変更すると、ユーザーが IAM アイデンティティセンターを介してサインインし、AWS リソースにアクセスする機能に影響する場合があります。以下の手順では、IAM アイデンティティセンターに保存されている外部 IdP からのメタデータを更新する方法について説明します。この手順を完了するには、IAM アイデンティティセンターの組織インスタンスが必要です。詳細については、「IAM アイデンティティセンターの組織インスタンスとアカウントインスタンス」を参照してください。

外部 ID プロバイダーからのメタデータを変更するには

1. IAM アイデンティティセンターコンソールを開きます。
2. [設定] を選択します。
3. [設定] ページの [ID ソース] タブを選択します。[アクション] > [認証の管理] を選択します。

4. [アイデンティティプロバイダーのメタデータ] セクションで、[IdP メタデータを編集] を選択します。このページでは、外部 IdP の IdP サインイン URL や IdP 発行者 URL を変更できます。必要な変更をすべて行ったら、[変更を保存] を選択します。

外部 ID プロバイダーで SAML および SCIM ID フェデレーションを使用する

IAM アイデンティティセンターは、ID フェデレーションのために以下の標準ベースのプロトコルを実装しています。

- ユーザー認証用の SAML 2.0
- SCIM のプロビジョニング

これらの標準的なプロトコルを実装している ID プロバイダー (IdP) は、以下の特別な注意事項を除き、IAM アイデンティティセンターと正常に相互運用できると考えられます。

- SAML
  - IAM Identity Center では、SAML の nameID 形式のメールアドレス (つまり `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`) が必要です。
  - アサーション内の nameID フィールドの値は、RFC 2822 (https://tools.ietf.org/html/rfc2822) のアドレス仕様準拠 (「`name@domain.com`」) の文字列 (https://tools.ietf.org/html/rfc2822#section-3.4.1) でなければなりません。
  - SAML アサーションの `Subject NameID` 値は、IAM Identity Center でプロビジョニングされたユーザーの [ユーザー名] と完全に一致する必要があります。外部 IdP がユーザーを正常に認証した場合でも、IAM Identity Center が `NameID` を [ユーザー名] と照合できない場合、サインインは失敗します。
  - メタデータファイルは 75000 文字を超えることはできません。
  - メタデータには、サインイン URL の一部として EntityID、X509 証明書、および SingleSignOnService が含まれている必要があります。
  - 暗号化キーはサポートされていません。
  - IAM アイデンティティセンターは、外部 IdPs に送信する SAML 認証リクエストの署名をサポートしていません。
  - IAM Identity Center を追加のリージョンにレプリケートし、マルチリージョン IAM Identity Center の利点を最大限に活用する場合は、IdP は複数のアサーションコンシューマーサービス (ACS) URL をサポートする必要があります。詳細については、「複数の 間で IAM アイデンティティセンターを使用するAWS リージョン」を参照してください。単一の ACS URL を使用する

と、追加のリージョンでのユーザーエクスペリエンスに影響する可能性があります。プライマリリージョンは、引き続き正常に機能します。単一の ACS URL による追加リージョンでのユーザーエクスペリエンスの詳細については、「the section called “複数の ACS URL なしで AWS マネージドアプリケーションを使用する”」および「the section called “複数の ACS URL を使用しない AWS アカウントアクセス回復性”」を参照してください。

- – SCIM
  - IAM Identity Center SCIM の実装は、SCIM RFC 7642、RFC 7643、RFC 7644、RFC 9865、および FastFed Basic SCIM Profile 1.0 の 2020 年 3 月のドラフトで規定されている相互運用性要件に基づいています。これらのドキュメントと現在の IAM Identity Center での実装との違いは、「IAM Identity Center SCIM 実装デベロッパーガイド」の「サポートされる API オペレーション」のセクションに記載されています。

上記の規格や注意事項に準拠していない IdP はサポートされません。これらの規格や注意事項への製品の適合性に関する質問や説明については、お客様の IdP にお問い合わせください。

お使いの IdP と IAM アイデンティティセンターの接続に問題がある場合は、以下を確認することをお勧めします。

- イベント名 ExternalIdPDirectoryLogin でフィルタリングした AWS CloudTrail ログ
- IdP 固有のログやデバッグログ
- IAM Identity Center の問題のトラブルシューティング

> **Note**
>
> IAM アイデンティティセンターの ID ソースに関するチュートリアル にあるような一部の IdP は、IAM アイデンティティセンター専用に構築された「アプリケーション」または「コネクター」の形式で、IAM アイデンティティセンター向けの簡素化された構成エクスペリエンスを提供します。お使いの IdP がこのオプションを提供している場合は、IAM アイデンティティセンター用に作成されたアイテムを慎重に選択して使用することをお勧めします。「AWS」、「AWS フェデレーション」、または類似の一般的な「AWS」と呼ばれるその他のアイテムは、他のフェデレーションアプローチやエンドポイントを使用している可能性があり、IAM アイデンティティセンターで期待通りに動作しない可能性があります。

SCIM プロファイルおよび SAML 2.0 の実装

SCIM および SAML は共に IAM アイデンティティセンターを構成する上で重要な注意事項です。

SAML 2.0 の実装

IAM アイデンティティセンターは、SAML (Security Assertion Markup Language) 2.0 との ID フェデレーションをサポートします。これにより、IAM アイデンティティセンターは、外部の ID プロバイダー (IdP) からの ID を認証することができます。SAML 2.0 は、SAML アサーションを安全に交換するためのオープンスタンダードです。SAML 2.0 は、SAML 権限 (ID プロバイダ (IdP) と呼ばれます) と SAML コンシューマ (サービスプロバイダ (SP) と呼ばれます) の間で、ユーザに関する情報を渡します。IAM アイデンティティセンターサービスは、この情報を使って、フェデレーテッドシングルサインオン (SSO) を提供します。シングルサインオンにより、ユーザーは既存の ID プロバイダーの認証情報に基づいて、AWS アカウント アカウントや設定されたアプリケーションにアクセスすることができます。

IAM アイデンティティセンターは、SAML IdP 機能を IAM アイデンティティセンターストア、AWS Managed Microsoft AD、または外部 ID プロバイダに追加します。それにより、ユーザーは、AWS マネジメントコンソール やサードパーティー製アプリケーション (Microsoft 365、Concur、Salesforce など) を含め、SAML をサポートするサービスへのシングルサインオンが可能になります。

しかし SAML プロトコルは、ユーザーやグループについての情報を得るために IdP へクエリする手段は提供しません。そのため、IAM アイデンティティセンターがこれらのユーザーやグループを IAM アイデンティティセンターにプロビジョニングして認識する必要があります。

SCIM プロファイル

IAM アイデンティティセンターは、クロスドメインアイデンティティ管理システム (SCIM) v2.0 規格に対応しています。SCIM は、IAM アイデンティティセンターの ID と IdP の ID を同期させます。これには、IdP と IAM アイデンティティセンターの間で行われるユーザーのプロビジョニング、アップデート、デプロビジョニングが含まれます。

SCIM を実装する方法の詳細については、「SCIM を使用して外部 ID プロバイダーからユーザーとグループをプロビジョニングする」を参照してください。IAM Identity Center の SCIM 実装の詳細については、「IAM Identity Center SCIM 実装デベロッパーガイド」 () を参照してください。

トピック

- SCIM を使用して外部 ID プロバイダーからユーザーとグループをプロビジョニングする

- SAML 2.0 証明書をローテーションする

SCIM を使用して外部 ID プロバイダーからユーザーとグループをプロビジョニングする

IAM アイデンティティセンターは、クロスドメインアイデンティティ管理システム (SCIM) v2.0 プロトコルを使用して、ID プロバイダー (IdP) から IAM アイデンティティセンターへのユーザーおよびグループ情報の自動プロビジョニング (同期化) をサポートしています。SCIM 同期を設定すると、ID プロバイダー (IdP) のユーザー属性と IAM アイデンティティセンターの名前付き属性のマッピングが作成されます。これにより、IAM アイデンティティセンターとお客様の IdP の間で、期待される属性が一致します。この接続を IdP で設定するには、IAM アイデンティティセンター用の SCIM エンドポイントと IAM アイデンティティセンターで作成したベアラートークンを使用します。

トピック

- 自動プロビジョニングを使用する際の注意事項
- SCIM プロビジョニングによる IdentityStore API アクセス
- アクセストークンの有効期限を監視する方法
- アクセストークンを生成する
- 自動プロビジョニングを有効にする
- アクセストークンを削除する
- 自動プロビジョニングを無効にする
- アクセストークンをローテーションする
- 自動プロビジョニングされたリソースの監査と調整
- 手動のプロビジョニング

自動プロビジョニングを使用する際の注意事項

SCIM のデプロイを開始する前に、まず、IAM アイデンティティセンターとの連携について、以下の注意事項を確認することをお勧めします。プロビジョニングに関する追加の注意事項については、お使いの IdP 向け IAM アイデンティティセンターの ID ソースに関するチュートリアル を参照してください。

- プライマリの E メールアドレスをプロビジョニングする場合、この属性値は各ユーザーに対して一意でなければなりません。一部の IdP では、プライマリ E メールアドレスが実在しない場合があります。例えば、E メールにしか見えない UPN (Universal Principal Name) だったりします。これらの IdP は、ユーザーの実際の E メールアドレスを含むセカンダリまたは「その他」の E メー

ルアドレスを持っている場合があります。Null 以外の一意なメールアドレスを IAM アイデンティティセンターのプライマリ E メールアドレス属性にマッピングするために、IdP の SCIM を設定する必要があります。また、ユーザーの Null 以外の一意なサインイン識別子を IAM アイデンティティセンターのユーザー名属性にマッピングする必要があります。ご利用の IdP に、サインイン識別子とユーザーの E メール名を兼ねた単一の値があるかどうかを確認してください。その場合、その IdP フィールドを IAM アイデンティティセンターのプライマリ E メールと IAM アイデンティティセンターのユーザー名の両方にマッピングすることができます。

- SCIM の同期が機能するためには、すべてのユーザーが First name (名)、Last name (姓)、Username (ユーザーネーム)、Display name (表示名) の値を指定する必要があります。これらのすべての値が設定されていないユーザーはプロビジョニングされません。
- サードパーティーのアプリケーションを使用する必要がある場合は、まず、アウトバウンド SAML のサブジェクト属性をユーザー名属性にマッピングする必要があります。サードパーティーのアプリケーションにルーティング可能な E メールアドレスが必要な場合、E メール属性を IdP に提供する必要があります。
- SCIM でプロビジョニングされたユーザーの場合、IdP が SAML `Subject NameID` として送信する属性が、SCIM 設定で [ユーザー名] にマッピングする属性と同じであることを確認してください。異なる場合、サインインは失敗します。
- SCIM のプロビジョニングとアップデートの間隔は、ID プロバイダーによって管理されます。ID プロバイダーのユーザーおよびグループに対する変更は、ID プロバイダーがそれらの変更を IAM アイデンティティセンターに送信した後に、 SSO にのみ反映されます。ユーザーやグループの更新の頻度については、ID プロバイダーにご確認ください。
- 現在、SCIM では多値属性 (特定のユーザーに対する複数の E メールや電話番号など) は提供されていません。SCIM を使用した IAM アイデンティティセンターに多値属性を同期させようとすると失敗します。失敗を回避するために、各属性には 1 つの値しか渡さないようにします。マルチバリューの属性を持つユーザーがいる場合は、IAM アイデンティティセンターへの接続のために、IdP の SCIM で重複する属性マッピングを削除または変更します。
- お客様の IdP での `externalId` SCIM マッピングが、一意で常に存在し、お客様のユーザにとって変更の可能性が低い値に対応していることを確認してください。例えば、IdP は、名前や E メールなどのユーザー属性の変更に影響されない、保証付きの `objectId` やその他の識別子を提供することができます。そうであれば、その値を SCIM の `externalId` フィールドにマッピングすることができます。これにより、ユーザーの名前や E メールアドレスを変更しても、AWS の資格、割り当て、権限が失われることはありません。
- アプリケーションや AWS アカウント アカウントに割り当てられていないユーザーは、IAM アイデンティティセンターにプロビジョニングできません。ユーザーとグループを同期させるには、

ユーザーとグループが、IAM アイデンティティセンターへの IdP の接続を表すアプリケーションやその他の設定に割り当てられていることを確認してください。

- ユーザープロビジョニング解除の動作は ID プロバイダーによって管理され、実装によって異なる場合があります。ユーザープロビジョニング解除の詳細については、ID プロバイダーにお問い合わせください。
- IdP に SCIM を使用して自動プロビジョニングを設定した後は、IAM アイデンティティセンターコンソールでユーザーを追加または編集できなくなります。ユーザーを追加または変更する必要がある場合は、外部 IdP または ID ソースから追加または変更する必要があります。

IAM Identity Center の SCIM 実装の詳細については、「IAM Identity Center SCIM 実装デベロッパーガイド」() を参照してください。

SCIM プロビジョニングによる IdentityStore API アクセス

外部 IdP から SCIM プロビジョニングを設定すると、ユーザーとグループメンバーシップの変更を許可する Identity Store API は引き続きアクセスできます。管理アカウントと委任管理者アカウントのプリンシパルは、これらを呼び出すことができます。

SCIM と併用してこれらの API を使用することには、有効な理由があります。例えば、Google Workspace などの一部の IdP は SCIM グループのプロビジョニングをサポートしておらず、Identity Store API を使用してグループを手動で作成および管理する必要があります。その他のユースケースとしては、迅速なユーザー無効化や、IdP 同期前のグループの事前プロビジョニングなどがあります。

> **Important**
>
> 組織で直接 API アクセスが必要ない場合は、SCIM でプロビジョニングされたディレクトリで Identity Store の変更を伴う API を使用すると、IAM Identity Center のディレクトリが外部 IdP からドリフトする可能性があることに注意してください。SCIM 同期は、ソース IdP からの差分に基づいて動作します。つまり、API を通じて行われた変更は、後続の SCIM 同期によって修正されない可能性があります。この結果、以下のようになります。
>
> - IAM Identity Center のユーザーまたはグループメンバーシップが外部 IdP と一致しなくなり、IdP が唯一の信頼できるソースであるという前提が崩れます。
> - プリンシパルが自身または他のユーザーを、AWS アカウントまたはアプリケーションへのアクセスを許可するグループに追加した場合、意図しない特権昇格が発生します。

- 外部 IdP に対して実施された使用権限レビューが AWS の実際のアクセス状態を反映していない可能性があるため、監査およびコンプライアンスのギャップが生じます。

API ベースの変更操作を防ぐ場合は、委任された管理者アカウントにサービスコントロールポリシー (SCP) をアタッチします。SCP は管理アカウント自体には適用されないことに注意してください。

以下の SCP の例では、Identity Store の変更を伴うすべてのアクションを拒否します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyIdentityStoreMutations",
      "Effect": "Deny",
      "Action": [
        "identitystore:Create*",
        "identitystore:Update*",
        "identitystore:Delete*"
      ],
      "Resource": "*"
    }
  ]
}
```

アクセストークンの有効期限を監視する方法

SCIM アクセストークンは 1 年の有効期間で生成されます。SCIM アクセストークンの有効期限が 90 日以内に設定されると、AWS は IAM アイデンティティセンターコンソールと AWS Health ダッシュボードでリマインダを送信し、トークンのローテーションを支援します。SCIM アクセストークンを有効期限が切れる前にローテーションすることで、ユーザーとグループの情報の自動プロビジョニングを継続的に保護できます。SCIM アクセストークンの有効期限が切れると、ID プロバイダーから IAM アイデンティティセンターへのユーザーとグループの情報の同期が停止するため、自動プロビジョニングでは情報を更新したり、情報を作成、削除したりできなくなります。自動プロビジョニングが中断されると、セキュリティリスクが高まり、サービスへのアクセスに影響が及ぶ可能性があります。

Identity Center コンソールのリマインダーは、SCIM アクセストークンをローテーションして、未使用または期限切れのアクセストークンを削除するまで続きます。AWS Health ダッシュボードイベン

トは、SCIM アクセストークンの有効期限が切れるまで 90 ~ 60 日の間は毎週、60 日から 30 日の間は週 2 回、30 日から 15 日の間は週 3 回、15 日間は毎日更新されます。

アクセストークンを生成する

以下の手順で、IAM アイデンティティセンターコンソールで新しいアクセストークンを生成します。

> **Note**
>
> この手順では、自動プロビジョニングが事前に有効になっている必要があります。詳細については、「自動プロビジョニングを有効にする」を参照してください。

新しいアクセストークンを生成するには

1. [IAM アイデンティティセンターコンソール] で、左のナビゲーションペインの [設定] を選択します。
2. [設定] ページで [ID ソース] タブを選択し、[アクション] > [プロビジョニングの管理] を選択します。
3. [自動プロビジョニング] ページで、 [アクセストークン] の [トークンを生成する] を選択します。
4. [新しいアクセストークンを生成] ダイアログで、新しいアクセストークンをコピーして安全な場所に保存します。
5. [閉じる] を選択してください。

自動プロビジョニングを有効にする

SCIM プロトコルを使用して、IdP から IAM アイデンティティセンターへのユーザーおよびグループの自動プロビジョニングを有効にするには、以下の手順を使用します。

> **Note**
>
> この手順を開始する前に、まずお客様の IdP に適用されるプロビジョニングに関する注意事項を確認することをお勧めします。詳細については、お使いの IdP の IAM アイデンティティセンターの ID ソースに関するチュートリアル を参照してください。

IAM アイデンティティセンターで自動プロビジョニングを有効にするには

1. 前提条件が整ったら、IAM アイデンティティセンターコンソールを開きます。
2. 左側のナビゲーションペインの [設定] を選択します。
3. [設定] ページで、[自動プロビジョニング] 情報ボックスを探し、[有効化] を選択します。これにより、すぐに IAM アイデンティティセンターの自動プロビジョニングが有効になり、必要なエンドポイントとアクセストークンの情報が表示されます。
4. [インバウンド自動プロビジョニング] ダイアログボックスで、SCIM エンドポイントとアクセストークンをコピーします。これらは、後で IdP でプロビジョニングを設定する際に貼り付ける必要があります。

   a. [SCIM エンドポイント] - 例えば https://scim.*us-east-2*.amazonaws.com/*11111111111-2222-3333-4444-555555555555*/scim/v2

   b. [アクセストークン] - [トークンを表示] を選択して値をコピーします。

   > **Warning**
   >
   > SCIM エンドポイントとアクセストークンを取得できるタイミングは、この時のみです。先に進む前に、これらの値をコピーしておいてください。このチュートリアルの後半で、お使いの IdP 上でこれらの値を入力して自動プロビジョニングを設定します。

5. [閉じる] を選択します。

この手順が完了したら、IdP で自動プロビジョニングを設定する必要があります。詳細については、お使いの IdP の IAM アイデンティティセンターの ID ソースに関するチュートリアル を参照してください。

アクセストークンを削除する

以下の手順で、IAM アイデンティティセンターコンソールで既存のアクセストークンを削除します。

既存のアクセストークンを削除するには

1. [IAM アイデンティティセンターコンソール] で、左のナビゲーションペインの [設定] を選択します。

2. [設定] ページで [ID ソース] タブを選択し、[アクション] > [プロビジョニングの管理] を選択します。
3. [自動プロビジョニング] ページで、[アクセストークン] から削除したいアクセストークンを選び、[削除] を選択します。
4. [Delete access token] (アクセストークンを削除する) ダイアログボックスで、情報を確認し、[DELETE] (削除) と入力して、[Delete access token] (アクセストークンを削除する) を選択します。

自動プロビジョニングを無効にする

以下の手順で、IAM アイデンティティセンターコンソールでの自動プロビジョニングを無効にします。

> **Important**
>
> この手順を行う前にアクセストークンを削除する必要があります。詳細については、「アクセストークンを削除する」を参照してください。

IAM アイデンティティセンターコンソールで自動プロビジョニングを無効にするには

1. [IAM アイデンティティセンターコンソール] で、左のナビゲーションペインの [設定] を選択します。
2. [設定] ページで [ID ソース] タブを選択し、[アクション] > [プロビジョニングの管理] を選択します。
3. [自動プロビジョニング] ページで、[無効にする] を選択します。
4. [Disable automatic provisioning] (自動プロビジョニングを無効にする) ダイアログボックスで、情報を確認し、[DISABLE] (無効) と入力して、[Disable automatic provisioning] (自動プロビジョニングを無効にする) を選択します。

アクセストークンをローテーションする

IAM アイデンティティセンターディレクトリは一度に 2 つまでのアクセストークンをサポートします。ローテーションの前に追加のアクセストークンを生成するには、期限切れまたは未使用のアクセストークンをすべて削除します。

SCIM アクセストークンの有効期限が近づいている場合は、以下の手順で IAM アイデンティティセンターコンソールで既存のアクセストークンをローテーションさせることができます。

アクセストークンをローテーションするには

1. [IAM アイデンティティセンターコンソール] で、左のナビゲーションペインの [設定] を選択します。
2. [設定] ページで [ID ソース] タブを選択し、[アクション] > [プロビジョニングの管理] を選択します。
3. [Automatic provisioning] (自動プロビジョニング) ページの [Access Token] (アクセストークン) でローテーションさせたいトークンのトークン ID をメモしておきます。
4. アクセストークンを生成する の手順に従って、新しいトークンを作成します。既に最大数の SCIM アクセストークンを作成している場合は、まず既存のトークンの 1 つを削除する必要があります。
5. ID プロバイダーのウェブサイトにアクセスし、新しいアクセストークンを SCIM プロビジョニング用に設定した後、新しい SCIM アクセストークンを使用して IAM アイデンティティセンターへの接続をテストします。新しいトークンを使ってプロビジョニングが正常に行われていることを確認したら、この手順の次のステップに進みます。
6. アクセストークンを削除する の手順で、先ほどの古いアクセストークンを削除します。また、どのトークンを削除するかを判断するために、トークンの作成日を利用することもできます。

自動プロビジョニングされたリソースの監査と調整

SCIM を使用すると、ユーザー、グループ、グループメンバーシップを ID ソースから IAM アイデンティティセンターに自動的にプロビジョニングできます。このガイドは、これらのリソースを検証して調整し、正確な同期を維持するのに役立ちます。

リソースを監査する理由

定期的な監査は、アクセスコントロールが正確であり、ID プロバイダー (IdP) が IAM アイデンティティセンターと適切に同期された状態を維持するのに役立ちます。これは、セキュリティコンプライアンスとアクセス管理にとって特に重要です。

監査できるリソース:

- Users
- グループ
- グループメンバーシップ

AWS ID ストア API または CLI コマンドを使用して、監査と調整を実行できます。次の例では、AWS CLI コマンドを使用します。API の代替手段については、「ID ストア API リファレンス」の「対応するオペレーション」を参照してください。

リソースを監査する方法

AWS CLI コマンドを使用してこれらのリソースを監査する方法の例を次に示します。

開始する前に、以下があることを確認してください。

- IAM アイデンティティセンターへの管理者アクセス。
- AWS CLI がインストールされ、設定済みであること。詳細については、AWS コマンドラインインターフェイスのユーザーガイドを参照してください。
- ID ストアコマンドに必要な IAM アクセス許可。

ステップ 1: 現在のリソースを一覧表示する

AWS CLI を使用して現在のリソースを表示できます。

> **Note**
>
> AWS CLI を使用する場合、`--no-paginate` を指定しない限り、ページ分割は自動的に処理されます。API を直接呼び出す場合 (SDK やカスタムスクリプトなど)、レスポンスで `NextToken` を処理します。これにより、複数のページにわたるすべての結果を取得できます。

Exampleユーザー向け

```
aws identitystore list-users \
  --region REGION \
  --identity-store-id IDENTITY_STORE_ID
```

Exampleグループ向け

```
aws identitystore list-groups \
  --region REGION \
  --identity-store-id IDENTITY_STORE_ID
```

Exampleグループメンバーシップ向け

```
aws identitystore list-group-memberships \
  --region REGION \
  --identity-store-id IDENTITY_STORE_ID
  --group-id GROUP_ID
```

ステップ 2: ID ソースと比較する

リストされているリソースを ID ソースと比較して、次のような不一致を特定します。

- IAM アイデンティティセンターでプロビジョニングする必要があるリソースがありません。
- IAM アイデンティティセンターから削除する必要がある追加のリソース。

Exampleユーザー向け

```
# Create missing users
aws identitystore create-user \
  --identity-store-id IDENTITY_STORE_ID \
  --user-name USERNAME \
  --display-name DISPLAY_NAME \
  --name GivenName=FIRST_NAME,FamilyName=LAST_NAME \
  --emails Value=EMAIL,Primary=true

# Delete extra users
aws identitystore delete-user \
  --identity-store-id IDENTITY_STORE_ID \
  --user-id USER_ID
```

Exampleグループ向け

```
# Create missing groups
aws identitystore create-group \
  --identity-store-id IDENTITY_STORE_ID \
  [group attributes]

# Delete extra groups
aws identitystore delete-group \
  --identity-store-id IDENTITY_STORE_ID \
  --group-id GROUP_ID
```

Exampleグループメンバーシップ向け

```
# Add missing members
aws identitystore create-group-membership \
  --identity-store-id IDENTITY_STORE_ID \
  --group-id GROUP_ID \
  --member-id '{"UserId": "USER_ID"}'

# Remove extra members
aws identitystore delete-group-membership \
  --identity-store-id IDENTITY_STORE_ID \
  --membership-id MEMBERSHIP_ID
```

考慮事項

- コマンドには、service quotas と API スロットリングが適用されます。
- 調整中に多くの違いが見つかった場合は、AWS ID ストアに小さな段階的な変更を加えます。これにより、複数のユーザーに影響を与える間違いを回避できます。
- SCIM 同期は、手動の変更を上書きできます。この動作を理解するには、IdP 設定を確認してください。

手動のプロビジョニング

一部の IdP では、クロスドメインアイデンティティ管理システム (SCIM) をサポートしていないか、互換性のない SCIM 実装をしています。そのような場合は、IAM Identity Center コンソールを通じて手動でユーザーをプロビジョニングすることができます。IAM アイデンティティセンターにユーザーを追加する際には、IdP に登録されているユーザー名と同一のユーザー名を設定します。少なくとも、一意の E メールアドレスとユーザー名が必要です。詳細については、「ユーザー名と E メールアドレスの一意性」を参照してください。

また、IAM アイデンティティセンターでは、すべてのグループを手動で管理する必要があります。そのためには、グループを作成し、IAM アイデンティティセンターコンソールを使ってグループを追加します。これらのグループは、お客様の IdP に存在するものと一致する必要はありません。詳細については、「グループ」を参照してください。

SAML 2.0 証明書をローテーションする

IAM アイデンティティセンターは、証明書を使用して、外部 ID プロバイダー (IdP)と IAM アイデンティティセンターとの間の SAML 信頼関係を確立します。IAM アイデンティティセンターで外部

IdP を追加する際には、外部 IdP から少なくとも 1 つの SAML 2.0 X.509 のパブリック証明書を取得する必要があります。その証明書は、通常、信頼を作成中の IdP SAML メタデータ交換時に自動的にインストールされます。

IAM アイデンティティセンターの管理者として、古い IdP 証明書を新しい証明書に置き換える必要がある場合があります。例えば、IdP 証明書の有効期限が近づいている場合は、証明書を交換する必要があります。古い証明書を新しい証明書に置き換えるプロセスは、証明書のローテーションと呼ばれています。

トピック

- SAML 2.0 証明書をローテーションする
- 証明書の有効期限切れステータスインジケーター

SAML 2.0 証明書をローテーションする

ID プロバイダーが発行した無効または期限切れの証明書をローテーションさせるために、定期的に証明書をインポートする必要がある場合があります。これにより、認証の乱れやダウンタイムを防ぐことができます。インポートされた証明書はすべて自動的に有効になります。証明書の削除は、関連する ID プロバイダで使用されなくなったことを確認した後に行います。

また、IdP によっては複数の証明書をサポートしていない場合があることも考慮する必要があります。この場合、これらの IdP で証明書をローテーションした場合、ユーザーの利用しているサービスが一時的に中断する可能性があります。その IdP との信頼関係が正常に再構築されたときに、サービスが再開されます。このオペレーションは、ピーク時を可能な限り避けて慎重に計画してください。

> **Note**
>
> セキュリティのベストプラクティスとして、既存の SAML 証明書に不正アクセスや不適切な取り扱いがあった場合には、直ちに証明書を削除してローテーションする必要があります。

IAM アイデンティティセンター証明書のローテーションは、以下の複数のステップで行われます。

- IdP から新しい証明書を取得する
- 新しい証明書を IAM アイデンティティセンターにインポートする
- IdP での新しい証明書を有効にする
- 古い証明書を削除する

以下のすべての手順を使用して、認証のダウンタイムを回避しながら、証明書のローテーションプロセスを完了します。

ステップ 1: IdP から新しい証明書を取得する

IdP の ウェブサイトにアクセスして、SAML 2.0 証明書をダウンロードします。証明書ファイルが PEM エンコード形式でダウンロードされていることを確認してください。ほとんどのプロバイダでは、IdP に複数の SAML 2.0 証明書を作成することができます。これらは、無効や非アクティブとしてマークされている可能性があります。

ステップ 2: IAM アイデンティティセンターにインポートする

以下の手順で、IAM アイデンティティセンターコンソールを使って新しい証明書をインポートします。

1. [IAM アイデンティティセンターコンソール] で [設定] を選択します。
2. [設定] ページで [ID ソース] タブを選択し、[アクション] > [認証の管理] を選択します。
3. [SAML 2.0 認証の管理] ページで、[証明書のインポート] を選択します。
4. [SAML 2.0 証明書のインポート] ダイアログで、[ファイルを選択] を選択し、証明書ファイルに移動して選択し、[証明書のインポート] を選択します。

この時点で、IAM アイデンティティセンターは、お客様がインポートした両方の証明書から署名されたすべての受信 SAML メッセージを信頼します。

ステップ 3: IdP で新しい証明書を有効にする

IdP の ウェブサイトに戻り、先ほど作成した新しい証明書をプライマリまたはアクティブとしてマークします。この時点で、IdP が署名したすべての SAML メッセージは、新しい証明書を使用する必要があります。

ステップ 4: 古い証明書を削除する

以下の手順で、IdP の証明書ローテーション処理を行います。少なくとも 1 つの有効な証明書が必要であり、それを削除することはできません。

> **Note**
>
> この証明書を削除する前に、ID プロバイダがこの証明書を使用して SAML レスポンスに署名しなくなったことを確認します。

1. リポジトリの [Manage SAML 2.0 certificates] (SAML 2.0 証明書の管理) ページで、削除する証明書を選択します。[Delete] (削除) を選択します。
2. [Delete SAML 2.0 certificate] (SAML 2.0 証明書の削除) ダイアログボックスで、**DELETE** をタイプして確認し、[Delete] (削除) を選択します。
3. IdP のウェブサイトに戻り、古い非アクティブな証明書を削除するために必要な手順を実行します。

証明書の有効期限切れステータスインジケーター

「Manage SAML 2.0 certificates」ページには、リスト内の各証明書名の横にある[有効期限] 列に色分けされたステータスインジケータアイコンが表示されます。以下は、IAM アイデンティティセンターが各証明書に対してどのアイコンを表示するかを決定するための基準です。

- 赤 — 証明書が現在期限切れであることを示します。
- 黄 — 証明書が 90 日以内に失効することを示します。
- 緑 — 証明書が有効であり、少なくともあと 90 日間有効であることを示します。

証明書の現在のステータスを確認するには

1. [IAM Identity Center コンソール] で [設定] を選択します。
2. [設定] ページで [ID ソース] タブを選択し、[アクション] > [認証の管理] を選択します。
3. [SAML 2.0 証明書の管理] ページの [SAML 2.0 証明書の管理] で、リストの証明書のステータスを [有効期限] 欄に表示します。

Microsoft AD ディレクトリ

AWS IAM アイデンティティセンター を使用すると、Active Directory (AD) の自己管理ディレクトリに接続することも、AWS Directory Service を使用して AWS Managed Microsoft AD 内のディレクトリに接続することもできます。この Microsoft AD ディレクトリでは、管理者が IAM Identity Center コンソールを使用してシングルサインオンアクセスを割り当てるときに、プル元の ID プールを定義します。会社のディレクトリを IAM アイデンティティセンターに接続すると、AD ユーザーまたはグループに AWS アカウント、アプリケーション、またはその両方へのアクセス権を付与することができます。

AWS Directory Service により、AWS クラウド でホストされているスタンドアロンの AWS Managed Microsoft AD ディレクトリを設定して実行できます。また、Directory Service を使用し

て、AWS リソースを既存のセルフマネージド AD に接続することも可能です。セルフマネージド AD と連動するように AWS Directory Service を設定するには、まず信頼関係を構築して、認証をクラウドに拡張する必要があります。

IAM Identity Center は、Directory Service が提供する接続を使用して、ソース AD インスタンスへのパススルー認証を実行します。AWS Managed Microsoft AD を ID ソースとして使用する場合、IAM Identity Center は AWS Managed Microsoft AD のユーザーや AD トラストで接続されたドメインのユーザーに対して機能します。4 つ以上のドメインにユーザーを配置したい場合、ユーザーは IAM Identity Center へのサインインを実行する際に、ユーザー名として `DOMAIN\user` 構文を使用する必要があります。

> **注意事項**
>
> - 前提条件の手順として、Directory Service の AWS Managed Microsoft AD にある AD コネクタまたはディレクトリが AWS Organizations 管理アカウント内に存在することを確認してください。
> - IAM Identity Center は、SAMBA4 ベースの Simple AD を接続先ディレクトリとしてサポートしていません。
> - IAM Identity Center は、外部セキュリティプリンシパル (FSP) を同期できません。AWS Managed Microsoft AD のグループに信頼できるドメインのメンバーが FSP として含まれている場合、そのメンバーは同期されません。

IAM アイデンティティセンターの ID ソースとして Active Directory を使用するプロセスのデモンストレーションについては、次の YouTube 動画を参照してください。

Active Directory を AWS IAM アイデンティティセンター の ID ソースとして使用する| Amazon Web Services

Active Directory を使用する際の考慮事項

Active Directory を ID ソースとして使用する場合、設定は次の前提条件を満たす必要があります。

- AWS Managed Microsoft AD を使用している場合は、AWS Managed Microsoft AD ディレクトリが設定されている場所と同じ AWS リージョン で IAM アイデンティティセンターを有効にする必要があります。IAM Identity Center では、割り当てデータに関するディレクトリと同じリージョンに保存されます。IAM Identity Center を管理するには、IAM Identity Center が設定されているリー

ジョンに切り替える必要がある場合があります。また、AWS のアクセスポータルでは、ディレクトリと同じアクセス URL が使用されます。

- 管理アカウントにある Active Directory を使用してください。

  既存の AD コネクタまたは AWS Managed Microsoft AD ディレクトリが AWS Directory Service に設定されており、AWS Organizations 管理アカウント内に存在する必要があります。一度に接続できる AD Connector ディレクトリは 1 つか、ディレクトリは AWS Managed Microsoft AD 1 つだけです。複数のドメインやフォレストをサポートする必要がある場合は、AWS Managed Microsoft AD を使用してください。詳細については、以下を参照してください。

  - AWS Managed Microsoft AD のディレクトリを IAM Identity Center に接続する
  - Active Directory の自己管理型ディレクトリを IAM Identity Center に接続する

- 委任された管理者アカウントにある Active Directory を使用してください。

  IAM Identity Center 委任管理者を有効にし、IAM ID センターのアイデンティティソースとして Active Directory を使用する予定の場合は、AWS Managed Microsoft AD委任された管理者アカウントにあるディレクトリに設定された既存の AD Connector AWS またはディレクトリを使用できます。

  IAM Identity Center ID ソースを他のソースから Active Directory に変更するか、Active Directory から他のソースに変更する場合、そのディレクトリは IAM Identity Center 委任管理者メンバーアカウント (存在する場合) に存在する (所有されている) 必要があります。それ以外の場合は、管理アカウントに含まれている必要があります。

Active Directory に接続してユーザーを指定する

すでに Active Directory を使用している場合は、以下のトピックがディレクトリを IAM アイデンティティセンターに接続する準備に役立ちます。

IAM アイデンティティセンターを使用して、Active Directory 内の AWS Managed Microsoft AD ディレクトリまたはセルフマネージドディレクトリに接続できます。

> **Note**
>
> IAM アイデンティティセンターは SAMBA4 ベースの Simple AD を ID ソースとしてサポートしていません。

AWS Managed Microsoft AD

1. Microsoft AD ディレクトリ のガイダンスを確認してください。
2. 「AWS Managed Microsoft AD のディレクトリを IAM Identity Center に接続する」のステップを実行してください。
3. 管理者権限を付与したいユーザーを IAM Identity Center と同期するように Active Directory を設定します。詳細については、「管理ユーザーを IAM Identity Center と同期する」を参照してください。

Active Directory 内の自己管理型ディレクトリ

1. Microsoft AD ディレクトリ のガイダンスを確認してください。
2. 「Active Directory の自己管理型ディレクトリを IAM Identity Center に接続する」のステップを実行してください。
3. 管理者権限を付与したいユーザーを IAM Identity Center と同期するように Active Directory を設定します。詳細については、「管理ユーザーを IAM Identity Center と同期する」を参照してください。

外部 IdP

1. 外部 ID プロバイダー のガイダンスを確認してください。
2. 「外部 ID プロバイダに接続する方法」のステップを実行してください。
3. IAM Identity Center にユーザーをプロビジョニングするように IdP を設定します。

> **Note**
>
> IdP から IAM Identity Center へのすべてのワークフォース ID のグループベースの自動プロビジョニングを設定する前に、管理権限を付与したい 1 人のユーザーを IAM Identity Center に同期することをお勧めします。

管理ユーザーを IAM Identity Center と同期する

Active Directory を IAM アイデンティティセンターに接続したら、管理権限を付与するユーザーを指定し、そのユーザーをディレクトリから IAM アイデンティティセンターに同期できます。

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。

3. [設定]ページで[ID ソース]タブを選択し、[アクション]を選択し、[同期を管理] を選択します。
4. [同期の管理] ページで、[ユーザー] タブを選択し、[ユーザーとグループの追加] を選択します。
5. [ユーザー] タブの [ユーザー] に正確なユーザー名を入力し、[追加] を選択します。
6. [追加されたユーザーとグループ] で、次の操作を行います。
   a. 管理者権限を付与するユーザーが指定されていることを確認します。
   b. ユーザー名の左側にあるチェックボックスをオンにします。
   c. [送信] を選択します。
7. [同期の管理] ページで、指定したユーザーが同期対象のユーザーリストに表示されます。
8. ナビゲーションペインで [ユーザー] を選択します。
9. [ユーザー] ページでは、指定したユーザーがリストに表示されるまでに時間がかかる場合があります。ユーザーリストを更新するには、[更新] アイコンをクリックします。

この時点では、ユーザーは管理アカウントにアクセスできません。このアカウントへの管理アクセスを設定するには、管理アクセス権限セットを作成し、そのアクセス権限セットにユーザを割り当てます。詳細については、「アクセス権限セットを作成します。」を参照してください。

ユーザーがアクティブディレクトリから来たときのプロビジョニング

IAM Identity Center は、Directory Service によって提供された接続を使用して、Active Directory のソースディレクトリにあるユーザー、グループ、メンバーシップ情報を IAM ID センターアイデンティティストアに同期します。ユーザー認証は Active Directory のソースディレクトリから直接行われるため、パスワード情報は IAM アイデンティティセンターに同期されません。この ID データは、アプリケーションによって使用され、LDAP アクティビティを Active Directory のソースディレクトリに戻すことなく、アプリ内検索、承認、コラボレーション シナリオを容易にします。

上記のプロビジョニングの詳細については、「ユーザーおよびグループのプロビジョニング」を参照してください。

トピック

- AWS Managed Microsoft AD のディレクトリを IAM Identity Center に接続する
- Active Directory の自己管理型ディレクトリを IAM Identity Center に接続する
- IAM アイデンティティセンターと外部 ID プロバイダーディレクトリ間の属性マッピング
- IAM Identity Center の構成可能な AD 同期

AWS Managed Microsoft AD のディレクトリを IAM Identity Center に接続する

AWS Directory Service によって管理されている AWS Managed Microsoft AD のディレクトリを IAM Identity Center に接続するには、次の手順を使用します。

IAM Identity Center に AWS Managed Microsoft AD 接続するには

1. IAM Identity Center コンソール を開きます。

> **Note**
>
> 次のステップに進む前に、IAM Identity Center コンソールで、AWS Managed Microsoft AD ディレクトリが存在するリージョンの 1 つを使用していることを確認してください。

2. [設定] を選択します。
3. [設定] ページで [ID ソース] タブを選択し、[アクション] > [ID ソースを変更]を選択します。
4. [ID ソースの選択] で [Active Directory] を選択し、[次へ] を選択します。
5. [アクティブディレクトリに接続] で、一覧から AWS Managed Microsoft AD のディレクトリを選択し、[次へ] を選択します。
6. [変更の確認] で情報を確認し、準備ができたら ACCEPT と入力し、[ID ソースを変更] を選択します。

> **Important**
>
> Active Directory 内のユーザーを IAM アイデンティティセンターの管理者ユーザーとして指定するには、まず Active Directory から管理権限を付与したいユーザーを IAM ID センターに同期する必要があります。これを行うには、「管理ユーザーを IAM Identity Center と同期する」の手順を実行します。

Active Directory の自己管理型ディレクトリを IAM Identity Center に接続する

Active Directory (AD) のセルフマネージドディレクトリのユーザーも、AWS のアクセスポータルで AWS アカウント やアプリケーションへのシングルサインオンアクセスが可能です。これらのユーザーのシングルサインオンアクセスを設定するには、次のいずれかを実行します。

- 双方向の信頼関係の構築 – AWS Managed Microsoft AD とセルフマネージド AD ディレクトリの間に双方向の信頼関係が構築されると、セルフマネージド AD ディレクトリのユーザーは、企業の認証情報を使ってさまざまな AWS のサービスやビジネスアプリケーションにサインインすることができます。一方向の信頼は IAM Identity Center では機能しません。

  AWS IAM アイデンティティセンター には、ユーザーとグループのメタデータを同期するためにドメインからユーザーとグループの情報を読み取るアクセス許可があるように、双方向の信頼が必要です。IAM Identity Center は、アクセス権限セットまたはアプリケーションへのアクセスを割り当てるときに、このメタデータを使用します。ユーザーおよびグループのメタデータは、ダッシュボードを別のユーザーやグループと共有する場合など、コラボレーションのためにアプリケーションによっても使用されます。Microsoft Active Directory の Directory Service から顧客のドメインへの信頼により、IAM Identity Center が顧客のドメインを信頼して認証を行うことを可能にします。逆方向の信頼は、AWS にユーザーとグループのメタデータを読み込む権限を与えます。

  双方向の信頼関係の設定の詳細については、「AWS Directory Service 管理者ガイド」の「信頼関係を作成する場合」を参照してください。

  > **Note**
  >
  > IAM アイデンティティセンターなどの AWS アプリケーションを使用して信頼されたドメインからの Directory Service ディレクトリユーザーを読み取るには、Directory Service アカウントが信頼されたユーザーの userAccountControl 属性に対するアクセス許可を持っている必要があります。この属性への読み取りアクセス許可がないと、AWS アプリケーションはアカウントが有効か無効かを判断することができません。
  > この属性への読み取りアクセスは、信頼の作成時にデフォルトで提供されます。この属性へのアクセスを拒否すると (非推奨)、Identity Center などのアプリケーションが信頼できるユーザーを読み取れなくなります。問題を解決するには、AWS リザーブド OU (先頭に AWS_ 付き) の下にある AWS サービスアカウントの `userAccountControl` 属性への読み取りアクセスを明示的に許可してください。

- AD Connector を作成する - AD Connector は、クラウドに情報をキャッシュすることなく、セルフマネージドの AD にディレクトリリクエストをリダイレクトできるディレクトリゲートウェイです。詳細については、「AWS Directory Service 管理ガイド」の [ディレクトリへの接続]を参照してください。AD Connector を使用するときの考慮事項は次のとおりです。
  - IAM Identity Center を AD Connector ディレクトリに接続している場合、今後のユーザーパスワードのリセットは、AD 内から行う必要があります。つまり、ユーザーは AWS アクセスポータルからパスワードをリセットできません。

- AD Connector を使用してアクティブディレクトリドメインサービスを IAM Identity Center に接続する場合、IAM Identity Center は AD Connector がアタッチされている単一ドメインのユーザーとグループにしかアクセスできません。複数のドメインやフォレストをサポートする必要がある場合は、Microsoft Active Directory の Directory Service をご利用ください。

> **Note**
>
> IAM Identity Center は SAMBA4 ベースの Simple AD ディレクトリでは機能しません。

IAM アイデンティティセンターと外部 ID プロバイダーディレクトリ間の属性マッピング

属性マッピングは、IAM アイデンティティセンターに存在する属性タイプと、外部 ID ソースの同様の属性 (Google Workspace、Microsoft Active Directory (AD)、Okta など) をマッピングするのに使用されます。IAM アイデンティティセンターは、ID ソースからユーザー属性を検索し、IAM アイデンティティセンターのユーザー属性に対してマッピングします。

IAM アイデンティティセンターが Google Workspace、Okta、または Ping などの外部 ID プロバイダー (IdP) を ID ソースとして使用するように同期されている場合は、IdP に属性をマッピングする必要があります。

IAM アイデンティティセンターは、設定ページの [属性マッピング] タブから一連の属性を事前に取得します。IAM アイデンティティセンターは、これらのユーザー属性を使用して、アプリケーションに送信される SAML アサーション (SAML 属性) を設定します。これらのユーザー属性は ID ソースから取得されます。アプリケーションによって、正常なシングルサインオンに必要な SAML 2.0 属性のリストは異なります。詳細については、「アプリケーションの属性を IAM Identity Center の属性にマップする」を参照してください。

IAM アイデンティティセンターは、Active Directory を ID ソースとして使用している場合、[Active Directory 設定] ページの [属性マッピング] セクションの下にある一連の属性も管理します。詳細については、「IAM アイデンティティセンターと Microsoft AD ディレクトリ間のユーザー属性のマッピング」を参照してください。

サポートされている外部 ID プロバイダ属性

以下の表は、サポートされているすべての外部 ID プロバイダー(IdP) 属性と、IAM アイデンティティセンターで アクセスコントロールの属性 を構成するときに使用できる属性にマッピングできる

ものをリストアップしたものです。SAML アサーションを使用する場合、IdP がサポートするすべて属性を使用できます。

IdP でサポートされている属性
${path:userName}
${path:name.familyName}
${path:name.givenName}
${path:displayName}
${path:nickName}
${path:emails[primary eq true].value}
${path:addresses[type eq "work"].streetAddress}
${path:addresses[type eq "work"].locality}
${path:addresses[type eq "work"].region}
${path:addresses[type eq "work"].postalCode}
${path:addresses[type eq "work"].country}
${path:addresses[type eq "work"].formatted}
${path:phoneNumbers[type eq "work"].value}
${path:userType}
${path:title}
${path:locale}
${path:timezone}
${path:enterprise.employeeNumber}
${path:enterprise.costCenter}

IdP でサポートされている属性
${path:enterprise.organization}
${path:enterprise.division}
${path:enterprise.department}
${path:enterprise.manager.value}

IAM アイデンティティセンターと Microsoft AD の間のデフォルトのマッピング

以下の表に示しているのは、IAM Identity Center のユーザー属性と Microsoft AD ディレクトリのユーザー属性とのデフォルトのマッピングです。IAM ID センターは IAM アイデンティティセンターのユーザー属性 列の属性リストのみをサポートします。

IAM Identity Center のユーザー属性	Active Directory のこの属性にマッピングされる
displayname	${displayname}
emails[?primary].value *	${mail}
externalid	${objectguid}
name.givenname	${givenname}
name.familyname	${sn}
name.middlename	${initials}
sid	${objectsid}
username	${userprincipalname}

* IAM Identity Center の E メール属性はディレクトリ内で一意である必要があります。

IAM アイデンティティセンターのグループ属性	Active Directory のこの属性にマッピングされる
externalid	${objectguid}
description	${description}
displayname	${samaccountname}@{associateddomain}

考慮事項

- 設定可能な AD 同期を有効にしたときに IAM アイデンティティセンターのユーザーとグループに何も割り当てられていない場合は、前の表のデフォルトマッピングが使用されます。これらのマッピングをカスタマイズする方法については、「同期の属性マッピングを設定する」を参照してください。
- IAM アイデンティティセンターの特定の属性は変更不可で、デフォルトで特定の Microsoft AD ディレクトリ属性にマップされるため、変更できません。

  例えば、「username」は IAM アイデンティティセンターの必須属性です。「username」に空の値を持つ AD ディレクトリ属性にマッピングする場合、IAM アイデンティティセンターは、windowsUpn 値を「username」のデフォルト値とみなします。現在のマッピングから「username」の属性マッピングを変更する場合は、「username」に依存する IAM アイデンティティセンターフローが期待どおりに動作するかどうかを確認してください。

IAM アイデンティティセンターでサポートされている Microsoft AD 属性

以下の表では、サポートされているディレクトリ Microsoft AD 属性のうち、IAM Identity Center のユーザー属性にマップできるものをすべて列挙します。

Microsoft AD ディレクトリでサポートされている属性
${samaccountname}
${description}
${objectguid}

Microsoft AD ディレクトリでサポートされている属性
${givenname}
${sn}
${initials}
${mail}
${userprincipalname}
${displayname}
${distinguishedname}
${proxyaddresses[?type == "SMTP"].value}
${proxyaddresses[?type == "smtp"].value}
${useraccountcontrol}

考慮事項

- サポートされている Microsoft AD ディレクトリの属性の任意の組み合わせを指定して、IAM アイデンティティセンターの 1 つの変更可能な属性にマップできます。

Microsoft AD でサポートされている IAM アイデンティティセンター属性

以下の表では、サポートされている IAM Identity Center 属性のうち、 Microsoft AD ディレクトリのユーザー属性にマップできるものをすべて列挙します。後で、アプリケーションの属性マッピングを設定するときに、これらの同じ IAM Identity Center の属性を、そのアプリケーションで使用されている実際の属性にマップできます。

Active Directory において IAM アイデンティティセンターでサポートされている属性
${user:AD_GUID}
${user:AD_SID}

Active Directory において IAM アイデンティティセンターでサポートされている属性
`${user:email}`
`${user:familyName}`
`${user:givenName}`
`${user:middleName}`
`${user:name}`
`${user:preferredUsername}`
`${user:subject}`

IAM アイデンティティセンターと Microsoft AD ディレクトリ間のユーザー属性のマッピング

IAM アイデンティティセンターのユーザー属性を Microsoft AD ディレクトリの対応する属性にマップする方法を指定するには、以下の手順を実行します。

IAM Identity Center の属性をディレクトリの属性にマップするには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [設定] ページで [アクセス制御用の属性] タブを選択し、[属性の管理] を選択します。
4. [アクセスコントロールの属性の管理] ページで、マップする IAM Identity Center の属性を見つけて、テキスト ボックスに値を入力します。例えば、IAM Identity Center ユーザー属性 **`email`** を Microsoft AD ディレクトリ属性 **`${mail}`** にマップするとします。
5. [Save changes] (変更の保存) をクリックします。

IAM Identity Center の構成可能な AD 同期

IAM Identity Center の設定可能な Active Directory (AD) 同期を使用すると、IAM Identity Center に自動的に同期される Microsoft Active Directory の ID を明示的に設定し、同期プロセスを制御できます。

- この同期メソッドを使用すると、次のことが行えます。

- IAM Identity Center に自動的に同期される Microsoft Active Directory 内のユーザーとグループを明示的に定義することにより、データの境界を制御します。ユーザーとグループを追加 したり、ユーザーやグループを削除 したりして、同期の範囲をいつでも変更できます。
- 同期されたユーザーとグループに、AWS アカウント への アプリケーションへのシングルサインオン アクセス またはアプリケーションへのアクセス権を割り当てます。アプリケーションは AWS マネージドアプリケーションでもカスタマーマネージドアプリケーションでもかまいません。
- 必要に応じて同期を 一時停止したり再開 したりして、同期プロセスを制御します。これにより、実稼働システムの負荷を調整できます。

前提条件と考慮事項

設定可能な AD Sync を使用する前に、以下の前提条件と考慮事項に注意してください。

- Active Directory 内のユーザーとグループを指定して同期する

  IAM アイデンティティセンターを使用して、新しいユーザーとグループに AWS アカウント および AWS のマネージドアプリケーションまたはカスタマーマネージドアプリケーションへのアクセスを割り当てる前に、Active Directory で同期するユーザーとグループを指定し、それらを IAM アイデンティティセンターに同期する必要があります。

  - 設定可能な AD 同期 — IAM Identity Center はドメインコントローラーでユーザーやグループを直接検索しません。代わりに、同期するユーザーとグループのリストを最初に指定する必要があります。IAM アイデンティティセンターに既に同期されているユーザーとグループがあるか、設定可能な AD Sync を使用して初めて同期する新しいユーザーとグループがあるかに応じて、このリスト (同期スコープとも呼ばれる) を以下のいずれかの方法で設定できます。
    - 既存のユーザーとグループ:すでに IAM Identity Center と同期されているユーザーとグループがある場合、設定可能な AD Sync の同期スコープには、それらのユーザーとグループのリストがあらかじめ入力されています。新しいユーザーまたはグループを割り当てるには、それらを同期スコープに具体的に追加する必要があります。詳細については、「ユーザーとグループを同期スコープに追加します」を参照してください。
    - 新しいユーザーとグループ: 新しいユーザーやグループに AWS アカウント およびアプリケーションへのアクセス権を割り当てる場合は、IAM Identity Center を使用して割り当てを行う前に、設定可能な AD Sync で同期スコープに追加するユーザーとグループを指定する必要があります。詳細については、「ユーザーとグループを同期スコープに追加します」を参照してください。

- Active Directory 内のネストされたグループへの割り当てを行う

  別のグループのメンバーであるグループは、ネストされたグループ (または子グループ) と呼ばれます。

  - 設定可能な AD 同期 — 設定可能な AD 同期を使用してネストされたグループを含む Active Directory 内のグループに割り当てを行うと、AWS アカウントまたはアプリケーションにアクセスできるユーザーの範囲が広くなる場合があります。この場合、割り当ては、ネストされたグループのユーザーを含むすべてのユーザーに適用されます。たとえば、グループ A にアクセス権を割り当て、グループ B がグループ A のメンバーである場合、グループ B のメンバーもこのアクセスを継承します。
- 自動化されたワークフローの更新

  IAM Identity Center ID ストア API アクションと IAM Identity Center 割り当て API アクションを使用して新しいユーザーとグループにアカウントとアプリケーションへのアクセスを割り当て、IAM Identity Center と同期する自動化ワークフローがある場合は、設定可能な AD 同期によって期待どおりに機能するように、2022 年 4 月 15 日までにそれらのワークフローを調整する必要があります。設定可能な AD Sync により、ユーザーとグループの割り当てとプロビジョニングが行われる順序、およびクエリの実行方法が変わります。

  - 設定可能な AD 同期 — プロビジョニングが最初に実行され、自動的には実行されません。代わりに、まずユーザーとグループを同期スコープに追加して、ID ストアに明示的に追加する必要があります。設定可能な AD Sync の同期設定を自動化するための推奨手順については、同期設定を自動化して、設定可能な AD 同期を実現します。 を参照してください。

トピック

- 設定可能な AD 同期の仕組み
- 同期の属性マッピングを設定する
- Active Directory から IAM アイデンティティセンターへの初回同期設定
- ユーザーとグループを同期スコープに追加します
- 同期スコープからユーザーとグループを削除します。
- 同期の一時停止と再開
- 同期設定を自動化して、設定可能な AD 同期を実現します。

設定可能な AD 同期の仕組み

IAM Identity Center は、以下のプロセスで ID ストアの AD ベースの ID データをリフレッシュします。前提条件の詳細については、「前提条件と考慮事項」を参照してください。

作成

Active Directory 内の自己管理型ディレクトリ、AWS Managed Microsoft AD または Directory Service によって管理されているディレクトリを IAM ID センターに接続したら、IAM ID センターのアイデンティティストアに同期する Active Directory ユーザーとグループを明示的に設定できます。選択した ID は、3 時間ごとに IAM Identity Center の ID ストアに同期されます。ディレクトリのサイズによっては、同期処理に時間がかかる場合があります。

割り当てられたグループのメンバーであるグループ (ネストされたグループまたは子グループと呼ばれる) も、ID ストアに書き込まれます。

新しいユーザーまたはグループが IAM Identity Center アイデンティティストアと同期された後にのみ、アクセス権を割り当てることができます。

更新

IAM Identity Center ID ストアの ID データは、Active Directory のソース ディレクトリから定期的にデータを読み込むことで、常にリフレッシュされた状態を保たれます。IAM アイデンティティセンターは、デフォルトでは 1 時間ごとの同期サイクルでお使いの Active Directory との間でデータを同期します。Active Directory のサイズによっては、データが IAM アイデンティティセンターに同期されるまでに 30 分から 2 時間かかる場合があります。

同期スコープにあるユーザーとグループのオブジェクトとそのメンバーシップは、IAM Identity Center で作成または更新され、Active Directory のソースディレクトリの対応するオブジェクトにマッピングされます。ユーザー属性については、IAM Identity Center コンソールの「アクセス制御用の属性」セクションにリストされている属性のサブセットのみが IAM Identity Center で更新されます。Active Directory で行った属性の更新が IAM アイデンティティセンターに反映されるには、1 回の同期サイクルが必要な場合があります。

IAM Identity Center ID ストアに同期するユーザーとグループのサブセットを更新することもできます。このサブセットに新しいユーザーまたはグループを追加するか、削除するかを選択できます。追加した ID は、次回の定期同期時に同期されます。サブセットから削除した ID は、IAM Identity Center ID ストアで更新されなくなります。28 日以上同期されていないユーザーは、IAM Identity Center ID ストアで無効になります。対応するユーザーオブジェクトは、同期スコープにまだ含まれている別のグループに属していない限り、次回の同期サイクル時に IAM Identity Center ID ストアで自動的に無効になります。

削除

対応するユーザーまたはグループオブジェクトが Active Directory のソース ディレクトリから削除されると、ユーザーとグループは IAM Identity Center ID ストアから削除されます。または、IAM Identity Center コンソールを使用して IAM Identity Center ID ストアからユーザーオブジェクトを明示的に削除することもできます。IAM Identity Center コンソールを使用する場合は、次回の同期サイクル中に IAM Identity Center に再同期されないように、同期スコープからユーザーを削除する必要もあります。

同期をいつでも一時停止と再開することもできます。28 日以上同期を一時停止すると、すべてのユーザーが無効になります。

同期の属性マッピングを設定する

利用可能な属性の詳細については、「IAM アイデンティティセンターと外部 ID プロバイダーディレクトリ間の属性マッピング」を参照してください。

IAM Identity Center でディレクトリへの属性マッピングを設定するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [設定]ページで[ID ソース]タブを選択し、[アクション]を選択し、[同期を管理] を選択します。
4. 「同期の管理」で、「属性マッピングを表示」を選択します。
5. 「Active Directory ユーザー属性」で、IAM Identity Center ID ストア属性 とActive Directory のユーザー属性を設定します。例えば、IAM Identity Center ID ストア属性 `email` を Active Directory のユーザーディレクトリ属性 `${objectguid}` にマップすることができます。

   > **Note**
   >
   > 「グループ属性」では、IAM アイデンティティセンターの ID ストア属性 と Active Directory グループの属性 は変更できません。

6. [Save changes] (変更の保存) をクリックします。これにより、「同期の管理」ページに戻ります。

Active Directory から IAM アイデンティティセンターへの初回同期設定

Active Directory から IAM アイデンティティセンターにユーザーとグループを初めて同期する場合は、以下の手順に従います。または、「アイデンティティソースを変更する」で説明されている手順

に従って、アイデンティティソースを IAM アイデンティティセンターから Active Directory に変更することもできます。

ガイド付きセットアップ

1. IAM Identity Center コンソール を開きます。

> **Note**
>
> 次のステップに進む前に、IAM Identity Center コンソールが AWS Managed Microsoft AD ディレクトリがある AWS リージョン の 1 つを使用していることを確認してください。

2. [設定] を選択します。
3. ページ上部の通知メッセージで、[ガイド付きセットアップを開始] を選択します。
4. 「ステップ 1 — オプション: 属性マッピングの設定」で、デフォルトのユーザーおよびグループ属性マッピングを確認します。変更が不要な場合は、[次へ] を選択します。変更が必要な場合は、変更を行い、[変更の保存] を選択します。
5. 「ステップ 2 — オプション: 同期範囲の設定」で、[ユーザー] タブを選択します。次に、同期スコープに追加するユーザーの正確なユーザー名を入力し、[追加] を選択します。次に、[グループ] タブを選択します。同期スコープに追加するグループの正確なグループ名を入力し、[追加] を選択します。その後、[Next] を選択します。後でユーザーとグループを同期スコープに追加する場合は、変更せずに [次へ] を選択します。
6. 「ステップ 3: 設定を確認して保存する」で、「ステップ 1: 属性マッピング」で属性マッピングを確認し、「ステップ 2: 同期スコープ」でユーザーとグループを確認します。[設定の保存] を選択します。これにより、「同期を管理」ページが表示されます。

ユーザーとグループを同期スコープに追加します

> **Note**
>
> 同期スコープにグループを追加するときは、AWS Managed Microsoft AD ドメイン内のグループからではなく、信頼できるオンプレミスドメインから直接グループを同期します。信頼できるドメインから直接同期されるグループには、IAM Identity Center がアクセスして正常に同期できる実際のユーザーオブジェクトが含まれています。

以下の手順に従って、Active Directory ユーザーとグループを IAM アイデンティティセンターに追加します。

ユーザーを追加するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [設定]ページで[ID ソース]タブを選択し、[アクション]を選択し、[同期を管理] を選択します。
4. [同期の管理] ページで、[ユーザー] タブを選択し、[ユーザーとグループの追加] を選択します。
5. [ユーザー] タブの [ユーザー] に正確なユーザー名を入力し、[追加] を選択します。
6. [追加したユーザーとグループ] で、追加するユーザーを確認します。
7. [送信] を選択します。
8. ナビゲーションペインで [ユーザー] を選択します。指定したユーザーがリストに表示されない場合は、更新アイコンを選択してユーザーのリストを更新します。

グループを追加するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. 設定ページで[ID ソース]タブを選択し、[アクション]を選択し、[同期を管理] を選択します。
4. 「同期の管理」ページで「グループ」タブを選択し、「ユーザーとグループの追加」を選択します。
5. [グループ] タブを選択します。[グループ] で、正確なグループ名を入力し、[追加] を選択します。
6. [追加したユーザーとグループ] で、追加するグループを確認します。
7. [送信] を選択します。
8. ナビゲーションペインで、[グループ] を選択します。指定したグループがリストに表示されない場合は、更新アイコンを選択してグループのリストを更新します。

同期スコープからユーザーとグループを削除します。

同期スコープからユーザーとグループを削除するとどうなるかについての詳細は、設定可能な AD 同期の仕組み を参照してください。

ユーザーを削除するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. 設定ページで[ID ソース]タブを選択し、[アクション]を選択し、[同期を管理] を選択します。
4. [ユーザー] タブを選択します。
5. [同期範囲のユーザー] で、削除するユーザーの横にあるチェックボックスをオンにします。すべてのユーザーを削除するには、「ユーザー名」の横にあるチェックボックスを選択します。
6. [を削除] を選択します。

グループを削除するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. 設定ページで[ID ソース]タブを選択し、[アクション]を選択し、[同期を管理] を選択します。
4. [グループ] タブを選択します。
5. [同期範囲のグループ] で、削除するユーザーの横にあるチェックボックスをオンにします。すべてのグループを削除するには、[グループ名] の横にあるチェックボックスをオンにします。
6. [を削除] を選択します。

同期の一時停止と再開

同期を一時停止すると、今後のすべての同期サイクルが一時停止され、Active Directory 内のユーザーとグループに加えた変更が IAM Identity Center に反映されなくなります。同期を再開すると、同期サイクルでは次に予定されている同期からこれらの変更が反映されます。

同期を一時停止するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [設定]ページで[ID ソース]タブを選択し、[アクション]を選択し、[同期を管理] を選択します。
4. [同期の管理] で [同期を一時停止] を選択します。

同期を再開するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [設定]ページで[ID ソース]タブを選択し、[アクション]を選択し、[同期を管理] を選択します。
4. [同期の管理] で [同期を再開] を選択します。

> **Note**
>
> [同期を再開] ではなく [同期を一時停止] が表示される場合は、Active Directory から IAM Identity Center への同期はすでに再開されています。

同期設定を自動化して、設定可能な AD 同期を実現します。

設定可能な AD 同期で自動化されたワークフローが期待どおりに機能するようにするには、次の手順を実行して同期設定を自動化することをお勧めします。

設定可能な AD Sync の同期設定を自動化するには

1. Active Directory で、IAM アイデンティティセンターに同期したいすべてのユーザーとグループを含む 親同期グループを作成します。例えば、グループに IAMIdentityCenterAllUsersAndGroups という名前を付けることができます。
2. IAM Identity Center で、親同期グループを設定可能な同期リストに追加します。IAM Identity Center は、親同期グループに含まれるすべてのユーザー、グループ、サブグループ、およびすべてのグループのメンバーを同期します。
3. Microsoft が提供する Active Directory ユーザーおよびグループ管理 API アクションを使用して、親同期グループにユーザーとグループを追加または削除します。

アイデンティティセンターディレクトリでユーザーを管理する

IAM Identity Center は、ユーザーとグループに以下の機能を提供します。

- ユーザーとグループを作成します。
- ユーザーをメンバーとしてグループに追加します。
- グループに、AWS アカウント とアプリケーションへの希望するレベルのアクセスを割り当てます。

IAM Identity Center ストア内のユーザーとグループを管理するために、Identity Center Actions に記載されている API オペレーションを AWS がサポートします。

IAM Identity Center にいるユーザーのプロビジョニング

IAM Identity Center で直接ユーザーやグループを作成した場合、プロビジョニングは自動的に行われます。これらの ID は、割り当てを行う際や、アプリケーションで使用する際にすぐに利用できます。詳細については、「ユーザーおよびグループのプロビジョニング」を参照してください。

ID ソースの変更

AWS Managed Microsoft AD でユーザーを管理したい場合は、Identity Center ディレクトリの使用はいつでも停止でき、代わりに Directory Service を使用して IAM Identity Center を Microsoft AD のディレクトリに接続できます。詳細については、「IAM アイデンティティセンターディレクトリと Active Directory 間の切り替え」の考慮事項を参照してください。

ユーザーを外部の ID プロバイダー (IdP) で管理したい場合は、IAM Identity Center を IdP に接続し、自動プロビジョニングを有効にすることができます。詳細については、「IAM アイデンティティセンターから外部 IdP への変更」の考慮事項を参照してください。

トピック

- アイデンティティセンターディレクトリにユーザーを追加する
- アイデンティティセンターディレクトリにグループを追加する
- グループにユーザーを追加
- IAM Identity Center でグループを削除
- IAM Identity Center でユーザーを削除する
- グループからユーザーを削除する
- Identity Center ディレクトリでユーザープロパティを編集する

アイデンティティセンターディレクトリにユーザーを追加する

Identity Center ディレクトリで作成するユーザーとグループは、IAM Identity Center でのみ使用することができます。次の手順に従って、 アイデンティティセンターディレクトリにユーザーを追加します。または、AWS API オペレーション CreateUser を呼び出してユーザーを追加することもできます。

Console

ユーザーを追加するには

1. IAM アイデンティティセンターコンソールを開きます。
2. [ユーザー] を選択します。
3. [Add user] (ユーザーを追加) をクリックして、以下の必要な情報を入力します。

   a. ユーザー名 — このユーザー名は AWS アクセスポータルにサインインするために必要で、後で変更することはできません。1 ~ 100 文字である必要があります。

   b. パスワード — パスワードの設定手順を記載した E メールを送信するか (デフォルトのオプション)、ワンタイムパスワードを生成できます。管理ユーザーを作成していて E メールを送信する場合は、アクセスできるメールアドレスを必ず指定してください。

      i. パスワード設定方法を記載した E メールをユーザーに送信する — このオプションでは、Amazon Web Services から [AWS IAM アイデンティティセンター への参加招待] という件名の E メールがユーザー宛に自動的に送信されます。この E メールは、会社の代表者ユーザーに対し、IAM アイデンティティセンターの AWS アクセスポータルにアクセスし、パスワードを登録するよう促します。この E メール招待状の有効期間は 7 日間です。有効期間を過ぎた場合は、[パスワードのリセット] > [パスワードのリセット手順を記載したメールをユーザーに送信] を選択して E メールを再送信できます。ユーザーが招待を受け入れる前に、ユーザーメールアドレス確認向けの [E メール検証リンクを送信] が表示されます。ただしこのステップはオプションで、ユーザーがそのまま招待を受け入れてパスワードを登録すると表示は消えます。

> **Note**
>
> 特定の地域では、IAM ID Center が別の AWS リージョン から Amazon Simple Email Service を使用するユーザーに E メールを送信します。E メールの送信方法については、Amazon SES を使用したクロスリージョン E メール を参照してください。
> IAM アイデンティティセンターサービスで送信されるすべてのメールは、アドレス `no-reply@signin.aws.com` または `no-reply@login.awsapps.com` のいずれかから送信されます。これらの送信者メールアドレスからの E メールを受け入れ、迷惑メールやスパムとして処理しないように、メールシステムを設定することをお勧めします。

ii. Generate a one-time password that you can share with the user (ユーザーと共有することができるワンタイムパスワードを生成する) – このオプションでは、E メールアドレスから手動でユーザーに送信できる、 AWS アクセスポータルの URL とパスワードの詳細が利用できます。ユーザーは自分の E メールアドレスを確認する必要があります。[E メール検証リンクを送信] を選択して、プロセスを開始できます。E メール検証リンクの有効期間は 7 日間です。有効期間を過ぎた場合は、[パスワードのリセット] > [ワンタイム パスワードを生成してユーザーと共有する] を選択してメールアドレス確認のためのリンクを再送信することができます。

c. E メールアドレス — E メールアドレスは一意である必要があります。

d. E メールアドレスを確認

e. 名 — 自動プロビジョニングを行うためには、ここに名前を入力する必要があります。詳細については、「SCIM を使用して外部 ID プロバイダーからユーザーとグループをプロビジョニングする」を参照してください。

f. 姓 — 自動プロビジョニングを行うためには、ここに名前を入力する必要があります。

g. 表示名

> **Note**
>
> (オプション) 該当する場合は、ユーザーの Microsoft 365 不変 ID などの追加属性の値を指定して、ユーザーに特定のビジネスアプリケーションへのシングルサインオンアクセスを提供できます。

4. [次へ] を選択します。

5. 該当する場合は、ユーザーを追加するグループを 1 つ以上選択し、[次へ] を選択します。

6. 「ステップ 1: ユーザーの詳細を指定する」と「ステップ 2: ユーザーをグループに追加 (オプション)」で指定した情報を確認します。いずれかのステップで [編集] を選択し、変更を加えます。両方のステップで正しい情報が指定されていることを確認したら、[ユーザーを追加] を選択します。

AWS CLI

ユーザーを追加するには

次の `create-user` コマンドは、アイデンティティセンターディレクトリに新しいユーザーを作成します。

```
aws identitystore create-user \
    --identity-store-id d-1234567890 \
    --user-name johndoe \
    --name "GivenName=John,FamilyName=Doe" \
    --display-name "John Doe" \
    --emails "Type=work,Value=johndoe@example.com"
```

出力:

```
{
    "UserId": "1234567890-abcdef",
    "IdentityStoreId": "d-1234567890"
}
```

> **Note**
>
> `create-user` CLI コマンドまたは CreateUser API オペレーションでユーザーを作成する場合、そのユーザーにはパスワードがありません。IAM アイデンティティセンターの設定を更新して、ユーザーが初めてサインオンを試みた後に検証 E メールを送信し、パスワードを設定できるようにします。この設定を有効にしない場合は、ワンタイムパスワードを生成し、これをユーザーと共有する必要があります。詳細については、「API または CLI で作成されたユーザーにワンタイムパスワードを E メールで送信する」を参照してください。

アイデンティティセンターディレクトリにグループを追加する

次の手順に従って、 アイデンティティセンターディレクトリにグループを追加します。または、AWS API オペレーション CreateGroup を呼び出してグループを追加することもできます。

Console

グループを追加するには

1. IAM アイデンティティセンターコンソールを開きます。
2. [グループ] を選択します。
3. [グループの作成] を選択します。

4. グループ名 と 説明を入力します - オプション。説明は、グループにどのようなアクセス権限が割り当てられているか (または割り当てられるか) に関する詳細を記載する必要があります。「ユーザーをグループに追加 - オプション」で、メンバーとして追加するユーザーを見つけます。それぞれの横にあるチェックボックスをオンにします。
5. [グループの作成] を選択してください。

AWS CLI

グループを追加するには

次の `create-group` コマンドは、アイデンティティセンターディレクトリに新しいグループを作成します。

```
aws identitystore create-group \
    --identity-store-id d-1234567890 \
    --display-name "Developers" \
    --description "Group that contains all developers"
```

出力:

```
{
    "GroupId": "1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p",
    "IdentityStoreId": "d-1234567890"
}
```

このグループをアイデンティティセンターディレクトリに追加すると、グループにシングルサインオンアクセスを割り当てることができます。詳細については、「AWS アカウント にユーザーまたはグループアクセスを割り当てる」を参照してください。

グループにユーザーを追加

以下の手順に従って、以前にアイデンティティセンターディレクトリに作成したグループのメンバーとしてユーザーを追加します。または、AWS API オペレーション CreateGroupMembership を呼び出して、ユーザーをグループのメンバーとして追加することもできます。

Console

グループのメンバーとしてユーザーを追加するには

1. IAM アイデンティティセンターコンソールを開きます。
2. [グループ] を選択します。
3. 更新する グループ名 を選択します。
4. グループ詳細ページの [このグループのユーザー] で、[ユーザーをグループに追加] を選択します。
5. [グループにユーザーを追加] ページの [その他のユーザー] で、メンバーとして追加するユーザーを見つけます。それぞれの横にあるチェックボックスをオンにします。
6. [ユーザーの追加] を選択します。

AWS CLI

グループのメンバーとしてユーザーを追加するには

次の `create-group-membership` コマンドは、アイデンティティセンターディレクトリのグループにユーザーを追加します。

```
aws identitystore create-group-membership \
    --identity-store-id d-1234567890 \
    --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \
    --member-id UserId=a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

出力:

```
{
    "MembershipId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "IdentityStoreId": "d-1234567890"
}
```

IAM Identity Center でグループを削除

IAM アイデンティティセンターディレクトリ内のグループを削除すると、そのグループのメンバーであるすべてのユーザーの AWS アカウント および アプリケーションへのアクセス権が削除されま

す。グループが削除された後、元に戻すことはできません。IAM アイデンティティセンター内のグループを削除するには、以下の手順に従います。

> **Important**
>
> このページの説明は、AWS IAM アイデンティティセンター に適用されます。これらは AWS Identity and Access Management (IAM) には適用されません。IAM アイデンティティセンターユーザー、グループ、およびユーザー認証情報は、IAM ユーザー、グループ、IAM ユーザー認証情報とは異なります。IAM でグループを削除する手順をお探しの場合は、「AWS Identity and Access Management ユーザーガイド」の「IAM ユーザーグループの削除」を参照してください。

Console

グループを削除するには

1. IAM Identity Center コンソールを開きます。
2. [グループ] を選択します。
3. グループを削除するには 2 つの方法があります。
   - グループ ページでは、複数のグループを選択して削除することができます。削除するグループ名を選択し、[グループの削除] を選択します。
   - 削除するグループ名を選択します。グループの詳細ページで、[グループの削除] を選択します。
4. グループを削除するかどうかの確認を求められる場合があります。
   - 複数のグループを一度に削除する場合は、[グループの削除] ダイアログボックスに **`Delete`** を入力して削除を確定します。
   - ユーザーを含む 1 つのグループを削除する場合は、削除するグループの名前を [グループの削除] ダイアログボックスに入力して削除を確定します。
5. [Delete group (グループの削除)] を選択します。削除するグループを複数選択した場合は、[# グループを削除] を選択します。

AWS CLI

グループを削除するには

次の delete-group コマンドは、指定されたグループをアイデンティティセンターディレクトリから削除します。

```
aws identitystore delete-group \
    --identity-store-id d-1234567890 \
    --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

IAM Identity Center でユーザーを削除する

IAM アイデンティティセンターディレクトリ内のユーザーを削除すると、AWS アカウント およびアプリケーションへのアクセスが削除されます。ユーザーを削除すると、このアクションを元に戻すことはできません。アイデンティティセンターディレクトリ内のユーザーを削除するには、以下の手順に従います。

> **Note**
>
> ユーザーアクセスを無効にするか、IAM Identity Center でユーザーを削除すると、そのユーザーはすぐに AWS アクセスポータルにサインインできなくなり、新しいサインイン セッションを作成できなくなります。詳細については、「IAM アイデンティティセンターの認証セッションについて」を参照してください。

> **Important**
>
> このページの説明は、AWS IAM アイデンティティセンター に適用されます。これらは AWS Identity and Access Management (IAM) には適用されません。IAM アイデンティティセンターユーザー、グループ、およびユーザー認証情報は、IAM ユーザー、グループ、IAM ユーザー認証情報とは異なります。IAM でユーザーを削除する手順をお探しの場合は、「AWS Identity and Access Management ユーザーガイド」の「IAM ユーザーの削除」を参照してください。

Console

ユーザーを削除するには

1. IAM アイデンティティセンターコンソールを開きます。
2. [ユーザー] を選択します。

3. ユーザーを削除するには 2 つの方法があります。

   - ユーザー ページでは、削除するユーザーを複数選択できます。削除するユーザー名を選択し、[ユーザーの削除] を選択します。
   - 削除するユーザー名を選択します。ユーザーの詳細ページで、[ユーザーの削除] を選択します。

4. 複数のユーザーを一度に削除する場合は、[ユーザーの削除] ダイアログボックスに **Delete** を入力して削除を確定します。
5. [ユーザーの削除] を選択します。削除するユーザーを複数選択した場合は、[# ユーザーを削除] を選択します。

AWS CLI

ユーザーを削除するには

次の delete-user コマンドは、アイデンティティセンターディレクトリからユーザーを削除します。

```
aws identitystore delete-user \
    --identity-store-id d-1234567890 \
    --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

グループからユーザーを削除する

グループからメンバーを削除するには、次の手順を実行します。または、AWS API オペレーション DeleteGroupMembership を呼び出して、グループからユーザーを削除することもできます。

Console

グループからユーザーを削除するには

1. IAM Identity Center コンソールを開きます。
2. [グループ] を選択します。
3. 更新するグループを選択します。
4. グループ詳細ページの [このグループのユーザー] で、削除するユーザーを選択します。
5. [グループからユーザーを削除]) を選択します。

6. [ユーザーの削除] ダイアログボックスで、[グループからユーザーを削除] を選択し、グループに割り当てられたアカウントとアプリケーションへのアクセス権をユーザーから削除することを確認します。

AWS CLI

グループからユーザーを削除するには

次の `delete-group-membership` コマンドは、グループからメンバーシップを削除します。

```
aws identitystore delete-group-membership
    --identity-store-id d-1234567890 \
    --membership-id a1b2c3d4-5678-90ab-cdef-EXAMPLE33333
```

Identity Center ディレクトリでユーザープロパティを編集する

以下の手順に従って、 アイデンティティセンターディレクトリでユーザーのプロパティを編集します。あるいは、AWS API オペレーション UpdateUser を呼び出してユーザープロパティを更新することもできます。

Console

IAM Identity Center でユーザープロパティを編集するには

1. IAM アイデンティティセンターコンソールを開きます。
2. [ユーザー] を選択します。
3. 編集するユーザーを選択します。
4. ユーザー [プロファイル] ページで、[プロファイルの詳細] の横にある [編集] を選択します。
5. [プロファイル詳細の編集] ページで、必要に応じてプロパティを更新します。次に、[変更の保存] を選択します。

> **Note**
>
> (オプション) 従業員番号 や Office 365 不変 ID などの追加の属性を変更して、IAM Identity Center 内のユーザーの ID をユーザーが使用する必要がある特定のビジネスアプリケーションにマップするのに役立ちます。

> **Note**
>
> E メールアドレス属性は編集可能なフィールドで、指定する値は一意である必要があります。

AWS CLI

IAM Identity Center でユーザープロパティを編集するには

次の `update-user` コマンドは、ユーザーのニックネームを更新します。

```
aws identitystore update-user \
    --identity-store-id d-1234567890 \
    --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --operations '{"AttributePath":"nickName","AttributeValue":"Johnny"}'
```

AWS リソースへのワークフォースアクセスを設定する

ワークフォースユーザーが IAM アイデンティティセンターを介して AWS リソースを認証およびアクセスする方法を設定します。このセクションでは、AWS 環境へのワークフォースユーザーアクセスを管理する以下のコンポーネントについて説明します。

- 認証セッション – インタラクティブポータルセッションからバックグラウンドアプリケーションセッションまで、IAM アイデンティティセンターがさまざまなタイプのユーザーセッションを管理する方法と、それらが相互にやり取りする方法を理解します。
- ユーザーアクセス管理 – セッション期間を設定し、ユーザーアカウントを無効にし、組織全体のアクセスブロックを実装して、セキュリティとコンプライアンスを維持します。
- パスワード管理 – アイデンティティセンターディレクトリで作成されたユーザーの場合、パスワード要件の設定、ユーザー認証情報の設定、ユーザーのパスワードリセットの管理を行います。
- 多要素認証 – アイデンティティセンターディレクトリで作成されたユーザーの場合、認証アプリケーション、セキュリティキー、または組み込み認証を使用して MFA でセキュリティを強化し、ユーザーのサインインを保護します。

トピック

- IAM アイデンティティセンターの認証セッションについて
- IAM アイデンティティセンターでセッション期間を設定する
- IAM アイデンティティセンターで AWS アカウントとアプリケーションへのユーザーアクセスを無効にする
- サービスコントロールポリシーでのユーザーアクセスの拒否
- IAM アイデンティティセンターユーザーのアクセス権を管理する

IAM アイデンティティセンターの認証セッションについて

ユーザーが AWS アクセスポータルにサインインすると、IAM アイデンティティセンターは、ユーザーの検証済み ID を表す認証セッションを作成します。

認証されると、ユーザーは、管理者が追加のサインインなしで使用許可を付与した、割り当てられたすべての AWS アカウント、 AWS マネージドアプリケーション、およびカスタマーマネージドアプリケーションにアクセスできます。

認証セッションのタイプ

ユーザーインタラクティブセッション

ユーザーが AWS アクセスポータルにサインインすると、IAM アイデンティティセンターはユーザーのインタラクティブセッションを作成します。このセッションは、IAM アイデンティティセンター内のユーザーの認証状態を表し、他のセッションタイプを作成するための基盤として機能します。ユーザーインタラクティブセッションは、IAM アイデンティティセンターで設定された期間、最大 90 日間継続できます。

ユーザーインタラクティブセッションは、主要な認証メカニズムです。これらは、ユーザーがサインアウトしたとき、または管理者がセッションを終了したときに終了します。これらのセッションの期間は、組織のセキュリティ要件に基づいて慎重に設定する必要があります。

ユーザーインタラクティブセッション期間の設定については、「the section called “セッション期間を設定する”」を参照してください。

アプリケーションセッション

アプリケーションセッションは、IAM Identity Center がシングルサインオンを通じて確立する、ユーザーと AWS マネージドアプリケーション (Kiro や Amazon Quick など) 間の認証された接続です。

デフォルトでは、アプリケーションセッションの有効期間は 1 時間ですが、基盤となるユーザーのインタラクティブセッションが有効である限り、自動的に更新されます。この更新メカニズムは、セキュリティコントロールを維持しながら、ユーザーにシームレスなエクスペリエンスを提供します。ユーザーのサインアウトまたは管理者アクションを通じてユーザーのインタラクティブセッションが終了すると、アプリケーションセッションは、通常 30 分以内に次の更新試行で終了します。

AWS アカウント へのアクセスにアカウントアクセスマネージャーを使用する場合、そのユーザーポータルは AWS アクセスポータルの AWS アカウントアクセスアプリケーションとして使用できます。AWS アカウントアクセスアプリケーションのセッションは、IAM Identity Center によってアプリケーションセッションとして管理されます。

ユーザーバックグラウンドセッション

ユーザーバックグラウンドセッションは、中断することなく数時間または数日間プロセスを実行する必要があるアプリケーション用に設計された、長期間のセッションです。現在、このセッションタイプは主に Amazon SageMaker Studio に適用されます。Amazon SageMaker Studio では、データサイエンティストが機械学習トレーニングジョブを実行するため、完了までに数時間かかる場合があります。

ユーザーバックグラウンドセッション期間の設定については、「ユーザーバックグラウンドセッション」を参照してください。

Kiro セッション

Kiro セッションを拡張して、デベロッパーが IDE で Kiro を使用して認証を最大 90 日間維持できるようにします。この機能は、コード作業中のログインの中断を減らします。

これらのセッションは他のセッションタイプから独立しており、ユーザーのインタラクティブセッションやその他の AWS マネージドアプリケーションには影響しません。IAM アイデンティティセンターを有効にした時期によっては、この機能がデフォルトで有効になっている場合があります。

Kiro の延長セッションの設定の詳細については、「???」を参照してください。

IAM ロールセッション

アクセス許可セットベースの IAM ロールセッション

IAM アイデンティティセンターは、ユーザーが AWS マネジメントコンソール または AWS CLI にアクセスするときに別のタイプのセッションを作成します。このような場合、IAM アイデンティティセンターはサインインセッションを使用して、ユーザーのアクセス許可セットで指定された IAM ロールを引き受けて IAM セッションを取得します。

アカウントアクセスマネージャー作成の IAM ロールセッション

AWS アカウント へのアクセスにアカウントアクセスマネージャーを使用する場合、アカウントアクセスマネージャーは割り当てられた IAM ロールを引き受けて、IAM ロールセッションを開始します。

> **Important**
>
> アプリケーションセッションとは異なり、IAM ロールセッションは一度確立されると独立して動作します。アクセス許可セット (またはアカウントアクセスマネージャーを使用する場合は IAM ロール) で設定された期間は保持されます。元のサインインセッションのステータスに関係なく、最大 12 時間です。この動作により、長時間実行される CLI オペレーションやコンソールセッションが予期せず終了することはありません。

IAM アイデンティティセンターでエンドユーザーセッションを行う方法

ユーザー主導

ユーザーが AWS アクセスポータルからサインアウトすると、サインインセッションが終了し、ユーザーが新しいリソースにアクセスできなくなります。

ただし、既存のアプリケーションセッションはすぐに終了しません。代わりに、次の更新を試みてサインインセッションが無効になったことが判明すると、約 30 分以内に終了します。既存の IAM ロールセッションは、アクセス許可セット設定 (またはアカウントアクセスマネージャーを使用する場合は IAM ロールの設定) に基づいて有効期限が切れるまで継続します。有効期限は最大 12 時間です。

管理者主導

組織内の IAM アイデンティティセンター管理権限を持つユーザー、通常は IT 管理者またはセキュリティチームが、ユーザーのセッションを終了できます。このアクションは、ユーザーが自分でサインアウトした場合と同じように機能するため、管理者は必要に応じてユーザーに再度サインインするように要求できます。この機能は、セキュリティポリシーが変更された場合や疑わしいアクティビティが検出された場合に役立ちます。

IAM アイデンティティセンター管理者がユーザーを削除するか、ユーザーのアクセスを無効にすると、そのユーザーは AWS アクセスポータルにアクセスできなくなり、新しいアプリケーションまたは IAM ロールセッションを開始するためにサインインし直すことができなくなります。ユーザーは 30 分以内に既存のアプリケーションセッションにアクセスできなくなります。既存の IAM ロールセッションは、IAM Identity Center アクセス許可セット (またはアカウントアクセスマネージャーを使用する場合は IAM ロール) で設定されたセッション持続時間に基づいて継続されます。セッションの最大継続時間は 12 時間となります。

セッションを終了するとユーザーアクセスがどうなるか

このリファレンスでは、管理アクションを実行したときの IAM アイデンティティセンターセッションの動作に関する詳細情報を提供します。このセクションの表は、AWS アクセスポータル、アプリケーション、および AWS アカウント セッションへのアクセスに対するユーザー管理アクションとアクセス許可の変更の期間と影響を示しています。

ユーザー管理

この表は、ユーザー管理の変更が AWSリソース、アプリケーションセッション、AWS アカウントセッションへのアクセスにどのように影響するかをまとめたものです。

アクション	ユーザーが IAM アイデンティティセンターにアクセスできなくなる	ユーザーが新しいアプリケーションセッションを作成できない	ユーザーが既存のアプリケーションセッションにアクセスできない	ユーザーが既存の AWS アカウント セッションにアクセスできなくなる
ユーザーのアクセスが無効	すぐに有効	すぐに有効	30 分以内	12 時間以内。期間は、アクセス許可セット (またはアカウントアクセスマネージャーを使用する場合は IAM ロール) 用に設定された IAM ロールセッションの有効期限によって異なります。
ユーザーを削除しました	すぐに有効	すぐに有効	30 分以内	12 時間以内。期間は、アクセス許可セット (またはアカウントアクセスマネージャーを使用する場合は IAM ロール) 用に設定された IAM ロールセッションの有効期限によって異なります。
ユーザーセッションが取り消されました	アクセスを回復するには、ユーザーが再度サインインする必要があります	すぐに有効	30 分以内	12 時間以内。期間は、アクセス許可セット (またはアカウントアクセスマネー

アクション	ユーザーが IAM アイデンティティセンターにアクセスできなくなる	ユーザーが新しいアプリケーションセッションを作成できない	ユーザーが既存のアプリケーションセッションにアクセスできない	ユーザーが既存の AWS アカウント セッションにアクセスできなくなる
				ジャーを使用する場合は IAM ロール) 用に設定された IAM ロールセッションの有効期限によって異なります。
ユーザーがサインアウトする	アクセスを回復するには、ユーザーが再度サインインする必要があります	すぐに有効	30 分以内	12 時間以内。期間は、アクセス許可セット (またはアカウントアクセスマネージャーを使用する場合は IAM ロール) 用に設定された IAM ロールセッションの有効期限によって異なります。

グループメンバーシップ

この表は、ユーザーアクセス許可とグループメンバーシップの変更が、AWS リソース、アプリケーションセッション、AWS アカウントセッションへのアクセスにどのように影響するかをまとめたものです。

アクション	ユーザーが IAM アイデンティティセンターにアクセスできなくなる	ユーザーが新しいアプリケーションセッションを作成できない	ユーザーが既存のアプリケーションセッションにアクセスできない	ユーザーが既存の AWS アカウント セッションにアクセスできなくなる
アプリケーションまたは AWS アカウント からユーザーアクセスを削除するには	いいえ - ユーザーは引き続き IAM アイデンティティセンターにアクセスできます	すぐに有効	30 分以内	12 時間以内。期間は、アクセス許可セット (またはアカウントアクセスマネージャーを使用する場合は IAM ロール) 用に設定された IAM ロールセッションの有効期限によって異なります。
アプリケーションまたは AWS アカウント が割り当てられたグループから削除されたユーザー	いいえ - ユーザーは引き続き IAM アイデンティティセンターにアクセスできます	すぐに有効	30 分以内	12 時間以内。期間は、アクセス許可セット (またはアカウントアクセスマネージャーを使用する場合は IAM ロール) 用に設定された IAM ロールセッションの有効期限によって異なります。
グループから削除されたアプリケーションまたは AWS アカウント アクセス	いいえ - ユーザーは引き続き IAM アイデンティティセン	すぐに有効	30 分以内	12 時間以内。期間は、アクセス許可セット (またはアカウントアクセスマネー

アクション	ユーザーが IAM アイデンティティセンターにアクセスできなくなる	ユーザーが新しいアプリケーションセッションを作成できない	ユーザーが既存のアプリケーションセッションにアクセスできない	ユーザーが既存の AWS アカウント セッションにアクセスできなくなる
	ターにアクセスできます			ジャーを使用する場合は IAM ロール) 用に設定された IAM ロールセッションの有効期限によって異なります。

> **Note**
>
> AWS アクセスポータルと AWS CLI には、そのグループからユーザーを追加または削除した直後に更新されたユーザーアクセス許可が反映されます。外部 ID プロバイダーを使用した場合、プロバイダーが更新を IAM Identity Center と同期した後に変更が有効になります。

タイミングの違いについて

- 即時有効 – IAM Identity Center は、グループメンバーシップとアクセス許可の変更をリアルタイムに評価します。次回ユーザーが新しいセッションを作成しようとしたときに、変更が適用されます。
- 30 分以内 – 既存のアプリケーションセッションは、次回更新しようとしたときに終了します。通常は 30 分以内に終了します。
- 12 時間以内 – IAM ロールセッションは独立して動作し、設定された期間が経過した場合にのみ終了します。

シングルログアウト

IAM アイデンティティセンターは、ID ソースとして機能する ID プロバイダーによって開始された SAML Single Logout (接続されたすべてのアプリケーションからユーザーがサインアウトするときに自動的にサインアウトするプロトコル) をサポートしていません。さらに、IAM アイデンティティセ

ンターを ID プロバイダーとして使用する SAML 2.0 アプリケーションには SAML Single Logout を送信しません。

セッション管理のベストプラクティス

効果的なセッション管理には、慎重な設定とモニタリングが必要です。組織は、セキュリティ要件に適したセッション期間を設定する必要があります。一般的に、機密性の高いアプリケーションや環境では短い期間を使用します。

ユーザーがロールを変更したり、組織を離れたりするときにセッションを終了するプロセスを実装することは、セキュリティの境界を維持するために不可欠です。アクティブなセッションの定期的なレビューをセキュリティモニタリングプラクティスに組み込み、異常なアクセスパターン、予期しないログイン時間や場所、通常の職務外のリソースへのアクセスなど、セキュリティ上の問題を示す可能性のある異常な動作を検出する必要があります。

IAM アイデンティティセンターでセッション期間を設定する

Kiro など IAM Identity Center と連携する AWS アクセスポータル およびアプリケーションを使用する場合、ワークフォースユーザーのセッション期間を設定できます。IAM Identity Center には、セッションタイプとして、ユーザーインタラクティブセッション、ユーザーバックグラウンドセッション、Kiro の延長セッションが用意されています。

トピック

- ユーザーインタラクティブセッション
- ユーザーバックグラウンドセッション
- Kiro の延長セッション
- ワークフォースユーザーのアクティブなセッションを表示および終了する
- ID ソース、AWS CLI、および AWS SDK を使用する際のセッション期間に関する考慮事項

ユーザーインタラクティブセッション

ユーザーインタラクティブセッションは、 AWS アクセスポータルへのユーザーのサインインまたはAWS マネージドアプリケーションへのアクセスに関連付けられたセッションです。AWS アクセスポータル およびアプリケーションへの認証セッション期間は、ユーザーが再認証なしでサインインを維持できる最大時間です。アクティブな AWS アクセスポータルセッションを終了すると、これらのマネージドアプリケーションのセッションも終了します。

ユーザーインタラクティブセッションのデフォルトのセッション期間は 8 時間です。最小 15 分から最大 90 日まで、異なる期間を指定できます。カスタム期間値は分単位で入力する必要があり、15 分から 129,600 分 (90 日) の間である必要があります。詳細については、「IAM アイデンティティセンターの認証セッションについて」を参照してください。

IAM Identity Center ID ソースがユーザーインタラクティブセッション期間にどのように影響するかといった考慮事項については、「the section called “ID ソース、AWS CLI、および AWS SDK に関する考慮事項”」を参照してください。

ユーザーインタラクティブセッションの期間を設定するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [設定] ページで、[認証] タブを選択します。
4. [認証] の [セッション期間] の横にある [設定] を選択します。[セッション期間の設定] のダイアログボックスが表示されます。
5. [セッション期間の設定] ダイアログボックスの [ユーザーインタラクティブセッション] で、ドロップダウン矢印を選択して、ユーザーの最大セッション期間を選択します。セッションの長さを選択し、[保存] を選択します。

   > **Note**
   >
   > セッション期間の変更は、新しいセッションにのみ適用されます。現在のセッションは元の期間を維持します。

6. [認証] タブに戻ります。タブの上に緑色の通知メッセージが表示され、セッション設定が正常に更新されたことを示します。

ユーザーバックグラウンドセッション

ユーザーバックグラウンドセッションを使用すると、ユーザーは Amazon SageMaker Studio などの AWS マネージドアプリケーションで長時間実行されるジョブを開始できます。ジョブの実行中にサインインしたままにする必要はありません。ジョブはすぐに実行され、IAM アイデンティティセンターの信頼できる ID 伝播機能を使用して、ジョブがバックグラウンドで実行されている間、ユーザーのアクセス許可が維持されるようにします。ユーザーがコンピュータをオフにした場合、IAM アイデンティティセンターのサインインセッションの有効期限が切れた場合、またはユーザーが AWS アクセスポータルからサインアウトした場合でも、ジョブは引き続き実行できます。この機能

を使用すると、データサイエンティスト、機械学習エンジニアなどは、アクティブなユーザーの関与なしにバックグラウンドで実行される分析と機械学習ワークフローを開始できます。

ユーザーバックグラウンドセッションは、Amazon SageMaker Studio などのサポートされている AWS マネージドアプリケーションでデフォルトで有効になっています。ただし、この機能を使用するには、ドメインを作成または更新するときに Amazon SageMaker Studio で信頼できる ID の伝播を有効にする必要があります。詳細については、「Amazon SageMaker AI ドメインで信頼できる ID の伝播を有効にする」を参照してください。

ユーザーバックグラウンドセッションのデフォルトのセッション期間は 7 日間です。最小 15 分から最大 90 日まで、異なる期間を指定できます。カスタム期間値は分単位で入力する必要があり、15 分から 129,600 分 (90 日) の間である必要があります。

ユーザーバックグラウンドセッションでは、次の考慮事項に注意してください。

- ユーザーバックグラウンドセッションは、ユーザーが Amazon SageMaker Studio でジョブを手動で開始した場合にのみ作成できます。この機能は、スケジュールされた自動化されたワークフローではサポートされていません。
- ユーザーバックグラウンドセッションをサポートする AWS リージョンのリストについては、「サポートされている AWS リージョン」を参照してください。
- CloudTrail でユーザー背景セッションを表示できます。詳細については、「ユーザー背景セッションの詳細の特定」を参照してください。
- 組織内のユーザーのアクティブなセッションを終了することもできます。詳細については、「ワークフォースユーザーのアクティブセッションを終了する」を参照してください。

ユーザーバックグラウンドセッションの期間を設定するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [設定] ページで、[認証] タブを選択します。
4. [認証] の [セッション期間] の横にある [設定] を選択します。[セッション期間の設定] ダイアログボックスが表示されます。
5. [セッション期間の設定] ダイアログボックスで、[ユーザー背景セッションを有効にする] チェックボックスがまだ選択されていない場合は、それを選択します。チェックボックスをオフにすると、ユーザーのバックグラウンドセッションが無効になります。

> **Note**
>
> ユーザーバックグラウンドセッションを無効にしても、現在のセッションは影響を受けません。

6. [ユーザー背景セッション] で、ドロップダウン矢印を選択して最大セッション期間を選択します。セッションの長さを選択し、[保存] を選択します。

> **Note**
>
> セッション期間の変更は、新しいセッションにのみ適用されます。現在のセッションは元の期間を維持します。

7. [認証] タブに戻ります。タブの上に緑色の通知メッセージが表示され、セッション設定が正常に更新されたことを示します。

> **Note**
>
> カスタマーマネージドアプリケーションは、ユーザーバックグラウンドセッションを作成できません。

Kiro の延長セッション

開発者が Kiro を統合開発環境 (IDE) の一部として使用している場合、Kiro のセッション期間を 90 日に設定できます。IAM Identity Center を有効にしたタイミングによっては、Kiro の延長セッション期間がデフォルトで有効になっている場合があります。この拡張セッションは、 AWS アクセスポータルやその他の AWS マネージドアプリケーションのセッション期間には影響しません。

IAM Identity Center ID ソースが延長セッション期間に与える影響といった考慮事項については、「the section called “ID ソース、AWS CLI、および AWS SDK に関する考慮事項”」を参照してください。

> **Note**
>
> Kiro は、デフォルトで有効になっている商用 AWS リージョンに設定されているコンソールからアクセスできます。IAM Identity Center インスタンスが Kiro に現在アクセスできない

リージョンにある場合、90 日間の延長セッション期間を有効化しても、デフォルト設定は上書きされません。つまり、90 日間の延長セッション期間を有効にするかどうかに関係なく、セッション期間は変更されません。詳細については、「Kiro 向けサポート対象 AWS リージョン」を参照してください。

Kiro のセッションを延長するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [設定] ページで、[認証] タブを選択します。
4. [認証] の [セッション期間] の横にある [設定] を選択します。[セッション期間の設定] のダイアログボックスが表示されます。
5. [セッション期間の設定] ダイアログボックスで、[Kiro の延長セッションを有効にする] チェックボックスを選択します。Kiro の延長セッションを無効にするには、このチェックボックスをオフにします。
6. [保存] を選択して、[設定] ページに戻ります。

ワークフォースユーザーのアクティブなセッションを表示および終了する

IAM アイデンティティセンター管理者は、ワークフォースユーザーのアクティブなセッションのリストを表示し、必要に応じてユーザーの 1 つ以上のセッションを終了できます。例えば、次の場合にユーザーのセッションを終了する必要がある場合があります。

- ユーザーがセッションを必要としなくなった。
- ユーザーが現在の認証状態を維持しない。これは、退職時やアクセス許可の変更時に発生する可能性があります。

IAM アイデンティティセンターコンソールを使用して、これらのセッションを表示および終了できます。ユーザーは、 AWS アクセスポータルを使用して独自のセッションを表示および終了することもできます。ワークフォースユーザーが管理者の支援なしでセッションを表示および終了する方法の詳細については、「アクティブなセッションの表示と終了」を参照してください。

> **Note**
>
> IAM アイデンティティセンターユーザーのアクティブなセッションを終了しても、AWS マネジメントコンソール または AWS CLI のアクティブな IAM ロールセッションは終了しません。詳細については、「IAM アイデンティティセンターの認証セッションについて」を参照してください。

ワークフォースユーザーのアクティブなセッションを終了するには (IAM アイデンティティセンターコンソール)

1. IAM Identity Center コンソール を開きます。
2. ユーザー を選択します。
3. [ユーザー] ページで、セッションを管理したいユーザーのユーザー名を選択します。これにより、ユーザーの情報が表示されるページに移動します。
4. ユーザーのページで、[アクティブセッション] タブを選択します。[アクティブセッション] の横の括弧内の数字は、このユーザーのアクティブセッション数を示します。
5. ユーザーバックグラウンドセッションの検索 (オプション)

   セッションを使用しているジョブの Amazon リソースネーム (ARN) でセッションを検索するには、[セッションタイプ] リストで [ユーザーバックグラウンドセッション] を選択し、検索ボックスにジョブ ARN を入力します。

   > **Note**
   >
   > ロードされたアクティブなセッションのみを終了できます。ユーザーが多数のセッションを持っている場合は、[アクティブなセッションをロード] を選択して追加のセッションを表示します。

6. 終了する各セッションの横にあるチェックボックスをオンにし、[セッションの終了] を選択します。
7. このユーザーのアクティブセッションを終了することを確認するダイアログボックスが表示されます。情報を確認し、続行する場合は、「`confirm`」と入力し、[セッションの終了] を選択します。
8. ユーザーのページに戻ります。選択したセッションが正常に終了したことを示す緑色の通知メッセージが表示されます。

ID ソース、AWS CLI、および AWS SDK を使用する際のセッション期間に関する考慮事項

以下は、Microsoft Active Directory (AD) または外部 ID プロバイダー (IdP) を ID ソースとして使用する場合、あるいは AWS Command Line Interface、AWS Software Development Kit (SDK)、またはその他の AWS 開発ツールを使用してプログラムで AWS サービスにアクセスする場合のセッション期間の設定に関する考慮事項です。

Kiro 用の Microsoft Active Directory、ユーザーインタラクティブセッション、および延長セッション

Microsoft Active Directory (AD) を ID ソースとして使用し、Kiro のユーザーインタラクティブセッションまたは延長セッションのセッション期間を設定する場合は、次の考慮事項に注意してください。

> **Note**
>
> これらの考慮事項は、ユーザーのバックグラウンドセッションには適用されません。

AWS Managed Microsoft AD を使用する場合でも AWS Directory Service で設定された AD Connector を使用する場合でも、Microsoft AD に定義されたユーザー Kerberos チケットの最大有効期間は、Kiro のユーザーインタラクティブセッションと延長セッションの有効期間に影響する可能性があります。この設定の詳細については、Microsoft ウェブサイトの「ユーザーチケットの最大有効期間」を参照してください。

- AWS Managed Microsoft AD: AWS Directory Service に設定された AWS Managed Microsoft AD を使用する場合、ユーザー Kerberos チケットの最大有効期間は 10 時間に固定されます。したがって、ユーザーインタラクティブセッション期間は、IAM Identity Center の設定と 10 時間のうち短い方に設定されます。例えば、ユーザーインタラクティブセッション期間を 12 時間に設定した場合、ユーザーは 10 時間後に AWS アクセスポータルで再認証する必要があります。Kiro の延長セッションにも、この同じ 10 時間の制限が適用されます。
- AD Connector: AWS Directory Service に設定された AD Connector を使用した場合、ユーザー Kerberos チケットの最大有効期間は、AD Connector の背後にある Microsoft AD に定義されています。デフォルト値は 10 時間で、ユーザーインタラクティブセッションと延長セッションに対して AWS Managed Microsoft AD と同じ効果があります。この制限は Microsoft AD で設定できる場合がありますが、IT 管理者と協力してリスクを検討することをお勧めします。この設定により、

他の Microsoft AD クライアントアプリケーションのセッション期間に影響を与える可能性があるためです。

Kiro の外部 ID プロバイダー、ユーザーインタラクティブセッション、および延長セッション

外部 ID プロバイダー (IdP) を使用していて、Kiro のユーザーインタラクティブセッションまたは延長セッションのセッション期間を設定する場合は、次の考慮事項に留意してください。

> **Note**
>
> これらの考慮事項は、ユーザーのバックグラウンドセッションには適用されません。

IAM アイデンティティセンターは SAML アサーションの `SessionNotOnOrAfter` 属性を使用して、セッションを有効に維持できる期間を決定します。

- SAML アサーションで `SessionNotOnOrAfter` が渡されない場合、AWS アクセスポータル (ユーザーインタラクティブ) セッションおよび延長セッションの期間は、外部 IdP セッション期間に影響されません。例えば、IdP セッション時間が 24 時間で、IAM Identity Center で 18 時間のセッション時間を設定した場合、ユーザーは 18 時間後に AWS アクセスポータルで再認証する必要があります。同様に、Kiro に 90 日間の延長セッションを設定した場合、Kiro ユーザーは 90 日後に再認証する必要があります。
- SAML アサーションで `SessionNotOnOrAfter` が渡された場合、セッション期間の値は、AWS アクセスポータル (ユーザーインタラクティブ) セッションまたは延長セッション期間と SAML IdP セッション期間のうちの短い方に設定されます。IAM アイデンティティセンターで 72 時間のセッション期間を設定し、IdP のセッション期間が 18 時間の場合、ユーザーは IdP で定義されている 18 時間の間、AWS リソースにアクセスできます。同様に、Kiro に 90 日間の延長セッションを設定した場合、Kiro ユーザーは 18 時間後に Kiro で再認証する必要があります。
- IdP のセッション期間が IAM アイデンティティセンターで設定されたセッション期間よりも長い場合、ユーザーは IdP との有効なログインセッションに基づいて、認証情報を再入力することなく、新しい IAM アイデンティティセンターセッションを開始できます。

AWS CLI と SDK セッション

AWS CLI、AWS SDK、またはその他の AWS 開発ツールを使用してプログラムで AWS サービスにアクセスする場合、AWS アクセスポータルと AWS マネージドアプリケーションのセッション期間の設定を適用するには、次の前提条件を満たす必要があります。

- IAM Identity Center コンソールで AWS アクセスポータルセッションの期間を設定する必要があります。
- 共有 AWS 設定ファイルでシングルサインオン設定用のプロファイルを定義する必要があります。このプロファイルは、AWS アクセスポータルへの接続に使用されます。SSO トークンプロバイダーの設定を使用することをお勧めします。この設定を使用して、AWS SDK、またはツールは、更新された認証トークンを自動的に取得できます。詳細については、「AWS SDK とツールリファレンスガイド」の「SSO トークンプロバイダーの設定」を参照してください。
- ユーザーは、セッション管理をサポートするバージョンの AWS CLI または SDK を実行する必要があります。

AWS CLI セッション管理をサポートする最小バージョン

AWS CLI セッション管理をサポートする最小バージョンは次のとおりです。

- AWS CLI V2 2.9 以降
- AWS CLI V1 1.27.10 以降

> **Note**
>
> アカウントアクセスのユースケースでは、ユーザーが AWS CLI を実行している場合、IAM アイデンティティセンターセッションの有効期限が切れる直前に権限セットを更新し、セッション期間を 20 時間に設定し、アクセス権限セットの期間を 12 時間に設定すると、AWS CLI セッションは最大 20 時間に 12 時間を加えた合計 32 時間が実行されます。IAM Identity Center CLI の使用の詳細については、AWS CLIコマンドリファレンス を参照してください。

IAM アイデンティティセンターのセッション管理をサポートする SDK の最小バージョン

IAM アイデンティティセンターのセッション管理をサポートする SDK の最小バージョンは次のとおりです。

SDK	最小バージョン
Python	1.26.10
PHP	3.245.0
Ruby	aws-sdk-core 3.167.0
Java V2	AWS SDK for Java v2 (2.18.13)
Go V2	SDK 全体: リリース-2022-11-11 および特定の Go モジュール: 認証情報/v1.13.0、構成/v1.18.0
JS V2	2.1253.0
JS V3	v3.210.0
C++	1.9.372
.NET	v3.7.400.0

IAM アイデンティティセンターで AWS アカウントとアプリケーションへのユーザーアクセスを無効にする

IAM Identity Center ディレクトリでユーザーアクセスを無効にすると、ユーザーの詳細の編集、パスワードのリセット、グループへのユーザーの追加、グループ メンバーシップの表示ができなくなります。ユーザーアクセスを無効にすると、ユーザーは AWS アクセスポータルにサインインできなくなり、割り当てられた AWS アカウントとアプリケーションにアクセスできなくなります。後でアクセスを復元する必要がある場合は、一時的なアクセスを削除するために [ユーザーアクセスを無効にする] を使用します。

以下の手順に従って、IAM Identity Center コンソールを使用して Identity Center ディレクトリのユーザーアクセスを無効にします。

> **Note**
>
> ユーザーアクセスを無効にするか、IAM Identity Center でユーザーを削除すると、そのユーザーはすぐに AWS アクセスポータルにサインインできなくなり、新しいサインイン セッションを作成できなくなります。詳細については、「IAM アイデンティティセンターの認証セッションについて」を参照してください。

IAM Identity Center でユーザーアクセスを無効にするには

1. IAM アイデンティティセンターコンソールを開きます。

   > **Important**
   >
   > このページの説明は、AWS IAM アイデンティティセンター に適用されます。これらは AWS Identity and Access Management (IAM) には適用されません。IAM Identity Center ユーザー、グループ、およびユーザー認証情報は、IAM ユーザー、グループ、IAM ユーザー認証情報とは異なります。IAM でユーザーを非アクティブ化する手順をお探しの場合は、AWS Identity and Access Management ユーザーガイドの「IAM ユーザーの管理」を参照してください。

2. [ユーザー] を選択します。
3. アクセスを無効にするユーザーのユーザー名を選択します。
4. アクセスを無効にするユーザーのユーザー名の下にある [一般的な情報] セクションで、[ユーザーアクセスを無効化] を選択します。
5. [ユーザーアクセスの無効化] のダイアログボックスで、[ユーザーアクセスの無効化] を選択します。

サービスコントロールポリシーでのユーザーアクセスの拒否

IAM アイデンティティセンターユーザーのアクセスが無効になっているか、ユーザーが削除された場合に、承認された API コールを行うアクセスをすぐに拒否するには、次の操作を行います。

1. 追加または更新します。ユーザーに割り当てられたアクセス許可セット (複数可) (またはアカウントアクセスマネージャーを使用する場合は IAM ロールポリシー) のインラインポリシーに、すべてのリソースに対するすべてのアクションに明示的な Deny 効果を追加します。
2. `aws:userid` または `identitystore:userid` 条件キーを指定します。

または、サービスコントロールポリシーを使用して、組織内のすべてのメンバーアカウントに対するユーザーのアクセスを拒否することもできます。

Exampleアクセスを拒否する SCP の例

この拒否ポリシーは、他のアクセス許可が付与されているかどうかにかかわらず、特定のユーザーのすべての AWS アクションをブロックします。このポリシーは、すべての `Allow` ポリシーを上書きします。

JSON

```
{
    "Version":"2012-10-17",
    "Statement" : [
        {
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                 "StringLike": {
                    "aws:UserId": "*:deleteduser@domain.com"
                }
            }
        }
    ]
}
```

JSON

```
{
    "Version":"2012-10-17",
    "Statement" : [
        {
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                 "StringEquals": {
                    "identitystore:UserId": "DELETEDUSER_ID"
                }
```

```
            }
        }
    ]
}
```

IAM アイデンティティセンターユーザーのアクセス権を管理する

IAM アイデンティティセンターディレクトリでユーザーのパスワードと多要素認証 (MFA) を管理する方法について説明します。これらのセキュリティ機能は、ユーザーアカウントの保護に役立ちます。

> **Note**
>
> これらの機能は、Active Directory ユーザーまたは外部 ID プロバイダーユーザーには適用されません。

管理者は、IAM アイデンティティセンターコンソールを使用してパスワードと MFA の両方を管理できます。これらのセキュリティ機能は、組み込みのアイデンティティセンターディレクトリでのみ機能します。

パスワード管理

パスワード管理には、次の機能が含まれます。

- E メールの指示によるパスワードのリセット
- ワンタイムパスワードを生成する
- API が作成したユーザーの自動 E メール検証を設定する

AWS は、複雑なルールやパスワードの再利用制限など、固定されたセキュリティ要件を適用します。

MFA

MFA はデフォルトで有効になっており、ユーザーごとに最大 8 つのデバイスをサポートしています。

対応するタイプは以下を含みます。

- 認証システムアプリケーション
- セキュリティキー
- 組み込みの生体認証機能

管理者は、ユーザーの MFA デバイスを登録および管理できます。

トピック

- ユーザーパスワードの設定
- アイデンティティセンターディレクトリユーザーの MFA

ユーザーパスワードの設定

アイデンティティセンターディレクトリで作成されたユーザーの場合、管理者はパスワードポリシーを管理し、初期パスワードなしでユーザーを処理し、必要に応じてパスワードをリセットできます。これらのパスワード管理機能は、組み込みのアイデンティティセンターディレクトリのユーザーにのみ適用されます。Active Directory または外部 ID プロバイダーを使用している場合は、それらのシステムでパスワードを管理する必要があります。

パスワード管理オプション

- パスワード要件 – パスワードを設定または変更するときにユーザーが満たす必要があるセキュリティ要件。これには、複雑さのルールと再利用の制限が含まれます。
- ワンタイムパスワード設定 – API または CLI を使用して作成された初期パスワードを持たないユーザーの E メール検証を設定します。即時アクセスのために一時的なパスワードを生成することもできます。
- パスワードのリセット – ロックアウトされている、または新しい認証情報を必要とするユーザーのパスワードをリセットします。E メールを使用してリセット手順を送信したり、ワンタイムパスワードを生成したりできます。

トピック

- IAM Identity Center で ID を管理する際のパスワード要件
- API または CLI で作成されたユーザーにワンタイムパスワードを E メールで送信する
- エンドユーザーの IAM Identity Center ユーザーパスワードをリセットします。

IAM Identity Center で ID を管理する際のパスワード要件

> **Note**
>
> これらの要件は、Identity Center ディレクトリで作成されたユーザーにのみ適用されます。認証用に IAM アイデンティティセンター以外の ID ソース (Active Directory や 外部の ID プロバイダーなど) を設定している場合、ユーザーのパスワードポリシーは IAM アイデンティティセンターではなく、それらのシステムで定義および適用されます。ID ソースが AWS Managed Microsoft AD の場合、詳細については、「AWS Managed Microsoft AD のパスワードポリシーの管理」を参照してください。

IAM Identity Center を ID ソースとして使用する場合、ユーザーは以下のパスワード要件を守ってパスワードを設定・変更する必要があります。

- パスワードでは、大文字と小文字が区別されます。
- パスワードの長さは8文字から64文字の間でなければなりません。
- パスワードには、次の 4 つカテゴリから少なくとも 1 文字を含める必要があります。
  - 小文字 a〜z
  - 大文字 A〜Z
  - 数字 (0〜9)
  - 英数字以外の文字 (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- 最後の3つのパスワードは再使用できません。
- 第三者から漏洩したデータセットを通じて公に知られているパスワードは使用できません。

API または CLI で作成されたユーザーにワンタイムパスワードを E メールで送信する

CreateUser API オペレーションまたは `create-user` CLI コマンドでユーザーを作成する場合、そのユーザーにはパスワードがありません。作成時にユーザーに E メールを指定した場合、IAM アイデンティティセンターの設定を更新して、最初のサインイン試行後に検証 E メールを送信できます。確認メールを受信したユーザーは、サインインするためのパスワードを設定する必要があります。

この設定を有効にしない場合は、ワンタイムパスワードを生成し、CreateUser API または `create-user` CLI コマンドを使用して作成したユーザーと共有する必要があります。

CreateUser API または **create-user** CLI コマンドを使用して作成されたユーザーに E メールアドレス確認メールを送信するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [設定] ページで、[認証] タブを選択します。
4. [標準認証] セクションで、[設定] を選択します。
5. [標準認証の設定]ダイアログボックスで、[E メール送信 OTP] チェックボックスをオンにします。次に、[保存] を選択します。ステータスが [無効] から [有効] に更新されます。

エンドユーザーの IAM Identity Center ユーザーパスワードをリセットします。

この手順は IAM アイデンティティセンターディレクトリでユーザーのパスワードをリセットする必要がある管理者を対象としています。IAM Identity Center コンソールを使用してパスワードをリセットします。

ID プロバイダーとユーザータイプに関する考慮事項

- MicrosoftActive Directory または外部プロバイダー — IAM ID Center を Microsoft Active Directory または外部プロバイダーに接続する場合、ユーザーパスワードのリセットは Active Directory 内または外部プロバイダー内から行う必要があります。つまり、これらのユーザーのパスワードを IAM アイデンティティセンターコンソールからリセットすることはできません。
- IAM ID センターディレクトリ内のユーザー — IAM アイデンティティセンターのユーザーであれば、自分の IAM アイデンティティセンターのパスワードをリセットできます。「AWS アクセスポータルのユーザーパスワードをリセットする」を参照してください。

IAM Identity Center のエンドユーザーのパスワードをリセットするには

> **Important**
>
> このページの説明は、AWS IAM アイデンティティセンター に適用されます。これらは AWS Identity and Access Management (IAM) には適用されません。IAM アイデンティティセンターユーザー、グループ、およびユーザー認証情報は、IAM ユーザー、グループ、IAM ユーザー認証情報とは異なります。IAM ユーザーのパスワードを変更する手順をお探しの場合は、「AWS Identity and Access Management ユーザーガイド」の「IAM ユーザーのパスワードの管理」を参照してください。

1. IAM アイデンティティセンターコンソールを開きます。
2. [ユーザー] を選択します。
3. パスワードをリセットするユーザーのユーザー名を選択します。
4. ユーザーの詳細ページで、[パスワードのリセット] を選択します。
5. [Reset password] (パスワードのリセット) ダイアログボックスで、次の選択肢のいずれかを選び、[Reset password] (パスワードのリセット) を選択します。

   a. Send an email to the user with instructions to reset the password (パスワードのリセット手順が記載された E メールをユーザーに送信する) – このオプションでは、Amazon ウェブサービスから、パスワードをリセットする方法について説明する E メールアドレスを自動的にユーザーに送信します。

   > **Warning**
   >
   > セキュリティ上のベストプラクティスとして、このオプションを選択する前に、このユーザーの E メールアドレスが正しいかどうかを確認してください。このパスワードリセットメールが、誤った、または誤って設定された E メールアドレスに送信された場合、悪意のある受信者がこの E メールを使用して、顧客の AWS 環境への不正アクセスを行う可能性があります。

   b. ワンタイムパスワードを生成し、ユーザーと共有します – このオプションでは、E メールアドレスから手動でユーザーに送信できる、パスワードの詳細が利用できます。

アイデンティティセンターディレクトリユーザーの MFA

> **Important**
>
> IAM Identity Center の MFA は、現在、外部 ID プロバイダー による使用はサポートされていません。

IAM アイデンティティセンターは、デフォルトで多要素認証 (MFA) がオンになっているように事前に設定されています。そのため、すべてのユーザーは、ユーザー名とパスワードに加えて MFA でサインインする必要があります。これにより、ユーザーは次の 2 つの要素を使用して AWS アクセスポータルにサインインする必要があります。

- ユーザー名とパスワード。これは最初の要素であり、ユーザーが知っていることです。

- コード、セキュリティキー、または生体認証のいずれか。これはもう 1 つの要素で、ユーザーが所有している (所有) または存在している (生体認証) ものです。第 2 の要素は、モバイルデバイスから生成された認証コード、コンピューターに接続されたセキュリティキー、またはユーザーの生体認証のスキャンのいずれかです。

これらの複数の要素を組み合わせることで、有効な MFA 課題が完了しない限り、AWS リソースへの不正アクセスを防ぐことができ、セキュリティが向上します。

各ユーザーは、モバイルデバイスまたはタブレットにインストールされるワンタイムパスワード認証アプリケーションである仮想認証アプリを最大 2 つと、組み込みの認証システムとセキュリティキーを含む 6 つの FIDO 認証システムを合計 8 台の MFA デバイスに登録できます。IAM Identity Center で使用可能な MFA タイプ の詳細を確認してください。

トピック

- IAM Identity Center で使用可能な MFA タイプ
- IAM アイデンティティセンターでの MFA の設定
- ユーザー用の MFA デバイスを登録する
- IAM アイデンティティセンターでの MFA デバイスの名前変更と削除

IAM Identity Center で使用可能な MFA タイプ

多要素認証 (MFA) は、ユーザーのセキュリティを強化するためのシンプルで効果的なメカニズムです。ユーザーの最初の要素であるパスワードは、ユーザーが記憶する秘密であり、ナレッジファクターとも呼ばれます。その他の要素としては、所有要素 (セキュリティキーなど、所有しているもの) や継承要素(生体認証のスキャンなど、ユーザーが持っているもの) があります。MFA を設定して、アカウントのセキュリティをさらに強化することを強くお勧めします。

IAM Identity Center MFA は、以下のデバイスタイプをサポートします。すべての MFA タイプは、ブラウザベースのコンソールを通じたアクセスと、AWS CLI IAM Identity Center による v2 の使用の両方でサポートされています。

- FIDO2 認証機能 は、組み込みの認証機能とセキュリティキーを含みます。
- 仮想認証アプリ
- RADIUS MFA 独自の実装は AWS Managed Microsoft AD を介して接続されます。

ユーザーは、最大 2 つの仮想認証アプリと 6 つの FIDO 認証機能を含む最大 8 台の MFA デバイスを 1 つの AWS アカウント に登録できます。新しいデバイスまたはブラウザからサインインしようとするとき、または不明な IP アドレスからサインインするときに MFA を要求するように MFA を設定することもできます。ユーザーの MFA を設定する方法の詳細については、「ユーザー認証に MFA タイプを選択する 」と「MFA デバイス強制の設定」を参照してください。

FIDO2 認証機能

FIDO2 は CTAP2 と WebAuthn を含む標準であり、パブリックキー暗号に基づいています。FIDO 認証情報は、認証情報が作成された Web サイト (AWS など) 固有のものであるため、フィッシング詐欺に対して強固です。

AWS は、FIDO 認証システムの最も一般的なフォームの要素は、組み込みの認証アプリシステムとセキュリティキーの 2 つです。FIDO 認証機能の最も一般的なタイプの詳細については、以下を参照してください。

トピック

- 組み込みの認証機能
- セキュリティキー
- パスワードマネージャー、パスキープロバイダー、その他の FIDO 認証機能

組み込みの認証機能

MacBook の TouchID や、Windows Hello 対応のカメラなどの多数のコンピューターや携帯電話は組み込みの認証アプリシステムを装備しています。デバイスに FIDO 互換の組み込みの認証アプリがある場合は、指紋、顔、またはデバイスの PIN を 2 つ目の要素として使用できます。

セキュリティキー

セキュリティキーは FIDO 互換の外部ハードウェア認証機能です。ご購入の上 USB、BLE、または NFC 経由でデバイスに接続できます。MFA を要求されたら、キーのセンサーでジェスチャーを完了するだけです。セキュリティキーの例としては YubiKeys や Feitian キーがあり、最も一般的なセキュリティキーはデバイス向けの FIDO 認証情報を作成します。互換性のあるFIDO 認定のセキュリティキーの全リストについては、「FIDO 認定製品」 をご覧ください。

パスワードマネージャー、パスキープロバイダー、その他の FIDO 認証機能

複数のサードパーティプロバイダーが、パスワードマネージャー、FIDO モードのスマートカード、その他のフォームの要素の機能として、モバイルアプリケーションの FIDO 認証をサポートしていま

す。これらの FIDO 互換デバイスは IAM Identity Center で動作しますが、このオプションを MFA で有効にする前に FIDO 認証機能をご自身でテストすることをお勧めします。

> **Note**
>
> FIDO 認証機能の中には、パスキーと呼ばれる検出可能な FIDO 認証情報を作成できるものもあります。パスキーは、パスキーを作成したデバイスにバインドされている場合もあれば、同期可能でクラウドにバックアップされている場合もあります。例えば、サポートされている Macbook で Apple Touch ID を使ってパスキーを登録し、ログイン時に画面に表示される指示に従って iCloud のパスキーで Google Chrome を使って Windows ラップトップからサイトにログインできます。どのデバイスが同期可能なパスキーをサポートしているか、および運用システムとブラウザ間の現在のパスキーの相互運用性をサポートしているかについての詳細は、FIDO Alliance And World Wide Web Consortium (W3C) が管理するリソースである passkeys.dev の デバイスサポート を参照してください。

仮想認証アプリ

認証アプリは、基本的にワンタイムパスワード (OTP) ベースのサードパーティー認証機能を備えています。モバイルデバイスやタブレットにインストールされた認証アプリケーションを、許可された MFA デバイスとして使用することができます。サードパーティー認証アプリケーションは、6 桁の認証コードを生成できる標準ベースのタイムベースドワンタイムパスワード (TOTP) アルゴリズムである RFC 6238 に準拠している必要があります。

MFA を求めるプロンプトが表示されたら、ユーザーは認証アプリから有効なコードを入力ボックスに入力する必要があります。ユーザーに割り当てられた各 MFA デバイスは一意であることが必要です。1 人の ユーザーに対して 2 つの認証アプリを登録することができます。

テスト済みの認証アプリ

TOTP 準拠のアプリケーションはどれも IAM Identity Center MFA と連携して動作します。以下の有名なサードパーティの認証アプリから選択できます。

オペレーティングシステム	テスト済みの認証アプリ
Android	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator

オペレーティングシステム	テスト済みの認証アプリ
iOS	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator

RADIUS MFA

リモート認証ダイヤルインユーザーサービス (RADIUS) は、ユーザーをネットワークサービスに接続するための認証、認可、アカウント管理を提供する業界標準のクライアント/サーバープロトコルです。Directory Service には、MFA ソリューションを実装した RADIUS サーバーに接続する RADIUS クライアントが含まれています。詳細については、「AWS Managed Microsoft AD の多要素認証を有効にする」を参照してください。

ユーザーポータルへのサインインには、IAM Identity Center で RADIUS MFA または MFA のいずれかを使用できますが、両方を使用することはできません。IAM Identity Center での MFA は、ポータルへのアクセスに AWS ネイティブの二要素認証が必要な場合に、RADIUS MFA の代わりに使用されます。

IAM Identity Center で MFA を有効にすると、ユーザーは AWS アクセスポータルにサインインするために MFA デバイスが必要になります。これまで RADIUS MFA を使用していた場合、IAM Identity Center で MFA を有効にすると、AWS アクセスポータルにサインインしたユーザーの RADIUS MFA が効果的に上書きされます。ただし、RADIUS MFA は、Amazon RDS for SQL Server など、Directory Service と連携する他のすべてのアプリケーションにサインインする際に、ユーザーに課題を与え続けます。

IAM Identity Center コンソールで MFA が 無効 になっていて、Directory Service で RADIUS MFA を設定している場合、RADIUS MFA が AWS アクセスポータルのサインインを管理します。これは、MFA が無効になっている場合、IAM Identity Center は RADIUS MFA 設定にフォールバックすることを意味します。

IAM アイデンティティセンターでの MFA の設定

ID ソースが IAM アイデンティティセンターの ID ストア、AWS Managed Microsoft AD または AD Connector で設定されている場合、IAM アイデンティティセンターの多要素認証 (MFA) 機能を設定できます。IAM Identity Center の MFA は、現在、外部 ID プロバイダー による使用はサポートされていません。

以下は、IAM アイデンティティセンターの設定と組織の設定に応じた一般的な MFA の推奨事項です。

- ユーザーには、有効なすべての MFA タイプについて、複数のバックアップ認証の登録を推奨します。これにより、MFA デバイスが壊れたり、置き忘れたりした場合に、ユーザーがアクセスできなくなることを防げます。
- ユーザーが E メールにアクセスするために AWS アクセスポータルにサインインする必要がある場合は、[E メールで送信されたワンタイムパスワードの提供を要求する]のオプションを選択しないでください。例えば、ユーザーは AWS アクセスポータルを Microsoft 365 使用して E メールを読む可能性があります。この場合、ユーザーは認証コードを取得することができず、AWS アクセスポータルにサインインすることができなくなります。詳細については、「MFA デバイス強制の設定」を参照してください。
- Directory Service で設定した RADIUS MFA を既に使用している場合は、IAM アイデンティティセンター内で MFA を有効化する必要はありません。IAM Identity Center の MFA は、IAM Identity Center Microsoft Active Directory ユーザーにとって、RADIUS MFA の代替となるものです。詳細については、「RADIUS MFA」を参照してください。
- 次の YouTube 動画では、MFA と IAM アイデンティティセンターの概要を説明します。

IAM アイデンティティセンター: 新しいインスタンスの多要素認証のデフォルト

トピック

- ユーザーに MFA を求める
- ユーザー認証に MFA タイプを選択する
- MFA デバイス強制の設定
- ユーザーが自分の MFA デバイスを登録できるようにする

ユーザーに MFA を求める

次のステップを使用して、ワークフォースユーザーが AWS アクセスポータルにサインインしようとするたびに多要素認証 (MFA) を求められる頻度を決定できます。開始する前に、IAM Identity Center で使用可能な MFA タイプ を理解することをお勧めします。

> **Important**
>
> このセクションの手順は AWS IAM アイデンティティセンター に適用されます。これらは AWS Identity and Access Management (IAM) には適用されません。IAM Identity Center ユーザー、グループ、およびユーザー認証情報は、IAM ユーザー、グループ、IAM ユーザー認証情報とは異なります。IAM ユーザーの MFA を無効化する手順をお探しの場合は、「AWS

Identity and Access Management ユーザーガイド」の「MFA デバイスの無効化」を参照してください。

> **Note**
>
> 外部の IdP を使用している場合は、[多要素認証] の項目は表示されません。MFA 設定を IAM Identity Center が管理するのではなく、外部の IdP が管理します。

MFA を設定するには

1. IAM Identity Center コンソールを開きます。
2. 左のナビゲーションペインの [設定] を選択します。
3. [設定] ページで、[認証] タブを選択します。
4. [多要素認証] セクションで、[設定] を選択します。
5. [多要素認証を設定] ページの [MFA のプロンプトをユーザーに表示] で、ビジネスに必要なセキュリティのレベルに基づいて、次の認証モードのいずれかを選択します。

   - サインインごと (常時オン)

     このモード (デフォルト設定) では、 IAM アイデンティティセンター は、登録された MFA デバイスを持つユーザーがサインインごとにプロンプトを表示することを要求します。これは最も安全な設定であり、AWS アクセスポータルにサインインするたびに MFA を使用することを要求することで、組織またはコンプライアンスポリシーが適用されます。例えば、PCI DSS は、高リスクの支払取引をサポートするアプリケーションにアクセスする際のすべてのサインイン時に MFA を使用することを強く推奨しています。
   - サインインコンテキストが変更された場合のみ (context-aware)

     このモードでは、IAM アイデンティティセンターはサインイン中にデバイスを信頼するオプションをユーザーに提供します。ユーザーがデバイスを信頼することを表明すると、IAM Identity Center はユーザーに MFA の入力を一度要求し、ユーザーが次にサインインする際のサインインコンテキスト (デバイス、ブラウザ、場所など) を分析します。後続のサインインでは、IAM Identity Center は、ユーザーが以前に信頼されたコンテキストでサインインしているかどうかを判断します。ユーザーのサインインコンテキストが変更されると、IAM Identity Center はユーザーに E メールアドレスとパスワードの認証情報に加えて MFA の入力を求めます。

このモードは、職場から頻繁にサインインするが、常時オンのオプションよりも安全性が低いユーザーに使いやすさを提供します。ユーザーは、サインインコンテキストが変更された場合にのみ MFA を要求されます。

- なし (無効)

  このモードでは、すべてのユーザーが標準のユーザー名とパスワードのみでサインインします。このオプションを選択すると、IAM アイデンティティセンター MFA を無効するため、お勧めではありません。

  ユーザーのアイデンティティセンターディレクトリでは MFA が無効になっていますが、ユーザー詳細で MFA デバイスを管理することはできません。また、アイデンティティセンターディレクトリのユーザーは AWS アクセスポータルから MFA デバイスを管理できません。

  > **Note**
  >
  > 既に Directory Service で RADIUS MFA を使用しており、今後もデフォルトの MFA タイプとして使用したい場合は、認証モードを無効のままにしておくと、IAM Identity Center の MFA 機能をバイパスできます。Disabled (無効) モードから Context-aware または Always-on モードに変更すると、既存の RADIUS MFA 設定が上書きされます。詳細については、「RADIUS MFA」を参照してください。

6. [変更の保存] を選択します。

関連トピック

- ユーザー認証に MFA タイプを選択する
- MFA デバイス強制の設定
- ユーザーが自分の MFA デバイスを登録できるようにする

ユーザー認証に MFA タイプを選択する

以下の手順で、AWS アクセスポータルで多要素認証 (MFA) を要求されたときに、ユーザーが認証できるデバイスタイプを選択します。

ユーザーの MFA タイプを設定するには

1. IAM Identity Center コンソール を開きます。
2. 左のナビゲーションペインの [設定] を選択します。

3. [設定] ページで、[認証] タブを選択します。
4. [多要素認証] セクションで、[設定] を選択します。
5. [多要素認証を設定] ページでは、[ユーザーはこれらの MFA タイプで認証できます] で、ビジネスニーズに応じて次のいずれかの MFA タイプを選択します。詳細については、「IAM Identity Center で使用可能な MFA タイプ」を参照してください。
   - セキュリティキーと内蔵認証システム
   - 認証システムアプリケーション
6. [Save changes] (変更の保存) をクリックします。

MFA デバイス強制の設定

以下の手順で、ユーザーが AWS アクセスポータルにサインインする際に、登録済みの MFA デバイスが必要かどうかを判断します。

IAM での MFA の詳細については、「AWS Multi-factor authentication in IAM」を参照してください。

ユーザーの MFA デバイスの強制を設定するには

1. IAM Identity Center コンソール を開きます。
2. 左のナビゲーションペインの [設定] を選択します。
3. [設定] ページで、[認証] タブを選択します。
4. [多要素認証] セクションで、[設定] を選択します。
5. [多要素認証の設定] ページでは、[ユーザーがまだ登録された MFA デバイスを持っていない場合] で、ビジネスニーズに応じて次のいずれかの選択肢を選択します。
   - サインイン時に MFA デバイスの登録を必須とする

     これは、IAM Identity Center の MFA を初めて設定するときのデフォルト設定です。このオプションは、まだ登録済みの MFA デバイスを持っていないユーザーに対して、パスワード認証に成功した後のサインイン時にデバイスの自己登録を要求する場合に使用します。これにより、ユーザーに認証デバイスを個別に登録したり、配信する必要がなく、組織内の AWS 環境を MFA で保護することができます。自己登録の際、ユーザーは事前に登録した IAM Identity Center で使用可能な MFA タイプ の中から任意のデバイスを登録することができます。登録完了後、ユーザーは新しく登録した MFA デバイスに親しみのある名前を付けることができ、その後、IAM Identity Center はユーザーを元の場所にリダイレクトします。ユーザーのデバイスが紛失または盗難にあった場合、そのデバイスをユーザーのアカウントから削除するだけ

で、IAM Identity Center は次回のサインイン時に新しいデバイスを自己登録することが必須となります。

- E メールで送られてくるワンタイムパスワードを入力してサインインすることを必須とする

  確認コードをユーザーに E メールで送信したい場合は、このオプションを使用します。E メールは特定のデバイスに限定されないため、このオプションは業界標準の多要素認証の基準を満たしません。ですが、パスワードだけを使用するよりもセキュリティが向上します。E メール認証は、ユーザーが MFA デバイスを登録していない場合にのみ求められます。Context-aware (コンテキスト認識) の認証方法が有効になっている場合、ユーザーは E メールを受信したデバイスを信頼済みとしてマークすることができます。その後、そのデバイス、ブラウザ、IP アドレスの組み合わせでログインする際に、E メールコードを確認する必要がなくなります。

  > **Note**
  >
  > IAM Identity Center 対応の ID ソースとして Active Directory を使用している場合、E メールアドレスは常に Active Directory `email` 属性に基づいて設定されます。カスタムのアクティブディレクトリ属性のマッピングは、この動作を上書きしません。

- Block their sign-in] (サインインをブロックする

  すべてのユーザーが AWS にサインインする前に MFA の使用を強制したい場合は、[Block Their Sign-In] (サインインをブロックする) オプションを使用します。

  > **Important**
  >
  > 認証方法に Context-aware (コンテキストアウェア) に設定されている場合、ユーザーはサインインページで [This is a trusted device] (信頼できるデバイス) チェックボックスを選択します。この場合、[Block their sign in] (サインインをブロックする) 設定を有効でも、そのユーザーには MFA の入力が求められません。これらのユーザーにプロンプトを表示させたい場合は、認証方法を Always On (常時オン) に変更してください。

- Allow them to sign in (サインインを許可する

  このオプションは、ユーザーが AWS アクセスポータルにサインインする際に、MFA デバイスを必要としないことを示します。MFA デバイスの登録を選択したユーザーは、MFA の入力を求められます。

6. [変更の保存] を選択します。

ユーザーが自分の MFA デバイスを登録できるようにする

IAM アイデンティティセンター管理者は、ユーザーが自分の MFA デバイスを登録することを許可することができます。

ユーザーが自分の MFA デバイスを登録できるようにするには

1. IAM Identity Center コンソール を開きます。
2. 左のナビゲーションペインの [設定] を選択します。
3. [設定] ページで、[認証] タブを選択します。
4. [多要素認証] セクションで、[設定] を選択します。
5. [多要素認証の設定] ページで [MFA デバイスを管理できるユーザー] に [ユーザーは自分の MFA デバイスを追加および管理できる] を選択します。
6. [変更の保存] を選択します。

> **Note**
>
> ユーザーの自己登録を設定した後、手順 MFA 用デバイスの登録 のリンクをユーザーに送信することをお勧めします。このトピックでは、自分の MFA デバイスを設定する方法を説明します。

ユーザー用の MFA デバイスを登録する

IAM アイデンティティセンター管理者は、IAM アイデンティティセンターコンソールで、特定のユーザーがアクセスできるように新しい MFA デバイスを設定できます。管理者は、ユーザーの MFA デバイスを登録するため、そのデバイスに物理的にアクセスする必要があります。例えば、スマートフォンで実行される MFA デバイスを使用するユーザー用に MFA を設定する場合、登録プロセスを完了するには、スマートフォンに物理的にアクセスする必要があります。あるいは、ユーザーが自分の MFA デバイスを構成して管理できるように許可することもできます。詳細については、「ユーザーが自分の MFA デバイスを登録できるようにする」を参照してください。

MFA デバイスを登録するには

1. IAM Identity Center コンソール を開きます。

2. 左のナビゲーションペインで、[ユーザー] を選択します。リスト内でユーザーを選択します。このステップでは、ユーザーの横にあるチェックボックスをオンにしないでください。
3. [MFA デバイス] タブを選択し、[MFA デバイスの登録] を選択します。
4. [MFA デバイスの登録] ページで、次の MFA デバイスタイプを選択し、指示に従います。

   - 認証システムアプリケーション

     1. [認証システムアプリケーションの設定] ページで、IAM Identity Center は QR コードのグラフィックを含む新しい MFA デバイスの設定情報を表示します。図は、QR コードに対応していないデバイスのマニュアル入力に利用できるシークレットキーを示しています。
     2. 物理的に MFA デバイスを使用して、次の操作を行います。

        a. 互換性のある MFA 認証システムアプリケーションを開きます。MFA デバイスで使用できるテスト済みアプリケーションのリストについては、「仮想認証アプリ」を参照してください。MFA アプリケーションが複数のアカウント (複数の MFA デバイス) をサポートしている場合は、新しいアカウント (新しい MFA デバイス) を作成するオプションを選択します。

        b. MFA アプリケーションが QR コードをサポートしているかどうかを判断し、[Set up the authenticator app] (認証アプリケーションの設定) ページで以下のいずれかの操作を行います。

           i. [Show QR code] (QR コードの表示) を選択し、アプリケーションを使用して QR コードをスキャンします。例えば、カメラアイコンまたは スキャンコード に似たオプションを選択します。次に、デバイスのカメラでコードをスキャンします。

           ii. [show secret key] (シークレットキーを表示する) を選択し、そのシークレットキーを MFA アプリケーションに入力します。

> **Important**
>
> MFA デバイスを IAM アイデンティティセンターに設定する際には、QR コードやシークレットキーのコピーを安全な場所に保存することをお勧めします。これにより、割り当てられたユーザーが携帯電話を紛失したり、MFA 認証アプリケーションを再インストールしなければならない場合に役立ちます。いずれの場合も、すぐにアプリケーションを再設定して同じ MFA 設定を使用することができます。これにより、ユーザーのために IAM Identity Center で新しい MFA デバイスを作成する必要がなくなります。

3. [Set up the authenticator app] (認証アプリケーションの設定) ページで、[Authenticator code] (認証コード) で、物理的な MFA デバイスに現在表示されているワンタイムパスワードを入力します。

> **Important**
>
> コードを生成したら、即時にリクエストを送信します。コードを生成した後にリクエストを送信するまで時間がかかりすぎる場合、MFA デバイスはユーザーと正常に関連付けられます。ただし、MFA デバイスは同期しません。これは、タイムベースドワンタイムパスワード (TOTP) の有効期間が短いために起こります。その場合は、デバイスを再同期できます。

4. [Assign MFA] (MFA の割り当て) を選択します。これで、MFA デバイスはワンタイムパスワードの生成を開始し、AWS で使用できるようになります。

- セキュリティキー

1. [Register your user's security key] (ユーザーのセキュリティキーの登録) ページでは、お使いのブラウザやプラットフォームの指示に従ってください。

> **Note**
>
> ここでの操作性は、運用システムやブラウザの違いによって異なりますので、お使いのブラウザやプラットフォームで表示される指示に従ってください。ユーザーのデバイスが正常に登録されると、登録したデバイスに識別しやすい表示名を付けるオプションが表示されます。変更する場合は、[Rename] (名前の変更) を選択し、新しい名前を入力してから [Save] (保存) を選択します。ユーザー自身がデバイスを管理できるオプションが有効の場合、ユーザーには AWS アクセスポータルに登録した親しみのある名前が表示されます。

IAM アイデンティティセンターでの MFA デバイスの名前変更と削除

IAM アイデンティティセンター管理者は、次の手順を使用して、ユーザーの MFA デバイスの名前を変更または削除できます。

MFA デバイスの名前を変更するには

1. IAM Identity Center コンソール を開きます。

2. 左のナビゲーションペインで、[ユーザー] を選択します。リスト内でユーザーを選択します。このステップでは、ユーザーの横にあるチェックボックスをオンにしないでください。
3. ユーザーの詳細ページで、[MFA デバイス] タブを選択し、デバイスを選択して、[名前の変更] を選択します。
4. プロンプトが表示されたら、新しい名前を入力し、[名前の変更] を選択します。

MFA デバイスを削除するには

1. IAM Identity Center コンソール を開きます。
2. 左のナビゲーションペインで、[ユーザー] を選択します。リスト内でユーザーを選択します。
3. ユーザーの詳細ページで、[MFA デバイス] タブを選択し、デバイスを選択して、[削除] を選択します。
4. 確認のため、DELETE と入力し、[Delete] (削除) を選択します。

アプリケーションへのアクセスを設定する

AWS IAM アイデンティティセンター を使用すると、アプリケーションへのシングル サインオン アクセスをどのユーザーに許可するかを制御できます。ユーザーは、ディレクトリの認証情報を使ってサインインすると、これらのアプリケーションにシームレスにアクセスできます。

IAM Identity Center は、IAM Identity Center とアプリケーションのサービスプロバイダーとの間の信頼関係を介して、これらのアプリケーションと安全にやり取りします。この信頼は、アプリケーションの種類に応じてさまざまな方法で作成できます。

IAM アイデンティティセンターは、AWS マネージドアプリケーションとカスタマーマネージドアプリケーションの 2 種類のアプリケーションをサポートします。AWS マネージド アプリケーションは、関連するアプリケーションコンソール内から直接、またはアプリケーション API を通じて設定されます。カスタマーマネージドアプリケーションは、IAM アイデンティティセンターコンソールに追加され、IAM アイデンティティセンターおよびサービスプロバイダーの両方で適切なメタデータを設定する必要があります。

IAM アイデンティティセンターと連携するようにアプリケーションを設定すると、そのアプリケーションにアクセスするユーザーまたはグループを管理できます。デフォルトでは、ユーザーはアプリケーションに割り当てられません。

組織内の特定の AWS アカウント の AWS マネジメントコンソールへのアクセスを従業員に許可することもできます。詳細については、「AWS アカウント へのアクセスを設定する」を参照してください。

トピック

- AWS マネージドアプリケーション
- カスタマーマネージドアプリケーション
- 信頼できる ID の伝播の概要
- 独自の OAuth 2.0 アプリケーションを設定するには
- IAM アイデンティティセンター証明書のローテーション
- IAM アイデンティティセンターコンソールのアプリケーションプロパティを理解する
- IAM Identity Center コンソールでアプリケーションへのユーザーアクセスを割り当てます。
- SAML 2.0 アプリケーションへのユーザーアクセスを削除する
- アプリケーションの属性を IAM Identity Center の属性にマップする

AWS マネージドアプリケーション

AWS IAM アイデンティティセンター は、ワークフォースユーザーを Kiro や Amazon Quick などの AWS マネージドアプリケーションに接続するタスクを合理化および簡素化します。IAM アイデンティティセンターを使用することで、既存の ID プロバイダーをいったん接続してディレクトリ内のユーザーやグループと同期したり、あるいは IAM アイデンティティセンターでユーザーを直接作成および管理したりできます。単一のフェデレーションポイントを提供することで、IAM アイデンティティセンターは、各アプリケーション向けにフェデレーションまたはユーザーとグループの同期を設定する操作を不要にし、管理作業を軽減します。ユーザーとグループの割り当てに関する共通ビューも得られます。

IAM アイデンティティセンターと連携する AWS アプリケーションの表については、「AWSIAM アイデンティティセンターで使用できる マネージドアプリケーション」を参照してください。

AWS マネージドアプリケーションへのアクセスの制御

AWS マネージドアプリケーションへのアクセスは次の 2 つの方法で制御されます。

- アプリケーションへの初回入力

  IAM アイデンティティセンターは、アプリケーションへの割り当てを通じてこれを管理します。デフォルトでは、AWS マネージドアプリケーションには割り当てが必要です。アプリケーション管理者である場合、アプリケーションへの割り当てを必須にするかどうかを選択できます。

  割り当てが必要な場合、ユーザーが AWS アクセスポータルにサインインすると、アプリケーションへの直接割当て、またはグループ割り当てによって割り当てられたユーザーのみがアプリケーションタイルを閲覧できます。

  割り当てが不要な場合は、すべての IAM アイデンティティセンターユーザーがアプリケーションにアクセスすることを許可できます。この場合、アプリケーション側はリソースへのアクセスを管理し、アプリケーションタイルは AWS アクセスポータルにアクセスするすべてのユーザーに対して表示されます。

  > **Important**
  >
  > IAM アイデンティティセンター管理者である場合は、IAM アイデンティティセンターコンソールを使用して AWS マネージドアプリケーションへの割り当てを削除できます。割り当てを削除する前に、アプリケーション管理者と調整することをお勧めします。また、割

り当てが必要かどうかを決定する設定を変更したり、アプリケーションの割り当てを自動化したりする予定がある場合は、アプリケーション管理者と調整する必要があります。

- アプリケーションリソースへのアクセス

  アプリケーションは、アプリケーション側で制御する独立したリソース割り当てを通じてアプリケーションリソースへのアクセスを管理します。

AWS マネージドアプリケーションには、アプリケーションリソースへのアクセス管理用の管理者ユーザーインターフェイスが用意されています。例えば、Quick 管理者は、グループメンバーシップに基づいてダッシュボードにアクセスするユーザーを割り当てることができます。ほとんどの AWS マネージドアプリケーションには、アプリケーションにユーザーを割り当てることができる AWS マネジメントコンソール 環境も用意されています。これらのアプリケーションのコンソール環境には、ユーザー割り当て機能とアプリケーションリソースへのアクセスを管理する機能を組み合わせるために、両方の機能が統合されている場合があります。

ID 情報の共有

AWS アカウント での ID 情報の共有に関する注意事項

IAM アイデンティティセンターは、アプリケーション全体で最もよく使用される属性をサポートします。これらの属性には、姓名、電話番号、E メールアドレス、住所、優先する言語が含まれます。この個人を特定できる情報を使用できるアプリケーションとアカウントを慎重に検討してください。

この情報へのアクセスは、次のいずれかの方法で制御できます。

- AWS Organizations の管理アカウントのみでアクセスを有効にするか、AWS Organizations の全アカウントでアクセスを有効にするかを選択できます。
- または、サービスコントロールポリシー (SCP) を使って、どのアプリケーションが AWS Organizations のどのアカウントの情報にアクセスできるかを制御することができます。

例えば、AWS Organizations 管理アカウントでのみアクセスを可能にした場合、メンバーアカウントのアプリケーションは情報にアクセスできません。すべてのアカウントでアクセスを有効にすると、SCP を使用して許可するアプリケーションを除く、すべてのアプリケーションによるアクセスを禁止できます。

サービスコントロールポリシーは、AWS Organizations の機能です。SCP をアタッチする手順については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシーのアタッチとデタッチ」を参照してください。

ID 情報を共有するための IAM アイデンティティセンターの設定

IAM アイデンティティセンターは、サインイン認証情報を除く、ユーザーおよびグループの属性を含む ID ストアを提供します。以下のいずれかの方法で、IAM Identity Center ID ストアのユーザーとグループを更新することができます。

- IAM Identity Center ID ストアをメインの ID ソースとして使用します。この方法を選択した場合、IAM アイデンティティセンターコンソールまたは AWS Command Line Interface (AWS CLI) 内からユーザー、サインイン認証情報およびグループを管理します。詳細については、「アイデンティティセンターディレクトリでユーザーを管理する」を参照してください。
- 以下のいずれかの ID ソースから IAM Identity Center の ID ストアにユーザーとグループのプロビジョニング (同期) を設定します。
  - Active Directory - 詳細については、「Microsoft AD ディレクトリ」を参照してください。
  - 外部 ID プロバイダー - 詳細については、「外部 ID プロバイダー」を参照してください。

  このプロビジョニング方法を選択した場合、ユーザーとグループの管理は ID ソース内で継続され、それらの変更は IAM アイデンティティセンターの ID ストアに同期されます。

どの ID ソースを選択しても、IAM アイデンティティセンターはユーザーやグループの情報を AWS マネージドアプリケーションと共有することができます。そのように、ID ソースを一度 IAM アイデンティティセンターに接続するだけで、AWS クラウド 内の複数のアプリケーションで ID 情報を共有することが可能になります。これにより、アプリケーションごとにフェデレーションや ID のプロビジョニングを個別に設定する必要がなくなります。また、この共有機能により、ユーザーに別の AWS アカウント で、多数のアプリケーションへのアクセスを簡単に与えることができます。

AWS マネージドアプリケーションの使用の制限

IAM アイデンティティセンターを初めて有効にすると、AWS Organizations 内のすべてのアカウントで AWS マネージドアプリケーションの ID ソースとして利用可能になります。アプリケーションを制約するには、サービスコントロールポリシー (SCP) を実装する必要があります。SCP は、組織内の ID (ユーザーとロール) が持つことができる最大の権限を一元的に管理するための AWS Organizations の機能です。SCP を使用して、IAM アイデンティティセンターのユーザーおよびグループ情報へのアクセスをブロックし、指定したアカウント以外ではアプリケーションを起動できな

いようにすることができます。詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。

以下の SCP の例では、IAM アイデンティティセンターのユーザーおよびグループ情報へのアクセスをブロックし、指定したアカウント(111111111111 および 222222222222)以外ではアプリケーションを起動できないようにすることができます。

```
{
  "Sid": "DenyIdCExceptInDesignatedAWSAccounts",
  "Effect": "Deny",
  "Action": [
    "identitystore:*",
    "sso:*",
    "sso-directory:*",
    "sso-oauth:*"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalAccount": [
        "111111111111",
        "222222222222"
      ]
    }
  }
}
```

AWSIAM アイデンティティセンターで使用できる マネージドアプリケーション

IAM アイデンティティセンターでは、既存の ID ソースを接続したり、ユーザーを 1 回作成したりできます。これにより、アプリケーション管理者は、個別のフェデレーションやユーザーとグループの同期なしで、次の AWS マネージドアプリケーションへのアクセスを管理できます。

AWSIAM アイデンティティセンターと統合する マネージドアプリケーション

次の表のすべての AWS マネージドアプリケーションは、IAM アイデンティティセンターの組織インスタンスと統合されています。この表は、サポートされている AWS マネージドアプリケーションの以下に関する情報も示しています。

- アプリケーションが IAM アイデンティティセンターのアカウントインスタンスとも統合されているかどうか
- アプリケーションが IAM アイデンティティセンターを介した信頼できる ID の伝播を有効化できるかどうか
- アプリケーションがカスタマーマネージド KMS キーで設定された IAM アイデンティティセンターをサポートしているかどうか
- アプリケーションが IAM Identity Center の追加リージョンでのデプロイをサポートしているかどうか

> **Note**
>
> IAM Identity Center の追加リージョンへのデプロイをサポートしているアプリケーションは、カスタマーマネージド KMS キーで設定された IAM Identity Center もサポートします。ここにリストされているすべての AWS マネージドアプリケーションが、プライマリリージョンでのデプロイをサポートしています。詳細については、「the section called “複数の AWS リージョンにまたがる AWS マネージドアプリケーションのデプロイと管理”」を参照してください。

AWS マネージドアプリケーション	IAM アイデンティティセンターのアカウントインスタンスとの統合	IAM アイデンティティセンターを介した信頼できる ID の伝播の有効化	カスタマーマネージド KMS キーで設定された IAM アイデンティティセンターをサポート	IAM Identity Center の追加リージョンでのデプロイをサポートする
Amazon Athena SQL	はい	はい	はい	はい
Amazon CodeCatalyst	はい	なし	はい	なし
Amazon DataZone	はい	はい	はい	なし
Amazon EKS の機能	はい	はい	はい	なし
Amazon EMR on EC2	はい	はい	はい	はい

AWS マネージドアプリケーション	IAM アイデンティティセンターのアカウントインスタンスとの統合	IAM アイデンティティセンターを介した信頼できる ID の伝播の有効化	カスタマーマネージド KMS キーで設定された IAM アイデンティティセンターをサポート	IAM Identity Center の追加リージョンでのデプロイをサポートする
Amazon EMR on EKS	はい	はい	はい	はい
Amazon EMR Serverless	はい	はい	はい	はい
Amazon EMR Studio	はい	はい	はい	はい
Amazon Kendra	なし	いいえ	はい	なし
Amazon Managed Grafana	なし	いいえ	はい	なし
Amazon Monitron	なし	いいえ	はい	なし
Amazon OpenSearch Service	はい	はい	はい	なし
Amazon OpenSearch Service Serverless Service	はい	はい	はい	なし
Amazon Q Business	はい	はい	はい	なし
Amazon Quick	はい	はい	はい	はい[4]
Amazon Redshift	はい 2	はい	はい	はい
Amazon S3 Access Grants	はい	はい	はい	はい
Amazon SageMaker Studio	いいえ	はい	はい	なし

AWS マネージドアプリケーション	IAM アイデンティティセンターのアカウントインスタンスとの統合	IAM アイデンティティセンターを介した信頼できる ID の伝播の有効化	カスタマーマネージド KMS キーで設定された IAM アイデンティティセンターをサポート	IAM Identity Center の追加リージョンでのデプロイをサポートする
Amazon SageMaker Unified Studio	はい	はい	はい	はい
Amazon WorkMail	はい	はい	はい	なし
Amazon WorkSpaces	はい	なし	はい	なし
Amazon WorkSpaces Secure Browser	なし	いいえ	はい	なし
AWS アカウントアクセス (アカウントアクセスマネージャー)	いいえ	はい	はい	いいえ[3]
AWS App Studio	はい	なし	いいえ	いいえ
AWS Deadline Cloud	はい	なし	はい	はい
AWS DevOps エージェント	はい	はい	はい	はい
AWS Glue	はい	はい	はい	はい
AWS IoT Events	なし	いいえ	いいえ	いいえ
AWS IoT SiteWise	いいえ	いいえ	いいえ	いいえ
AWS Lake Formation	はい	はい	はい	はい
AWS re:Post Private	はい	なし	はい	なし
AWS Supply Chain	はい	なし	はい	なし

AWS マネージドアプリケーション	IAM アイデンティティセンターのアカウントインスタンスとの統合	IAM アイデンティティセンターを介した信頼できる ID の伝播の有効化	カスタマーマネージド KMS キーで設定された IAM アイデンティティセンターをサポート	IAM Identity Center の追加リージョンでのデプロイをサポートする
AWS セキュリティエージェント	はい	はい	はい	なし
AWS Systems Manager	いいえ	いいえ	はい	はい - Fleet Manager Remote Desktop
AWS Transfer Family ウェブアプリ	はい	はい	はい	はい
AWS Transform	はい	なし	はい	なし
AWS Verified Access	いいえ	いいえ	はい	なし
Kiro	あり[1]	はい	はい	なし
マルチパーティー承認	いいえ	はい	はい	なし
OpenSearch user interface (Dashboards)	はい	はい	はい	なし

[1] Kiro では、ユーザーが AWS ウェブサイト上の全 Kiro 機能にアクセスする必要がある場合を除き、IAM Identity Center のアカウントインスタンスがサポートされます。詳細については、「Kiro ユーザーガイド」の「Kiro のセットアップ」を参照してください。

[2] Amazon Redshift の場合、IAM Identity Center のアカウントインスタンスがサポートされています。ただし、Query Editor v2 など、アカウントインスタンスでサポートされていないアクセス許可セットを必要とするアプリケーションを除きます。

[3] IAM Identity Center のプライマリリージョンでアカウントアクセスマネージャーを有効にします。

[4] Amazon Quick は、AWS コマンドラインインターフェイス (CLI) を介して IAM Identity Center の追加リージョンにデプロイできます。追加リージョンへの Amazon Quick のデプロイの詳細については、「Amazon Quick ユーザーガイド」の「IAM Identity Center の使用」を参照してください。

> **Note**
>
> Connect Customer や AWS Client VPN など一部の AWS サービスは、IAM Identity Center で使用できますが、この表には記載されていません。これは、SAML のみを使用して IAM Identity Center と統合されるため、カスタマーマネージドアプリケーションに分類されるためです。

クイックスタート: AWS マネージドアプリケーションをテストするための IAM アイデンティティセンターのセットアップ

管理者が IAM アイデンティティセンターへのアクセスをまだ提供していない場合は、このトピックのステップを使用して、AWS マネージドアプリケーションをテストするための IAM アイデンティティセンターを設定できます。IAM アイデンティティセンターを有効にし、IAM アイデンティティセンターでユーザーを直接作成し、そのユーザーを AWS マネージドアプリケーションに割り当てる方法について説明します。

このトピックでは、次のいずれかの方法で IAM アイデンティティセンターを有効にする方法に関するクイックスタートステップについて説明します。

- AWS Organizations の場合 – このオプションを選択すると、IAM アイデンティティセンターの組織インスタンスが作成されます。
- 特定の AWS アカウント のみ – このオプションを選択すると、IAM アイデンティティセンターのアカウントインスタンスが作成されます。

これらのインスタンスタイプの詳細については、「IAM アイデンティティセンターの組織インスタンスとアカウントインスタンス」を参照してください。

前提条件

IAM アイデンティティセンターを有効にする前に、以下を確認してください。

- AWS アカウント がある – AWS アカウント がない場合は、「AWS アカウント管理リファレンスガイド」の「AWS アカウント の開始方法」を参照してください。

- AWS マネージドアプリケーションは IAM アイデンティティセンターと連携 – AWSIAM アイデンティティセンターで使用できる マネージドアプリケーション のリストを確認して、テストする AWS マネージドアプリケーションが IAM アイデンティティセンターとの連携していることを確認します。
- リージョン別の考慮事項を確認した – テストする AWS マネージドアプリケーションが、IAM アイデンティティセンターを有効にする AWS リージョン でサポートされていることを確認します。詳細については、AWS マネージドアプリケーションのドキュメントを参照してください。

> **Note**
>
> AWS マネージドアプリケーションは、IAM アイデンティティセンターを有効にする予定のリージョンと同じリージョンにデプロイする必要があります。

AWS マネージドアプリケーションをテストするための IAM アイデンティティセンターの組織インスタンスのセットアップ

> **Note**
>
> このトピックでは、 を使用して IAM アイデンティティセンターを AWS Organizations で有効にする方法について説明します。これは、IAM アイデンティティセンターを有効にするために推奨される方法です。

アクセス許可を確認する

AWS Organizations で IAM アイデンティティセンターを有効にするには、次のいずれかの方法で AWS 管理コンソールにサインインする必要があります。

- AWS アカウント で IAM アイデンティティセンターを有効にする AWS Organizations で管理権限を持つユーザー。
- ルートユーザー (他の管理ユーザーが存在しない場合を除き、推奨されません)。

> **Important**
>
> ルートユーザーは、アカウントのすべての AWS サービスとリソースにアクセスできます。セキュリティのベストプラクティスとして、他の認証情報がない場合は、アカウント

のルート認証情報を使用して AWS リソースにアクセスしないでください。これらの認証情報は無制限のアカウントアクセスを提供し、取り消すのが困難です。

ステップ 1. AWS Organizations で IAM アイデンティティセンターを有効にする

1. 以下のいずれかを行って、AWS マネジメントコンソール にサインインします。
   - AWS[新規の (ルートユーザー)] – [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、アカウント所有者としてサインインします。次のページでパスワードを入力します。
   - [既にスタンドアロン AWS アカウント を使用している AWS (IAM 認証情報)] — 管理者権限を持つ IAM 認証情報を使用してサインインします。
2. AWS 管理コンソールのホームページで、IAM アイデンティティセンターサービスを選択するか、IAM アイデンティティセンターコンソールに移動します。
3. [有効にする] を選択して、AWS Organizations で IAM アイデンティティセンターを有効にします。これを行うと、IAM アイデンティティセンターの組織インスタンスが作成されます。

ステップ 2. IAM アイデンティティセンターでの管理ユーザーの作成

この手順では、組み込みのアイデンティティセンターディレクトリでユーザーを直接作成する方法について説明します。このディレクトリは、管理者がワークフォースユーザーの管理に使用する可能性のある他のディレクトリに接続されていません。IAM アイデンティティセンターでユーザーを作成したら、このユーザーの新しい認証情報を指定します。このユーザーとしてサインインして AWS マネージドアプリケーションをテストすると、企業リソースへのアクセスに使用する既存の認証情報ではなく、新しい認証情報でサインインします。

> **Note**
>
> テスト目的でのみユーザーを作成する場合は、この方法を使用することが推奨されます。

1. IAM アイデンティティセンターコンソールのナビゲーションペインで、[ユーザー]、[ユーザーを追加] の順に選択します。
2. コンソールのガイダンスに従ってユーザーを追加します。「パスワード設定手順を記載した E メールをこのユーザーに送信」を選択したまま、アクセスできる E メールアドレスを指定していることを確認します。

3. ナビゲーションペインで、AWS アカウント を選択し、アカウントの横にあるチェックボックスをオンにして、ユーザーまたはグループの割り当てを選択します。
4. [ユーザー] タブを選択し、追加したユーザーの横にあるチェックボックスをオンにして、[次へ] を選択します。
5. [アクセス許可セットの作成] を選択し、コンソールのガイダンスに従って `AdministratorAccess` の事前定義されたアクセス許可セットを作成します。
6. 完了すると、新しいアクセス許可セットがリストに表示されます。ブラウザウィンドウの[アクセス許可セット] タブを閉じて、[ユーザーとグループの割り当て] タブに戻り、アクセス[許可セットの作成] の横にある更新アイコンを選択します。
7. [ユーザーとグループのブラウザの割り当て] タブに、新しいアクセス許可セットがリストに表示されます。アクセス許可セットの名前の横にあるチェックボックスを選択し、[次] へを選択し、[送信] を選択します。
8. コンソールからサインアウトします。

ステップ 3. 管理アクセス権を持つユーザーとして AWS アクセスポータルにサインインする

AWS アクセスポータルは、作成したユーザーに AWS 管理コンソールへのアクセスを提供するウェブポータルです。AWS アクセスポータルにサインインする前に、IAM アイデンティティセンターへの参加の招待を承諾し、ユーザー認証情報をアクティブ化する必要があります。

1. E メールの件名で「AWS IAM アイデンティティセンターへの参加を招待する」を確認してください。
2. [招待を受け入れる] を選択し、サインアップページのガイダンスに従って、ユーザーの新しいパスワードの設定、サインイン、MFA デバイスの登録を行います。
3. MFA デバイスを登録すると、 AWS アクセスポータルが開きます。
4. AWS アクセスポータルで、AWS アカウント を選択し、AdministratorAccess を選びます。AWS 管理コンソールにリダイレクトされます。

ステップ 4. IAM アイデンティティセンターを使用するように AWS マネージドアプリケーションを設定する

1. AWS 管理コンソールにサインインしている間、使用する AWS マネージドアプリケーションのコンソールを開きます。

2. コンソールのガイダンスに従って、IAM アイデンティティセンターを使用するように AWS マネージドアプリケーションを設定します。このプロセス中に、作成したユーザーをアプリケーションに割り当てることができます。

AWS マネージドアプリケーションをテストするための IAM アイデンティティセンターのアカウントインスタンスの設定

> **Note**
>
> IAM アイデンティティセンターのアカウントインスタンスにより、デプロイは単一の AWS アカウント に制限されます。このインスタンスは、テストする AWS アプリケーションと同じ AWS リージョン で有効にする必要があります。

アプリを確認する

IAM アイデンティティセンターと連携するすべての AWS マネージドアプリケーションは、IAM アイデンティティセンターの組織インスタンスで使用できます。ただし、これらのアプリケーションの一部のみを IAM アイデンティティセンターのアカウントインスタンスで使用できます。AWSIAM アイデンティティセンターで使用できる マネージドアプリケーション のリストを確認します。

ステップ 1. IAM アイデンティティセンターのアカウントインスタンスを有効にする

1. 以下のいずれかを行って、AWS マネジメントコンソール にサインインします。
   - AWS[新規の (ルートユーザー)] – [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、アカウント所有者としてサインインします。次のページでパスワードを入力します。
   - [既にスタンドアロン AWS アカウント を使用している AWS (IAM 認証情報)] — 管理者権限を持つ IAM 認証情報を使用してサインインします。
2. AWS 管理コンソールのホームページで、IAM アイデンティティセンターサービスを選択するか、IAM アイデンティティセンターコンソールに移動します。
3. [有効化] を選択します。
4. [AWS Organizations で IAM アイデンティティセンターを有効にする] ページで、[IAM アイデンティティセンターのアカウントインスタンスを有効にする]を選択します。

5. [IAM アイデンティティセンターのアカウントインスタンスを有効にする]ページで、情報を確認し、オプションでこのアカウントインスタンスに関連付けるタグを追加します。次に、[Enable] (有効化) を選択します。

ステップ 2. IAM アイデンティティセンターでユーザーを作成する

この手順では、組み込みのアイデンティティセンターディレクトリでユーザーを直接作成する方法について説明します。このディレクトリは、管理者がワークフォースユーザーの管理に使用する可能性のある他のディレクトリに接続されていません。IAM アイデンティティセンターでユーザーを作成したら、このユーザーの新しい認証情報を指定します。このユーザーとしてサインインして AWS マネージドアプリケーションをテストすると、新しい認証情報でサインインします。新しい認証情報では、他の企業リソースにアクセスすることはできません。

> **Note**
>
> テスト目的でのみユーザーを作成する場合は、この方法を使用することが推奨されます。

1. IAM アイデンティティセンターコンソールのナビゲーションペインで、[ユーザー]、[ユーザーを追加] の順に選択します。
2. コンソールのガイダンスに従ってユーザーを追加します。「パスワード設定手順を記載した E メールをこのユーザーに送信」を選択したまま、アクセスできる E メールアドレスを指定していることを確認します。
3. コンソールからサインアウトします。

ステップ 3. IAM アイデンティティセンターのユーザーとして AWS アクセスポータルにサインインします。

AWS アクセスポータルは、作成したユーザーに AWS 管理コンソールへのアクセスを提供するウェブポータルです。AWS アクセスポータルにサインインする前に、IAM アイデンティティセンターへの参加の招待を承諾し、ユーザー認証情報をアクティブ化する必要があります。

1. E メールの件名で「AWS IAM アイデンティティセンターへの参加を招待する」を確認してください。
2. [招待を受け入れる] を選択し、サインアップページのガイダンスに従って、ユーザーの新しいパスワードの設定、サインイン、MFA デバイスの登録を行います。

3. MFA デバイスを登録すると、 AWS アクセスポータルが開きます。アプリケーションが利用可能になると、[アプリケーション] タブに表示されます。

> **Note**
>
> AWSアカウントインスタンスをサポートするアプリケーション を使用すると、ユーザーは追加のアクセス許可を必要とせずにアプリケーションにサインインできます。したがって、[アカウント] タブは空のままになります。

ステップ 4. IAM アイデンティティセンターを使用するように AWS マネージドアプリケーションを設定する

1. AWS 管理コンソールにサインインしている間、使用する AWS マネージドアプリケーションのコンソールを開きます。
2. コンソールのガイダンスに従って、IAM アイデンティティセンターを使用するように AWS マネージドアプリケーションを設定します。このプロセス中に、作成したユーザーをアプリケーションに割り当てることができます。

AWS マネージドアプリケーションに関する詳細の表示

アプリケーションのコンソールまたは API を使用して AWS マネージドアプリケーションを IAM アイデンティティセンターに接続すると、そのアプリケーションは IAM アイデンティティセンターに登録されます。アプリケーションが IAM アイデンティティセンターに登録されると、IAM アイデンティティセンターコンソール上でアプリケーションの詳細を確認および変更できます。

アプリケーションに関する情報には、ユーザーとグループの割り当てが必要かどうか、該当する場合は ID を伝播するために割り当てられたユーザーとグループ、および信頼できるアプリケーションが含まれます。信頼できる ID 伝播の詳細については、「信頼できる ID の伝播の概要」を参照してください。

AWS マネージドアプリケーションに関する情報を IAM アイデンティティセンターコンソールで確認および変更するには

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. [AWS マネージド] タブを選択します。

4. 確認したいマネージドアプリケーションのリンクを選択します。
5. AWS マネージドアプリケーションに関する情報を変更する場合は、[アクション] を選択し、[詳細の編集] を選択します。
6. アプリケーションの表示名、説明、およびユーザーやグループの割り当て方法を変更できます。

   a. 表示名を変更するには、表示名フィールドに希望の名前を入力し、[変更の保存] を選択します。

   b. 説明を変更するには、[説明] フィールドに希望の説明文を入力し、[変更の保存] を選択します。

   c. ユーザーとグループの割り当て方法を変更するには、必要な変更を行い、[変更の保存] を選択します。詳細については、「the section called “ユーザー、グループ、プロビジョニング”」を参照してください。

AWS マネージドアプリケーションの無効化

AWS マネージドアプリケーションに対してユーザーが認証されないようにするには、IAM アイデンティティセンターコンソールでそのアプリケーションを無効にできます。

AWS マネージドアプリケーションを無効にするには

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. [アプリケーション] ページの [AWS マネージドアプリケーション] で、無効にするアプリケーションを選択します。
4. アプリケーションを選択した状態で、[アクション] を選択し、[無効にする] を選択します。
5. [アプリケーションの無効化] ダイアログボックスで、[無効化] を選択します。
6. [AWS マネージドアプリケーション] リストでは、アプリケーションの状態は [非アクティブ」と表示されます。

> **Note**
>
> AWS マネージドアプリケーションが無効になっている場合は、[アクション] を選択してから [有効化] を選択することで、アプリケーションに対して認証できるユーザーを復元できます。

ID 拡張コンソールセッションの有効化

コンソールの ID 拡張セッションは、ユーザーのエクスペリエンスをパーソナライズするための追加のユーザーコンテキストを提供することで、ユーザーの AWS コンソールセッションを拡張します。この機能は現在、AWS アプリやウェブサイト上の Amazon Q の Amazon Q Developer Pro ユーザー向けにサポートされています。

既存のアクセスパターンや AWS コンソールへのフェデレーションを変更することなく、ID 拡張コンソールセッションを有効にできます。ユーザーが IAM を使用して AWS コンソールにサインインする場合 (例えば、IAM ユーザーとしてサインインする場合や、IAM によるフェデレーティッドアクセスを通じてサインインする場合)、これらの方法を引き続き使用できます。AWS アクセスポータルにサインインしたユーザーは、IAM アイデンティティセンターユーザー認証情報を引き続き使用できます。

トピック

- 前提条件と考慮事項
- ID 拡張コンソールセッションを有効にする方法
- ID 拡張コンソールセッションの仕組み

前提条件と考慮事項

ID 拡張コンソールセッションを有効にする前に、以下の前提条件と考慮事項を確認してください。

- ユーザーが Amazon Q Developer Pro サブスクリプションを通じて AWS アプリやウェブサイトで Amazon Q にアクセスする場合は、ID 拡張コンソールセッションを有効にする必要があります。

  > **Note**
  >
  > Amazon Q Developer ユーザーは、ID 拡張セッションなしで Amazon Q にアクセスできますが、Amazon Q Developer Pro サブスクリプションにはアクセスできません。

- ID 拡張コンソールセッションには、IAM アイデンティティセンターの組織インスタンスが必要です。
- IAM アイデンティティセンターをオプトイン AWS リージョンで有効にした場合、Amazon Q との統合はサポートされません。
- ID 拡張コンソールセッションを有効にするには、次のアクセス許可が必要です。
  - `sso:CreateApplication`

- sso:GetSharedSsoConfiguration
- sso:ListApplications
- sso:PutApplicationAssignmentConfiguration
- sso:PutApplicationAuthenticationMethod
- sso:PutApplicationGrant
- sso:PutApplicationAccessScope
- signin:CreateTrustedIdentityPropagationApplicationForConsole
- signin:ListTrustedIdentityPropagationApplicationsForConsole

- ユーザーが ID 拡張コンソールセッションを使用できるようにするには、ID ベースのポリシーで sts:setContext アクセス許可を付与する必要があります。詳細については、「ユーザーに ID 拡張コンソールセッションを使用するアクセス許可を付与する」を参照してください。

ID 拡張コンソールセッションを有効にする方法

ID 拡張コンソールセッションは、Amazon Q コンソールまたは IAM アイデンティティセンターコンソールで有効にできます。

Amazon Q コンソールで ID 拡張コンソールセッションを有効にする

ID 拡張コンソールセッションを有効にする前に、ID ソースが接続された IAM アイデンティティセンターの組織インスタンスが必要です。IAM アイデンティティセンターを既に設定している場合は、ステップ 3 に進みます。

1. IAM Identity Center コンソール を開きます。[有効化] を選択し、IAM アイデンティティセンターの組織インスタンスを作成します。詳細については、「IAM Identity Center を有効にする」を参照してください。
2. ID ソースを IAM アイデンティティセンターに接続し、ユーザーを IAM アイデンティティセンターにプロビジョニングします。既存の ID ソースを IAM アイデンティティセンターに接続するか、あるいは別に使用している ID ソースがない場合は イデンティティセンターディレクトリを利用できます。詳細については、「IAM アイデンティティセンターの ID ソースに関するチュートリアル」を参照してください。
3. IAM アイデンティティセンターの設定が完了したら、Amazon Q コンソールを開き、「Amazon Q Developer User Guide」の「Subscriptions」のステップに従います。ID 拡張コンソールセッションを必ず有効にしてください。

> **Note**
>
> ID 拡張コンソールセッションを有効にするのに十分なアクセス許可がない場合は、IAM アイデンティティセンター管理者に依頼して IAM アイデンティティセンターコンソール上でこのタスクを実行してもらってください。詳細については、次の手順を参照してください。

IAM アイデンティティセンターコンソールで ID 拡張コンソールセッションを有効にする

IAM アイデンティティセンター管理者は、別の管理者から IAM アイデンティティセンターコンソールでの ID 拡張コンソールセッションの有効化を依頼されることがあります。

1. IAM Identity Center コンソール を開きます。
2. ナビゲーションペインで [設定] を選択します。
3. [ID 拡張セッションを有効にする] で、[有効化] を選択します。
4. 次に表示されるメッセージに対して、[有効化] を再度選択します。
5. ID 拡張コンソールセッションの有効化が完了すると、[設定] ページの上部に確認メッセージが表示されます。
6. [詳細] セクションに表示される [ID 拡張セッション] のステータスが [有効] になっているはずです。

ID 拡張コンソールセッションの仕組み

IAM アイデンティティセンターでユーザーの現在のコンソールセッションを拡張することで、アクティブな IAM アイデンティティセンターユーザー ID と IAM アイデンティティセンターセッション ID を含むようにすることができます。

ID 拡張コンソールセッションには、次の 3 つの値が含まれます。

- Identity Store ユーザー ID (identitystore:UserId) - この値は、IAM アイデンティティセンターに接続されている ID ソース内のユーザーを一意に識別するのに使用されます。
- ID ストアディレクトリ ARN (identitystore:IdentityStoreArn) - この値は、IAM アイデンティティセンターに接続され、`identitystore:UserId` の属性検索を可能にする ID ストアの ARN です。
- IAM アイデンティティセンターセッション ID - この値は、ユーザーの IAM アイデンティティセンターセッションがまだ有効かどうかを示します。

値は同じですがさまざまな方法で取得され、ユーザーがサインインする方法に応じてプロセスのさまざまなポイントに追加されます。

- IAM アイデンティティセンター(AWS アクセスポータル): この場合、ユーザーの ID ストアユーザー ID と ARN 値は、アクティブな IAM アイデンティティセンターセッション内で既に指定されています。IAM アイデンティティセンターには、セッション ID のみを追加することで現在のセッションを拡張する機能があります。
- その他のサインイン方法: ユーザーが IAM ユーザー、IAM ロール、または IAM のフェデレーションユーザーとして AWS にサインインする場合、これらの値は提供されません。IAM アイデンティティセンターは、ID ストアユーザー ID、ID ストアディレクトリ ARN、およびセッション ID を追加することで現在のセッションを拡張します。

カスタマーマネージドアプリケーション

IAM アイデンティティセンターは、ワークフォースユーザーとグループに対する集中 ID サービスとして機能します。すでに ID プロバイダー (IdP) を使用している場合は、IAM アイデンティティセンターを IdP と統合して、ユーザーとグループを IAM アイデンティティセンターにプロビジョニングし、ご自分の IdP を認証に使用することができます。単一の接続において、IAM アイデンティティセンターは複数の AWS のサービスに対して IdP を提示し、OAuth 2.0 アプリケーションがユーザーに代わってこれらのサービスのデータへのアクセスをリクエストできるようにします。また、IAM アイデンティティセンターを使用して、SAML 2.0 アプリケーションへのアクセスをユーザーに割り当てることができます。これには、Connect Customer や AWS Client VPN といった AWS サービスが含まれます。これらのサービスは、SAML のみを使用して IAM Identity Center と統合されるため、カスタマーマネージドアプリケーションに分類されます。

- アプリケーションが JSON Web Tokens (JWT) をサポートしている場合は、IAM アイデンティティセンターの信頼できる ID の伝播機能を使用して、アプリケーションがユーザーに代わって AWS のサービスのデータへのアクセスをリクエストできるように手配できます。信頼できる ID の伝播機能は OAuth 2.0 認証フレームワーク上に構築されており、アプリケーションが外部の OAuth 2.0 認証サーバーから取得した ID トークンを IAM アイデンティティセンターが発行し、AWS のサービスによって認識されるトークンと交換するためのオプションが含まれています。詳細については、「信頼できる ID の伝播のユースケース」を参照してください。
- アプリケーションが SAML 2.0 をサポートしている場合は、IAM アイデンティティセンターの組織インスタンスに接続できます。IAM アイデンティティセンターを使用して、SAML 2.0 アプリケーションへのアクセスを割り当てることができます。

> **Note**
>
> カスタマーマネージドアプリケーションを、カスタマーマネージド KMS キーを使用する IAM Identity Center インスタンスと統合する場合は、アプリケーションが IAM Identity Center サービス API を呼び出すかどうかを確認します。その場合は、「ベースライン KMS キーポリシー」を参照して、必要なアクセス許可を確認してください。

トピック

- SAML 2.0 および OAuth 2.0 アプリケーションへのシングルサインオンアクセス
- カスタマー管理 SAML 2.0 アプリケーションの設定
- カスタマーマネージドアプリケーションで AWS アカウントアクセスを有効にする

SAML 2.0 および OAuth 2.0 アプリケーションへのシングルサインオンアクセス

IAM アイデンティティセンターでは、SAML 2.0 アプリケーションまたは OAuth 2.0 アプリケーションへのシングルサインオンアクセスをユーザーに提供できます。以下のトピックでは、SAML 2.0 と OAuth 2.0 の大まかな概観を説明します。

トピック

- SAML 2.0
- OAuth 2.0

SAML 2.0

SAML 2.0 は、SAML 認証機関 (ID プロバイダーまたは IdP) と SAML 2.0 コンシューマー (サービスプロバイダーまたは SP) との間でユーザーに関する情報を渡す SAML アサーションを安全に交換するための業界標準です。IAM Identity Center は、この情報を使用して、AWS アクセスポータル内でアプリケーションの使用が許可されているユーザーに、フェデレーションシングルサインオンアクセスを提供します。

> **Note**
>
> IAM アイデンティティセンターは、SAML アプリケーションからの受信 SAML 認証リクエストの署名の検証をサポートしていません。

OAuth 2.0

OAuth 2.0 は、アプリケーションがパスワードを共有せずにユーザーデータに安全にアクセスして共有できるようにするプロトコルです。この機能により、アプリケーションによるリソースへのアクセスを、安全かつ標準化された方法でユーザーに許可できます。アクセスは、さまざまな OAuth 2.0 付与フローによって容易になります。

IAM アイデンティティセンターを使用すると、パブリッククライアントで実行されるアプリケーションは、ユーザーに代わってプログラムで AWS アカウントおよびサービスにアクセスするための一時的な認証情報を取得できます。パブリッククライアントは通常、ローカルでアプリケーションを実行するのに使用されるデスクトップ、ノートパソコン、またはその他のモバイルデバイスです。パブリッククライアントで実行される AWS アプリケーションの例としては、AWS Command Line Interface (AWS CLI)、AWS Toolkit、および AWS Software Development Kits (SDK) などがあります。これらのアプリケーションが認証情報を取得できるように、IAM アイデンティティセンターは次の OAuth 2.0 フローの一部をサポートしています。

- コード交換用検証キー (PKCE) を使用した認証コードの付与 (RFC 6749 および RFC 7636)
- デバイス認可付与 (RFC 8628)

> **Note**
>
> これらの許可タイプは、この機能をサポートする AWS のサービスでのみ使用できます。これらのサービスは、すべての AWS リージョンでこの許可タイプをサポートしていない場合があります。リージョンごとの違いについては、AWS のサービスの関連ドキュメントを参照してください。

OpenID Connect (OIDC) は、OAuth 2.0 フレームワークに基づく認証プロトコルです。OIDC は、認証に OAuth 2.0 を使用する方法を指定します。IAM アイデンティティセンター OIDC サービス API を介してアプリケーションは OAuth 2.0 クライアントを登録し、これらのフローのいずれかを使用して IAM アイデンティティセンターで保護された API へのアクセス許可を提供するアクセストーク

ンを取得します。アプリケーションは、目的の API ユーザーを宣言するためのアクセススコープを指定します。IAM アイデンティティセンター管理者として ID ソースを設定した後、アプリケーションのエンドユーザーがまだサインインプロセスを完了していない場合は、サインインプロセスを完了する必要があります。その後、エンドユーザーは、アプリケーションが API コールを行うことに同意する必要があります。これらの API コールは、ユーザー自身の権限を使用して行われます。これに対して IAM アイデンティティセンターは、ユーザーが同意したアクセススコープを含むアクセストークンをアプリケーションに返します。

OAuth 2.0 許可フローの使用

OAuth 2.0 許可フローは、フローをサポートする AWS マネージドアプリケーションでのみ使用できます。OAuth 2.0 フローを使用するには、お使いの IAM アイデンティティセンターインスタンスと使用する AWS マネージドアプリケーション (サポートされている必要があります) を、単一の AWS リージョンにデプロイする必要があります。AWS マネージドアプリケーションのリージョンごとの可用性と、使用する IAM アイデンティティセンターのインスタンスについては、AWS のサービスのドキュメントを参照してください。

OAuth 2.0 フローを使用するアプリケーションを使用するには、エンドユーザーがアプリケーションの接続先 URL を入力してお使いの IAM アイデンティティセンターインスタンスに登録する必要があります。アプリケーションによっては、管理者が IAM アイデンティティセンターインスタンスの AWS アクセスポータル URL または発行者 URL をユーザーに提供する必要があります。これらの 2 つの設定は、IAM アイデンティティセンターコンソールの [設定] ページで確認できます。クライアントアプリケーションの設定の詳細については、そのアプリケーションのドキュメントを参照してください。

アプリケーションにサインインして同意するエンドユーザーエクスペリエンスの詳細は、そのアプリケーションが PKCE を使用した認可コード付与 と デバイス認可付与 のいずれを使用しているかどうかによって異なります。

PKCE を使用した認可コード付与

このフローは、ブラウザを持つデバイスで実行されるアプリケーションによって使用されます。

1. ブラウザウィンドウが開きます。
2. ユーザーがまだ認証されていない場合、ブラウザはユーザーをリダイレクトして認証完了を促します。
3. 認証後、次の項目を表示した同意画面がユーザーに対して表示されます。
   - アプリケーションの名前
   - アプリケーションが使用のための同意を求めるアクセス範囲

4. ユーザーは同意プロセスをキャンセルすることができます。同意すると、アプリケーションはそのユーザーの持つアクセス許可に基づいてアクセス処理を進めます。

デバイス認可付与

このフローは、ブラウザの有無にかかわらず、デバイスで実行されるアプリケーションで使用できます。アプリケーションがフローを開始すると、アプリケーションは、フローの後半でユーザーが確認する必要がある URL とユーザーコードを表示します。フローを開始するアプリケーションがユーザーが同意したデバイスとは異なるデバイスで実行されている場合に備えて、このユーザーコードが必要となります。このコードにより、ユーザーが他のデバイスで開始したフローに同意していることを保証します。

> **Note**
>
> `device.sso.region.amazonaws.com` を使用するクライアントがある場合は、コード交換 (PKCE) の証明キーを使用するように認可フローを更新する必要があります。IAM アイデンティティセンターでの MFA の詳細については、「AWS Command Line Interface ユーザーガイド」の「AWS CLI を使用した多要素認証」を参照してください。

1. ブラウザを持つデバイスからフローが開始されると、ブラウザウィンドウが開きます。フローがブラウザを持たないデバイスで開始された場合、ユーザーは別のデバイスでブラウザを開き、アプリケーションが提示した URL に移動する必要があります。
2. いずれの場合も、ユーザーが認証されていない場合、ブラウザはユーザーをリダイレクトして認証完了を促します。
3. 認証後、次の項目を表示した同意画面がユーザーに対して表示されます。
   - アプリケーションの名前
   - アプリケーションが使用のための同意を求めるアクセス範囲
   - アプリケーションがユーザーに提示したユーザーコード
4. ユーザーは同意プロセスをキャンセルすることができます。同意すると、アプリケーションはそのユーザーの持つアクセス許可に基づいてアクセス処理を進めます。

アクセススコープ

スコープは、OAuth 2.0 フローを介してアクセスできるサービスへのアクセスを定義します。スコープは、リソースサーバーとも呼ばれるサービスが、アクションやサービスリソースに関連する権限

をグループ化する方法であり、OAuth 2.0 クライアントがリクエストできる操作を大まかに指定します。OAuth 2.0 クライアントが IAM アイデンティティセンター OIDC サービスに登録すると、クライアントは意図されるアクションを宣言するスコープを指定します。これに対してユーザーは同意する必要があります。

OAuth 2.0 クライアントは、「OAuth 2.0 (RFC6749)」のセクション 3.3 で定義されている `scope` 値を使用して、アクセストークンにリクエストされるアクセス権限を指定します。クライアントがアクセストークンをリクエストする際には、最大 25 件のスコープを指定できます。PKCE またはデバイス認可付与フローで認証コード付与中にユーザーが同意すると、IAM アイデンティティセンターは返されるアクセストークンにスコープをエンコードします。

AWS は、サポートされている について IAM アイデンティティセンターにスコープを追加します。AWS のサービス次の表に、パブリッククライアントを登録する際に IAM アイデンティティセンター OIDC サービスがサポートするスコープを示します。

パブリッククライアントの登録時に IAM Identity Center OIDC サービスがサポートするアクセススコープ

範囲	説明	がサポートするサービス
`sso:account:access`	IAM Identity Center が管理するアカウントとアクセス権限セットにアクセスします。	IAM アイデンティティセンター
`codewhisperer:analysis`	Kiro コード分析へのアクセスを有効にします。	AWS ビルダー ID と IAM アイデンティティセンター
`codewhisperer:completions`	Kiro インラインコードの提案へのアクセスを有効にします。	AWS ビルダー ID と IAM アイデンティティセンター
`codewhisperer:conversations`	Kiro チャットへのアクセスを有効にします。	AWS ビルダー ID と IAM アイデンティティセンター
`codewhisperer:taskassist`	ソフトウェア開発のための Kiro エージェントへのアクセスを有効にします。	AWS ビルダー ID と IAM アイデンティティセンター

範囲	説明	がサポートするサービス
codewhisperer:transformations	コード変換のために Kiro エージェントへのアクセスを有効にします。	AWS ビルダー ID と IAM アイデンティティセンター
codecatalyst:read_write	Amazon CodeCatalyst リソースの読み取りと書き込みが可能なため、既存のすべてのリソースにアクセスできます。	AWS ビルダー ID と IAM アイデンティティセンター
verified_access:application:connect	AWS Verified Access の有効化	AWS Verified Access
redshift:connect	Amazon Redshift に接続する	Amazon Redshift
datazone:domain:access	DataZone ドメイン実行ロールにアクセスする	Amazon DataZone
nosqlworkbench:datamodeladviser	データモデルの作成と読み取り	NoSQL Workbench
transform:read_write	コード変換のために AWS 変換エージェントへのアクセスを有効にする	AWS Transform

カスタマー管理 SAML 2.0 アプリケーションの設定

SAML 2.0 をサポートするカスタマーマネージドアプリケーションを使用している場合は、SAML 2.0 を介して IdP を IAM アイデンティティセンターにフェデレーションし、IAM アイデンティティセンターを使用してそれらのアプリケーションへのユーザーアクセスを管理できます。IAM アイデンティティセンターコンソールでよく使用されるアプリケーションのカタログから SAML 2.0 アプリケーションを選択するか、独自の SAML 2.0 アプリケーションを設定できます。

> **Note**
>
> OAuth 2.0 をサポートするカスタマーマネージドアプリケーションがあり、ユーザーがこれらのアプリケーションから AWS のサービス にアクセスする必要がある場合、信頼できる ID の伝播を使用できます。信頼できる ID の伝播を使用すると、ユーザーはアプリケーションにサインインでき、そのアプリケーションは AWS のサービス 内のデータにアクセスするためのリクエストでユーザーの ID を渡すことができます。

トピック

- IAM アイデンティティセンターアプリケーションカタログからアプリケーションを設定する
- 独自の SAML 2.0 アプリケーションをセットアップする

IAM アイデンティティセンターアプリケーションカタログからアプリケーションを設定する

IAM アイデンティティセンターコンソールのアプリケーションカタログを使用して、IAM アイデンティティセンターと連携するよく使用されている多くの SAML 2.0 アプリケーションを追加することができます。例としては、Salesforce、Box、Microsoft 365 などがあります。

ほとんどのアプリケーションで、IAM アイデンティティセンターとアプリケーションのサービスプロバイダーとの間の信頼関係を設定する方法に関する詳細情報が提供されます。この情報は、カタログでアプリケーションを選択すると、アプリケーションの設定ページで利用できます。アプリケーションを設定したら、必要に応じて IAM アイデンティティセンターのユーザーまたはグループにアクセス権を割り当てることができます。

IAM アイデンティティセンターとアプリケーションのサービスプロバイダーとの間で SAML 2.0 の信頼関係を設定するには、以下の手順を実行します。

この手順を開始する前に、信頼をより効率的に設定できるように、サービスプロバイダーのメタデータ交換ファイルがあることが役に立ちます。このファイルがない場合でも、まだこの手順を使用してその信頼を手動で設定できます。

アプリケーションカタログからアプリケーションを追加および設定するには

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。

3. [カスタマーマネージド] タブを選択します。
4. [アプリケーションの追加] を選択します。
5. [アプリケーションタイプを選択] ページの [セットアッププリファレンス] で、[カタログからアプリケーションを選択したい] を選択します。
6. [アプリケーションカタログ] で、追加するアプリケーションの名前を検索ボックスに入力し始めます。
7. 検索結果に表示されたら、一覧からアプリケーションの名前を選択し、[次へ] を選択します。
8. [アプリケーションを設定] ページの [表示名] と [説明] フィールドには、アプリケーションに関連する詳細があらかじめ入力されています。この情報は編集することができます。
9. 「IAM Identity Center」で、以下の作業を行います。

    a. IAM Identity Center SAML メタデータファイルの横にある [ダウンロード] を選択して、ID プロバイダーのメタデータをダウンロードします。

    b. [IAM Identity Center 証明書] の横にある [証明書のダウンロード] を選択して、ID プロバイダーの証明書をダウンロードします。

    > **Note**
    >
    > 後で、サービスプロバイダーのウェブサイトからアプリケーションを設定するときに、これらのファイルが必要になります。そのプロバイダーからの手順に従います。

10. (オプション) [アプリケーションプロパティ] の下で、[アプリケーション開始 URL]、[リレー状態]、[セッション期間] を指定できます。詳細については、「IAM アイデンティティセンターコンソールのアプリケーションプロパティを理解する」を参照してください。
11. [Application metadata] (アプリケーションメタデータ) で、以下のいずれかを行います。

    a. メタデータファイルがある場合は、[アプリケーション SAML メタデータファイルをアップロードする] を選択します。次に、[ファイルを選択] を選択してメタデータファイルを検索して選択します。

    b. メタデータファイルがない場合は、[メタデータ値を手動で入力する] のリンクをクリックして、[アプリケーション ACS URL] および [アプリケーション SAML 対象者] の値を指定します。

12. [Submit] を選択してください。追加したアプリケーションの詳細ページが表示されます。

独自の SAML 2.0 アプリケーションをセットアップする

SAML 2.0 を使用した ID フェデレーションを可能にする独自のアプリケーションを設定し、それらを IAM アイデンティティセンターに追加できます。独自の SAML 2.0 アプリケーションを設定する手順のほとんどは、IAM アイデンティティセンターコンソールのアプリケーションカタログから SAML 2.0 アプリケーションを設定するのと同じです。ただし、独自の SAML 2.0 アプリケーションのために、追加の SAML 属性マッピングを提供する必要があります。これらのマッピングは、IAM アイデンティティセンターがアプリケーションに対して SAML 2.0 アサーションを正しく追加できるようにします。アプリケーションを初めて設定するときに、この SAML 属性マッピングを追加できます。また、IAM アイデンティティセンターコンソールのアプリケーションの詳細ページでも、SAML 2.0 属性マッピングを追加できます。

以下の手順を使用して、IAM アイデンティティセンターと SAML 2.0 アプリケーションのサービスプロバイダーとの間で SAML 2.0 の信頼関係を設定します。この手順を開始する前に、信頼をより効率的に設定できるように、サービスプロバイダーの証明書とメタデータエクスチェンジファイルがあることを確認してください。

独自の SAML 2.0 アプリケーションを設定するには

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. [カスタマーマネージド] タブを選択します。
4. [アプリケーションの追加] を選択します。
5. [アプリケーションタイプを選択] ページの [セットアッププリファレンス] で、[セットアップしたいアプリケーションがある] を選択します。
6. [アプリケーションタイプ] で、[SAML 2.0] を選択します。
7. [次へ] を選択します。
8. [アプリケーションの設定] ページの [アプリケーションの設定] で、**MyApp** のようにアプリケーションの [表示名] を入力します。[Description] を入力します。
9. 「IAM Identity Center」で、以下の作業を行います。
    a. IAM Identity Center SAML メタデータファイルの横にある [ダウンロード] を選択して、ID プロバイダーのメタデータをダウンロードします。
    b. [IAM アイデンティティセンターの証明書] で、[ダウンロード] を選択して、ID プロバイダーの証明書をダウンロードします。

> **Note**
>
> 後で、サービスプロバイダーのウェブサイトからカスタムアプリケーションを設定するときに、これらのファイルが必要になります。

10. (オプション) [アプリケーションプロパティ] の下で、[アプリケーション開始 URL]、[リレー状態]、[セッション期間] も指定できます。詳細については、「IAM アイデンティティセンターコンソールのアプリケーションプロパティを理解する」を参照してください。
11. [アプリケーションメタデータ] で [メタデータの値を手動で入力] を選択します。次に、[アプリケーション ACS URL] および [アプリケーション SAML 対象者] の値を指定します。
12. [Submit] を選択してください。追加したアプリケーションの詳細ページが表示されます。

カスタマーマネージドアプリケーションで AWS アカウントアクセスを有効にする

IAM Identity Center でカスタマーマネージドアプリケーションの AWS アカウントアクセスを有効にするには、信頼できるトークン発行者を設定します。信頼できるトークン発行者とは、認証されたユーザーに代わって署名付きトークンを発行する OAuth 2.0 認可サーバーです。IAM Identity Center は、これらのトークンを認証情報と交換して、それらのユーザーに割り当てられた AWS アカウントとロールにアプリケーションからアクセスできるようにします。信頼できるトークン発行者は、AWS マネージドアプリケーションへのアクセスにも使用できます。詳細については、「信頼できるトークン発行者によるアプリケーションの使用」を参照してください。

> **Note**
>
> この機能は、IAM Identity Center の組織インスタンスに対してのみ有効にできます。カスタマーマネージドアプリケーションの `sso:account:access` スコープを有効にできるのは、管理アカウント管理者または委任管理者だけです。メンバーアカウントのアプリケーションビルダーの場合は、IAM Identity Center 管理者に連絡して、アプリケーションのこのスコープを有効にしてください。

仕組み

管理者がカスタマーマネージドアプリケーションの `sso:account:access` スコープを有効にすると、次のワークフローが発生します。

1. ユーザーが外部 ID プロバイダー (IdP) を介してアプリケーションにサインインします。
2. アプリケーションが IdP から署名付き JWT トークンを受け取ります。
3. アプリケーションが、JWT ベアラー付与タイプ (`urn:ietf:params:oauth:grant-type:jwt-bearer`) で `CreateTokenWithIAM` API を呼び出して、このトークンを IAM Identity Center トークンと交換します。この呼び出しには、Signature Version 4 (SigV4) 認証が必要です。詳細については、「IAM Identity Center OIDC API リファレンス」の「CreateTokenWithIAM」を参照してください。
4. アプリケーションは IAM Identity Center トークンを使用してポータル API オペレーション (`ListAccounts`、`ListAccountRoles`、`GetRoleCredentials`) を呼び出し、ユーザーに割り当てられたアカウントとロールを検出して、ユーザーに代わって一時的な AWS 認証情報を取得します。
5. ユーザーは、追加のサインイン手順なしでアプリケーションを介して AWS リソースにアクセスします。

アプリケーションのセットアップ時に更新トークン付与を有効にした場合、`CreateTokenWithIAM` はアクセストークンと共に更新トークンも返します。アプリケーションは、この更新トークンを使用して、JWT ベアラートークンの交換手順全体を繰り返すことなく、新しいアクセストークンを取得できます。アクセストークンを更新するには、`refresh_token` 付与タイプで `CreateTokenWithIAM` を呼び出します。

前提条件

カスタマーマネージドアプリケーションのアカウントアクセスを有効にする前に、以下が必要です。

- JSON Web Tokens (JWT) をサポートする、IAM Identity Center で設定されたカスタマーマネージドアプリケーション。アプリケーションには、認証情報を安全に保存できるバックエンドサーバーコンポーネントが必要です。単一ページアプリケーション (SPA) などのブラウザベースのアプリケーションやその他のパブリッククライアントは、この機能ではサポートされていません。
- アプリケーションにアタッチされた信頼できるトークン発行者。
- AWS Organizations 管理アカウントまたは IAM Identity Center 用の委任管理者アカウントへのアクセス。メンバーアカウントのアプリケーションビルダーが、このスコープを直接有効にすることはできません。

アカウントアクセスを有効にする

カスタマーマネージドアプリケーションの **sso:account:access** スコープを有効にするには

1. 組織の管理アカウントまたは委任管理者アカウントを使用して AWS マネジメントコンソールにサインインします。
2. IAM アイデンティティセンターコンソールを開きます。
3. ナビゲーションペインで、[アプリケーション] を選択します。
4. [カスタマーマネージド] タブを選択します。
5. 設定するアプリケーションの名前を選択します。
6. [AWS アカウントアクセス] セクションで、[AWS アカウントアクセスを有効にする] をオンにします。

アカウントアクセスを有効にすると、アプリケーションから Identity ポータル API オペレーションを呼び出して、アカウントとロールをリストし、認証ユーザーがアクセスを許可されているロールの一時的な AWS 認証情報を取得できます。

> **Important**
>
> アプリケーションの `sso:account:access` スコープを有効にすると、そのアプリケーションは、アクセス許可セットの割り当てを介して、認証ユーザーが利用できるすべてのアカウントとロールにアクセスできます。アプリケーションを特定のアカウントやロールに制限することはできません。この機能を有効にする前に、このアクセスレベルを十分に理解してください。

プログラム的なアクセス

PutApplicationAccessScope API を使用すると、カスタマーマネージドアプリケーションの `sso:account:access` スコープをプログラムで有効にできます。組織の管理アカウントまたは委任管理者アカウントから API を呼び出す必要があります。

AWS CLI

```
aws sso-admin put-application-access-scope \
  --application-arn
 arn:aws:sso::123456789012:application/ssoins-1234567890abcdef/apl-1234567890abcdef \
```

```
  --scope "sso:account:access"
```

API リクエスト:

```
{
  "ApplicationArn":
 "arn:aws:sso::123456789012:application/ssoins-1234567890abcdef/apl-1234567890abcdef",
  "Scope": "sso:account:access"
}
```

アカウントアクセスを無効にするには、同じアプリケーション ARN とスコープ値で `DeleteApplicationAccessScope` API を使用します。

詳細については、「IAM Identity Center API リファレンス」の「PutApplicationAccessScope」と「DeleteApplicationAccessScope」を参照してください。

セキュリティのベストプラクティス

- `sso:account:access` スコープは、認証ユーザーが利用できるすべてのアカウントとロールへのアクセス権をアプリケーションに付与します。特定のアカウントやロールへのアクセスを制限することはできません。このスコープは、このレベルのアクセスを必要とするアプリケーションに対してのみ有効にします。
- IAM Identity Center のアクセストークンと更新トークンはバックエンドサーバーに保持します。クライアント側のコードには絶対に公開しないでください。
- アプリケーションログ、エラーメッセージ、またはデバッグ出力にトークンや認証情報を記録しないでください。
- URL クエリパラメータでトークンを渡さないでください。アクセストークンには `x-amz-sso_bearer_token` ヘッダーを使用します。
- AWS CloudTrail を使用して、アプリケーションによる API コールをモニタリングします。

関連情報

- カスタマーマネージドアプリケーション
- 信頼できるトークン発行者によるアプリケーションの使用
- AWS アクセスポータル API リファレンス

信頼できる ID の伝播の概要

信頼できる ID の伝播は、IAM アイデンティティセンターの機能であり、 の管理者がグループの関連付けなどのユーザー属性に基づいてアクセス許可 AWS のサービス を付与できるようにします。信頼できる ID の伝播では、ID コンテキストが IAM ロールに追加され、AWS リソースへのアクセスをリクエストするユーザーを識別します。このコンテキストは他の AWS のサービス に伝達されます。

ID コンテキストは、 がアクセスリクエストを受信したときに認可の決定を行うために AWS のサービス が使用する情報で構成されます。この情報には、リクエスタ (IAM アイデンティティセンターユーザーなど)、アクセスがリクエストAWS のサービスされる (Amazon Redshift など)、アクセス範囲 (読み取り専用アクセスなど) を識別するメタデータが含まれます。受信側 AWS のサービス は、このコンテキストとユーザーに割り当てられたアクセス許可を使用して、リソースへのアクセスを承認します。

信頼できる ID の伝播の利点

信頼できる ID の伝播により、AWS のサービス の管理者は、ワークフォースの企業 ID を使用して、データなどのリソースにアクセス許可を付与できます。さらに、サービスログまたは AWS CloudTrail を確認することで、誰がどのデータにアクセスしたかを監査できます。IAM アイデンティティセンター管理者の場合、信頼できる ID の伝播を有効にするように他の AWS のサービス 管理者から求められることがあります。

信頼できる ID の伝播の有効化

信頼できる ID の伝播を有効にするプロセスには、次の 2 つのステップが含まれます。

1. IAM アイデンティティセンターを有効にし、既存の ID ソースを IAM アイデンティティセンターに接続する - 既存の ID ソースでワークフォース ID を引き続き管理します。IAM アイデンティティセンターに接続すると、ユースケース内のすべての AWS のサービス が共有できるワークフォースへの参照が作成されます。また、データ所有者が将来のユースケースで使用できるようになります。
2. ユースケースの AWS のサービス を IAM アイデンティティセンターに接続する - 信頼できる ID の伝播ユースケースの各 AWS のサービス の管理者は、それぞれのサービスドキュメントのガイダンスに従って、サービスを IAM アイデンティティセンターに接続します。

> **Note**
>
> ユースケースにサードパーティーまたはお客様が開発したアプリケーションが含まれる場合は、アプリケーションユーザーと IAM アイデンティティセンターを認証する ID プロバイダー間の信頼関係を設定することで、信頼できる ID の伝播を有効にします。これにより、アプリケーションは前述の信頼できる ID の伝播フローを活用できます。
> 詳細については、「信頼できるトークン発行者によるアプリケーションの使用」を参照してください。

信頼できる ID の伝播の仕組み

次の図は、信頼できる ID の伝播の大まかなワークフローを示しています。

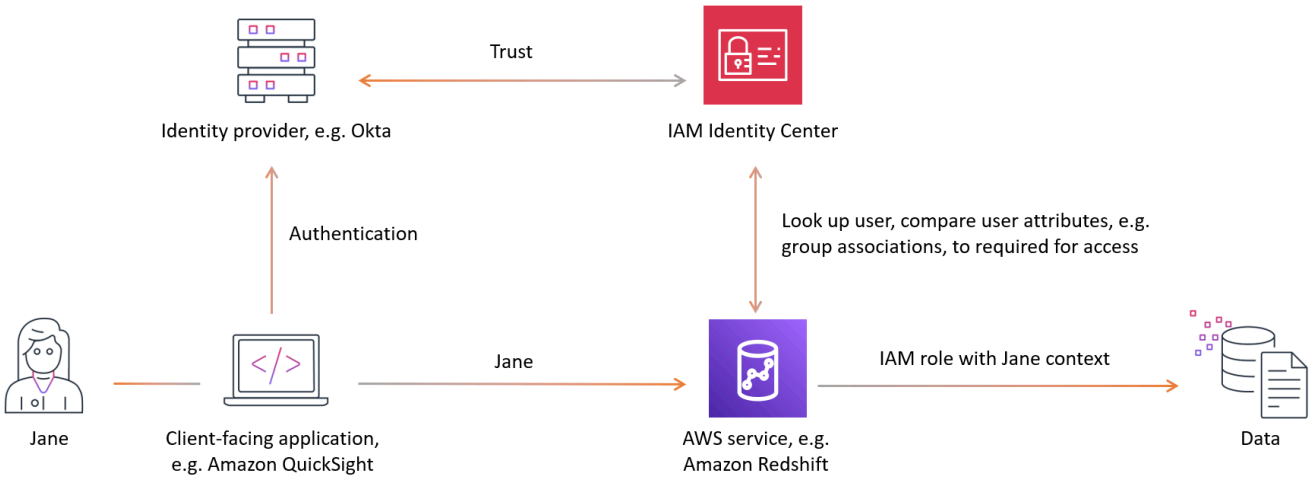


1. ユーザーは、Quick などのクライアント向けアプリケーションで認証します。
2. クライアント向けアプリケーションは、AWS のサービス を使用してデータをクエリするためのアクセスをリクエストし、ユーザーに関する情報を含めます。

   > **Note**
   >
   > 信頼できる ID 伝達のユースケースには、サービスドライバーを使用して AWS のサービス とやり取りするツールが含まれます。これがユースケースに適用されるかどうかは、ユースケースガイダンスで確認できます。

3. AWS のサービス は、IAM アイデンティティセンターでユーザー ID を検証し、グループの関連付けなどのユーザー属性とアクセスに必要なユーザー属性を比較します。AWS のサービス は、ユーザーまたはそのグループに必要なアクセス許可がある限り、アクセスを許可します。
4. AWS のサービス は、AWS CloudTrail およびそのサービスログにユーザー識別子をログに記録する場合があります。詳細については、サービスのドキュメントを確認してください。

次の図は、信頼できる ID の伝播ワークフローで前述したステップの概要を示しています。



トピック

- 前提条件と考慮事項
- 信頼できる ID の伝播のユースケース
- 認可サービス

前提条件と考慮事項

信頼できる ID の伝播を設定する前に、以下の前提条件と考慮事項を確認してください。

トピック

- 前提条件
- 考慮事項
- カスタマーマネージドアプリケーションの考慮事項

前提条件

信頼できる ID の伝播を使用するには、環境が以下の前提条件を満たしていることを確認してください。

- IAM アイデンティティセンターを有効にしてプロビジョニングする
  - 信頼できる ID の伝播を使用するには、ユーザーがアクセスする AWS アプリケーションとサービスが有効になっているのと同じ AWS リージョン で IAM アイデンティティセンターを有効にする必要があります。詳細については、「IAM Identity Center を有効にする」を参照してください。

    - IAM アイデンティティセンター組織インスタンス推奨 — AWS Organizations の管理アカウントで有効にする IAM アイデンティティセンターの組織インスタンスを使用することをお勧めします。IAM アイデンティティセンターの組織インスタンスの管理をメンバーアカウントに委任できます。IAM アイデンティティセンターのアカウントインスタンスを選択する場合、信頼できる ID の伝播を使用してユーザーにアクセスさせるものはすべてのAWS のサービス は、IAM アイデンティティセンターを有効にするのと同じ AWS アカウント に存在する必要があります。詳細については、「IAM アイデンティティセンターのアカウントインスタンス」を参照してください。
  - 既存の ID プロバイダーを IAM アイデンティティセンターに接続し、ユーザーとグループを IAM アイデンティティセンターにプロビジョニングします。詳細については、「IAM アイデンティティセンターの ID ソースに関するチュートリアル」を参照してください。
- 信頼できる ID の伝播ユースケースの AWS マネージドアプリケーションとサービスを IAM アイデンティティセンターに接続します。信頼できる ID の伝播を使用するには、AWS マネージドアプリケーションを IAM アイデンティティセンターと接続する必要があります。

考慮事項

信頼できる ID の伝播を設定し使用するときは、次の考慮事項に留意してください。

- IAM アイデンティティセンターの組織インスタンスとアカウントインスタンス
  - IAM アイデンティティセンターの組織インスタンスは、ユースケースを複数の AWS アカウント、ユーザー、および AWS のサービス に拡張するための最も制御性と柔軟性を提供します。組織インスタンスを使用できない場合は、IAM アイデンティティセンター のアカウントインスタンスでユースケースがサポートされている可能性があります。AWS のサービス IAM アイデンティティセンターのアカウントインスタンスをサポートするユースケースの詳細については、「AWSIAM アイデンティティセンターで使用できる マネージドアプリケーション」を参照してください。
- マルチアカウント許可 (アクセス許可セット) は不要です
  - 信頼できる ID の伝播では、マルチアカウント許可 (アクセス許可セット) を設定する必要はありません。IAM アイデンティティセンターを有効にして、信頼できる ID の伝播にのみ使用できます。

カスタマーマネージドアプリケーションの考慮事項

ワークフォースは、Tableau やカスタム開発アプリケーションなど、 AWS によって管理されていないクライアント向けアプリケーションをユーザーが操作した場合でも、信頼できる ID の伝播からメ

リットを得ることができます。これらのアプリケーションのユーザーは、IAM アイデンティティセンター でプロビジョニングされない場合があります。IAM アイデンティティセンターでは、AWS リソースへのユーザーアクセスをスムーズに認識および承認するために、ユーザーを認証する ID プロバイダーと IAM アイデンティティセンター間の信頼関係を設定できます。詳細については、「信頼できるトークン発行者によるアプリケーションの使用」を参照してください。

さらに、アプリケーションの信頼できる ID の伝播を設定するには、以下が必要です。

- アプリケーションは認証に OAuth 2.0 フレームワークを使用する必要があります。信頼できる ID の伝播は SAML 2.0 統合をサポートしていません。
- アプリケーションは IAM アイデンティティセンターによって認識される必要があります。ユースケースに固有のガイダンスに従ってください。

信頼できる ID の伝播のユースケース

IAM アイデンティティセンター管理者は、ユーザー向けアプリケーションから AWS のサービス への信頼できる ID の伝播の設定を支援するように求められる場合があります。このリクエストをサポートするには、次の情報が必要です。

- ユーザーはどのクライアント向けアプリケーションとインターフェイスしますか?
- どの AWS のサービス がデータのクエリとデータへのアクセスの認可に使用されますか?
- どの AWS のサービス がデータへのアクセスを許可しますか?

サードパーティーアプリケーションやカスタム開発アプリケーションを含まない信頼できる ID の伝播のユースケースを有効にする役割は次のとおりです。

1. IAM アイデンティティセンターを有効にします。
2. 既存の ID ソースを IAM アイデンティティセンターに接続します。

これらのユースケースの信頼できる ID 設定の残りのステップは、接続された AWS のサービス およびアプリケーション内で実行されます。接続された AWS のサービス またはアプリケーションの管理者は、サービス固有の包括的なガイダンスについて、それぞれのユーザーガイドを参照してください。

サードパーティーアプリケーションまたはカスタム開発アプリケーションを含む信頼できる ID の伝播のユースケースを有効にするためのロールには、IAM Identity Center を有効にする の手順と ID のソースを接続する 手順のほかに、以下が含まれます。

1. ID プロバイダー (IdP) のサードパーティーまたはカスタム開発アプリケーションへの接続を設定します。
2. IAM アイデンティティセンターを有効にして、サードパーティーまたはカスタム開発アプリケーションを認識します。
3. IAM アイデンティティセンターで信頼できるトークン発行者として IdP を設定する。詳細については、「信頼できるトークン発行者によるアプリケーションの使用」を参照してください。

接続されたアプリケーションの管理者および AWS のサービス は、サービス固有の包括的なガイダンスについて、それぞれのユーザーガイドを参照してください。

分析、データレイクハウス、機械学習のユースケース

次の分析および機械学習サービスを使用して、信頼できる伝播のユースケースを有効にできます。

- Amazon Redshift - ガイダンスについては、「Amazon Redshift で信頼できる ID の伝播」を参照してください。
- Amazon EMR - ガイダンスについては、「Amazon EMR による信頼できる ID の伝播」を参照してください。
- Amazon Athena - ガイダンスについては、「Amazon Athena による信頼できる ID の伝播」を参照してください。
- SageMaker Studio - ガイダンスについては、「Amazon SageMaker Studio による信頼できる ID の伝播」を参照してください。

その他のユースケース

IAM アイデンティティセンターと信頼できる ID の伝播は、次の追加 AWS のサービス を使用して有効にできます。

- Amazon Q Business - ガイダンスについては、以下を参照してください。
  - IAM アイデンティティセンターを使用したアプリケーションの管理ワークフロー。
  - IAM アイデンティティセンターを使用した Amazon Q Business アプリケーションの設定。
  - IAM アイデンティティセンターの信頼できる ID の伝播を使用して Amazon Q Business を設定します。
- Amazon OpenSearch Service - ガイダンスについては、以下を参照してください。
  - IAM Identity Center Trusted Identity Propagation Support for Amazon OpenSearch Service。

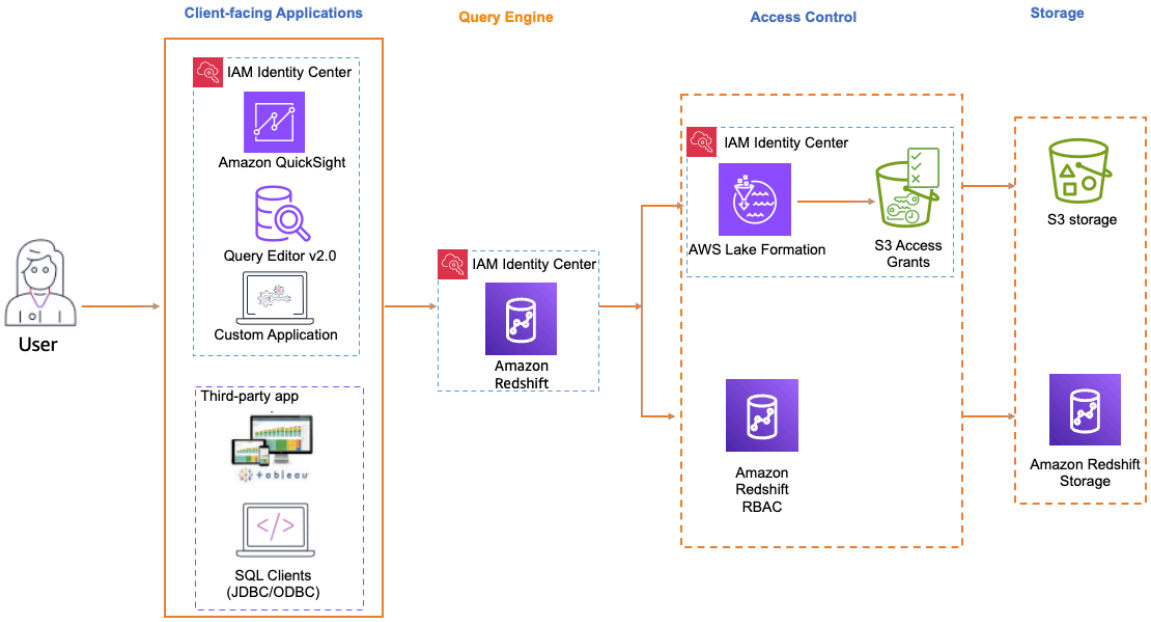
  - Centralized OpenSearch user interface (Dashboards) with Amazon OpenSearch Service。
- AWS Transfer Family - ガイダンスについては、以下を参照してください。
  - Transfer Family ウェブアプリ。

トピック

- Amazon Redshift で信頼できる ID の伝播
- Amazon EMR による信頼できる ID の伝播
- Amazon Athena による信頼できる ID の伝播
- Amazon SageMaker Studio による信頼できる ID の伝播

Amazon Redshift で信頼できる ID の伝播

信頼できる ID の伝播を有効にする手順は、ユーザーが AWS マネージドアプリケーションとやり取りするか、カスタマーマネージドアプリケーションとやり取りするかによって異なります。次の図は、Amazon Redshift または AWS Lake Formation や Amazon S3 Access Grants などの認可サービスが提供するアクセスコントロールを使用して Amazon Redshift データをクエリする、クライアント向けアプリケーション (AWS マネージドまたは AWS 外部) の信頼できる ID の伝播設定を示しています。



Amazon Redshift への信頼できる ID の伝播が有効になっている場合、Redshift 管理者は、ID プロバイダーとして IAM アイデンティティセンターのロールを自動的に作成し、Redshift ロールを IAM ア

イデンティティセンターのグループにマッピングし、Redshift ロールベースのアクセスコントロールを使用してアクセスを許可するように Redshift を設定できます。

サポートされているクライアント向けアプリケーション

AWS マネージドアプリケーション

次の AWS マネージドクライアント向けアプリケーションは、Amazon Redshift への信頼できる ID の伝播をサポートしています。

- Amazon RedshiftQuery Editor V2
- Quick

> **Note**
>
> Amazon Redshift Spectrum を使用して AWS Glue Data Catalog の外部データベースまたはテーブルにアクセスする場合は、きめ細かなアクセスコントロールを提供するように Lake Formation と Amazon S3 Access Grants を設定することを検討してください。

カスタマーマネージドアプリケーション

次のカスタマーマネージドアプリケーションは、Amazon Redshift への信頼できる ID の伝播をサポートしています。

- Tableau TableauDesktop、 Tableau Server、および Tableau Prep を含む
  - Tableau のユーザーに対して信頼できる ID の伝播を有効にするには、「AWSビッグデータブログ」の「IAM アイデンティティセンターを使用した Tableau および Okta と Amazon Redshift の統合」を参照してください。
- SQL クライアント (DBeaver および DBVisualizer)
  - SQL クライアント (DBeaver および DBVisualizer) のユーザーに対して信頼できる ID の伝播を有効にするには、「AWS ビッグデータブログ」の「Integrate Identity Provider (IdP) with Amazon Redshift Query Editor V2 and SQL Client using IAM Identity Center for seamless Single Sign-On」を参照してください。

Amazon Redshift Query Editor V2 で信頼できる ID の伝播を設定する

次の手順では、Amazon Redshift Query Editor V2 から Amazon Redshift への信頼できる ID の伝播を実現する方法について説明します。

前提条件

このチュートリアルを開始する前に、以下を設定する必要があります。

1. IAM アイデンティティセンターを有効にします。組織インスタンスが推奨されます。詳細については、「前提条件と考慮事項」を参照してください。
2. ID のソースから IAM アイデンティティセンターにユーザーとグループをプロビジョニングします。

信頼できる ID 伝播を有効にするには、IAM アイデンティティセンターコンソールで IAM アイデンティティセンターコンソール 管理者が実行するタスクと、Amazon Redshift コンソールで Amazon Redshift 管理者が実行するタスクが含まれます。

IAM アイデンティティセンター管理者が実行するタスク

IAM アイデンティティセンター管理者が次のタスクを完了する必要があります。

1. Amazon Redshift クラスターまたは Serverless インスタンスが存在するアカウントに、次のアクセス許可ポリシーを使用して IAM ロールを作成します。詳細については、「IAM ロールの作成」を参照してください。

   - 次のポリシーの例には、このチュートリアルを完了するために必要なアクセス許可が含まれています。このポリシーを使用するには、サンプルポリシーの##################を独自の情報に置き換えます。その他の手順については、「ポリシーの作成」または「ポリシーの編集」を参照してください。

     アクセス許可ポリシー:

     JSON

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

```
            "Effect": "Allow",
            "Action": [
                "redshift:DescribeQev2IdcApplications",
                "redshift-serverless:ListNamespaces",
                "redshift-serverless:ListWorkgroups",
                "redshift-serverless:GetWorkgroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowIDCPermissions",
            "Effect": "Allow",
            "Action": [
                "sso:DescribeApplication",
                "sso:DescribeInstance"
            ],
            "Resource": [
                "arn:aws:sso:::instance/Your-IAM-Identity-Center-Instance
 ID",
                "arn:aws:sso::111122223333:application/Your-IAM-Identity-
Center-Instance-ID/*"
            ]
        }
    ]
}
```

信頼ポリシー:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "redshift-serverless.amazonaws.com",
                    "redshift.amazonaws.com"
                ]
            },
```

```
            "Action": [
                "sts:AssumeRole",
                "sts:SetContext"
            ]
        }
    ]
}
```

2. IAM アイデンティティセンターが有効になっているAWS Organizations管理アカウントに許可セットを作成します。次のステップでこれを使用して、フェデレーティッドユーザーが Redshift クエリエディタ V2 にアクセスできるようにします。

   a. IAM アイデンティティセンターコンソールに移動し、 [マルチアカウント許可] で、[アクセス許可セット] を選択します。

   b. [Create permission set] (アクセス許可セットの作成) を選択します。

   c. [カスタムアクセス許可セット] を選択し、[次へ] を選択します。

   d. [AWS 管理ポリシー] で、**AmazonRedshiftQueryEditorV2ReadSharing** を選択します。

   e. [インラインポリシー] で、次のポリシーを追加します。

      JSON

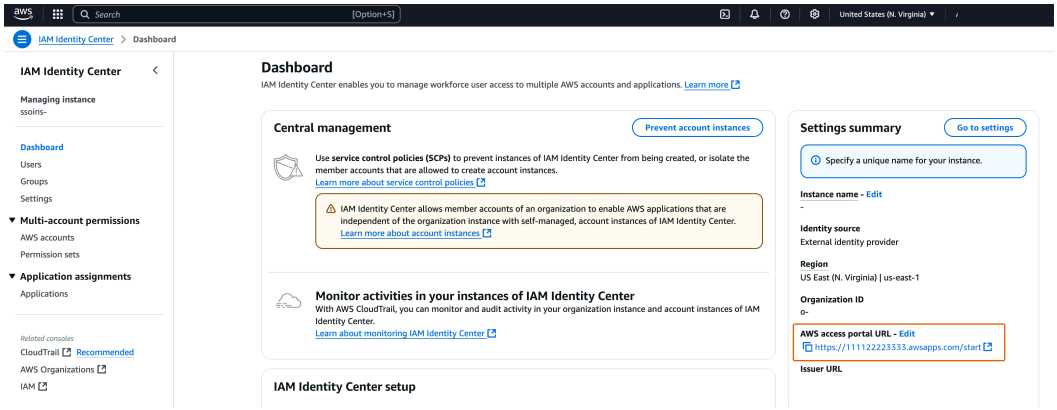
```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "redshift:DescribeQev2IdcApplications",
                "redshift-serverless:ListNamespaces",
                "redshift-serverless:ListWorkgroups",
                "redshift-serverless:GetWorkgroup"
            ],
            "Resource": "*"
        }
    ]
}
```

f. [次へ] を選択し、アクセス許可セット名の名前を指定します。例えば、**Redshift-Query-Editor-V2**。

g. [リレー状態 – オプション] で、`https://your-region.console.aws.amazon.com/sqlworkbench/home` の形式を使用して、デフォルトのリレー状態をクエリエディタ V2 URL に設定します。

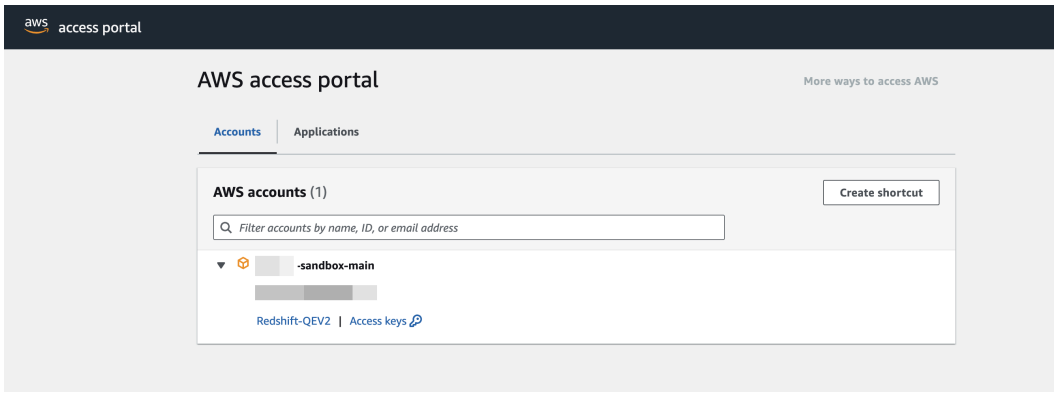
h. 設定を確認し、[作成] を選択します。

i. IAM アイデンティティセンターダッシュボードに移動し、[概要の設定] セクションから AWS アクセスポータル URL をコピーします。



j. 新しいシークレットブラウザウィンドウを開き、URL を貼り付けます。

これにより、AWS アクセスポータルに移動し、IAM アイデンティティセンターユーザーでサインインしていることを確認できます。



アクセス許可セットの詳細については、「権限セットを使用して AWS アカウントを管理する」を参照してください。

3. Redshift クエリエディタ V2 へのフェデレーティッドユーザーのアクセスを有効にします。

a. AWS Organizations 管理アカウントで、IAM アイデンティティセンターを開きます。

b. ナビゲーションペインの [マルチアカウント権限] で、AWS アカウント を選択します。

c. [AWS アカウント] ページで、アクセスを割り当てる AWS アカウント を選択します。

d. 「ユーザーまたはグループを割り当て」を選択します。

e. [ユーザーとグループの割り当て] ページで、アクセス許可セットを作成するユーザーまたはグループを選択します。その後、[Next] を選択します。

f. [アクセス許可セットの割り当て] ページで、前のステップで作成したアクセス許可セットを選択します。その後、[Next] を選択します。

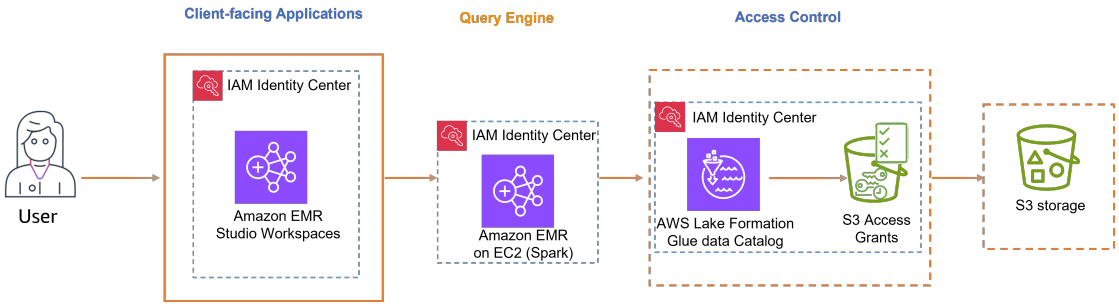
g. [割り当てを確認と送信] ページで選択内容を確認し、[送信] を選択します。

Amazon Redshift 管理者が実行するタスク

Amazon Redshift への信頼できる ID の伝播を有効にするには、Amazon Redshift クラスター管理者または Amazon Redshift Serverless 管理者が Amazon Redshift コンソールで多数のタスクを実行する必要があります。詳細については、 AWS ビッグデータブログの「Integrate Identity Provider (IdP) with Amazon Redshift Query Editor V2 and SQL Client using IAM Identity Center for seamless Single Sign-On」を参照してください。

Amazon EMR による信頼できる ID の伝播

次の図は、AWS Lake Formation と Amazon S3 Access Grants が提供するアクセスコントロールを備えた Amazon EC2 での Amazon EMR を使用した、Amazon EMR Studio の信頼できる ID 伝播設定を示しています。



サポートされているクライアント向けアプリケーション

- Amazon EMR Studio

信頼できる ID の伝播を有効にするには、次の手順に従います。

- Amazon EMR クラスターのクライアント向けアプリケーションとして Amazon EMR Studio をセットアップします。

- Apache Spark を使用して Amazon EC2 で Amazon EMR クラスターをセットアップします。
- 推奨: AWS Lake Formation と Amazon S3 Access Grants は、S3 内の AWS Glue Data Catalog および基盤となるデータロケーションへのきめ細かなアクセスコントロールを提供します。

Amazon EMR Studio で信頼できる ID の伝播を設定する

次の手順では、Apache Spark を実行している Amazon Athena ワークグループまたは Amazon EMR クラスターに対するクエリで、信頼できる ID の伝播用に Amazon EMR Studio を設定する方法について説明します。

前提条件

このチュートリアルを開始する前に、以下を設定する必要があります。

1. IAM アイデンティティセンターを有効にします。組織インスタンスが推奨されます。詳細については、「前提条件と考慮事項」を参照してください。
2. ID のソースから IAM アイデンティティセンターにユーザーとグループをプロビジョニングします。

Amazon EMR Studio からの信頼できる ID 伝播の設定を完了するには、EMR Studio 管理者が次のステップを実行する必要があります。

ステップ 1. EMR Studio に必要な IAM ロールを作成する

このステップでは、Amazon EMR Studio 管理者は と IAM サービスロール、および EMR Studio の IAM ユーザーロールを作成します。

1. EMR Studio サービスロールを作成する - EMR Studio はこの IAM ロールを引き受けて、ワークスペースとノートブックを安全に管理し、クラスターに接続し、データインタラクションを処理します。

   a. IAM コンソール (https://console.aws.amazon.com/iam/) に移動し、IAM ロールを作成します。

   b. AWS のサービス を信頼されたエンティティとして選択し、Amazon EMR を選択します。次のポリシーをアタッチして、ロールのアクセス許可と信頼関係を定義します。

      これのポリシーを使用するには、サンプルポリシーの##################を独自の情報に置き換えます。その他の手順については、「ポリシーの作成」または「ポリシーの編集」を参照してください。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ObjectActions",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "Your-AWS-Account-ID"
                }
            }
        },
        {
            "Sid": "BucketActions",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetEncryptionConfiguration"
            ],
            "Resource": [
                "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "Your-AWS-Account-ID"
                }
            }
        }
    ]
}
```

すべてのサービスロールのアクセス許可のリファレンスについては、「EMR Studio サービスロールのアクセス許可」を参照してください。

2. IAM アイデンティティセンター認証用の EMR Studio ユーザーロールを作成する - EMR Studio は、ユーザーが IAM アイデンティティセンターを通じてサインインしてワークスペース、EMR クラスター、ジョブ、git リポジトリを管理するときに、このロールを引き受けます。このロールは、信頼できる ID の伝播ワークフローを開始するために使用されます。

> **Note**
>
> EMR Studio ユーザーロールには、AWS Glue カタログ内のテーブルの Amazon S3 ロケーションにアクセスするためのアクセス許可を含める必要はありません。AWS Lake Formation アクセス許可と登録されたレイクロケーションは、一時的なアクセス許可を受け取るために使用されます。

次のポリシー例は、EMR Studio のユーザーが Athena ワークグループを使用してクエリを実行できるようにするロールで使用できます。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDefaultEC2SecurityGroupsCreationInVPCWithEMRTags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSecurityGroup"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/for-use-with-amazon-emr-managed-
policies": "true"
                }
            }
```

```
        },
        {
            "Sid": "AllowAddingEMRTagsDuringDefaultSecurityGroupCreation",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true",
                    "ec2:CreateAction": "CreateSecurityGroup"
                }
            }
        },
        {
            "Sid": "AllowSecretManagerListSecrets",
            "Action": [
                "secretsmanager:ListSecrets"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Sid": "AllowSecretCreationWithEMRTagsAndEMRStudioPrefix",
            "Effect": "Allow",
            "Action": "secretsmanager:CreateSecret",
            "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true"
                }
            }
        },
        {
            "Sid": "AllowAddingTagsOnSecretsWithEMRStudioPrefix",
            "Effect": "Allow",
            "Action": "secretsmanager:TagResource",
            "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*"
        },
        {
            "Sid": "AllowPassingServiceRoleForWorkspaceCreation",
```

```
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::111122223333:role/service-
role/AmazonEMRStudio_ServiceRole_Name"
            ],
            "Effect": "Allow"
        },
        {
            "Sid": "AllowS3ListAndLocationPermissions",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        },
        {
            "Sid": "AllowS3ReadOnlyAccessToLogs",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-logs-Your-AWS-Account-ID-Region/
elasticmapreduce/*"
            ],
            "Effect": "Allow"
        },
        {
            "Sid": "AllowAthenaQueryExecutions",
            "Effect": "Allow",
            "Action": [
                "athena:StartQueryExecution",
                "athena:GetQueryExecution",
                "athena:GetQueryResults",
                "athena:StopQueryExecution",
                "athena:ListQueryExecutions",
                "athena:GetQueryResultsStream",
                "athena:ListWorkGroups",
                "athena:GetWorkGroup",
                "athena:CreatePreparedStatement",
                "athena:GetPreparedStatement",
                "athena:DeletePreparedStatement"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "AllowGlueSchemaManipulations",
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:GetPartition",
                "glue:GetPartitions"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowQueryEditorToAccessWorkGroup",
            "Effect": "Allow",
            "Action": "athena:GetWorkGroup",
            "Resource": "arn:aws:athena:*:111122223333:workgroup*"
        },
        {
            "Sid": "AllowConfigurationForWorkspaceCollaboration",
            "Action": [
                "elasticmapreduce:UpdateEditor",
                "elasticmapreduce:PutWorkspaceAccess",
                "elasticmapreduce:DeleteWorkspaceAccess",
                "elasticmapreduce:ListWorkspaceAccessIdentities"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "elasticmapreduce:ResourceTag/creatorUserId":
"${aws:userId}"
                }
            }
        },
        {
            "Sid": "DescribeNetwork",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
```

```
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ListIAMRoles",
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AssumeRole",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "*"
        }
    ]
}
```

次の信頼ポリシーは、EMR Studio がロールを引き受けることを許可します。

> **Note**
>
> EMR Studio WorkSpaces と EMR Notebooks を利用するには、追加のアクセス許可が必要です。詳細については、「EMR Studio ユーザーのアクセス許可ポリシーを作成する」を参照してください。

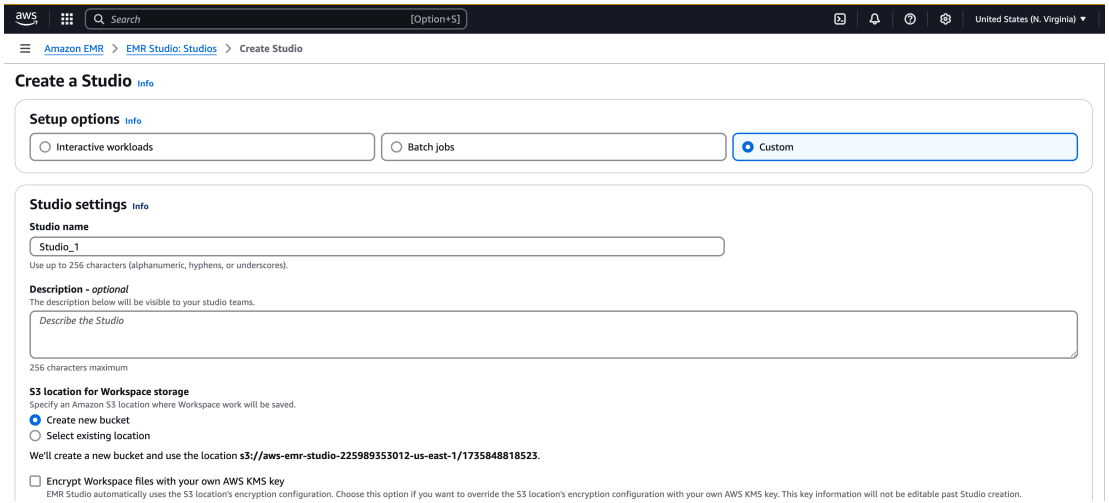
詳細については、次のリンクを参照してください。

- 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
- EMR Studio サービスロールのアクセス許可

ステップ 2. EMR Studio を作成および設定する

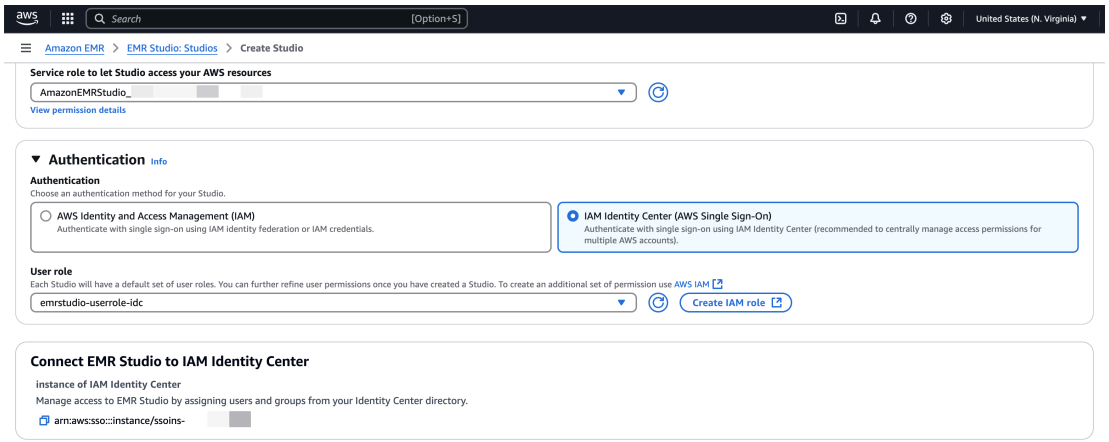
このステップでは、EMR Studio コンソールで Amazon EMR Studio を作成し、ステップ 1. EMR Studio に必要な IAM ロールを作成する で作成した IAM ロールを使用します。

1. EMR Studio コンソールに移動し、[Studio の作成] と [カスタムセットアップ] オプションを選択します。新しいバケットを作成するか、既存の S3 バケットを使用します。このチェックボックスをオンにすると、独自の KMS キーを使用してワークスペースファイルを暗号化できます。詳細については、 を参照してください。AWS Key Management Service



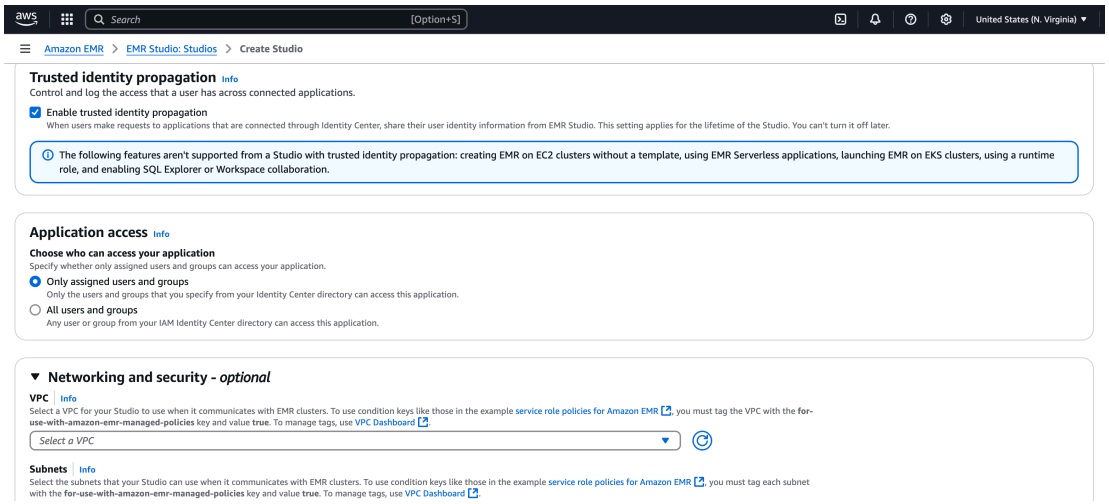
2. [Studio がリソースにアクセスできるようにするサービスロール]で、メニューから ステップ 1. EMR Studio に必要な IAM ロールを作成する で作成したサービスロールを選択します。

3. [認証] の下にある [IAM アイデンティティセンター] を選択します。ステップ 1. EMR Studio に必要な IAM ロールを作成する で作成されたユーザーロールを選択します。



4. [信頼できる ID の伝播] チェックボックスをオンにします。[アプリケーションアクセス] セクションで [割り当てられたユーザーとグループのみ] を選択します。これにより、このスタジオへのアクセスを許可されたユーザーとグループのみに許可できます。

5. (オプション) - EMR クラスターでこの Studio を使用している場合は、VPC とサブネットを設定できます。

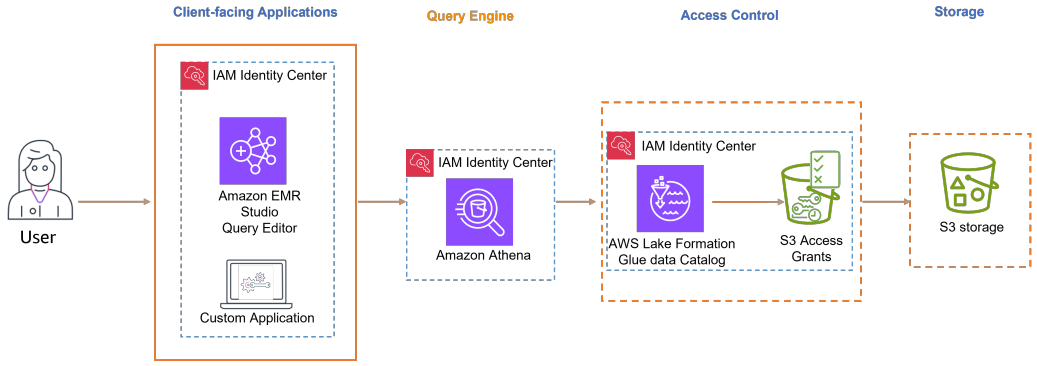


6. すべての詳細を確認し、[Studio を作成]を選択します。
7. Athena WorkGroup または EMR クラスターを設定したら、Studio の URL にサインインして次の操作を行います。
   a. クエリエディタを使用して Athena クエリを実行します。
   b. Jupyter ノートブックを使用してワークスペースで Spark ジョブを実行します。

Amazon Athena による信頼できる ID の伝播

信頼できる ID の伝播を有効にする手順は、ユーザーが AWS マネージドアプリケーションとやり取りするか、カスタマーマネージドアプリケーションとやり取りするかによって異なります。次の図は、Amazon Athena を使用して Amazon S3 データをクエリし、AWS Lake Formation および Amazon S3 Access Grants によってアクセスコントロールされる、クライアント向けアプリケーション (AWS マネージドまたは AWS 外部) の信頼できる ID の伝播設定を示しています。

> **Note**
>
> - Amazon Athena での信頼できる ID の伝播には Trino を使用する必要があります。
> - ODBC および JDBC ドライバーを介して Amazon Athena に接続された Apache Spark および SQL クライアントはサポートされていません。



AWS マネージドアプリケーション

次の AWS マネージドクライアント向けアプリケーションは、Athena による信頼できる ID 伝播をサポートしています。

- Amazon EMR Studio

信頼できる ID の伝播を有効にするには、次の手順に従います。

- Amazon EMR Studioを Athena のクライアント向けアプリケーションとしてセットアップします。信頼できる ID の伝播が有効になっている場合、Athena クエリを実行するには、EMR Studio のクエリエディタが必要です。
- Athena ワークグループをセットアップします。
- AWS Lake Formation を設定して、IAM アイデンティティセンターのユーザーまたはグループに基づいて AWS Glue テーブルのきめ細かなアクセスコントロールを有効にします。
- Amazon S3 Access Grants をセットアップして、S3 の基盤となるデータロケーションへの一時的なアクセスを有効にします。

> **Note**
>
> Lake Formation と Amazon S3 Access Grants はどちらも、AWS Glue Data Catalog へのアクセスコントロールと Amazon S3 での Athena のクエリ結果に必要です。

カスタマーマネージドアプリケーション

カスタム開発アプリケーションのユーザーに対して信頼できる ID 伝播を有効にするには、「AWS セキュリティブログ」の「Access AWS のサービス services programmatically using trusted identity

propagation」を参照してください。https://aws.amazon.com/blogs/security/access-aws-services-programmatically-using-trusted-identity-propagation/

Amazon Athena ワークグループによる信頼できる ID 伝播の設定

次の手順では、信頼できる ID の伝播用に Amazon Athena ワークグループを設定する手順を説明します。

前提条件

このチュートリアルを開始する前に、以下を設定する必要があります。

1. IAM アイデンティティセンターを有効にします。組織インスタンスが推奨されます。詳細については、「前提条件と考慮事項」を参照してください。
2. ID のソースから IAM アイデンティティセンターにユーザーとグループをプロビジョニングします。
3. この設定には、Amazon EMR Studio、AWS Lake Formation、および Amazon S3 Access Grants が必要です。

Athena による信頼できる ID の伝播の設定

Athena で信頼できる ID の伝播を設定するには、Athena 管理者が以下を行う必要があります。

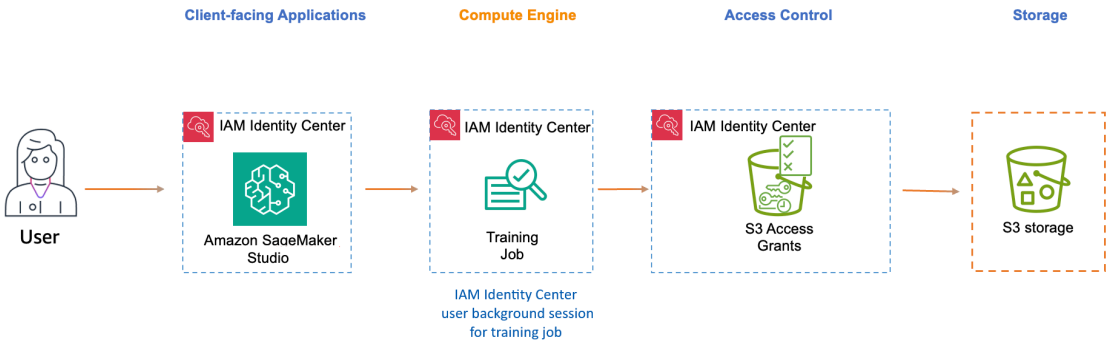
1. IAM アイデンティティセンターが有効な Athena ワークグループを使用する際の考慮事項と制限事項を確認します。
2. IAM アイデンティティセンターが有効な Athena ワークグループを作成します。

Amazon SageMaker Studio による信頼できる ID の伝播

Amazon SageMaker Studio は IAM アイデンティティセンターと統合され、ユーザーバックグラウンドセッションと信頼できる ID の伝播をサポートします。ユーザーバックグラウンドセッションを使用すると、ユーザーは SageMaker Studio で長時間実行されるジョブを開始できます。ジョブの実行中にサインインしたままにする必要はありません。ジョブは、ジョブを開始したユーザーのアクセス許可を使用して、すぐにバックグラウンドで実行されます。ユーザーがコンピュータをオフにした場合、IAM アイデンティティセンターのサインインセッションの有効期限が切れた場合、またはユーザーが AWS アクセスポータルからサインアウトした場合でも、ジョブは引き続き実行できます。ユーザーバックグラウンドセッションのデフォルトのセッション期間は 7 日間ですが、最大期間として 90 日間を指定できます。信頼できる ID 伝播により、ユーザーの ID またはグループメン

バーシップに基づいて Amazon S3 バケットなどの AWS リソースにきめ細かなアクセスを提供できます。

次の図は、Amazon S3 バケットに保存されているデータにアクセスできる SageMaker Studio の信頼できる ID の伝播設定を示しています。ユーザーバックグラウンドセッションは IAM アイデンティティセンター で有効になっており、SageMaker Studio トレーニングジョブをバックグラウンドで実行できます。トレーニングデータのアクセスコントロールは、Amazon S3 Access Grants によって提供されます。



AWS マネージドアプリケーション

次の AWS マネージドクライアント向けアプリケーションは、信頼できる ID 伝播をサポートしています。

- Amazon SageMaker Studio

信頼できる ID の伝播とユーザーバックグラウンドセッションを有効にするには、次の手順に従います。

- SageMaker Studio をクライアント向けアプリケーションとしてセットアップします。
- Amazon S3 Access Grants をセットアップして、Amazon S3 の基盤となるデータロケーションへの一時的なアクセスを有効にします。

Sagemaker Studio で信頼できる ID 伝播を設定する

次の手順では、信頼できる ID の伝播とユーザーバックグラウンドセッション用に SageMaker Studio を設定する手順を説明します。

前提条件

このチュートリアルを開始する前に、まず以下のタスクを完了する必要があります。

1. IAM アイデンティティセンターを有効にします。組織インスタンスが必要です。詳細については、「前提条件と考慮事項」を参照してください。
2. ID のソースから IAM アイデンティティセンターにユーザーとグループをプロビジョニングします。
3. IAM アイデンティティセンターコンソールでユーザーバックグラウンドセッションが有効になっていることを確認します。デフォルトでは、ユーザー背景セッションは有効になっており、セッション期間は 7 日間に設定されています。この期間は、変更することができます。

SageMaker Studio から信頼できる ID の伝播を設定するには、SageMaker Studio 管理者が次のステップを実行する必要があります。

ステップ 1: 新規または既存の SageMaker Studio ドメインで信頼できる ID の伝播を有効にする

SageMaker はドメインを使用して、ユーザープロファイル、アプリケーション、関連するリソースを整理します。信頼できる ID の伝播を有効にするには、次の手順で説明するように、SageMaker Studio ドメインを作成するか、既存のドメインを変更する必要があります。

1. SageMaker AI コンソールを開き、[ドメイン]に移動して、次のいずれかを実行します。
   - [組織向けのセットアップ] を使用して、新しい SageMaker Studio ドメインを作成します。

     [組織向けのセットアップ]を選択し、次の操作を行います。
     - 認証方法として AWS アイデンティティセンター を選択します。
     - [このドメインですべてのユーザーの信頼できる ID 伝播を有効にする] チェックボックスをオンにします。
   - 既存の SageMaker Studio ドメインを変更します。
     - 認証に IAM アイデンティティセンターを使用する既存のドメインを選択します。

       > **Important**
       >
       > 信頼できる ID の伝播は、認証に IAM アイデンティティセンターを使用する SageMaker Studio ドメインでのみサポートされます。ドメインが認証に IAM を使

用している場合、認証方法を変更することはできないため、信頼できる ID の伝播を有効にすることはできません。

- ドメイン設定を編集します。[認証とアクセス許可] の設定を編集して、信頼できる ID の伝播を有効にします。

2. ステップ 2: デフォルトのドメイン実行ロールを設定するに進みます。このロールは、SageMaker Studio ドメインのユーザーが Amazon S3 などの他の AWS サービスにアクセスするために必要です。

ステップ 2: デフォルトのドメイン実行ロールとロール信頼ポリシーを設定する

ドメイン実行ロールは、SageMaker Studio ドメインがドメイン内のすべてのユーザーに代わって引き受ける IAM ロールです。このロールに割り当てるアクセス許可によって、SageMaker Studio が実行できるアクションが決まります。

1. ドメイン実行ロールを作成または選択するには、次のいずれかを実行します。

   - [組織向けのセットアップ] を使用してロールを作成または選択します。
     - SageMaker AI コンソールを開き、「ステップ 2: ロールと ML アクティビティを設定して新しいドメイン実行ロールを作成するか、既存のロールを選択する」のコンソールガイダンスに従います。
     - 残りのセットアップステップを完了して、SageMaker Studio ドメインを作成します。
   - 実行ロールを手動で作成します。
     - IAM コンソールを開き、実行ロールを自分で作成します。

2. ドメイン実行ロールにアタッチされている信頼ポリシーを更新して、`sts:AssumeRole` と `sts:SetContext` の 2 つのアクションを含めます。SageMaker Studio ドメインの実行ロールを検索する方法については、「ドメイン実行ロールを取得する」を参照してください。

   信頼ポリシーは、ロールを引き受けることができる ID を指定します。このポリシーは、SageMaker Studio サービスがドメイン実行ロールを引き受けられるようにするために必要です。これら 2 つのアクションを追加して、ポリシーに次のように表示されるようにします。

```
{

    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "sagemaker.amazonaws.com"
                ]
            },
            "Action": [
                "sts:AssumeRole",
                "sts:SetContext"
            ]
        }
    ]
}
```

ステップ 3: ドメイン実行ロールに必要な Amazon S3 Access Grant アクセス許可を検証する

Amazon S3 Access Grants を使用するには、以下のアクセス許可を含むアクセス許可ポリシーを (インラインポリシーまたはカスタマー管理ポリシーとして) SageMaker Studio ドメイン実行ロールにアタッチする必要があります。

```
{

    "Version": "2012-10-17",

    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetDataAccess",
                "s3:GetAccessGrantsInstanceForPrefix"
                ],
            "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
        }
    ]
}
```

これらのアクセス許可を含むポリシーがない場合は、「AWS Identity and Access Managementユーザーガイド」の「IAM ID アクセス許可の追加と削除」の手順に従います。

ステップ 4: グループとユーザーをドメインに割り当てる

「グループとユーザーを追加する」の手順に従って、グループとユーザーを SageMaker Studio ドメインに割り当てます。

ステップ 5: Amazon S3 Access Grants を設定する

Amazon S3 Access Grants を設定するには、「IAM アイデンティティセンターを介した信頼できる ID 伝播のための Amazon S3 Access Grants の設定」のステップに従います。ステップバイステップの手順を使用して、以下のタスクを完了します。

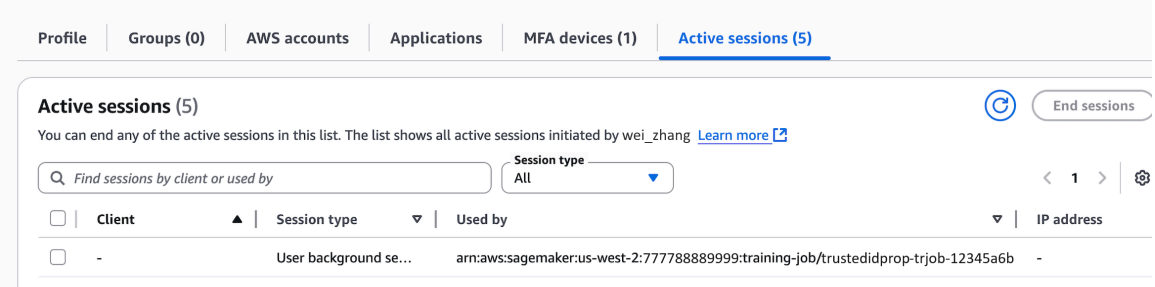
1. Amazon S3 Access Grants インスタンスを作成します。
2. そのインスタンスにロケーションを登録します。
3. 特定の IAM アイデンティティセンターユーザーまたはグループが、指定された Amazon S3 ロケーションまたはそれらのロケーション内のサブセット (特定のプレフィックスなど) にアクセスできるようにする権限を作成します。

ステップ 6: SageMaker トレーニングジョブを送信し、ユーザーバックグラウンドセッションの詳細を表示する

SageMaker Studio で、新しい Jupyter Notebook を起動し、トレーニングジョブを送信します。ジョブの実行中に、次の手順を実行してセッション情報を表示し、ユーザーのバックグラウンドセッションコンテキストがアクティブであることを確認します。

1. IAM Identity Center コンソール を開きます。
2. ユーザー を選択します。
3. [ユーザー] ページで、セッションを管理したいユーザーのユーザー名を選択します。これにより、ユーザーの情報が表示されるページに移動します。
4. ユーザーのページで、[アクティブセッション] タブを選択します。[アクティブセッション] の横の括弧内の数字は、このユーザーのアクティブセッション数を示します。
5. セッションを使用しているジョブの Amazon リソースネーム (ARN) でセッションを検索するには、[セッションタイプ] リストで [ユーザーバックグラウンドセッション] を選択し、検索ボックスにジョブ ARN を入力します。

以下は、ユーザーバックグラウンドセッションを使用しているトレーニングジョブがユーザーの [アクティブセッション] タブにどのように表示されるかの例です。



ステップ 7: CloudTrail ログを表示して CloudTrail で信頼できる ID の伝播を検証する

信頼できる ID の伝播を有効にすると、 onBehalfOf 要素の下の CloudTrail イベントログにアクションが表示されます。には、トレーニングジョブを開始した IAM アイデンティティセンターユーザーの ID userId が反映されます。次の CloudTrail イベントは、信頼できる ID の伝播プロセスをキャプチャします。

```
                        "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA123456789EXAMPLE:SageMaker",
    "arn": "arn:aws:sts::111122223333:assumed-role/SageMaker-
ExecutionRole-20250728T125817/SageMaker",
    "accountId": "111122223333",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROA123456789EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/service-role/SageMaker-
ExecutionRole-20250728T125817",
            "accountId": "111122223333",
            "userName": "SageMaker-ExecutionRole-20250728T125817"
        },
        "attributes": {
            "creationDate": "2025-07-29T17:17:10Z",
            "mfaAuthenticated": "false"
        }
    },
    "onBehalfOf": {
        "userId": "2801d3e0-f0e1-707f-54e8-f558b19f0a10",
        "identityStoreArn": "arn:aws:identitystore::777788889999:identitystore/
d-1234567890"
    }
},
```

ランタイムの考慮事項

管理者が、ユーザーバックグラウンドセッション期間よりも短い長時間実行されるトレーニングジョブまたは処理ジョブに MaxRuntimeInSeconds を設定すると、SageMaker Studio は MaxRuntimeInSeconds またはユーザーバックグラウンドセッション期間の最小値でジョブを実行します。

MaxRuntimeInSeconds の詳細については、「Amazon SageMaker API リファレンス」の「`CreateTrainingJob` StoppingCondition」パラメータのガイダンスを参照してください。

認可サービス

すべての分析とデータレイクハウスのユースケースで、以下を使用してきめ細かなアクセスコントロールを実現できます。

- AWS Lake Formationガイダンスについては、「」を参照してください。AWS Lake Formation を IAM アイデンティティセンターで設定する
- Amazon S3 Access Grants - ガイダンスについては、「IAM アイデンティティセンターを使用した Amazon S3 Access Grants の設定」を参照してください。

AWS Lake Formation を IAM アイデンティティセンターで設定する

AWS Lake Formation は、AWS でのデータレイクの作成と管理を簡素化するマネージドサービスです。データ収集、カタログ化、セキュリティを自動化し、さまざまなデータ型を保存および分析するための一元化されたリポジトリを提供します。Lake Formation は、きめ細かなアクセスコントロールを提供し、さまざまな AWS 分析サービスと統合することで、組織はデータレイクを効率的にセットアップ、保護し、インサイトを得ることができます。

Lake Formation が IAM アイデンティティセンターと信頼できる ID の伝播を使用してユーザー ID に基づいてデータアクセス許可を付与できるようにするには、次の手順に従います。

前提条件

このチュートリアルを開始する前に、以下を設定する必要があります。

- IAM アイデンティティセンターを有効にします。組織インスタンスが推奨されます。詳細については、「前提条件と考慮事項」を参照してください。

信頼できる ID の伝播を設定するステップ

1. 「Lake Formation と IAM アイデンティティセンターとの接続」のガイダンスに従って、IAM アイデンティティセンターを AWS Lake Formation と統合します。

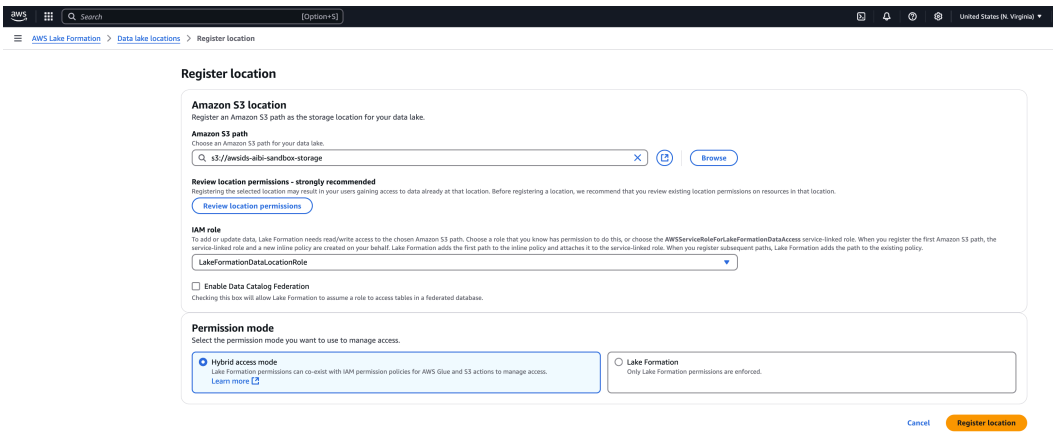
> **Important**
>
> AWS Glue Data Catalog テーブルがない場合は、AWS Lake Formation を使用して IAM アイデンティティセンターのユーザーとグループにアクセス許可を付与するためにテーブルを作成する必要があります。詳細については、「AWS Glue Data Catalog でのオブジェクトの作成」を参照してください。

2. データレイクの場所を登録します。

   Glue テーブルのデータが保存されている S3 の場所を登録します。これにより、Lake Formation はテーブルのクエリ時に必要な S3 ロケーションへの一時的なアクセスをプロビジョニングし、サービスロール (WorkGroup で設定された Athena サービスロールなど) に S3 アクセス許可を含める必要がなくなります。

   a. AWS Lake Formation コンソールのナビゲーションペインの[管理] セクションにある [データレイクの場所] に移動します。[ロケーションを登録] を選択します。

      これにより、Lake Formation は S3 データロケーションにアクセスするために必要なアクセス許可を持つ一時的な IAM 認証情報をプロビジョニングできます。



   b. Amazon S3 パスフィールドに AWS Glue テーブルのデータロケーションの S3 パスを入力します。

   c. [IAM ロール] セクションで、信頼された ID の伝播で使用する場合は、サービスにリンクされたロールを選択しないでください。次のアクセス許可で別のロールを作成します。

これらのポリシーを使用するには、サンプルポリシーの##################を独自の情報に置き換えます。その他の手順については、「ポリシーの作成」または「ポリシーの編集」を参照してください。アクセス許可ポリシーは、パスで指定された S3 の場所へのアクセスを許可する必要があります。

i. アクセス許可ポリシー:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::Your-S3-Bucket/*"
            ]
        },
        {
            "Sid":
 "LakeFormationDataAccessPermissionsForS3ListBucket",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::Your-S3-Bucket"
            ]
        },
        {
            "Sid": "LakeFormationDataAccessServiceRolePolicy",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
```

```
            "Resource": [
                "arn:aws:s3:::*"
            ]
        }
    ]
}
```

ii. 信頼関係: これには、信頼できる ID の伝播に必要な `sts:SectContext` を含める必要があります。

JSON

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

> **Note**
>
> ウィザードによって作成された IAM ロールはサービスにリンクされたロールであり、`sts:SetContext` は含まれません。

d. IAM ロールを作成したら、[場所の登録]を選択します。

AWS アカウント 間の Lake Formation による信頼できる ID の伝播

AWS Lake Formation は、AWS アカウント 間でテーブルを共有するために AWS Resource Access Manager (RAM) の使用をサポートしており、付与者アカウントと被付与者アカウントが同じ AWS

リージョン にあり、同じ AWS Organizations にあり、かつ IAM アイデンティティセンターの同じ組織インスタンスを共有している場合、信頼できる ID 伝播と連携します。詳細については、「Lake Formation でのクロスアカウントデータ共有」を参照してください。

IAM アイデンティティセンターを使用した Amazon S3 Access Grants の設定

Amazon S3 Access Grants は、ID ベースのきめ細かなアクセスコントロールを S3 ロケーションに付与する柔軟性を提供します。Amazon S3 Access Grants を使用すると、企業のユーザーやグループに Amazon S3 バケットアクセスを直接付与できます。IAM アイデンティティセンターで S3 Access Grants を有効にし、信頼できる ID の伝播を実現するには、次の手順に従います。

前提条件

このチュートリアルを開始する前に、以下を設定する必要があります。

- IAM アイデンティティセンターを有効にします。組織インスタンスが推奨されます。詳細については、「前提条件と考慮事項」を参照してください。

IAM アイデンティティセンターを介した信頼できる ID 伝播のための S3 Access Grants の設定

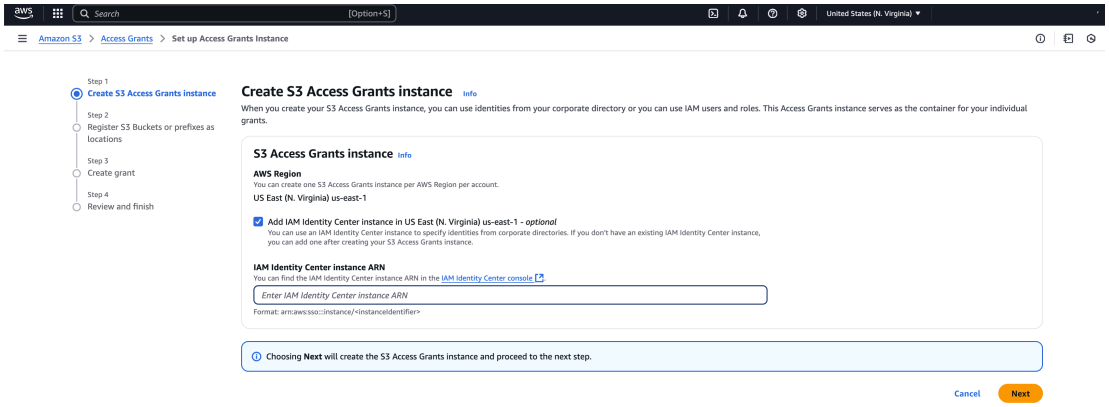
登録された場所を持つ Amazon S3 Access Grantsインスタンスが既にある場合は、次の手順に従います。

1. IAM アイデンティティセンターインスタンスを関連付けます。
2. 許可を作成します。

Amazon S3 Access Grants をまだ作成していない場合は、次の手順に従います。

1. S3 Access Grants インスタンスを作成する - AWS リージョン ごとに 1 つの S3 Access Grants インスタンスを作成できます。S3 Access Grants インスタンスを作成するときは、[IAM アイデンティティセンターインスタンスの追加] チェックボックスをオンにし、IAM アイデンティティセンターインスタンスの ARN を指定してください。[次へ] を選択してください。

   次の図は、Amazon S3 Access Grants コンソールにおける [S3 Access Grants インスタンスを作成する] ページを示しています。



2. ロケーションの登録 - アカウントの AWS リージョン に [Amazon S3 Access Grantsインスタンスを作成] を行ったら、そのインスタンスに S3 ロケーションを登録します。S3 Access Grants のロケーションは、デフォルトの S3 ロケーション (S3://)、バケット、またはプレフィックスを IAM ロールにマッピングします。S3 Access Grants は、この Amazon S3 ロールを引き受けて、その特定の場所にアクセスする被付与者に一時的な認証情報を提供します。アクセス権限を作成する前に、まず S3 Access Grants インスタンスに少なくとも 1 つのロケーションを登録する必要があります。

   [ロケーションスコープ] には、そのリージョン内のすべてのバケットを含む s3:// を指定します。これは、ほとんどのユースケースで推奨されるロケーションスコープです。高度なアクセス管理のユースケースがある場合は、バケット s3://*bucket*/*prefix-with-path* 内の特定のバケット s3://*bucket* またはプレフィックスにロケーションスコープを設定できます。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「ロケーションの登録」を参照してください。

   > **Note**
   >
   > アクセスを許可する AWS Glue テーブルの S3 の場所がこのパスに含まれていることを確認します。

   この手順では、 ロケーションの IAM ロールを設定する必要があります。このロールには、ロケーションスコープにアクセスするためのアクセス許可が含まれている必要があります。このロールは、S3 コンソールウィザードを使用して作成できます。この IAM ロールのポリシーで S3 Access Grants インスタンス ARN を指定する必要があります。S3 Access Grants インスタンス ARN のデフォルト値は arn:aws:s3:*Your-Region*:*Your-AWS-Account-ID*:access-grants/default です。

次のアクセス許可ポリシーの例では、作成した IAM ロールに対するアクセス許可を Amazon S3 に付与します。また、それに続く信頼ポリシーの例では、S3 Access Grants サービスプリンシパルが IAM ロールを引き受けることを許可します。

a. アクセス許可ポリシー:

これらのポリシーを使用するには、サンプルポリシーの*####################*を独自の情報に置き換えます。その他の手順については、「ポリシーの作成」または「ポリシーの編集」を参照してください。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ObjectLevelReadPermissions",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:GetObjectAcl",
                "s3:GetObjectVersionAcl",
                "s3:ListMultipartUploadParts"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "111122223333"
                },
                "ArnEquals": {
                    "s3:AccessGrantsInstanceArn": [
                    "arn:aws:s3:::access-grants/instance-id"
                    ]
                }
            }
        },
        {
            "Sid": "ObjectLevelWritePermissions",
```

```
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectVersionAcl",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:AbortMultipartUpload"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ],
            "Condition": {
                "StringEquals": {
                "aws:ResourceAccount": "111122223333"
                },
                "ArnEquals": {
                    "s3:AccessGrantsInstanceArn": [
                    "arn:aws:s3:::access-grants/instance-id"
                    ]
                }
            }
        },
        {
            "Sid": "BucketLevelReadPermissions",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ],
            "Condition": {
                "StringEquals": {
                "aws:ResourceAccount": "111122223333"
                },
                "ArnEquals": {
                    "s3:AccessGrantsInstanceArn": [
                    "arn:aws:s3:::access-grants/instance-id"
                    ]
                }
            }
        },
        {
```

```
            "Sid": "OptionalKMSPermissionsForSSEEncryption",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

b. 信頼ポリシー

IAM ロールの信頼ポリシーで、作成した IAM ロールに対して、S3 Access Grants サービス (access-grants.s3.amazonaws.com) のプリンシパルアクセス権を付与します。これを実行するために、次のステートメントを含む JSON ファイルを作成できます。アカウントに信頼ポリシーを追加するには、「カスタム信頼ポリシーを使用したロールの作成」を参照してください。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1234567891011",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole",
                "sts:SetSourceIdentity"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333",
                    "aws:SourceArn": "Your-Custom-Access-Grants-Location-
ARN"
                }
            }
        },
```

```
        {
            "Sid": "Stmt1234567891012",
            "Effect": "Allow",
            "Action": "sts:SetContext",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333",
                    "aws:SourceArn": "Your-Custom-Access-Grants-Location-
ARN"
                },
                "ForAllValues:ArnEquals": {
                    "sts:RequestContextProviders":
 "arn:aws:iam::aws:contextProvider/IdentityCenter"
                }
            }
        }
    ]
}
```

Amazon S3 Access Grants を作成する

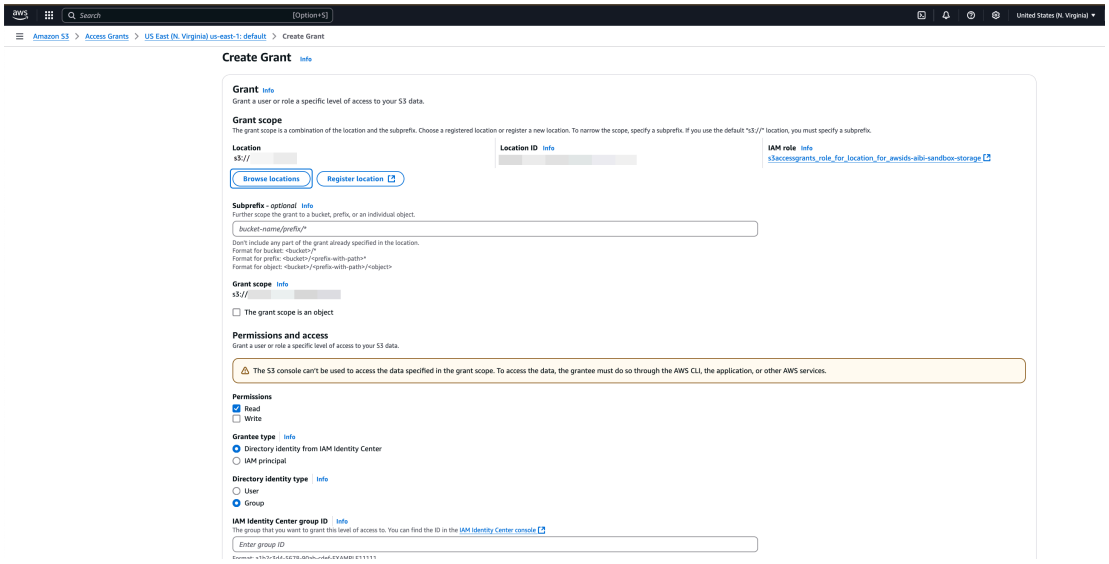
登録された場所を持つ Amazon S3 Access Grants インスタンスがあり、IAM アイデンティティセンターインスタンスを関連付けている場合は、アクセス許可を作成できます。S3 コンソールの[アクセス許可の作成] ページで、以下を完了します。

許可を作成する

1. 前のステップで作成したロケーションを選択します。サブプレフィックスを追加することで、アクセス許可の範囲を縮小できます。サブプレフィックスは、バケット内の `bucket`、`bucket/prefix`、または オブジェクトです。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「サブプレフィックス」を参照してください。
2. [アクセス許可とアクセス] で、必要に応じて [読み取り] または[書き込み]を選択します。
3. [付与者のタイプ]で、ディレクトリアイデンティティフォーム IAM アイデンティティセンターを選択します。
4. IAM アイデンティティセンターのユーザー ID またはグループ ID を指定します。ユーザー ID とグループ ID は、IAM アイデンティティセンターコンソールの[ユーザー] と [グループ] セクションにあります。[次へ] を選択してください。

5. [確認して完了] ページで、S3 Access Grant の設定を確認し、[アクセス許可の作成] を選択します。

   次の図は、Amazon S3 Access Grants コンソールの [アクセス許可の作成] ページを示しています。



独自の OAuth 2.0 アプリケーションを設定するには

信頼できる ID の伝播により、カスタマーマネージドアプリケーションはユーザーに代わって AWS サービス内のデータへのアクセスをリクエストできます。データアクセス管理はユーザーの ID に基づいているため、管理者はユーザーの既存のユーザーやグループのメンバーシップに基づいてアクセスを付与できます。ユーザーの ID、ユーザーに代わって実行されたアクション、およびその他のイベントは、サービス固有のログと CloudTrail イベントに記録されます。

信頼できる ID の伝播を使用すると、ユーザーはカスタマーマネージドアプリケーションにサインインでき、そのアプリケーションは AWS のサービス 内のデータにアクセスするリクエストでユーザーの ID を渡すことができます。

> **Important**
>
> AWS のサービス にアクセスするには、カスタマーマネージドアプリケーションが IAM アイデンティティセンターの外部にある信頼できるトークン発行者からトークンを取得する必要があります。信頼できるトークン発行者とは、署名付きトークンを作成する OAuth 2.0 認可サーバーです。これらのトークンは、AWS のサービス へのアクセスのリクエストを開始す

るアプリケーション (受信側アプリケーション) を承認します。詳細については、「信頼できるトークン発行者によるアプリケーションの使用」を参照してください。

トピック

- 信頼できる ID の伝播用のカスタマーマネージドの OAuth 2.0 アプリケーションを設定する
- 信頼されたアプリケーションを指定する
- 信頼できるトークン発行者によるアプリケーションの使用

信頼できる ID の伝播用のカスタマーマネージドの OAuth 2.0 アプリケーションを設定する

カスタマーマネージドの OAuth 2.0 アプリケーションを信頼できる ID の伝播用に設定するには、まず IAM アイデンティティセンターに追加する必要があります。次の手順を使用して、IAM アイデンティティセンターにアプリケーションを追加します。

トピック

- ステップ 1: アプリケーションタイプを選択する
- ステップ 2: アプリケーションの詳細を指定する
- ステップ 3: 認証設定を指定する
- ステップ 4: アプリケーション認証情報を指定する
- ステップ 5: 確認して設定する

ステップ 1: アプリケーションタイプを選択する

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. [カスタマーマネージド] タブを選択します。
4. [アプリケーションの追加] を選択します。
5. [アプリケーションタイプを選択] ページの [セットアッププリファレンス] で、[セットアップしたいアプリケーションがある] を選択します。
6. [アプリケーションタイプ] で [OAuth 2.0] を選択します。
7. [次へ] を選択して次のページ、ステップ 2: アプリケーションの詳細を指定する に進みます。

ステップ 2: アプリケーションの詳細を指定する

1. [アプリケーションの詳細を指定] ページの [アプリケーションの名前と説明] で、**MyApp** のようなアプリケーションの [表示名] を入力します。[Description] を入力します。
2. [ユーザーとグループの割り当て方法] で、次のいずれかのオプションを選択します。

   - [割り当ては必須です] — このアプリケーションに割り当てられている IAM アイデンティティセンターユーザーとグループのみにアプリケーションへのアクセスを許可します。

     アプリケーションタイルの表示 — [AWS アクセス ポータルのアプリケーションの表示] が [表示] に設定されている場合、アプリケーションに直接割り当てられたユーザーまたはグループ割り当てによって割り当てられたユーザーのみが AWS アクセスポータルでアプリケーションタイルを表示できます。
   - [割り当ては不要です] — 権限のあるすべての IAM アイデンティティセンターユーザーとグループにこのアプリケーションへのアクセスを許可します。

     アプリケーションタイルの表示 — [AWS アクセスポータルのアプリケーションの表示] が [非表示] に設定されていない限り、アプリケーションタイルは AWS アクセスポータルにサインインするすべてのユーザーに表示されます。
3. 「AWS アクセスポータル」で、ユーザーがアプリケーションにアクセスできる URL を入力し、アプリケーションタイルを AWS アクセスポータルに表示するか非表示にするかを指定します。[非表示] を選択すると、割り当てられたユーザーでもアプリケーションタイルを表示できなくなります。
4. [タグ (オプション)] で、[新しいタグを追加] を選択し、[キー] と [値 (オプション)] の値を指定します。

   タグの詳細については[AWS IAM アイデンティティセンター リソースのタグ付け]を参照してください。
5. [次へ] を選択し、次のページ、[ステップ 3: 認証設定を指定する] に進みます。

ステップ 3: 認証設定を指定する

OAuth 2.0 をサポートするカスタマーマネージドアプリケーションを IAM アイデンティティセンターに追加するには、信頼できるトークン発行者を指定する必要があります。信頼できるトークン発行者とは、署名付きトークンを作成する OAuth 2.0 認可サーバーです。これらのトークンにより、AWS マネージドアプリケーション (受信側アプリケーション) へのアクセスのリクエスト (リクエスト元アプリケーション) を開始するアプリケーションを認可します。

1. [認証設定を指定する] ページの、[信頼できるトークン発行者] で、次のいずれかを実行します。

   - 既存の信頼できるトークン発行者を使用するには:

     使用する信頼できるトークン発行者の名前の横にあるチェックボックスを選択します。

   - 新しい信頼できるトークン発行者を追加するには:

     1. [信頼できるトークン発行者を作成] を選択します。
     2. 新しいブラウザタブが開きます。IAM アイデンティティセンターコンソールに信頼できるトークン発行者を追加する方法 のステップ 5～8 を実行します。
     3. これらの手順を完了したら、アプリケーション設定に使用しているブラウザウィンドウに戻り、追加した信頼できるトークン発行者を選択します。
     4. 信頼できるトークン発行者の一覧で、さきほど追加した信頼できるトークン発行者の名前の横にあるチェックボックスをオンにします。

        信頼できるトークン発行者を選択すると、[選択したトラステッドトークン発行者の設定] セクションが表示されます。

2. [選択したトラステッドトークン発行者の設定] で、[Aud クレーム] を入力します。[Aud クレーム] は、信頼できるトークン発行者が生成したトークンの対象者 (受信者) を識別します。詳細については、「Aud クレーム」を参照してください。
3. このアプリケーションを使用しているときにユーザーが再認証する必要がないようにするには、[更新トークン許可を有効にする] を選択します。このオプションを選択すると、セッションの有効期限が切れるか、ユーザーがセッションを終了するまで、60 分ごとにセッションのアクセストークンが更新されます。
4. [次へ] を選択し、次のページ、ステップ 4: アプリケーション認証情報を指定する に進みます。

ステップ 4: アプリケーション認証情報を指定する

この手順のステップを完了して、アプリケーションが信頼できるアプリケーションとのトークン交換アクションを実行するときに使用する認証情報を指定します。これらの認証情報は、リソースベースのポリシーで使用されます。このポリシーでは、ポリシーで指定されているアクションを実行するアクセス許可持つプリンシパルを指定する必要があります。信頼できるアプリケーションが同じ AWS アカウント にあっても、プリンシパルを指定する必要があります。

> **Note**
>
> ポリシーでアクセス許可を設定するときは、タスクの実行に必要なアクセス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。

このポリシーには `CreateTokenWithIAM` API アクションが必要です。このポリシーの詳細と、環境に応じて適応できる例については、「IAM Identity Center のリソースベースのポリシーの例」を参照してください。

1. [アプリケーション認証情報を指定] ページで、次のいずれかを実行します。

   - 1 つ以上の IAM ロールをすばやく指定するには:

     1. [1 つ以上の IAM ロールを入力する] を選択します。
     2. [IAM ロールを入力] で、既存の IAM ロールの Amazon リソースネーム (ARN) を指定します。ARN を指定するには、次の構文を使用します。IAM リソースはグローバルに識別されるため、ARN のリージョンの割り当ては空白です。

        ```
        arn:aws:iam::account:role/role-name-with-path
        ```

        詳細については、「AWS Identity and Access Management ユーザーガイド」の「リソースベースのポリシーを使用したクロスアカウントアクセス」および「IAM ARN」を参照してください。

   - ポリシーを手動で編集するには (非 AWS 認証情報以外を指定する場合は必須):

     1. [アプリケーションポリシーを編集] を選択します。
     2. JSON テキストボックスにテキストを入力または貼り付けてポリシーを変更します。
     3. 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ます。詳細については、「AWS Identity and Access Management ユーザーガイド」の「IAM ポリシーの検証」を参照してください。

2. [次へ] を選択して次のページ、ステップ 5: 確認して設定する に進みます。

ステップ 5: 確認して設定する

1. [確認して設定] ページで、選択した内容を確認します。変更を加えるには、必要な構成セクションを選択し、[編集] を選択して必要なだけ変更を加えます。

2. 完了したら、[アプリケーションを追加] を選択します。
3. 追加したアプリケーションが [カスタマーマネージドアプリケーション] リストに表示されます。
4. IAM アイデンティティセンターでカスタマーマネージドアプリケーションを設定したら、ID を伝播するための AWS のサービス または信頼できるアプリケーションを 1 つ以上指定する必要があります。これにより、ユーザーはカスタマーマネージドアプリケーションにサインインして、信頼できるアプリケーションのデータにアクセスできるようになります。

   詳細については、「信頼されたアプリケーションを指定する」を参照してください。

信頼されたアプリケーションを指定する

カスタマーマネージドアプリケーションを設定したら、ID を伝播するための信頼できる AWS サービスまたは信頼できるアプリケーションを 1 つ以上指定する必要があります。カスタマーマネージドアプリケーションのユーザーがアクセスする必要のあるデータを含む AWS サービスを指定します。ユーザーがカスタマーマネージドアプリケーションにサインインすると、そのアプリケーションはユーザーの ID を信頼できるアプリケーションに渡します。

以下の手順を使用して、サービスを選択し、そのサービスで信頼する個々のアプリケーションを指定します。

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. [カスタマーマネージド] タブを選択します。
4. [カスタマーマネージドアプリケーション] リストで、アクセスのリクエストを開始する OAuth 2.0 アプリケーションを選択します。これはユーザーがサインインするアプリケーションです。
5. [詳細ページ] の [ID の伝播のための信頼されたアプリケーション] で、[信頼されたアプリケーションを指定] を選択します。
6. [セットアップタイプ] で、[個々のアプリケーションとアクセスの指定] を選択して、[次へ] を選択します。
7. [サービスを選択] ページで、カスタマーマネージドアプリケーションが ID の伝播に関して信頼できるアプリケーションを含む AWS サービスを選択し、[次へ] を選択します。

   選択するサービスによって、信頼できるアプリケーションが定義されます。次のステップでは、アプリケーションを選択できます。

8. [アプリケーションを選択] ページで、[個々のアプリケーション] を選択し、アクセスのリクエストを受信できる各アプリケーションのチェックボックスを選択して、[次へ] を選択します。
9. [アクセスの設定] ページの [設定方法] で、次のいずれかを実行します。
   - [アプリケーションごとにアクセスを選択] — このオプションを選択すると、アプリケーションごとに異なるアクセスレベルを設定できます。アクセスレベルを設定するアプリケーションを選択し、[アクセスを編集] を選択します。[適用するアクセスのレベル] で、必要に応じてアクセスレベルを変更し、[変更の保存] を選択します。
   - [すべてのアプリケーションに同じアクセスレベルを適用する] — アプリケーションごとにアクセスレベルを設定する必要がない場合は、このオプションを選択します。
10. [次へ] を選択します。
11. [設定を確認] ページで、選択した内容を確認します。変更を加えるには、必要な設定セクションを選択し、[アクセスを編集] を選択して、必要なだけ変更を加えます。
12. 完了したら、[信頼アプリケーション] を選択します。

信頼できるトークン発行者によるアプリケーションの使用

信頼できるトークン発行者ならば、AWS の外部で認証を行うアプリケーションに対して信頼できる ID の伝播を使用できます。信頼できるトークン発行者があれば、これらのアプリケーションに、ユーザーに代わって AWS マネージドアプリケーションへのアクセスをリクエストすることを許可できます。

以下のトピックでは、信頼できるトークン発行者の仕組みを説明し、設定ガイダンスを提供します。

トピック

- 信頼できるトークン発行者の概要
- 信頼できるトークン発行者の前提条件と考慮事項
- JTI クレームの詳細
- 信頼できるトークン発行者の構成設定
- 信頼できるトークン発行者の設定
- ID が強化された IAM ロールセッション

信頼できるトークン発行者の概要

信頼できる ID の伝播は、AWS の外部で認証を行うアプリケーションが、信頼できるトークン発行者を使用してユーザーに代わってリクエストを行えるようにするメカニズムを提供します。信頼できるトークン発行者とは、署名付きトークンを作成する OAuth 2.0 認可サーバーです。これらのトークンにより、AWS のサービス (受信側アプリケーション) へのアクセスリクエスト (リクエスト元アプリケーション) を開始するアプリケーションを認可します。リクエスト元アプリケーションは、信頼できるトークン発行者が認証するユーザーに代わってアクセス要求を開始します。ユーザーは、信頼できるトークン発行者と IAM アイデンティティセンターの両方に認識されています。

リクエストを受信する AWS のサービス は、Identity Center ディレクトリに表示されているユーザーとグループメンバーシップに基づいて、リソースに対するきめ細かい承認を管理します。AWS のサービス は外部のトークン発行者からのトークンを直接使用することはできません。

この問題を解決するために、IAM アイデンティティセンターでは、リクエスト元アプリケーション、またはリクエスト元アプリケーションが使用する AWS ドライバーが、信頼できるトークン発行者が発行したトークンを IAM アイデンティティセンターが生成したトークンと交換する方法を提供しています。IAM アイデンティティセンターによって生成されるトークンは、対応する IAM アイデンティティセンターのユーザーを指します。リクエスト元のアプリケーションまたはドライバーは、新しいトークンを使用して受信側のアプリケーションへのリクエストを開始します。新しいトークンは IAM アイデンティティセンター内の対応するユーザーを参照するため、受信側アプリケーションは IAM アイデンティティセンターに表示されているユーザーまたはグループメンバーシップに基づいて、リクエストされたアクセスを承認できます。

> **Important**
>
> OAuth 2.0 認可サーバーを信頼できるトークン発行者として追加するかどうかは、慎重に検討する必要があるセキュリティ上の決定です。以下のタスクを実行するには、信頼できるトークン発行者のみを選択してください。
>
> - トークンに指定されているユーザーを認証します。
> - そのユーザーによる受信側のアプリケーションへのアクセスを許可します。
> - IAM アイデンティティセンターが IAM アイデンティティセンターが作成したトークンと交換できるトークンを生成します。

信頼できるトークン発行者の前提条件と考慮事項

信頼できるトークン発行者を設定する前に、次の前提条件と考慮事項を確認します。

- 信頼できるトークン発行者の設定

  OAuth 2.0 認可サーバー (信頼できるトークン発行者) を設定する必要があります。信頼されたトークン発行者は、通常、IAM アイデンティティセンターの ID ソースとして使用する ID プロバイダーですが、必ずしもそうである必要はありません。信頼できるトークン発行者を設定する方法については、関連する ID プロバイダーのドキュメントを参照してください。

  > **Note**
  >
  > 信頼できるトークン発行者の各ユーザーの ID を IAM アイデンティティセンターの対応するユーザーにマップさえすれば、最大 10 の信頼できるトークン発行者を IAM アイデンティティセンターで使用するように設定できます。

- トークンを作成する OAuth 2.0 認可サーバー (信頼できるトークン発行者) には、IAM アイデンティティセンターがトークンの署名を検証するためのパブリックキーの取得に使用できる OpenID Connect (OIDC) ディスカバリーエンドポイントが必要です。詳細については、「OIDC ディスカバリーエンドポイント URL (発行者 URL)」を参照してください。
- 信頼できるトークン発行者が発行するトークン

  信頼できるトークン発行者からのトークンは、次の要件を満たす必要があります。

  - トークンは署名済みであり、かつ RS256 アルゴリズムを使用した JSON Web トークン (JWT) 形式である必要があります。
  - トークンには、次のクレームが含まれている必要があります。
    - 発行者 (iss) – トークンを発行したエンティティ。この値は、信頼できるトークン発行者の OIDC 検出エンドポイント (発行者 URL) で設定されている値と一致する必要があります。
    - 対象 (sub) – 認証対象ユーザー。
    - オーディエンス (aud) – トークンの意図された受信者。これは、トークンが IAM アイデンティティセンターからトークンと交換された後のアクセス先となる AWS のサービス です。詳細については、「Aud クレーム」を参照してください。
    - 有効期限 (exp) – トークンの有効期限が切れるまでの時間。
  - トークンは、ID トークンでもアクセストークンでもかまいません。
  - トークンには、1 人の IAM アイデンティティセンターユーザーに一意にマッピングできる属性が必要です。

> **Note**
>
> Microsoft Entra ID からの JWT のカスタム署名キーの使用はサポートされていません。Microsoft Entra ID からのトークンを信頼できるトークン発行者で使用するには、カスタム署名キーを使用できません。

- オプションのクレーム

  IAM アイデンティティセンターは RFC 7523 で定義されているすべてのオプションのクレームをサポートしています。詳細については、この RFC の「セクション 3: JWT 形式と処理要件」を参照してください。

  例えば、トークンには JTI (JWT ID) クレーム を含めることができます。このクレームが存在する場合は、同じ JTI を持つトークンがトークンの交換に再利用されるのを防ぐことができます。JTI クレームの詳細については、「JTI クレームの詳細」を参照してください。

- 信頼できるトークン発行者と連携するための IAM アイデンティティセンターの設定

  また、IAM アイデンティティセンターを有効にし、IAM アイデンティティセンターの ID ソースを設定し、信頼できるトークン発行者のディレクトリ内のユーザーに対応するユーザーをプロビジョニングする必要があります。

  これを行うには、次のいずれかを実行する必要があります。

  - クロスドメイン ID 管理システム (SCIM) 2.0 プロトコルを使用して、ユーザーを IAM アイデンティティセンターと同期します。
  - IAM アイデンティティセンターでユーザーを直接作成します。

JTI クレームの詳細

IAM アイデンティティセンターが既に交換したトークンを交換するリクエストを IAM アイデンティティセンターが受け取った場合、そのリクエストは失敗します。トークン交換のためのトークンの再利用を検出して防止するために、JTI クレームを含めることができます。IAM アイデンティティセンターは、トークン内のクレームに基づいてトークンの再利用を防止します。

すべての OAuth 2.0 認可サーバーがトークンに JTI クレームを追加するわけではありません。OAuth 2.0 認可サーバーの中には、JTI をカスタムクレームとして追加できないものもあります。JTI クレームの使用をサポートする OAuth 2.0 認可サーバーは、このクレームを ID トークンのみ、アクセス

トークンのみ、またはその両方に追加する場合があります。詳細については、OAuth 2.0 認可サーバーのドキュメントを参照してください。

トークンを交換するアプリケーションの構築については、IAM アイデンティティセンターAPI ドキュメントを参照してください。正しいトークンを取得して交換するようにカスタマーマネージドアプリケーションを設定する方法については、そのアプリケーションのドキュメントを参照してください。

信頼できるトークン発行者の構成設定

次のセクションでは、信頼できるトークン発行者をセットアップして使用するために必要な設定について説明します。

トピック

- OIDC ディスカバリーエンドポイント URL (発行者 URL)
- 属性マッピング
- Aud クレーム

OIDC ディスカバリーエンドポイント URL (発行者 URL)

IAM アイデンティティセンターコンソールに信頼できるトークン発行者を追加するときは、OIDC ディスカバリーエンドポイント URL を指定する必要があります。この URL は通常、その相対 URL である `/.well-known/openid-configuration` で呼ばれます。IAM アイデンティティセンターコンソールでは、この URL は 発行者 URL と呼ばれます。

> **Note**
>
> ディスカバリーエンドポイントの URL は、*`.well-known/openid-configuration`* まで、これを含まず貼り付ける必要があります。`.well-known/openid-configuration` が URL に含まれている場合、信頼されたトークン発行者設定は機能しません。IAM アイデンティティセンターはこの URL を検証しないため、URL が正しく形成されていない場合、信頼できるトークン発行者の設定は通知なしで失敗します。
> OIDC 検出エンドポイント URL は、ポート 80 および 443 を介してのみ到達可能である必要があります。

IAM アイデンティティセンターはこの URL を使用して、信頼できるトークン発行者に関する追加情報を取得します。例えば、IAM アイデンティティセンターは、この URL を使用して、信頼できるトークン発行者が生成するトークンの検証に必要な情報を取得します。IAM アイデンティティセン

ターに信頼できるトークン発行者を追加するときは、この URL を指定する必要があります。URL を確認するには、アプリケーション用のトークンの生成に使用する OAuth 2.0 認可サーバープロバイダーのドキュメントを参照するか、プロバイダーに直接問い合わせて支援を求めてください。

属性マッピング

属性マッピングにより、IAM アイデンティティセンターは、信頼できるトークン発行者が発行したトークンに示されているユーザーを IAM アイデンティティセンター内の 1 人のユーザーと照合できます。IAM アイデンティティセンターに信頼できるトークン発行者を追加するときは、属性マッピングを指定する必要があります。この属性マッピングは、信頼できるトークン発行者が生成するトークンのクレームに使用されます。このクレームの値は IAM アイデンティティセンターの検索に使用されます。この検索では、指定された属性を使用して IAM アイデンティティセンター内の 1 人のユーザーを取得します。このユーザーは AWS 内のユーザーとして使用されます。選択したクレームは、IAM アイデンティティセンターID ストア内の使用可能な属性の固定リスト内の 1 つの属性にマッピングする必要があります。IAM アイデンティティセンターID ストア属性の、ユーザー名、E メール、外部 ID のいずれか一つを選択できます。IAM アイデンティティセンターで指定する属性の値は、ユーザーごとに一意である必要があります。

Aud クレーム

Aud クレームは、トークンの対象となる対象者 (受信者) を識別します。アクセスをリクエストするアプリケーションが IAM アイデンティティセンターにフェデレーションされていない ID プロバイダーを通じて認証される場合、その ID プロバイダーを信頼できるトークン発行者として設定する必要があります。アクセスリクエストを受信するアプリケーション (受信側アプリケーション) は、信頼できるトークン発行者が生成したトークンを IAM アイデンティティセンターが生成したトークンと交換する必要があります。

信頼できるトークン発行者に登録されている受信側アプリケーションの aud クレーム値を取得する方法については、信頼できるトークン発行者のドキュメントを参照するか、信頼できるトークン発行者の管理者に支援を問い合わせてください。

信頼できるトークン発行者の設定

IAM アイデンティティセンターの外部認証を行うアプリケーションに対し、信頼できる ID を伝播きるようにするには、1 人以上の管理者が、信頼できるトークン発行者を設定する必要があります。信頼できるトークン発行者とは、リクエストを開始するアプリケーション (リクエスト元アプリケーション) にトークンを発行する OAuth 2.0 認可サーバーです。トークンは、これらのアプリケーションがユーザーに代わって受信側アプリケーション (AWS のサービス) へのリクエストを開始することを承認します。

トピック

- 管理者の役割と責任の調整
- 信頼できるトークン発行者を設定するタスク
- IAM アイデンティティセンターコンソールに信頼できるトークン発行者を追加する方法
- IAM アイデンティティセンターコンソールで信頼できるトークン発行者の設定を表示または編集する方法
- 信頼できるトークン発行者を使用するアプリケーションのセットアッププロセスおよびリクエストフロー

管理者の役割と責任の調整

場合によっては、単独の管理者が、信頼できるトークン発行者の設定に必要なすべてのタスクを実行することもあります。複数の管理者がこれらのタスクを実行する場合は、緊密な調整が必要です。以下の表は、複数の管理者がどのように連携して信頼できるトークン発行者を設定し、それを使用するように AWS サービスを設定するかを説明するものです。

> **Note**
>
> アプリケーションには、IAM アイデンティティセンターと統合されていて、信頼できる ID の伝播をサポートしている AWS サービスであればどれでもかまいません。

詳細については、「信頼できるトークン発行者を設定するタスク」を参照してください。

[Role] (ロール)	これらのタスクを実行する	コーディネートする
IAM アイデンティティセンター管理者	外部 IdP を、信頼できるトークン発行者として、IAM アイデンティティセンターコンソールに追加します。 IAM アイデンティティセンターと外部 IdP 間の正しい属性マッピングを設定するのに役立ちます。 信頼できるトークン発行者が IAM アイデンティティセンターコン	外部 IdP (信頼できるトークン発行者) 管理者 AWS サービス管理者

[Role] (ロール)	これらのタスクを実行する	コーディネートする
	ソールに追加されたことを AWS サービス管理者に通知します。	
外部 IdP (信頼できるトークン発行者) 管理者	トークンを発行するように外部 IdP を設定します。 IAM アイデンティティセンターと外部 IdP 間の正しい属性マッピングを設定するのに役立ちます。 対象者名 (Aud 要求) を AWS サービス管理者に提供します。	IAM アイデンティティセンター管理者 AWS サービス管理者
AWS サービス管理者	AWS サービスコンソールで信頼できるトークン発行者をチェックします。信頼できるトークンの発行者は、IAM アイデンティティセンター管理者が IAM アイデンティティセンターコンソールにそれを追加すると、AWS サービスコンソールに表示できるようになります。 信頼できるトークン発行者を使用するように AWS サービスを設定します。	IAM アイデンティティセンター管理者 外部 IdP (信頼できるトークン発行者) 管理者

信頼できるトークン発行者を設定するタスク

信頼できるトークン発行者を設定するには、IAM アイデンティティセンター管理者、外部 IdP (信頼できるトークン発行者) 管理者、およびアプリケーション管理者が次のタスクを完了する必要があります。

> **Note**
>
> アプリケーションには、IAM アイデンティティセンターと統合されていて、信頼できる ID の伝播をサポートしている AWS サービスであればどれでもかまいません。

1. 信頼できるトークン発行者を IAM アイデンティティセンターに追加する — IAM アイデンティティセンターの管理者は、IAM アイデンティティセンターコンソールまたは API を使用して信頼できるトークン発行者を追加します。この設定では、以下を指定する必要があります。

   - 信頼できるトークン発行者の名前。
   - OIDC ディスカバリーエンドポイント URL (IAM アイデンティティセンターコンソールでは、この URL は 発行者 URL と呼ばれます)。検出エンドポイントは、ポート 80 および 443 を介してのみ到達可能である必要があります。
   - ユーザー検索用の属性マッピング。この属性マッピングは、信頼できるトークン発行者が生成するトークンのクレームに使用されます。このクレームの値は IAM アイデンティティセンターの検索に使用されます。検索では、指定された属性を使用して IAM アイデンティティセンター内の 1 人のユーザーを取得します。

2. AWS サービスを IAM アイデンティティセンターに接続する — AWS サービス管理者は、アプリケーション用のコンソールまたはアプリケーション API を使用して、そのアプリケーションを IAM アイデンティティセンターに接続する必要があります。

   信頼できるトークン発行者が IAM アイデンティティセンターコンソールに追加されると、AWS サービスコンソールにも表示され、AWS サービス管理者が選択できるようになります。

3. トークン交換の使用を設定する — AWS サービスコンソールでは、AWS サービス管理者は、信頼できるトークン発行者が発行したトークンを受け入れるように AWS サービスを設定します。これらのトークンは IAM アイデンティティセンターによって生成されたトークンと交換されます。これには、ステップ 1 の信頼できるトークン発行者の名前と、AWS サービスに対応する Aud クレーム値を指定する必要があります。

   信頼できるトークン発行者は、発行するトークンに Aud クレーム値を入れて、そのトークンが AWS サービスによる使用を目的としていることを示します。この値を取得するには、信頼できるトークン発行者の管理者に問い合わせてください。

IAM アイデンティティセンターコンソールに信頼できるトークン発行者を追加する方法

複数の管理者がいる組織では、このタスクは IAM アイデンティティセンター管理者が実行します。IAM アイデンティティセンター管理者である場合は、信頼できるトークン発行者として使用する外部 IdP を選択する必要があります。

IAM アイデンティティセンターコンソールに信頼できるトークン発行者を追加するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [設定] ページで、[認証] タブを選択します。
4. [信頼できるトークン発行者] で [信頼できるトークン発行者を作成] を選択します。
5. 「信頼できるトークンを発行するための外部 IdP を設定する」ページの「信頼できるトークン発行者の詳細」で、次の操作を行います。

   - [発行者 URL] には、信頼できる ID の伝播用のトークンを発行する外部 IdP の OIDC ディスカバリー URL を指定します。ディスカバリーエンドポイントの URL は、`.well-known/openid-configuration` まで、これを含まず貼り付ける必要があります。外部 IdP の管理者がこの URL を提供できます。

     > **Note**
     >
     > 注: この URL は、信頼できる ID 伝搬のために発行されたトークン内の発行者 (iss) クレームの URL と一致する必要があります。

   - [信頼できるトークンの発行者名] には、IAM アイデンティティセンターとアプリケーションコンソールで、この信頼できるトークン発行者を識別する名前を入力します。
6. [マップ属性] で、次の操作を行います。

   - [ID プロバイダー属性] では、IAM アイデンティティセンターID ストアの属性にマップする属性をリストから選択します。
   - [IAM アイデンティティセンター属性] では、属性マッピングに対応する属性を選択します。
7. [タグ (オプション)] で [新しいタグを追加] を選択し、[キー] と任意で [値 (オプション)] の値を指定します。

   タグの詳細については AWS IAM アイデンティティセンター リソースのタグ付け を参照してください。

8. [信頼できるトークン発行者を作成] を選択します。
9. 信頼できるトークン発行者の作成が完了したら、アプリケーション管理者に連絡して信頼できるトークン発行者の名前を伝えて、管理者が信頼できるトークン発行者が該当するコンソールに表示されることを確認できるようにします。
10. アプリケーション管理者は、該当するコンソールでこの信頼できるトークン発行者を選択する必要があります。これにより、信頼できる ID が伝播されるように構成されたアプリケーションからユーザーがアプリケーションにアクセスできるようになります。

IAM アイデンティティセンターコンソールで信頼できるトークン発行者の設定を表示または編集する方法

IAM アイデンティティセンターコンソールに信頼できるトークン発行者を追加すると、関連設定を表示および編集できます。

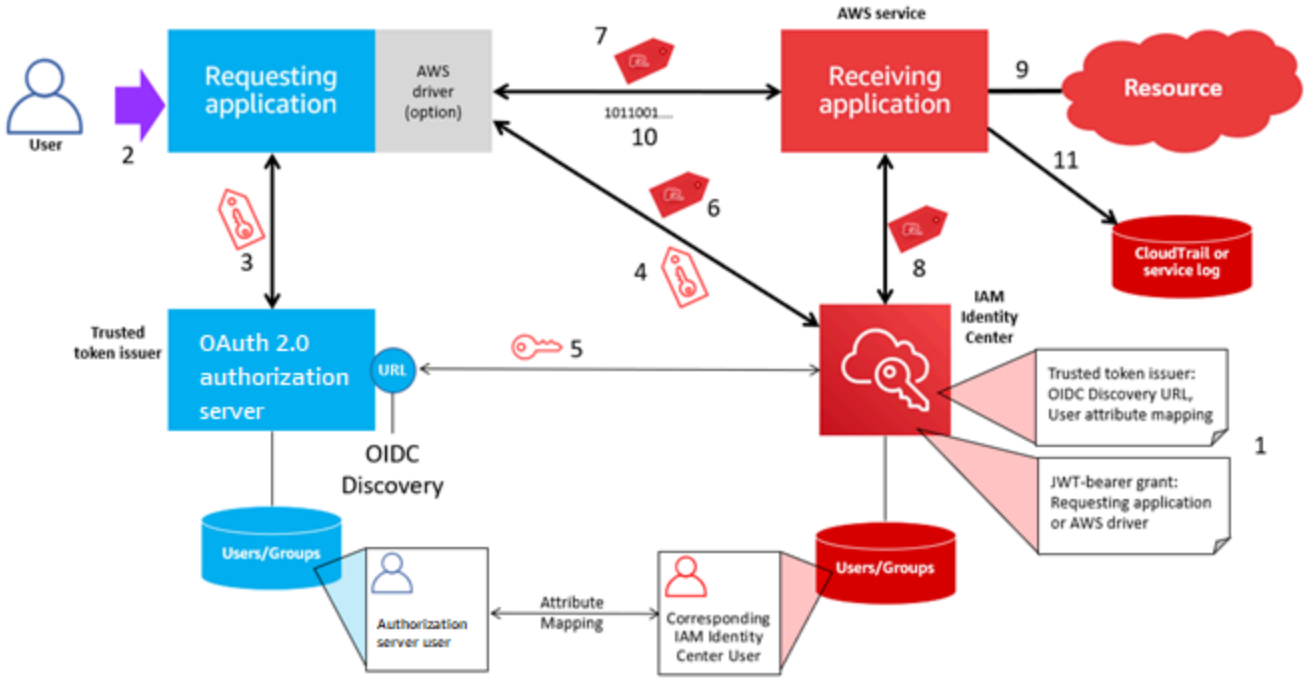
信頼できるトークン発行者の設定を編集する予定がある場合は、その信頼できるトークン発行者を使用するように設定されているアプリケーションにユーザーがアクセスできなくなる可能性があることに注意してください。ユーザーアクセスを妨げないように、設定を編集する前に、信頼できるトークン発行者を使用するように構成されているアプリケーションの管理者と連絡を取ることをお勧めします。

IAM アイデンティティセンターコンソールで信頼できるトークン発行者の設定を表示または編集するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [設定] ページで、[認証] タブを選択します。
4. [信頼できるトークン発行者] で、表示または編集する信頼できるトークン発行者を選択します。
5. [アクション] を選択し、[編集] を選択します。
6. [信頼できるトークンの発行者を編集] ページで、必要に応じて設定を表示または編集します。信頼できるトークンの発行者名、属性マッピング、およびタグを編集することができます。
7. [Save changes] (変更の保存) をクリックします。
8. [信頼できるトークン発行者を編集] ダイアログボックスに、変更を加えるかどうかを確認するメッセージが表示されます。[確認] を選択します。

信頼できるトークン発行者を使用するアプリケーションのセットアッププロセスおよびリクエストフロー

このセクションでは、信頼できるトークン発行者を使用して信頼できる ID の伝播を行うアプリケーションのセットアッププロセスとリクエストフローについて説明します。次の図は、このプロセスの概要を示しています。



次の手順で、このプロセスに関する追加情報を提供します。

1. IAM アイデンティティセンターと受信側の AWS マネージドアプリケーションが、信頼できるトークン発行者を使用するように設定します。詳細については、「信頼できるトークン発行者を設定するタスク」を参照してください。
2. リクエストフローは、ユーザーがリクエスト元のアプリケーションを開くと開始されます。
3. リクエスト元のアプリケーションは、信頼できるトークン発行者からトークンをリクエストして、受信側の AWS マネージドアプリケーションへのリクエストを開始します。ユーザーがまだ認証されていない場合、このプロセスによって認証フローがトリガーされます。このトークンには次の情報が含まれます。
   - ユーザーのサブジェクト (Sub)。
   - IAM アイデンティティセンターが IAM アイデンティティセンター内の対応するユーザーを検索するために使用する属性。

- 信頼できるトークン発行者が受信側の AWS マネージドアプリケーションに関連付ける値を含む対象者 (Aud) クレーム。他のクレームが存在する場合、これらは IAM アイデンティティセンターでは使用されません。

4. リクエスト元のアプリケーションまたは使用する AWS ドライバーは、トークンを IAM アイデンティティセンターに渡し、そのトークンを IAM アイデンティティセンターが生成するトークンと交換するようリクエストします。AWS ドライバーを使用する場合、このユースケースに合わせてドライバーを設定する必要がある場合があります。詳細については、関連する AWS マネージドアプリケーションのドキュメントを参照してください。
5. IAM アイデンティティセンターは OIDC Discovery エンドポイントを使用して、トークンの信頼性を検証するために使用できるパブリックキーを取得します。次に IAM アイデンティティセンターは次の処理を行います。
   - このトークンを検証します。
   - Identity Center ディレクトリを検索します。これを行うには、IAM アイデンティティセンターはトークンで指定されたマッピングされた属性を使用します。
   - ユーザーが受信側のアプリケーションにアクセスする権限を持っていることを確認します。AWS マネージドアプリケーションがユーザーとグループへの割り当てを要求するように設定されている場合、ユーザーはアプリケーションに対して直接またはグループベースの割り当てを行う必要があります。また、そうでない場合は、要求は拒否されます。AWS マネージドアプリケーションがユーザーとグループの割り当てを必要としないように設定されている場合、処理は続行されます。

     > **Note**
     >
     > AWS サービスには、ユーザーとグループへの割り当てが必要かどうかを決定するデフォルト設定の構成があります。これらのアプリケーションを信頼できる ID の伝播と組み合わせて使用する予定の場合は、これらのアプリケーションの [割り当ては必須です] 設定を変更しないことをお勧めします。特定のアプリケーションリソースへのユーザーアクセスを許可するきめ細かいアクセス許可を設定した場合でも、[割り当ては必須です] 設定を変更すると、これらのリソースへのユーザーアクセスが中断されるなど、予期しない動作が発生する可能性があります。

   - リクエスト元のアプリケーションが、受信側の AWS マネージドアプリケーションに対して有効なスコープを使用するように構成されていることを確認します。
6. 前の検証ステップが成功すると、IAM アイデンティティセンターは新しいトークンを作成します。新しいトークンは不透明 (暗号化された) トークンで、これには IAM アイデンティティセンター内の対応するユーザーの ID、受信側の AWS マネージドアプリケーションの対象者 (Aud)、

およびリクエスト元のアプリケーションが受信側の AWS マネージドアプリケーションにリクエストする際に使用できるスコープが含まれます。

7. リクエスト元のアプリケーションまたはそれが使用するドライバーは、受信アプリケーションへのリソースリクエストを開始し、IAM アイデンティティセンターが生成したトークンを受信アプリケーションに渡します。
8. 受信側のアプリケーションは IAM アイデンティティセンターを呼び出して、ユーザーの ID とトークンにエンコードされたスコープを取得します。Identity Center ディレクトリからユーザー属性またはユーザーのグループメンバーシップを取得するようにリクエストする場合もあります。
9. 受信側のアプリケーションは、その認可設定を使用して、リクエストされたアプリケーションリソースへのアクセスがユーザーに許可されているかどうかを判断します。
10. リクエストされたアプリケーションリソースへのアクセスがユーザーに許可されている場合、受信側のアプリケーションはそのリクエストに応答します。
11. ユーザーの ID、ユーザーに代わって実行されたアクション、およびその他のイベントは、受信側のアプリケーションログと CloudTrail イベントに記録されます。この情報を記録する具体的な方法は、アプリケーションによって異なります。

ID が強化された IAM ロールセッション

AWS Security Token Service (STS) を使用すると、アプリケーションはアイデンティティが強化された IAM ロールセッションを取得できます。ID 拡張ロールセッションには、呼び出す AWS のサービス にユーザー識別子を格納する ID コンテキストが追加されています。AWS のサービス は、IAM アイデンティティセンターでユーザーのグループメンバーシップと属性を検索し、それらを使用してユーザーのリソースへのアクセスを承認できます。

AWS アプリケーションは、 AWS STS AssumeRole API アクションにリクエストを行い、リクエストの `ProvidedContexts` パラメータにユーザーの識別子 (`userId`) を含むコンテキストアサーションを `AssumeRole` に渡すことで、ID 拡張 IAM ロールセッションを取得できます。コンテキストアサーションは、`SSO OIDC` から `CreateTokenWithIAM` へのリクエストに応答して受け取った `idToken` クレームから取得されます。AWS アプリケーションが ID 拡張ロールセッションを使用してリソースにアクセスすると、CloudTrail は `userId`、開始セッション、および実行されたアクションをログ記録します。詳細については、「ID 拡張 IAM ロールセッションの記録」を参照してください。

トピック

- ID が強化された IAM ロールセッションのタイプ
- ID 拡張 IAM ロールセッションの記録

ID が強化された IAM ロールセッションのタイプ

AssumeRole リクエストに提供されたコンテキストアサーションに応じて、AWS STS は 2 種類の ID が強化された IAM ロールセッションを作成できます。IAM アイデンティティセンターから ID トークンを取得しているアプリケーションは、IAM ロールセッションに sts:identity_context (推奨) または sts:audit_context (下位互換性のためにサポート) を追加できます。なお、ID 拡張 IAM ロールセッションでは、これらのコンテキストアサーションの 1 つしか持つことができず、両方を持つことはできません。

sts:identity_context で作成された ID が強化された IAM ロールセッション

ID 拡張ロールセッションに sts:identity_context が含まれている場合、呼び出された AWS のサービス は、リソース認可がロールセッションで表されるユーザーに基づくか、ロールに基づくかを決定します。ユーザーベースの認可をサポートする AWS のサービス は、ユーザーまたはユーザーがメンバーであるグループにアクセスを割り当てるコントロールをアプリケーションの管理者に提供します。

AWS のサービスユーザーベースの認証をサポートしていない は、 を無視します。sts:identity_contextCloudTrail は、IAM アイデンティティセンターユーザーのユーザー ID を、ロールによって実行されたすべてのアクションとともに記録します。詳細については、「ID 拡張 IAM ロールセッションの記録」を参照してください。

このタイプの ID 拡張ロールセッションを AWS STS から取得するために、 アプリケーションは、ProvidedContexts リクエストパラメータを使用して AssumeRole リクエストの sts:identity_context フィールドの値を提供します。arn:aws:iam::aws:contextProvider/IdentityCenter を ProviderArn の値として使用します。

認証動作の詳細については、受信側 AWS のサービス のドキュメントを参照してください。

sts:audit_context で作成された ID が強化された IAM ロールセッション

以前、sts:audit_context は、AWS のサービス が承認の決定にこれを使用せずにユーザー ID を記録できるようにするために使用されていました。AWS のサービス は 1 つのコンテキスト - sts:identity_context - を使用して、これを実現したり、承認の決定を行ったりできるようになりました。信頼できる ID 伝播のすべての新しいデプロイで sts:identity_context を使用することをお勧めします。

ID 拡張 IAM ロールセッションの記録

userId またはを用いて作成された ID 拡張 IAM ロールセッションを使用して AWS のサービス にリクエストが行われると、ユーザーの IAM アイデンティティセンター が onBehalfOf 要素内の CloudTrail にログ記録されます。CloudTrail にイベントをログ記録する方法は、AWS のサービスによって異なります。すべての AWS のサービスが onBehalfOf 要素をログ記録するわけではありません。

以下は、ID 拡張ロールセッションを使用して AWS のサービスに対して行われるリクエストが CloudTrail にログ記録される方法の例です。

```
"userIdentity": {
      "type": "AssumedRole",
      "principalId": "AROAEXAMPLE:MyRole",
      "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
      "accountId": "111111111111",
      "accessKeyId": "ASIAEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAEXAMPLE",
            "arn": "arn:aws:iam::111111111111:role/MyRole",
            "accountId": "111111111111",
            "userName": "MyRole"
        },
        "attributes": {
            "creationDate": "2023-12-12T13:55:22Z",
            "mfaAuthenticated": "false"
        }
    },
    "onBehalfOf": {
        "userId": "11111111-1111-1111-1111-1111111111",
        "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/
d-111111111"
    }
}
```

IAM アイデンティティセンター証明書のローテーション

IAM アイデンティティセンターは、証明書を使用して IAM アイデンティティセンターとアプリケーションのサービスプロバイダーとの間の SAML 信頼関係をセットアップします。IAM Identity Center

でアプリケーションを追加すると、セットアップ時にそのアプリケーションで使用する IAM Identity Center 証明書が自動的に作成されます。デフォルトでは、この自動生成された IAM Identity Center 証明書の有効期間は 5 年間です。

IAM Identity Center の管理者として、特定のアプリケーションのために、古い証明書を新しいものに置き換える必要がある場合があります。例えば、証明書の有効期限が近づいている場合、証明書を交換する必要があります。古い証明書を新しい証明書に置き換えるプロセスは、証明書のローテーションと呼ばれています。

証明書をローテーションする前の注意事項

IAM Identity Center で証明書をローテーションするプロセスを開始する前に、以下について検討してください。

- 認証ローテーションプロセスでは、IAM Identity Center とサービスプロバイダーの間の信頼関係を再構築する必要があります。信頼を再確立するには、IAM Identity Center 証明書の交代 に記載されている手順を行います。
- サービスプロバイダーの証明書を更新すると、信頼関係が正常に再構築されるまで、ユーザーに一時的なサービス障害が発生する場合があります。このオペレーションは、ピーク時を可能な限り避けて慎重に計画してください。

IAM Identity Center 証明書の交代

IAM Identity Center 証明書のローテーションは、以下の複数のステップで行われます。

- 新しい証明書を生成する
- 新しい証明書をサービスプロバイダのウェブサイトに追加する
- 新しい証明書をアクティブにする
- 非アクティブな証明書を削除する

特定のアプリケーションの証明書ローテーションプロセスを完了するには、次の手順をすべて行います。

ステップ 1: 新しい証明書を生成する

生成した新しい IAM Identity Center 証明書は、以下のプロパティを使用するように設定できます。

- 有効期間 — 新しい IAM Identity Center 証明書の有効期限が切れるまでの期間 (月単位) を指定します。
- キーサイズ — キーが暗号アルゴリズムで使用するビット数を決定します。この値は、1024 ビット RSA または 2048 ビット RSA のいずれかに設定できます。暗号化におけるキーサイズの仕組みに関する一般情報については、「Key size」(キーサイズ) を参照してください。
- アルゴリズム — SAML アサーション/レスポンスの署名時に IAM Identity Center が使用するアルゴリズムを指定します。この値は SHA-1 または SHA-256 のいずれかを設定できます。AWS サービスプロバイダーにより SHA-1 を指定された場合以外は、可能なかぎり、SHA-256 を使用することをお勧めします。暗号化アルゴリズムの仕組みに関する一般情報については、「Public-key cryptography」(パブリックキー暗号) を参照してください。

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. アプリケーションのリストで、新しい証明書を生成するアプリケーションを選択します。
4. [Application details] (アプリケーションの詳細) ページで、[Settings] (設定) タブをクリックします。[IAM ID センターのメタデータ] で [証明書の管理] を選択します。[設定] タブがない場合や、設定が使用できない場合は、このアプリケーションの証明書をローテーションする必要はありません。
5. [IAM Identity Center 証明書] ページで、[新しい証明書を生成] を選択します。
6. [新しい IAM Identity Center 証明書を生成する] ダイアログボックスで、[有効期間]、[アルゴリズム]、[キーサイズ] に適切な値を指定します。次に [Generate] (生成) をクリックします。

ステップ 2: サービスプロバイダーのウェブサイトを更新する

以下の手順で、アプリケーションのサービスプロバイダーとの信頼関係を再構築します。

> **Important**
>
> 新しい証明書をサービスプロバイダーにアップロードすると、ユーザーが認証を受けられなくなる可能性があります。この問題を解決するには、次のステップの説明にあるとおり、新しい証明書をアクティブに設定します。

1. IAM Identity Center コンソールで、先ほど新しい証明書を生成したアプリケーションをクリックします。

2. [Application details] (アプリケーションの詳細) ページで、[Edit configuration] (設定の変更) タブをクリックします。
3. [View instructions] (手順を表示する) をクリックし、特定のアプリケーションサービスプロバイダーのウェブサイトの指示に従って、新しく生成された証明書を追加します。

ステップ 3: 新しい証明書をアクティブにする

アプリケーションには、最大 2 つの証明書を割り当てることができます。IAM アイデンティティセンターは、すべての SAML アサーションに署名するためにアクティブに設定されている証明書を使用します。

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. アプリケーションのリストで [your application] (お客様のアプリケーション) をクリックします。
4. [Application details] (アプリケーションの詳細) ページで、[Settings] (設定) タブをクリックします。[IAM Identity Center のメタデータ] で [証明書の管理] を選択します。
5. [IAM Identity Center 証明書] ページで、アクティブに設定したい証明書を選択し、[アクション] をクリックし、そして、[アクティブとして設定] をクリックします。
6. [Set the selected certificate as active] (選択した証明書をアクティブにする) ダイアログで、証明書をアクティブにすると信頼関係の再構築が必要になることを確認して、[Make active] (アクティブにする) をクリックします。

ステップ 4: 古い証明書を削除する

以下の手順で、アプリケーションの証明書ローテーション処理を行います。削除できるのは、Inactive (無効) 状態の証明書のみです。

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. アプリケーションのリストで [your application] (お客様のアプリケーション) をクリックします。
4. アプリケーションの詳細ページで、[Configuration] (構成) タブを選択します。[IAM Identity Center のメタデータ] で [証明書の管理] を選択します。

5. [IAM Identity Center 証明書] ページで、削除する証明書を選択します。[Actions] (アクション) を選択してから、[Delete] (削除) を選択します。
6. [Delete certificate] (証明書の削除) ダイアログボックスで、[Delete] (削除) をクリックします。

証明書の有効期限切れステータスインジケーター

IAM アイデンティティセンターコンソールでは、[アプリケーション] ページに各アプリケーションのプロパティのステータス表示アイコンが表示されます。これらのアイコンは、リストの各証明書名の横にある [有効期限] 列に表示されます。以下は、IAM アイデンティティセンターが各証明書に対してどのアイコンを表示するかの基準です。

- 赤 — 証明書が現在期限切れであることを示します。
- 黄 — 証明書の有効期限が 90 日以下であることを示します。
- 緑 — 証明書が現在有効であり、少なくとも 90 日間有効であることを示します。

証明書のステータスを確認するには

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. アプリケーションの一覧で、[Expires on] (有効期限) 列に表示されている証明書のステータスを確認します。

IAM アイデンティティセンターコンソールのアプリケーションプロパティを理解する

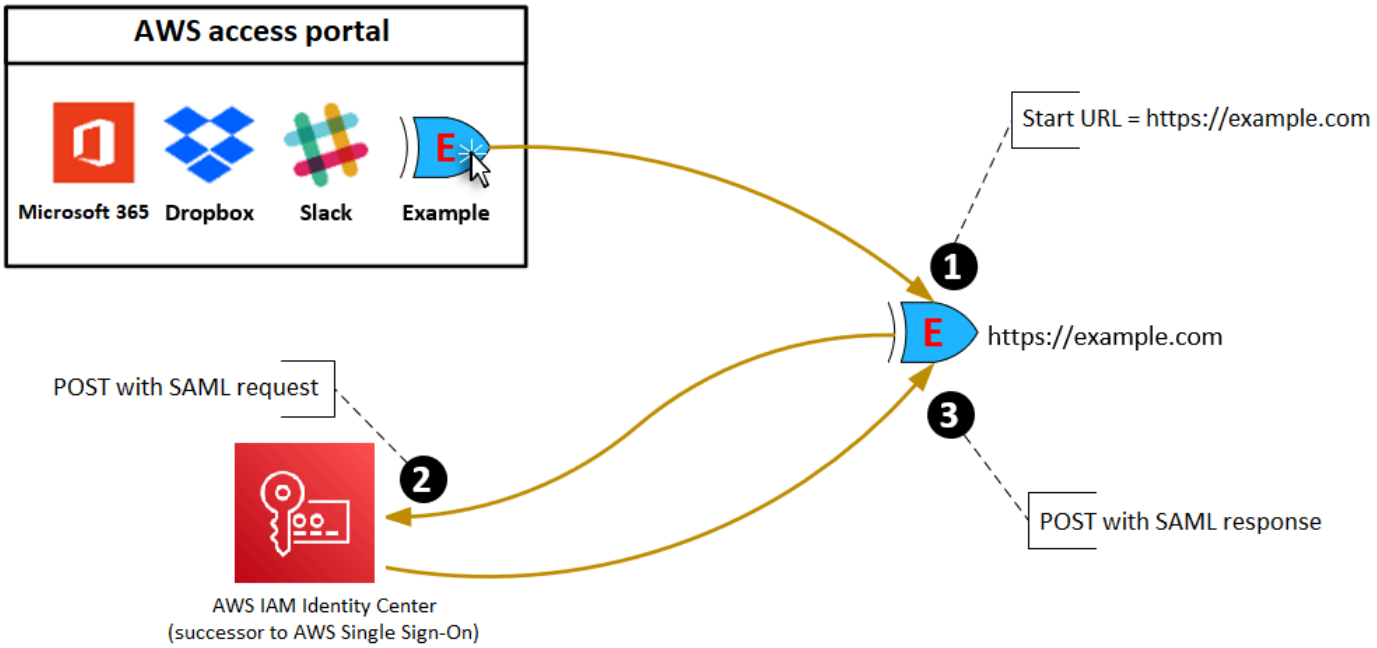
IAM Identity Center では、アプリケーションの開始 URL、リレーステート、セッション時間を設定することで、ユーザーエクスペリエンスをカスタマイズできます。

アプリケーション開始 URL

アプリケーション開始 URL を使用して、アプリケーションでフェデレーションプロセスを開始できます。一般的な用途は、サービスプロバイダー (SP) 開始バインディングのみをサポートするアプリケーション用です。

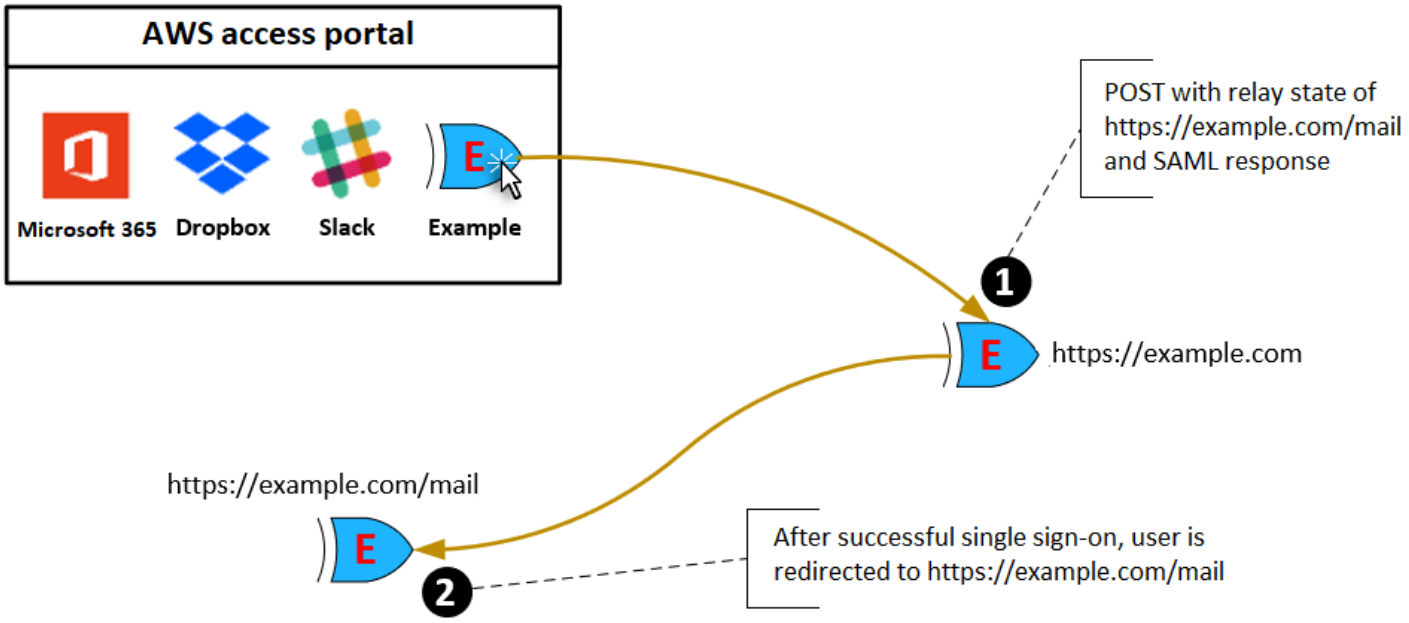
以下のステップと図は、ユーザーが AWS アクセスポータルでアプリケーションを選択したときのアプリケーション開始 URL の認証ワークフローを示しています。

1. ユーザーのブラウザは、アプリケーション開始 URL (この場合は https://example.com) の値を使用して認証リクエストをリダイレクトします。
2. アプリケーションは、IAM Identity Center にSAMLRequest付きのHTMLPOSTを送信します。
3. 次に IAM Identity Center は HTMLPOST を SAMLResponse でアプリケーションに送り返します。



リレーステート

フェデレーション認証プロセス中に、リレーステートはアプリケーション内でユーザーをリダイレクトします。SAML 2.0 の場合、この値は、変更されずにアプリケーションに渡されます。アプリケーションのプロパティ設定が完了すると、IAM Identity Center が SAML レスポンスとともにリレーステート値をアプリケーションに送信します。



セッション期間

セッション期間は、アプリケーションのユーザー セッションが有効な時間の長さです。SAML 2.0 では、これは、SAML アサーションの要素 `saml2:AuthNStatement` の `SessionNotOnOrAfter` の日付を設定するために使用されます。

セッション期間は次のいずれかの方法でアプリケーションによって解釈されます。

- アプリケーションはこれを使用して、ユーザーのセッションに許可される最大時間を決定できます。アプリケーションによっては、より短い時間のユーザーセッションを生成する可能性があります。これは、設定されたセッションの長さよりも短い期間のユーザーセッションのみをアプリケーションがサポートする場合に発生する可能性があります。
- アプリケーションはこれを正確な期間として使用でき、管理者に値の設定を許可しない場合があります。これは、アプリケーションが特定のセッションの長さのみをサポートするときに発生する可能性があります。

セッション期間の使用の詳細については、ご使用のアプリケーションのドキュメントを参照してください。

IAM Identity Center コンソールでアプリケーションへのユーザーアクセスを割り当てます。

アプリケーションカタログ内の SAML 2.0 アプリケーションまたはカスタム SAML 2.0 アプリケーションへのシングルサインオンアクセスをユーザーに割り当てることができます。

グループ割り当てに関する考慮事項:

- アクセス権をグループに直接割り当てます。アクセス権限の管理をシンプルにするためには、個々のユーザーではなくグループに直接アクセスを割り当てることをお勧めします。グループを使用すると、個々のユーザーにこれらのアクセス権限を適用するのではなく、ユーザーグループに対してアクセス権限を付与または拒否できます。ユーザーが別の組織に異動した場合、そのユーザーを別のグループに移動させるだけです。その後、ユーザーは新しい組織に必要な権限を自動的に受け取ります。
- ネストされたグループはサポートされません。アプリケーションへのアクセス許可をユーザーに割り当てる場合、IAM Identity Center はネストされたグループへのユーザーの追加はサポートしていません。ユーザーがネストされたグループに追加されると、サインイン時に「アプリケーションがありません」というメッセージが表示される場合があります。割り当ては、ユーザーが属している直属のグループに対して行われなければなりません。

ユーザーまたはグループにアプリケーションへのアクセスを割り当てるには

> **Important**
>
> AWS マネージドアプリケーションでは、関連するアプリケーションコンソール内から、または API を介して直接ユーザーを追加する必要があります。

1. IAM Identity Center コンソール を開きます。

   > **Note**
   >
   > ユーザーを AWS Managed Microsoft AD で管理する場合は、次の手順に進む前に、IAM アイデンティティセンターコンソールで、AWS Managed Microsoft AD ディレクトリがある AWS リージョンを使用していることを確認してください。

2. [Applications] (アプリケーション) を選択します。

3. アプリケーションのリストで、アクセスを割り当てるアプリケーション名を選択します。
4. アプリケーションの詳細ページの [割り当てられたユーザー] セクションで、[割り当てられたユーザー] をクリックします。
5. [ユーザーの割り当て] ダイアログボックスにユーザーの表示名またはグループ名を入力します。複数のユーザーまたはグループを指定するには、検索結果に表示される該当するアカウントを選択します。
6. [ユーザーの割り当て] を選択します。

SAML 2.0 アプリケーションへのユーザーアクセスを削除する

アプリケーションカタログの SAML 2.0 アプリケーションまたはカスタム SAML 2.0 アプリケーションへのユーザーアクセスを削除するには、この手順を実行します。認証セッションと期間の詳細については、「IAM アイデンティティセンターの認証セッションについて」を参照してください。

アプリケーションへのユーザーアクセスを削除するには

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. アプリケーションのリストで、ユーザーアクセスを削除するアプリケーションを選択します。
4. アプリケーションの詳細ページの [割り当てられたユーザー] セクションで、削除するユーザーまたはグループを選択してから、[削除] を選択します。
5. [Remove access] (アクセスの削除) ダイアログボックスで、ユーザー名またはグループ名を確認します。次に、[Remove access] (アクセスの削除) を選択します。

アプリケーションの属性を IAM Identity Center の属性にマップする

一部のサービスプロバイダーでは、ユーザーのサインインに関する追加のデータを渡すためにカスタム SAML アサーションが必要です。その場合は、以下の手順を使用して、アプリケーションのユーザー属性を IAM Identity Center の対応する属性にマップする方法を指定します。

アプリケーションの属性を IAM Identity Center の属性にマップするには

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。

3. アプリケーションのリストで、属性をマップするアプリケーションを選択します。
4. アプリケーション詳細ページで [アクション] を選択し、[属性マッピングを編集] を選択します。
5. [新規属性マッピングの追加] を選択します。
6. 最初のテキストボックスに、アプリケーションの属性を入力します。
7. 2 番目のテキストボックスに、アプリケーションの属性にマップする IAM Identity Center の属性を入力します。たとえば、アプリケーションの属性 **`Username`** を IAM Identity Center のユーザー属性 **`email`** にマップできます。IAM Identity Center で許可されるユーザー属性のリストについては、「IAM アイデンティティセンターと外部 ID プロバイダーディレクトリ間の属性マッピング」の表を参照してください。
8. この一覧の 3 番目の列で、メニューから属性に該当する形式をクリックします。
9. [Save changes] (変更の保存) をクリックします。

AWS アカウント へのアクセスを設定する

IAM Identity Center の組織インスタンスは、AWS Organizations と統合されています。これにより、各アカウントへのアクセスを個別に設定することなく、複数の AWS アカウント にわたるアクセス許可を一元管理できます。

次の表は、考慮すべきアカウントアクセス管理オプションを比較したものです。

	IAM ロールとアカウントアクセスマネージャー	IAM アイデンティティセンターのアクセス許可セット	直接 IAM フェデレーションを使用する IAM ロール
適しているチーム	ワークフォースユーザーとグループに、アカウントごとに異なるカスタム IAM ロールが付与されます。ロールの作成とプロビジョニングを分散させて、ユーザーへのロールの割り当てを一元化します。	読み取り専用や管理者などベースラインワークフォースアクセスを統一します。ロールの作成とプロビジョニングを一元化します。	ワークロード
範囲 –	1 つの AWS 組織に複数のアカウント	1 つの AWS 組織に複数のアカウント	アカウントあたり
IAM ロールのプロビジョニング	• Infrastructure as code (IaC) • AWS IAM コンソールから手動でプロビジョニング	自動的にプロビジョニングされる	• Infrastructure as code (IaC) • AWS IAM コンソールまたは外部 IdP コンソールから手動でプロビジョニング
ロール・トゥ・アイデンティティマッピ	アカウントアクセスマネージャー	IAM アイデンティティセンター	外部 IdP

	IAM ロールとアカウントアクセスマネージャー	IAM アイデンティティセンターのアクセス許可セット	直接 IAM フェデレーションを使用する IAM ロール
ングは以下のところにあります			
エンドユーザーエクスペリエンス	ユーザーがアカウントアクセスポータル URL から AWS アカウント にアクセスします。IAM Identity Center 認証が必要です。	ユーザーが AWS アクセスポータル URL から AWS アカウントにアクセスします。	ユーザーは、IdP ポータルのアカウント固有の SAML アプリケーション (アイコン) を介して AWS アカウント にアクセスします。
AWS CLI ユーザーエクスペリエンス	ユーザーは AWS にサインインし、ウェブブラウザで特定のロールを持つ AWS アカウント にアクセスします。ユーザーはコマンドラインに「aws login」と入力して、ブラウザから IAM ロールセッションの認証情報を取得します。IAM ロールセッションの期間中、ユーザーは再認証することなく AWS CLI を引き続き使用できます。	ユーザーは「aws configure sso」と入力して、目的のアカウントとロールのペアを含むプロファイルを設定します。ユーザーは「aws sso login」と入力し、プロファイルを使用して新しいセッションを開始します。アクティブな IAM Identity Center セッションがない場合、ユーザーはブラウザで認証します。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」を参照してください。	AWS SDK 認証情報プロバイダーを使用したカスタム統合

AWS アカウント タイプ

AWS Organizations には次の 2 種類の AWS アカウント があります。

- 管理アカウント - 組織を作成するために使用する AWS アカウント。
- メンバーアカウント - 組織に属する残りの AWS アカウント。

AWS アカウント タイプの詳細については、「AWS Organizations ユーザーガイド」の「AWS Organizations 用語とコンセプト」を参照してください。

IAM アイデンティティセンターの「委任管理者」としてメンバーアカウントを登録することもできます。このアカウントのユーザーは、ほとんどの IAM Identity Center 管理タスクを実行できます。詳細については、「委任された管理」を参照してください。

次の表は、タスクとアカウントタイプごとに、IAM Identity Center 管理タスクをアカウント内のユーザーが実行できるかどうかを示しています。

IAM Identity Center 管理タスク	メンバーアカウント	委任された管理者アカウント	管理アカウント
ユーザーまたはグループの読み取り (グループ自体とグループのメンバーシップの読み取り)	✓ はい	✓ はい	✓ はい
ユーザーまたはグループを追加、編集、削除する	✗ なし	✓はい*	✓ はい
ユーザーアクセスの有効化または無効化	✗ いいえ	✓ はい	✓ はい
受信属性を有効化、無効化、管理する	✗ いいえ	✓ はい	✓ はい
ID ソースの変更または管理	✗ いいえ	✓ はい	✓ はい

IAM Identity Center 管理タスク	メンバーアカウント	委任された管理者アカウント	管理アカウント
カスタマーマネージドアプリケーションの作成、編集、削除	⊗ いいえ	⊘ はい	⊘ はい
AWS マネージドアプリケーションの作成、編集、削除	⊘ はい	⊘ はい	⊘ はい
MFA を設定	⊗ いいえ	⊘ はい	⊘ はい
管理アカウントにプロビジョニングされていない権限セットを管理する	⊗ いいえ	⊘ はい	⊘ はい
管理アカウントにプロビジョニングされた権限セットを管理する	⊗ なし	⊗ いいえ	⊘ はい
IAM Identity Center を有効にする	⊗ なし	⊗ いいえ	⊘ はい
IAM Identity Center 設定を削除する	⊗ なし	⊗ いいえ	⊘ はい
管理アカウントのユーザーアクセスを有効または無効にします。	⊗ なし	⊗ いいえ	⊘ はい
メンバーアカウントを委任管理者として登録または登録解除する	⊗ なし	⊗ いいえ	⊘ はい

* 管理アカウントへのユーザーとグループの割り当てに関する委任管理のベストプラクティスを参照してください。

AWS アカウント アクセスの割り当て

「アクセス許可セット」を使用すると、組織内のユーザーやグループに AWS アカウント へのアクセスを割り当てる方法を簡素化することができます。権限セットは IAM Identity Center に保存され、ユーザーおよびグループが持つこの AWS アカウント に対するアクセスのレベルを定義します。1 つの権限セットを作成して、組織内の複数の AWS アカウント に割り当てることができます。同じユーザに複数の権限セットを割り当てることもできます。

アカウントアクセスマネージャーを使用することもできます。これは、組織のアカウント内の IAM Identity Center のユーザーやグループに既存の IAM ロールを割り当てることができる IAM 機能です。アカウントアクセスマネージャーを単独で使用することも、アクセス許可セットと組み合わせて使用することもできます。アカウントアクセスマネージャーを使用すると、カスタム信頼ポリシー、ABAC のロールタグ、設定可能なロールパスなどの IAM ロールの完全な機能セットにアクセスできます。

アクセス権限セットの詳細については、「アクセス許可セットの作成、管理と削除」を参照してください。

> **Note**
>
> また、ユーザーにアプリケーションへのシングルサインオンアクセスを割り当てることもできます。詳細については、「アプリケーションへのアクセスを設定する」を参照してください。

エンドユーザーエクスペリエンス

AWS アクセスポータル は、IAM アイデンティティセンターユーザーに、ウェブポータルを介して割り当てられたすべての AWS アカウント およびアプリケーションへのシングルサインオンアクセスを提供します。AWS アクセスポータルは、AWS リソースを管理するためのサービスコンソールの集合体である AWS マネジメントコンソール とは異なります。

権限セットを作成すると、このセットに指定した名前は、使用可能なロールとして AWS アクセスポータルに表示されます。ユーザーは AWS アクセスポータルにサインインし、AWS アカウント を

選択し、次にロールを選択します。ロールを選択した後、AWS マネジメントコンソール を使用して AWS サービスにアクセスするか、一時的な資格情報を取得してプログラム的に AWS サービスにアクセスすることができます。

プログラムで AWS マネジメントコンソール を開くか、一時的な認証情報を取得して AWS にアクセスするには、次の手順を実行する必要があります。

1. ユーザーはブラウザーウィンドウを開き、入力されたサインイン URL を使用して AWS アクセスポータルに移動します。
2. ディレクトリ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ます。
3. 認証後、AWS アクセスポータルページで [アカウント] タブを選択し、アクセスできる AWS アカウントのリストを表示させます。
4. ここから使用したい AWS アカウントを選択します。
5. AWS アカウント の名前の下に、ユーザが割り当てられている権限セットが利用可能な ロールとして表示されます。たとえば、ユーザー `john_stiles` を `PowerUser` 権限セットに割り当てている場合、AWS アクセスポータルに表示されるロール名は `PowerUser/john_stiles` となります。複数のアクセス権限セットが割り当てられている場合は、使用する ロールを選択する。ユーザーはロールを選択して AWS マネジメントコンソールにアクセスできます。
6. ロールに加えて、AWS アクセスポータルユーザーは、[アクセスキー] を選択して、コマンドラインまたはプログラムによるアクセスのための一時的な認証情報を取得できます。

ワークフォースユーザーに提供できるステップバイステップガイドについては、AWS アクセスポータルのセットアップと使用 と AWS CLI または AWS SDK の IAM Identity Center のユーザー認証情報を取得します。 を参照してください。

アクセスの強制と制限

IAM Identity Center を有効にすると、IAM Identity Center はサービスにリンクされたロールを作成します。サービスコントロールポリシーを使用することもできます。

アクセス権の委任と強制

サービスにリンクされたロールは、AWS のサービスに直接リンクされた一意のタイプの IAM ロールです。IAM Identity Center を有効にすると、IAM Identity Center は組織内の各 AWS アカウント にサービスリンクされたロールを作成できます。このロールは、IAM Identity Center が、組織内の特定の AWS アカウント へのシングルサインオンアクセスを持つユーザーを AWS Organizations に委譲

し、実施できるようにするための事前定義された権限を提供します。このロールを使用するには、アカウントへのアクセス権を持つユーザーを 1 人以上割り当てる必要があります。詳細については、「IAM アイデンティティセンターのサービスリンクロールについて」および「IAM Identity Center のサービスリンクロールの使用」を参照してください。

メンバーアカウントからのアイデンティティストアへのアクセスを制限する

IAM Identity Center で使用される Identity Store サービスの場合、メンバーアカウントにアクセスできるユーザーは、「読み取り」権限を必要とする API アクションを使用できます。メンバーアカウントは、「sso-directory」および「identitystore」ネームスペースの両方に対して「読み取り」アクションにアクセスできます。詳細については、「Service Authorization Reference」の「Actions, resources, and condition keys for AWS IAM アイデンティティセンター directory」と「Actions, resources, and condition keys for AWS Identity Store」を参照してください。

メンバーアカウントのユーザーが Identity Store で API 操作を使用できないようにするには、「サービスコントロールポリシー (SCP) をアタッチ」できます。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。次の SCP の例では、メンバーアカウントのユーザーがアイデンティティストア内のあらゆる API オペレーションにアクセスできないようにします。

```
    {
        "Sid": "ExplicitlyBlockIdentityStoreAccess",
        "Effect": "Deny",
        "Action": ["identitystore:*", "sso-directory:*"],
        "Resource": "*"
    }
```

> **Note**
>
> AWS マネージドアプリケーションが IAM アイデンティティセンターと適切に機能するようにするには、アプリケーションをデプロイした AWS アカウント にこの SCP を適用しないようにする必要があります。また、委任管理を使用する場合は、この SCP を委任管理アカウントに適用しないでください。詳細については、「ベストプラクティス」を参照してください。

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。

委任された管理

委任管理により、登録済みのメンバーアカウントに割り当てられたユーザーが IAM Identity Center の大部分の管理タスクを簡単に実行できます。IAM Identity Center を有効にすると、デフォルトで AWS Organizations の管理アカウントに IAM Identity Center インスタンスが作成されます。これは当初、IAM Identity Center が組織のすべてのメンバーアカウントにわたってロールをプロビジョニング、プロビジョニング解除、更新できるようにするために設計されたものです。IAM Identity Center インスタンスは常に管理アカウントに存在する必要があるが、IAM Identity Center の管理を AWS Organizations のメンバーアカウントに委任することで、管理アカウントの外部から IAM Identity Center を管理する機能を拡張することができます。

委任管理を有効にすると、次の利点があります。

- 管理アカウントへのアクセスを必要とするユーザーの数を最小限に抑え、セキュリティ上の懸念を軽減します。
- 特定の管理者が、アプリケーションや組織のメンバーアカウントにユーザーやグループを割り当てることができます。

IAM Identity Center と AWS Organizations の連携の詳細については、「AWS アカウント へのアクセスを設定する」を参照してください。追加情報や、委任管理の設定方法を示す企業シナリオの例を確認するには、「AWS セキュリティブログ」の「IAM アイデンティティセンター委任管理入門」を参照してください。

トピック

- ベストプラクティス
- 前提条件
- メンバーアカウントを作成する
- メンバーアカウントを登録解除する
- 委任管理者として登録されているメンバーアカウントが表示されます。

ベストプラクティス

委任管理を設定する前に考慮すべきいくつかのベストプラクティスを以下に示します。

- 管理アカウントへの最小権限の付与 — 管理アカウントは特権の高いアカウントであり、最小権限の原則に従うため、管理アカウントへのアクセスをできるだけ少数のユーザーに制限することを強

くお勧めします。委任管理者機能は、管理アカウントへのアクセスを必要とするユーザーの数を最小限に抑えることを目的としています。また、一時的な昇格されたアクセスを使用して、必要な場合にのみこのアクセスを許可することもできます。

- 管理アカウント専用のアクセス許可セット – 管理アカウント専用のアクセス許可セットを使用します。セキュリティ上の理由から、管理アカウントへのアクセスに使用されるアクセス許可セットは、管理アカウントの IAM アイデンティティセンター管理者のみが変更できます。委任管理者は、管理アカウントでプロビジョニングされたアクセス許可セットを変更することはできません。
- 管理アカウントのアクセス許可セットにのみユーザーを割り当てる (グループではなく) – 管理アカウントには特別な権限があるため、コンソールまたは AWS Command Line Interface (CLI) でこのアカウントへのアクセスを割り当てるときは注意が必要です。管理アカウントにアクセスできるアクセス許可セットにグループを割り当てると、それらのグループのメンバーシップを変更するアクセス許可を持つすべてのユーザーは、それらのグループとの間でユーザーを追加または削除できるため、管理アカウントにアクセスできるユーザーに影響します。これは、ID プロバイダー (IdP) 管理者、Microsoft Active Directory Domain Service (AD DS) 管理者、IAM アイデンティティセンター管理者など、ID ソースを制御できるすべてのグループ管理者です。したがって、管理アカウントでアクセスを許可するアクセス許可セットにユーザーを直接割り当て、グループを回避する必要があります。グループを使用して管理アカウントへのアクセスを管理する場合は、IdP に適切なコントロールが設定されていることを確認し、それらのグループを変更できるユーザーを制限し、それらのグループへの変更 (または管理アカウントのユーザーの認証情報への変更) を必要に応じてログに記録して確認します。
- Active Directory ロケーションを検討 — IAM Identity Center のアイデンティティソースとして Active Directory を使用する予定の場合は、IAM Identity Center の委任管理者機能を有効にしたメンバーアカウント内のディレクトリを探してください。IAM アイデンティティセンター ID ソースを他のソースから Active Directory に変更するか、Active Directory から他のソースに変更する場合、そのディレクトリは IAM アイデンティティセンター委任管理者メンバーアカウントに存在している必要があります。Active Directory を管理アカウントに配置する場合は、委任された管理者に必要なアクセス許可がないため、管理アカウントでセットアップを実行する必要があります。

外部 ID ソースを使用して委任管理アカウントの IAM アイデンティティセンター ID ストアアクションを制限する

IdP や Directory Service などの外部 ID ソースを使用する場合は、IAM アイデンティティセンター管理者が委任された管理アカウント内から実行できる ID ストアアクションを制限するポリシーを実装する必要があります。書き込みおよび削除オペレーションは慎重に検討する必要があります。一般的に、外部 ID ソースは、ユーザーとその属性、およびグループメンバーシップの信頼できるソースです。ID ストア API または コンソールを使用してこれらを変更すると、通常の同期サイクル中に変更

が上書きされます。これらのオペレーションは、信頼できる ID ソースの排他的な制御に任せることをお勧めします。これにより、グループメンバーシップコントロールを IdP 管理者に任せるのではなく、IAM アイデンティティセンター管理者がグループメンバーシップを変更して、グループが割り当てたアクセス許可セットまたはアプリケーションへのアクセスを許可することも防止されます。また、委任管理アカウントから SCIM ベアラートークンを作成できるユーザーも保護する必要があります。これにより、メンバーアカウントの管理者が SCIM クライアントを介してグループとユーザーを変更できるようになる可能性があるためです。

委任管理者アカウントからの書き込みまたは削除オペレーションが適切である場合があります。例えば、メンバーを追加せずにグループを作成し、IdP 管理者がグループを作成するのを待たずにアクセス許可セットに割り当てることができます。IdP 管理者がグループをプロビジョニングし、IdP 同期プロセスがグループメンバーを確立するまで、その割り当てには誰もアクセスできません。また、IdP 同期プロセスがユーザーまたはグループによるアクセスの削除を待てない間にサインインまたは認可を防ぐには、ユーザーまたはグループを削除することをお勧めします。ただし、このアクセス許可を悪用すると、ユーザーにとって破壊的になる可能性があります。ID ストアのアクセス許可を割り当てるときは、最小特権の原則を使用する必要があります。サービスコントロールポリシー (SCP) を使用して、委任管理アカウント管理者が許可する ID ストアアクションをコントロールできます。

以下の SCP の例では、ID ストア API と AWS マネジメントコンソール を使用してユーザーをグループに割り当てることを禁止しています。これは、ID ソースが外部である場合に推奨されます。これは、Directory Service または外部 IdP からのユーザー同期には影響しません (SCIM 経由)。

> **Note**
>
> 外部 ID ソースを使用していても、組織はユーザーとグループのプロビジョニングのために ID ストア API に完全または部分的に依存する可能性があります。したがって、この SCP をアクティブ化する前に、ユーザープロビジョニングプロセスがこの ID ストア API オペレーションを使用していないことを確認する必要があります。また、グループメンバーシップの管理を特定のグループに制限する方法については、次のセクションを参照してください。

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

```
  ]
}
```

管理アカウントへのアクセスを許可するグループのみにユーザーを追加しないようにするには、グループ ARN を使用してこれらの特定のグループを `arn:${Partition}:identitystore:::group/${GroupId}` の形式で参照できます。ID ストアで使用できるこのリソースタイプとその他のリソースタイプは、「サービス認可リファレンス」の「AWS ID ストアで定義されるリソースタイプ」に記載されています。SCP に追加の ID ストア API を含めることを検討することもできます。詳細については、「ID ストア API リファレンス」の「アクション」を参照してください。

SCP に次のポリシーステートメントを追加することで、委任された管理者による SCIM ベアラートークンの作成を防ぐことができます。これは両方の外部 ID ソースに適用できます。

> **Note**
>
> 委任管理者が SCIM でユーザープロビジョニングを設定したり、定期的な SCIM ベアラートークンローテーションを実行したりする必要がある場合は、委任管理者がこれらのタスクを完了できるように、この API へのアクセスを一時的に許可する必要があります。

```
{ "Effect": "Deny",
  "Action": ["sso-directory:CreateBearerToken"],
  "Resource": [ "*" ]
}
```

ローカルマネージドユーザーの委任管理アカウントで IAM アイデンティティセンター ID ストアアクションを制限する

外部 IdP または Directory Service を使用するのではなく、IAM アイデンティティセンターでユーザーとグループを直接作成する場合は、ユーザーの作成、パスワードのリセット、およびグループメンバーシップのコントロールを行えるユーザーに対して予防措置を講じる必要があります。これらのアクションにより、管理者は、サインインできるユーザーと、グループのメンバーシップを通じてアクセスできるユーザーに大きな権限が与えられます。これらのポリシーは、SCP としてではなく、IAM アイデンティティセンター管理者に使用するアクセス許可セット内のインラインポリシーとして実装するのが最適です。次のインラインポリシーの例には、2 つの目的があります。まず、特定のグループにユーザーを追加しないようにします。これを使用して、委任管理者が管理アカウン

トへのアクセスを許可するグループにユーザーを追加しないようにできます。次に、SCIM ベアラートークンの発行を防ぎます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "identitystore:CreateGroupMembership"
      ],
      "Resource": [
        "arn:partition:identitystore:::group/group-id-1",
        "arn:partition:identitystore:::group/group-id-2"
      ]
    },
    {
      "Effect": "Deny",
      "Action": [
        "sso-directory:CreateBearerToken"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

partition はお使いの AWS パーティション (aws、aws-cn、または aws-us-gov) に置き換え、*group-id-1* と *group-id-2* は保護する ID ストアグループの ID に置き換えます。

IAM アイデンティティセンター設定管理を PermissionSet 管理から分離する

外部 ID ソースの変更、SCIM トークン管理、セッションタイムアウト設定などの管理タスクをタスクから分離して、管理アカウントから個別の管理者アクセス許可セットを作成して、アクセス許可セットを作成、変更、割り当てます。

SCIM ベアラートークンの発行を制限する

SCIM ベアラートークンを使用すると、IAM アイデンティティセンターの ID ソースが Okta や Entra ID などの外部 IdP である場合、外部 ID ソースは SCIM プロトコルを介してユーザー、グループ、グループメンバーシップをプロビジョニングできます。次の SCP を設定して、委任された管理者に

よる SCIM ベアラートークンの作成を防ぐことができます。委任管理者が SCIM でユーザープロビジョニングを設定したり、定期的な SCIM ベアラートークンローテーションを実行したりする必要がある場合は、委任管理者がこれらのタスクを完了できるように、この API へのアクセスを一時的に許可する必要があります。

```
    { "Effect": "Deny",
      "Action": ["sso-directory:CreateBearerToken"],
      "Resource": [ "*" ]
}
```

アクセス許可セットタグとアカウントリストを使用して、特定のアカウントの管理を委任する

IAM アイデンティティセンター管理者に割り当てるアクセス許可セットを作成して、アクセス許可セットを作成できるユーザーと、どのアクセス許可セットをどのアカウントに割り当てることができるかを委任できます。これは、アクセス許可セットにタグ付けし、管理者に割り当てるアクセス許可セットでポリシー条件を使用することによって行われます。たとえば、ユーザーが特定の方法でタグ付けされたアクセス許可セットを作成できるようにするアクセス許可セットを作成できます。また、管理者が特定のアカウントに特定のタグが付いたアクセス許可セットの割り当てができるようにするポリシーを作成することもできます。これにより、管理者に委任された管理アカウントに対するアクセスと権限を変更する権限を与えることなく、アカウントに対する管理を委任できます。例えば、委任管理アカウントでのみ使用するアクセス許可セットにタグを付けることで、特定のユーザーにのみ、委任管理アカウントに影響するアクセス許可セットと割り当てを変更するアクセス許可を付与するポリシーを指定できます。また、委任管理アカウント以外のアカウントのリストを管理するアクセス許可を他のユーザーに付与することもできます。詳細については、「AWS セキュリティブログ」の「AWS IAM アイデンティティセンター でのアクセス許可セットの管理とアカウント割り当ての委任」を参照してください。

前提条件

アカウントを委任管理者として登録する前に、まず次の環境を展開する必要があります。

- AWS Organizations は、デフォルトの管理アカウントに加えて、少なくとも 1 つのメンバーアカウントを有効にして設定する必要があります。
- ID ソースが Active Directory に設定されている場合は、IAM Identity Center の構成可能な AD 同期機能を有効にする必要があります。

メンバーアカウントを作成する

委任管理を設定するには、まず組織のメンバーアカウントを委任管理者として登録する必要があります。そのメンバーアカウント内の十分な権限を持つユーザーは、IAM Identity Center への管理アクセス権を持ちます。メンバーアカウントが委任管理用に正常に登録されると、そのメンバーアカウントは「委任管理者アカウント」と呼ばれます。委任管理者アカウントが実行できるタスクの詳細については、AWS アカウント タイプ を参照してください。

IAM Identity Center では、一度に 1 つのメンバーアカウントのみを委任管理者として登録できます。メンバーアカウントは、管理アカウントの認証情報を使用してサインインしている場合にのみ登録できます。

以下の手順に従って、AWS組織内の特定のメンバーアカウントを委任管理者として登録して IAM Identity Center への管理アクセスを許可します。

> **Important**
>
> この操作により、IAM Identity Center の管理アクセスが、このメンバーアカウントの管理者ユーザーに委任されます。この委任された管理者アカウントに対して十分な権限を持つすべてのユーザーは、以下を除くすべての IAM Identity Center 管理タスクをアカウントから実行できます。
>
> - IAM Identity Center を有効にする
> - IAM Identity Center 設定を削除する
> - 管理アカウントにプロビジョニングされた権限セットの管理
> - 他のメンバーアカウントを委任管理者として登録または登録解除する
> - 管理アカウントでのユーザーアクセスの有効化または無効化
>
> 委任管理者はグループメンバーシップを編集できます。

メンバーアカウントを登録する

1. AWS Organizations の管理アカウント認証情報を使用して AWS マネジメントコンソール にサインインします。委任管理者の登録 API を実行するには、管理アカウントの認証情報が必要です。

2. IAM Identity Center が有効になっているリージョンを選択し、「IAM Identity Center コンソール」を開きます。
3. [設定] を選択し、[管理] タブを選択します。
4. [の委任管理者]セクションで、[登録] を選択します。
5. [委任管理者の登録] ページで、登録したい AWS アカウント を選択し、[アカウントを登録] を選択します。

メンバーアカウントを登録解除する

メンバーアカウントは、管理アカウントの認証情報を使用してサインインした場合にのみ、登録解除できます。

以下の手順を使用して、委任管理者として指定されていたAWS組織内のメンバーアカウントの登録を解除し、IAM Identity Center から管理者アクセス権を削除します。

> **Important**
>
> アカウントの登録を解除すると、すべての管理者ユーザーがそのアカウントから IAM Identity Center を管理できなくなります。その結果、このアカウントから IAM Identity Center ID、アクセス管理、認証、またはアプリケーションアクセスを管理できなくなります。この操作は、IAM Identity Center で構成された権限や割り当てには影響しないため、エンドユーザーはAWSアクセスポータル内からアプリや AWS アカウント に引き続きアクセスできる、エンドユーザーへの影響はありません。

メンバーアカウントを登録解除する

1. AWS Organizations の管理アカウント認証情報を使用して AWS マネジメントコンソール にサインインします。委任管理者の登録解除 API を実行するには、管理アカウントの認証情報が必要です。
2. IAM Identity Center が有効になっているリージョンを選択し、[IAM Identity Center コンソール] を開きます。
3. [設定] を選択し、[管理] タブを選択します。
4. [委任管理者]セクションで、[登録解除] を選択します。
5. [アカウントの登録解除] ダイアログボックスでセキュリティ上の影響を確認し、メンバーアカウントの名前を入力して内容がわかっていることを確認します。

6. [アカウントの登録解除] を選択します。

委任管理者として登録されているメンバーアカウントが表示されます。

以下の手順を使用して、IAM Identity Center の委任管理者として構成されている AWS Organizations のメンバーアカウントを確認します。

登録済みのメンバーアカウントを表示するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [詳細] セクションで、[委任管理者] の下にある登録済みアカウント名を探します。この情報は、[管理] タブを選択し、[委任管理者] セクションで表示することでも確認できます。

AWS アカウントへの一時的な昇格アクセス

AWS アカウント へのアクセスはすべて、ある程度の特権を伴うものです。本番環境などの設定変更等、機密性の高い操作には、影響のおよぶ範囲や度合いを考慮して、特別な対応が必要になります。一時的な昇格アクセス (ジャストインタイムアクセスとも呼ばれる) は、特定のタスクを指定された期間に実行するための権限を要求、承認、および追跡する方法です。一時的な昇格アクセスは、権限セットや多要素認証など、他の形式のアクセス制御を補完します。

> **Note**
>
> ビジネス継続性を確保するために、 AWS マネジメントコンソール への緊急アクセスを設定することをお勧めします。

さまざまなお客様のニーズに対応するため、AWS IAM アイデンティティセンター は AWS セキュリティコンピーテンシーパートナーのソリューションと統合されます。AWS は、これらのソリューションが一時的な昇格されたアクセス要件の一般的なセットに対応していることを検証します。各パートナーソリューションを詳しく検討したうえで、事業内容、クラウド環境のアーキテクチャ、予算など、お客様固有のニーズや優先事項に最も適したソリューションをお選びください。

検証済みのソリューションには、Apono Access Management Platform、CyberArk Secure Cloud Access、Okta Access Requests、Tenable (以前は Ermetic) などがあります。

パートナーは、 パートナーセンター AWS セキュリティコンピテンシーアプリケーションを使用してソリューションを指名できます。詳細については、AWS セキュリティコンピテンシーパートナーを参照してください。

> **Note**
>
> リソースベース、Amazon Elastic Kubernetes Service、または AWS Key Management Service を使用している場合は、just-in-time ソリューションを選択する前に、「リソースポリシーのアクセス許可セットの参照、Amazon EKS クラスター設定マップ、AWS KMS キーポリシー」を参照してください。

AWS アカウント へのシングルサインオン· アクセス

接続しているディレクトリのユーザーに、共通の職務に基づいて AWS Organizations の組織の管理アカウントやメンバーアカウントの権限を割り当てることができます。または、特定のセキュリティ要件を満たすようにカスタムのアクセス権限を使用することもできます。例えば、データベース管理者には、開発用アカウントでは Amazon RDS に対する広範なアクセス権限を付与しますが、本番稼働用アカウントではそれらのアクセス権限を制限します。IAM Identity Center によって、AWS アカウント で必要なすべてのユーザーアクセス権限が自動的に設定されます。

> **Note**
>
> ユーザーやグループに AWS Organizations 管理アカウントでの操作権限を付与する必要があるかもしれません。高い特権を持つアカウントであるため、追加のセキュリティ制限により、この設定を行う前に、IAMFullAccess ポリシーまたは同等の権限を持つことが必要です。これらの追加のセキュリティ制限は、AWS 組織のどのメンバーアカウントにも必要ありません。

トピック

- AWS アカウント にユーザーまたはグループアクセスを割り当てる
- AWS アカウントへのユーザーおよびグループのアクセスを削除する
- ユーザーアクセス権の取り消し
- マスターアカウントでユーザーとグループにシングルサインオン· アクセスを割り当てる権限を委任する

AWS アカウント にユーザーまたはグループアクセスを割り当てる

接続先ディレクトリのユーザーとグループにシングルサインオン· アクセスを割り当て、アクセス権限セットによってそれらのユーザーとグループのアクセスレベルを決定するには、以下の手順を実行します。

既存のユーザーやグループ向けのアクセスを確認するには、「権限セットを表示および変更する」を参照してください。

> **Note**
>
> アクセス権限の管理をシンプルにするために、個々のユーザーではなくグループに直接アクセスを割り当てることをお勧めします。グループを使用すると、個々のユーザーにこれらのアクセス権限を適用するのではなく、ユーザーグループに対してアクセス権限を付与または拒否できます。ユーザーが別の組織に異動した場合、そのユーザーを別のグループに移動するだけで、新しい組織に必要なアクセス権限がそのユーザーに自動的に付与されます。

AWS アカウント にユーザーまたはグループアクセスを割り当てるには

1. IAM Identity Center コンソール を開きます。

   > **Note**
   >
   > 次のステップに進む前に、IAM Identity Center コンソールで、AWS Managed Microsoft AD ディレクトリが存在するリージョンを使用していることを確認してください。

2. ナビゲーションペインの [マルチアカウント権限] で、AWS アカウント を選択します。
3. AWS アカウント ページには、組織のツリービューリストが表示されます。アクセスを割り当てる AWS 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。IAM アイデンティティセンターの管理アクセスを設定する場合は、管理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。

   > **Note**
   >
   > ユーザーとグループにシングルサインオン· アクセスを割り当てる場合、1 つの権限セットにつき一度に 10 AWS アカウントまで選択できます。同じユーザーおよびグループのグループに 10 個以上の AWS アカウント を割り当てるには、他のアカウントの必

要に応じてこの手順を繰り返します。プロンプトが表示されたら、同じユーザー、グループ、権限セットを選択します。

4. [ユーザーまたはグループの割り当て] を選択します。
5. ステップ 1: ユーザーとグループの選択では、[ユーザーとグループを「*AWS-account-name*」に割り当てる] ページで、次の操作を行います。

   1. [ユーザー] タブで、シングルサインオン・アクセスを許可するユーザーを 1 人以上選択します。

      結果をフィルタリングするには、検索ボックスに目的のユーザーの名前を入力します。

   2. [グループ] タブで、シングルサインオン・アクセスを許可するグループを 1 つ以上選択します。

      結果をフィルターする場合は、検索ボックスに目的のグループの名前を入力します。

   3. 選択したユーザーとグループを表示するには、[選択したユーザーとグループ] の横にある横向きの三角形を選択します。
   4. 正しいユーザーとグループが選択されたことを確認したら、[次へ] を選択します。
6. ステップ 2: アクセス許可セットの選択 では、[アクセス許可セットを「*AWS-account-name*」に割り当てる] ページで、次の操作を行います。

   1. 1 つまたは複数の権限セットを選択します。必要に応じて、新しい権限セットを作成して選択できます。

      - 1 つ以上の既存の権限セットを選択するには、[権限セット] で、前のステップで選択したユーザーとグループに適用する権限セットを選択します。
      - 1 つ以上の新しい権限セットを作成するには、[権限セットの作成] を選択し、アクセス権限セットを作成します。 の手順に従います。適用する権限セットを作成したら、IAM Identity Center コンソールで「AWS アカウント」に戻り、[ステップ 2: 権限セットを選択する] が表示されるまで指示に従います。このステップに到達したら、作成した新しい権限セットを選択し、この手順の次のステップに進みます。

   2. 正しい権限セットが選択されていることを確認したら、[次へ] を選択します。
7. ステップ 3: 確認と送信では、[「*AWS-account-name*」への割り当てを確認と送信] ページで、次の操作を行います。

   1. 選択したユーザ、グループ、権限セットを確認します。

2. 正しいユーザ、グループ、権限セットが選択されていることを確認したら、[提出] を選択します。

考慮事項

- ユーザーとグループへの割り当てプロセスが完了するまでに数分かかることがあります。プロセスが正常に完了するまで、このページを開いたままにしておきます。
-

> **Note**
>
> ユーザーやグループに AWS Organizations 管理アカウントでの操作権限を付与する必要があるかもしれません。高い特権を持つアカウントであるため、追加のセキュリティ制限により、この設定を行う前に、IAMFullAccess ポリシーまたは同等の権限を持つことが必要です。これらの追加のセキュリティ制限は、AWS 組織のどのメンバーアカウントにも必要ありません。

8. 以下のいずれかに当てはまる場合は、ユーザーに MFA を求める の手順に従って IAM Identity Center の MFA を有効にしてください。

- ID ソースとしてデフォルトの Identity Center ディレクトリを使用しています。
- AWS Managed Microsoft AD ディレクトリまたは Active Directory の自己管理ディレクトリを ID ソースとして使用しており、AWS Directory Service で RADIUS MFA を使用していません。

> **Note**
>
> 外部 ID プロバイダーを使用している場合は、IAM アイデンティティセンターではなく外部 IdP が MFA 設定を管理することに注意してください。IAM Identity Center の MFA は、外部 IIdPs による使用はサポートされていません。

管理ユーザーのアカウントへのアクセス権をセットアップすると、対応する IAM ロールが IAM Identity Center により作成されます。このロールは IAM アイデンティティセンターによって制御され、関連する AWS アカウントで作成され、アクセス権限セットで指定されたポリシーがロールにアタッチされます。

または、AWS CloudFormation を使用してアクセス権限セットを作成して割り当て、それらのアクセス権限セットにユーザを割り当てることもできます。ユーザーは、AWS アクセスポータルにサインイン するか、AWS Command Line Interface (AWS CLI) コマンドを使用できます。

> **Note**
>
> このトピックでは、アクセス許可セットを使用したアクセスの割り当てについて説明します。完全な IAM ロール機能セットを使用して既存の IAM ロールを IAM Identity Center のユーザーやグループに割り当てるには、「IAM ユーザーガイド」の「アカウントアクセスマネージャー」を参照してください。

AWS アカウントへのユーザーおよびグループのアクセスを削除する

この手順を使用して、接続ディレクトリ内の 1 つまたは複数のユーザとグループのAWS アカウントへのシングルサインオン· アクセスを削除します。または、delete-account-assignment を使用することもできますAWS CLI。

> **Note**
>
> IAM アイデンティティセンターユーザーまたはグループのプロビジョニングを解除する必要がある場合は、まずユーザーとグループからアクセス許可セットの割り当てをすべて削除してから、ユーザーとグループを削除する必要があります。

AWS アカウント へのユーザーおよびグループのアクセスを削除するには

1. IAM Identity Center コンソール を開きます。
2. ナビゲーションペインの [マルチアカウントのアクセス許可] で、[AWS アカウント] を選択します。
3. [AWS アカウント] ページには、組織のツリービューリストが表示されます。シングルサインオン· アクセスを削除したいユーザーとグループを含む AWS アカウント の名前を選択します。
4. AWS アカウント の [概要] ページの [割り当てられたユーザーとグループ] で、1 人以上のユーザーまたはグループの名前を選択し、[アクセスを削除] を選択します。
5. [アクセス許可の削除] ダイアログで、ユーザーまたはグループの名前が正しいことを確認し、[アクセス許可の削除] を選択します。

ユーザーアクセス権の取り消し

IAM アイデンティティセンターユーザーのアクティブな権限セットセッションを取り消す一般的な手順は次のとおりです。この手順では、認証情報を侵害したユーザー、またはシステム内に存在する悪質な行為者のすべてのアクセス権を削除することを前提としています。前提条件として、権限セットによって作成されたアクティブな IAM ロールセッションを取り消す準備をする のガイダンスに従っている必要があります。「すべてを拒否する」ポリシーがサービスコントロールポリシー (SCP) 内に存在することを前提としています。

> **Note**
>
> AWS では、コンソールのみのオペレーションを除くすべてのステップを処理するオートメーションを構築することをお勧めしています。

1. アクセス権を取り消す必要があるユーザーのユーザー ID を取得します。ID ストア API を使用して、ユーザー名でユーザーを検索できます。
2. 拒否ポリシーを更新して、サービスコントロールポリシー (SCP) のステップ 1 のユーザー ID を追加します。このステップを完了すると、ターゲットユーザーはアクセス権を失い、ポリシーの影響下にあるすべてのロールでアクションを実行できなくなります。
3. そのユーザーに対するすべての権限セットの割り当てを削除します。アクセス権がグループメンバーシップを介して割り当てられている場合は、すべてのグループとすべての直接権限セットの割り当てからユーザーを削除します。このステップにより、ユーザーは追加の IAM ロールを引き受けることができなくなります。アクティブな AWS アクセスポータルセッションを持っているユーザーを無効にした場合、そのユーザーはアクセスが削除されるまでは新しいロールを引き受けることができます。
4. アカウントアクセスマネージャーで、ユーザーのすべての IAM ロール割り当てを削除します。アクセス権がグループメンバーシップを介して割り当てられている場合は、すべてのグループとすべての直接 IAM ロールの割り当てからユーザーを削除します。このステップにより、ユーザーはアカウントアクセスマネージャーで管理されている追加の IAM ロールを引き受けることができなくなります。アクティブな AWS アカウントアクセスポータルセッションを持っているユーザーを無効にした場合、そのユーザーはアクセスが削除されるまでは新しいロールを引き受けることができます。
5. ID プロバイダー (IdP) または Microsoft Active Directory を ID ソースとして使用する場合は、ID ソース内でユーザーを無効にします。ユーザーを無効にすると、追加の AWS アクセスポータルセッションが作成されなくなります。IdP または Microsoft Active Directory API ドキュメントを

使用して、このステップを自動化する方法について説明します。ID ソースとして IAM アイデンティティセンターディレクトリを使用している場合は、ユーザーアクセスをまだ無効にしないでください。ステップ 7 でユーザーアクセスを無効にします。

6. IAM アイデンティティセンターコンソールで、ユーザーを検索し、アクティブなセッションを削除します。

   a. [ユーザー] を選択します。

   b. アクティブなセッションを削除したいユーザーを選択します。

   c. ユーザー詳細ページで、[アクティブセッション] タブを選択します。

   d. 削除するセッションの横にあるチェックボックスを選択して、[セッションを削除] を選択します。

   ユーザーセッションを削除すると、ユーザーはすぐに AWS アクセスポータルにアクセスできなくなります。セッション期間についての詳細をご確認ください。

7. IAM アイデンティティセンターコンソールでユーザーアクセスを無効化します。

   a. [ユーザー] を選択します。

   b. アクセスを無効化したいユーザーを選択します。

   c. ユーザー詳細ページで、[一般情報] を展開し、[ユーザーアクセスを無効にする] ボタンを選択して、ユーザーが今後ログインできないようにします。

8. 拒否ポリシーは少なくとも 12 時間保持すること。そうでないと、アクティブな IAM ロールセッションを持つユーザーであれば IAM ロールのアクションを復元できてしまいます。12 時間経過すると、アクティブなセッションはすべて失効するため、ユーザーは IAM ロールに再度アクセスできなくなります。

> **Important**
>
> ユーザーセッションを停止する前にユーザーアクセスを無効にすると (ステップ 6 を実施する前にステップ 7 を完了した場合)、IAM Identity Center コンソールからユーザーセッションを停止する操作ができなくなります。ユーザーセッションを停止する前に誤って先にユーザーアクセスを無効にしてしまった場合は、ユーザーをいったん有効にしてセッションを停止してから、アクセスを再度無効にすることができます。

これにより、もしパスワードが侵害されたのであれば、ユーザーの認証情報を変更して割り当てを復元することができます。

マスターアカウントでユーザーとグループにシングルサインオン・アクセスを割り当てる権限を委任する

IAM Identity Center コンソールを使用して、管理アカウントへのシングルサインオン・アクセスを割り当てるのは特権的アクションです。デフォルトでは、AWS アカウントのルートユーザー または AWSSSOMasterAccountAdministrator および IAMFullAccess AWS 管理ポリシーがアタッチされているユーザーのみが、 管理アカウントにシングルサインオン・アクセスを割り当てることができます。AWSSSOMasterAccountAdministrator および IAMFullAccess ポリシーは、AWS Organizations 組織内の管理アカウントへのシングルサインオン・アクセスを管理します。

または、AWS CLI を使用して、アクセス許可セットの作成、ポリシーのアタッチ、割り当てを行うことができます。各ステップのコマンドを以下に示します。

- アクセス許可セットを作成するには: create-permission-set
- アクセス許可セットAWS Managed Policy にアタッチするには: attach-managed-policy-to-permission-set\
- カスタマー管理ポリシーをアクセス許可セットにアタッチするには: attach-customer-managed-policy-to-permission-set
- アクセス許可セットをプリンシパルに割り当てるには: create-account-assignment

ディレクトリ内のユーザーへのシングルサインオン・アクセスを管理するためにアクセス権限を委任するには、次の手順を実行します。

ディレクトリ内のユーザーへのシングルサインオン・アクセスを管理するためのアクセス権限を付与するには

1. 管理アカウントのルートユーザーまたは管理アカウントに IAM 管理者権限を持つ別の IAM ユーザーとして IAM Identity Center コンソールにサインインします。
2. アクセス権限セットを作成します。 の手順に従って権限セットを作成し、次の操作を行います。

    1. [新しい権限セットの作成] ページで [カスタム権限セットの作成] チェックボックスをオンにし、[次へ:詳細] を選択します。

2. [新しい権限セットの作成] ページで、カスタム権限セットの名前と、必要に応じて説明を指定します。必要に応じて、セッション期間を変更し、リレーステート URL を指定します。

   > **Note**
   >
   > リレーステート URL には、AWS マネジメントコンソール に含まれている URL を指定する必要があります。例えば、次のようになります。
   > **`https://console.aws.amazon.com/ec2/`**
   > 詳細については、「AWS マネジメントコンソールにすばやくアクセスできるようにリレーステートを設定する」を参照してください。

3. [どのポリシーを権限セットに含めたいですか?] で、[AWS管理ポリシーを添付する] チェックボックスを選択します。
4. IAM ポリシーのリストで、AWSSSOMasterAccountAdministrator および IAMFullAccess AWS マネージドポリシーを選択します。これらのポリシーは、将来的にこのアクセス権限セットへのアクセスが割り当てられるすべてのユーザーとグループにアクセス権限を付与します。
5. [Next: Tags] (次へ: タグ) を選択します。
6. [Add tags (optional)] (タグの追加 (オプション)) で [Key] (キー) と [Value (optional)] (値 (オプション)) の値を指定して、[Next: Review] (次へ: レビュー) を選択します。タグの詳細については、AWS IAM アイデンティティセンター リソースのタグ付けを参照してください。
7. 選択した値を確認したら、[Create] (作成) を選択します。

3. AWS アカウント にユーザーまたはグループアクセスを割り当てる の手順に従って、作成した権限セットに適切なユーザーとグループを割り当てます。
4. 割り当てられたユーザーに以下を周知すること: ユーザーが AWS アクセスポータルにサインインして[アカウント] タブを選択した時、委任権限による認証を受けるには適切なロール名を選択する必要があります。

権限セットを使用して AWS アカウントを管理する

アクセス権限セットは、1 つまたは複数の [IAM policies] (IAM ポリシー) のコレクションの定義を作成および維持するテンプレートです。アクセス権限セットは、組織内のユーザーやグループに AWS アカウント のアクセス権を簡単に割り当てることができます。例えば、AWS RDS、DynamoDB、および Aurora サービスを管理するためのポリシーを含むデータベース管理者アクセス許可セットを作成し、その単一のアクセス許可セットを使用して、AWS組織 内のターゲット AWS アカウント のリストへのアクセスをデータベース管理者に付与できます。

> **Note**
>
> アクセス許可セットを機能させるには、組織インスタンスでマルチアカウントアクセス許可が有効になっている必要があります。デフォルトでは、組織インスタンスを作成すると、マルチアカウントアクセス許可が有効になります。まだ有効にしていない場合は、[設定] ページの [管理] タブを使用してマルチアカウントアクセス許可を有効にすると、アクセス許可セットを作成できます。UpdateInstance API を使用して、マルチアカウントアクセス許可を有効にすることもできます。

IAM Identity Center は、アクセス権限セットを使用して 1 つ以上 AWS アカウント のユーザーまたはグループにアクセス権を割り当てます。アクセス権限セットを割り当てると、IAM Identity Center は、対応する IAM Identity Center 制御の IAM ロールを各アカウントに作成し、アクセス権限セットで指定されたポリシーをそれらのロールに適用します。IAM Identity Center はロールを管理し、IAM Identity Center ユーザーポータルまたは AWS CLI を使用して、定義した承認済みユーザーがロールを引き受けることを許可します。 アクセス権限セットを変更すると、IAM Identity Center は、対応する IAM ポリシーとロールがそれに応じて更新されることを保証します。

アクセス許可セットには、AWS マネージドポリシー、カスタマー管理ポリシー、インラインポリシー、およびAWS 職務機能の管理ポリシーを追加できます。アクセス許可の境界として、AWS マネージドポリシーまたはカスタマー管理ポリシーを割り当てることもできます。

アクセス権限セットを作成するには、「アクセス許可セットの作成、管理と削除」を参照してください。

アクセス管理で、カスタム信頼ポリシー、ロールタグ、設定可能なロールパスなど、アクセス許可セットが提供する機能を超える機能が必要な場合は、IAM でアカウントアクセスマネージャーを使用できます。アカウントアクセスマネージャーを使用すると、既存の IAM ロールを IAM Identity Center のユーザーやグループに割り当てることができます。それを個別に使用するか、アクセス許可セットと組み合わせて使用することにより、IAM ロールの全機能セットにアクセスできます。

最小特権権のアクセス許可を適用するアクセス許可セットを作成する

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うには、管理権許可セットを作成した後に、より制限の厳しいアクセス許可セットを作成して 1 人以上のユーザーに割り当てます。前の手順で作成したアクセス許可セットは、ユーザが必要とするリソースへのアクセス量を評価するための出発点となります。最小特権のアクセス許可に切り替えるには、IAM Access Analyzer を実行して、AWS マネージドポリシーを持つプリンシパルをモニタリングできます。どのアクセス許可を

使用しているかを学習したら、カスタムポリシーを作成するか、チームに必要なアクセス許可のみを持つポリシーを生成できます。

IAM Identity Center を使用すると、同じユーザーに複数のアクセス権限セットを割り当てることができます。管理ユーザーには、より制限の厳しいアクセス許可セットを追加で割り当てる必要もあります。そうすれば、常に管理アクセス許可を使用するのではなく、必要な権限のみで AWS アカウントにアクセスできるようになります。

例えば、開発者の場合、IAM アイデンティティセンターで管理ユーザーを作成した後に、PowerUserAccess アクセス許可を付与する新しいアクセス許可セットを作成し、そのアクセス許可セットを自身に割り当てることができます。AdministratorAccess 権限を使用する管理者権限セットとは異なり、PowerUserAccess　権限セットでは IAM ユーザーとグループの管理はできません。AWS　アクセスポータルにサインインして AWS アカウントにアクセスする場合、PowerUserAccessではなく、AdministratorAccess アカウントで開発タスクを実行することを選択できます。

次の考慮事項に注意が必要です。

- より制限の厳しいアクセス権限セットをすぐに作成するには、カスタムアクセス権限セットではなく定義済みのアクセス権限セットを使用してください。

  定義済みの権限 を使用する定義済みのアクセス権限セットでは、使用可能なポリシーのリストから 1 つの AWS マネージドポリシーを選択します。各ポリシーは、AWS サービスやリソースへの特定のアクセスレベル、または一般的な職務に必要な権限を付与します。これらのポリシーそれぞれの詳細については、「AWS職務機能の管理ポリシー」を参照してください。
- アクセス権限セットのセッション期間を構成して、ユーザーが AWS アカウント にサインインしている時間を制御できます。

  ユーザーが AWS アカウント にフェデレーションし、AWS 管理コンソールまたは AWSコマンドラインインターフェイス (AWSCLI) を使用する場合、IAM Identity Center はアクセス権限セットのセッション期間設定を使用してセッション期間を制御します。デフォルトでは、AWS がユーザーをセッションからサインアウトするまでにユーザーが AWS アカウント にサインインできる時間を決定する セッション期間 の値は 1 時間に設定されています。最大値は 12 時間まで指定できます。詳細については、「AWS アカウントのセッション期間を設定する」を参照してください。
- AWS アクセスポータルのセッション期間を設定して、Workforce ユーザーがポータルにサインインする期間を制御することもできます。

  デフォルトでは、Workforce ユーザーが AWS アクセスポータルにサインインしてから再認証が必要になるまでの時間を決定する「最大セッション期間」の値は 8 時間です。最大値は 90 日まで指

定できます。詳細については、「IAM アイデンティティセンターでセッション期間を設定する」を参照してください。

- AWS アクセスポータルにサインインするときに、最小特権の権限を付与するロールを選択します。

  作成してユーザーに割り当てた各アクセス許可セットは、AWS アクセスポータルで使用可能なロールとして表示されます。そのユーザーとしてポータルにサインインするときは、アカウント内のタスクの実行に使用できる最も制限の厳しいアクセス権限セットに対応するロールを (`AdministratorAccess` ではなく) 選択してください。
- IAM Identity Center に他のユーザーを追加し、そのユーザーに既存または新規のアクセス権限セットを割り当てることができます。

  詳細については、「AWS アカウント にユーザーまたはグループアクセスを割り当てる」を参照してください。

トピック

- AWS マネージドポリシーの事前定義済みの権限
- AWS マネージドポリシーとカスタマーマネージドポリシーのカスタム権限
- アクセス許可セットの作成、管理と削除
- アクセス権限セットのプロパティを構成する

AWS マネージドポリシーの事前定義済みの権限

AWS マネージドポリシーを使用して定義済みのアクセス権限セットを作成できます。

定義済みの権限を含むアクセス権限セットを作成する場合、AWS マネージドポリシーのリストから 1 つのポリシーを選択します。使用可能なポリシーの中で、共通権限ポリシー と職務機能ポリシーから選択できます。

共通のアクセス許可ポリシー

組織全体 AWS アカウント のリソースへのアクセスを可能にする AWS マネージドポリシーのリストから選択してください。以下のいずれかのポリシーを追加できます。

- AdministratorAccess
- PowerUserAccess
- ReadOnlyAccess

- ViewOnlyAccess

職務機能ポリシー

組織内のジョブに関連する可能性のある AWS アカウント 内のリソースへのアクセスを可能にする AWS マネージドポリシーのリストから選択します。以下のいずれかのポリシーを追加できます。

- Billing
- DataScientist
- DatabaseAdministrator
- NetworkAdministrator
- SecurityAudit
- SupportUser
- SystemAdministrator

使用可能な共通権限ポリシーとジョブ機能ポリシーの詳細については、「AWS Identity and Access Managementユーザーガイド」の「AWS 職務機能の管理ポリシー」を参照してください。

アクセス権限セットの作成方法については、「アクセス許可セットの作成、管理と削除」を参照してください。

AWS マネージドポリシーとカスタマーマネージドポリシーのカスタム権限

[カスタム権限] 機能を使用して、AWS Identity and Access Management (IAM) にある任意の AWS マネージドポリシーやカスタマーマネージドポリシーをインラインポリシーと組み合わせてカスタム権限セットを作成することができます。また、権限の境界を含めることで、他のポリシーにより権限セットのユーザーに付与することのできる最大の権限を制限することもできます。

アクセス権限セットの作成方法については、「アクセス許可セットの作成、管理と削除」を参照してください。

アクセス権限セットに適用できるポリシータイプ

トピック

- インラインポリシー
- AWS マネージドポリシー

- カスタマー管理ポリシー
- アクセス許可の境界

インラインポリシー

インラインポリシーをアクセス権限セットに適用します。インラインポリシーは IAM ポリシーとしてフォーマットされたテキストブロックで、アクセス権限セットに直接追加します。新しいアクセス権限セットを作成するときに、ポリシーを貼り付けるか、IAM Identity Center コンソールのポリシー作成ツールを使用して新しいポリシーを生成できます。AWSポリシージェネレーター を使用して IAM ポリシーを作成することもできます。

インラインポリシーを使用してアクセス権限セットをデプロイすると、IAM Identity Center はアクセス権限セットを割り当てた AWS アカウント に IAM ポリシーを作成します。IAM Identity Center は、アクセス権限セットをアカウントに割り当てるとポリシーを作成します。そのポリシーは、ユーザーが引き受ける AWS アカウント の IAM ロールに適用されます。

インラインポリシーを作成してアクセス権限セットを割り当てると、IAM Identity Center によって AWS アカウント にポリシーが構成されます。カスタマー管理ポリシー でアクセス権限セットを作成する場合は、アクセス権限セットを割り当てる前に AWS アカウント ご自分でポリシーを作成する必要があります。

AWS マネージドポリシー

AWSマネージドポリシーをアクセス許可セットに適用できます。 AWSマネージドポリシーは、AWS 管理を行う IAM ポリシーです。これとは対照的に、カスタマー管理ポリシー は、アカウント内の IAM ポリシーは自分で作成して管理するものです。 AWS マネージドポリシーは、AWS アカウント の一般的な最小特権のユースケースに対応しています。AWS マネージドポリシーは、IAM Identity Center が作成するロールのアクセス権限として、または アクセス許可の境界 として割り当てることができます。

AWS は、AWSリソースにジョブ固有のアクセス権限を割り当てる AWS職務機能の管理ポリシー を管理します。アクセス権限セットに 定義済みの権限 を使用する場合は、職務ポリシーを 1 つ追加できます。カスタム権限 を選択すると、複数の職務ポリシーを追加できます。

AWS アカウント には、特定の AWS のサービス および AWS のサービス の組み合わせに対する AWS 管理の IAM ポリシーも多数含まれています。カスタム権限 を持つアクセス権限セットを作成すると、多数の追加の AWS マネージドポリシーの中からアクセス権限セットに割り当てる管理ポリシーを選択できます。

AWS はすべての AWS アカウント に AWS マネージドポリシーを設定します。AWS マネージドポリシーを含むアクセス許可セットをデプロイするには、最初に AWS アカウント でポリシーを作成する必要はありません。カスタマー管理ポリシー でアクセス権限セットを作成する場合は、アクセス権限セットを割り当てる前に AWS アカウント ご自分でポリシーを作成する必要があります。

AWS マネージドポリシーの詳細については、「IAM ユーザーガイド」の「AWSマネージドポリシー」を参照してください。

カスタマー管理ポリシー

カスタマー管理ポリシーをアクセス許可セットに適用できます。カスタマー管理ポリシーは、アカウント内で顧客が作成および維持する IAM ポリシーです。これとは対照的に、AWS マネージドポリシー は、アカウント内の IAM ポリシーは AWS 維持されます。カスタマー管理ポリシーは、IAM アイデンティティセンターが作成するロールのアクセス許可として、または アクセス許可の境界 として割り当てることができます。

カスタマー管理ポリシーを使用して権限セットを作成する場合、IAM Identity Center が権限セットを割り当てる各 AWS アカウント に同じ名前とパスの IAM ポリシーを作成する必要があります。カスタムパスを指定する場合は、必ず各 AWS アカウント に同じパスを指定してください。詳細については、「IAM ユーザーガイド」の「親しみやすい名前とパス」を参照してください。IAM Identity Center は、作成した IAM ポリシーを、AWS アカウント で作成した IAM ロールにアタッチします。ベストプラクティスとして、アクセス権限セットを割り当てる各アカウントのポリシーに同じアクセス権限を適用します。詳細については、「権限セットに IAM ポリシーを使用する」を参照してください。

> **Note**
>
> カスタマー管理ポリシーがアクセス許可セットにアタッチされている場合、ポリシーの名前では大文字と小文字は区別されません。

詳細については、IAM ユーザーガイドの「カスタマー管理ポリシー」を参照してください。

アクセス許可の境界

アクセス許可セットには アクセス許可の境界を適用できます。アクセス許可の境界は、ID ベースのポリシーが IAM プリンシパルに付与できるアクセス許可の上限を設定する、AWS 管理または顧客管理の IAM ポリシーです。アクセス許可の境界を適用する場合、インラインポリシー、カスタマー管理ポリシー、および AWS マネージドポリシーは、そのアクセス許可の境界によって付与されるアクセス権限を超えるアクセス権限を付与することはできません。アクセス許可の境界ではアクセス権限

は付与されませんが、その代わりに IAM が境界を超えるすべてのアクセス権限を無視するようになります。

カスタマー管理ポリシーをアアクセス許可の境界として使用して権限セットを作成する場合、IAM Identity Center が権限セットを割り当てる各 AWS アカウント に同じ名前の IAM ポリシーを作成する必要があります。IAM Identity Center は、IAM ポリシーをアクセス許可の境界として AWS アカウント で作成する IAM ロールに適用します。

詳細については、IAM ユーザーガイド の IAM エンティティのアクセス許可の境界を参照してください。

アクセス許可セットの作成、管理と削除

アクセス権限セットは、ユーザーおよびグループが持つこの AWS アカウント アカウントに対するアクセスのレベルを定義します。権限セットは IAM Identity Center に保存され、1 つまたは複数の AWS アカウント にプロビジョニングできます。複数のアクセス権限セットを 1 人のユーザーに割り当てることができます。IAM Identity Center でのアクセス許可セットの使用方法の詳細については、権限セットを使用して AWS アカウントを管理する を参照してください。

> **Note**
>
> IAM アイデンティティセンターコンソールでアクセス許可セットを作成できます。

アクセス許可セットを作成するときは、次の考慮事項に留意してください。

- 組織インスタンス

  アクセス許可セットを使用するには、IAM アイデンティティセンターの組織インスタンスを使用する必要があります。詳細については、「IAM アイデンティティセンターの組織インスタンスとアカウントインスタンス」を参照してください。
- あらかじめ定義されたアクセス許可セットから始める

  定義済みの権限 を使用する定義済みのアクセス権限セットでは、使用可能なポリシーのリストから 1 つの AWS マネージドポリシーを選択します。各ポリシーは、AWS サービスやリソースへの特定のアクセスレベル、または一般的な職務に必要な権限を付与します。これらのポリシーそれぞれの詳細については、「AWS職務機能の管理ポリシー」を参照してください。使用状況データを収集したら、アクセス許可セットをより制限の厳しいものに調整できます。
- 管理セッションの期間を妥当な作業期間に制限する

ユーザーが AWS アカウント にフェデレーションし、AWS マネジメントコンソール または AWS コマンドラインインターフェイス (AWSCLI) を使用する場合、IAM アイデンティティセンターはアクセス許可セットのセッション期間設定を使用してセッション期間を制御します。ユーザーセッションがセッション時間に達すると、コンソールからサインアウトされ、再度サインインするよう求められます。セキュリティのベストプラクティスとして、ロールを実行するために必要な長さを超えるセッション期間を設定しないことをお勧めします。デフォルトでは、[セッション期間] は 1 時間です。最大値は 12 時間まで指定できます。詳細については、「AWS アカウントのセッション期間を設定する」を参照してください。

- ワークフォースユーザーポータルのセッション期間を制限する

  ワークフォースユーザーはポータルセッションを使用してロールを選択し、アプリケーションにアクセスします。デフォルトでは、Workforce ユーザーが AWS アクセスポータルにサインインしてから再認証が必要になるまでの時間を決定する「最大セッション期間」の値は 8 時間です。最大値は 90 日まで指定できます。詳細については、「IAM アイデンティティセンターでセッション期間を設定する」を参照してください。

- 最小特権アクセス許可を与えるロールを使用する

  作成してユーザーに割り当てた各アクセス許可セットは、AWS アクセスポータルで使用可能なロールとして表示されます。そのユーザーとしてポータルにサインインするときは、アカウント内のタスクの実行に使用できる最も制限の厳しいアクセス権限セットに対応するロールを (`AdministratorAccess` ではなく) 選択してください。ユーザー招待を送信する前に、アクセス許可セットをテストして必要なアクセス許可が提供されていることを確認してください。

> **Note**
>
> AWS CloudFormation を使用してアクセス許可セットを作成して割り当て、それらのアクセス許可セットにユーザーを割り当てることもできます。

トピック

- アクセス権限セットを作成します。
- 権限セットを表示および変更する
- 権限セット管理の委任
- 権限セットに IAM ポリシーを使用する
- IAM アイデンティティセンターでアクセス許可セットを削除する

- IAM アイデンティティセンターで権限セットを削除する

アクセス権限セットを作成します。

この手順を使用して、1 つの AWS 管理ポリシーを使用する定義済みの権限セット、または最大 10 個の AWS 管理ポリシーまたはカスタマー管理ポリシーとインラインポリシーを使用するカスタム権限セットを作成します。IAM の Service Quotas コンソール で、ポリシーの最大数 10 への調整をリクエストできます。IAM Identity Center コンソールで権限セットを作成できます。

> **Note**
>
> アクセス許可セットを使用するには、IAM アイデンティティセンターの組織インスタンスを使用する必要があります。詳細については、「IAM アイデンティティセンターの組織インスタンスとアカウントインスタンス」を参照してください。

アクセス権限セットを作成するには

1. IAM Identity Center コンソール を開きます。
2. [マルチアカウント権限] で、[権限セット] を選択します。
3. [Create permission set] (アクセス許可セットの作成) を選択します。
4. [権限セットタイプの選択] ページの [権限セットタイプ] で、権限セットタイプを選択します。
5. 権限セットタイプに基づいて、権限セットに使用したいポリシーを 1 つ以上選択します。

   - 定義済み権限セット
     1. [事前定義された許可セットのポリシー] で、リスト内の IAM Job 機能ポリシーまたは [共通権限ポリシー] のいずれかを選択し、[次へ] を選択します。詳細については、「AWS Identity and Access Management ユーザーガイド」の「AWS ジョブ機能の管理ポリシー」および「AWS マネージドポリシー」を参照してください。
     2. ステップ 6 に進み、[権限セットの詳細を指定する] ページの設定を完了します。
   - カスタム権限セット
     1. [次へ] を選択します。
     2. [ポリシーとアクセス許可の境界を指定する] ページで、新しい権限セットに適用する IAM ポリシーの種類を選択します。デフォルトでは、最大 10 個の [AWS管理ポリシー] と [顧客管理ポリシー] を任意に組み合わせて権限セットに追加できます。このクォータは IAM によって設定されます。これを増やすには、アクセス許可セットを割り当てたい各 AWS ア

カウント で、Service Quotas コンソールの「IAM ロールにアタッチされている IAM クォータ管理ポリシー」の追加をリクエストします。

- [AWS管理ポリシー] を拡張して、AWSが構築し維持する IAM からのポリシーを追加します。詳細については、「AWS マネージドポリシー」を参照してください。

  a. [AWS権限セット] でユーザーに適用する管理ポリシーを検索して選択します。

  b. 別の種類のポリシーを追加する場合は、そのコンテナを選択して選択します。適用するポリシーをすべて選択したら、[次へ] を選択します。ステップ 6 に進み、[権限セットの詳細を指定する] ページの設定を完了します。

- [顧客管理ポリシー] を展開して、作成して管理するポリシーを IAM から追加します。詳細については、「カスタマー管理ポリシー」を参照してください。

  a. [ポリシーを追加] を選択し、権限セットに追加するポリシーの名前を入力します。権限セットを割り当てる各アカウントで、入力した名前でポリシーを作成します。ベストプラクティスとして、各アカウントのポリシーに同じ権限を割り当ててください。

  b. [もっと追加する] を選択して別のポリシーを追加します。

  c. 別の種類のポリシーを追加する場合は、そのコンテナを選択して選択します。適用するポリシーをすべて選択したら、[次へ] を選択します。ステップ 6 に進み、[権限セットの詳細を指定する] ページの設定を完了します。

- [インラインポリシー] を展開して、カスタム JSON 形式のポリシーテキストを追加します。インラインポリシーは既存の IAM リソースに対応していません。インラインポリシーを作成するには、表示されたフォームにカスタムポリシー言語を入力します。IAM Identity Center は、メンバーアカウントに作成した IAM リソースにポリシーを追加します。詳細については、「インラインポリシー」を参照してください。

  a. インタラクティブエディタ内の必要なアクションとリソースをインラインポリシーに追加します。[新しいステートメントを追加] を使用して、ステートメントを追加できます。

  b. 別の種類のポリシーを追加する場合は、そのコンテナを選択して選択します。適用するポリシーをすべて選択したら、[次へ] を選択します。ステップ 6 に進み、[権限セットの詳細を指定する] ページの設定を完了します。

- [アクセス許可の境界] を拡張して、権限セット内の他のポリシーが割り当てることができる最大の権限として、AWS管理またはカスタマー管理の IAM ポリシーを追加します。詳細については、「アクセス許可の境界」を参照してください。

  a. [アクセス許可の境界を使用する] を選択して、アクセス許可の上限を設定します。

b. [AWS管理ポリシー] を選択し、IAM からポリシーを設定し、AWS がアクセス許可の境界として構築・維持します。[カスタマー管理ポリシー] を選択して、[お客様] が IAM から作成して維持するポリシーをアクセス許可の境界として設定します。

c. 別の種類のポリシーを追加する場合は、そのコンテナを選択して選択します。適用するポリシーをすべて選択したら、[次へ] を選択します。ステップ 6 に進み、[権限セットの詳細を指定する] ページの設定を完了します。

6. [権限セットの詳細指定] ページで、以下を実行します。

1. [権限セット名] に、IAM Identity Center でこの権限セットを識別するための名前を入力します。このアクセス許可セットに指定した名前は、使用可能なロールとして AWS アクセスポータルに表示されます。ユーザーは、AWS アクセスポータルにサインインし、AWS アカウント を選択し、ロールを選択します。

> **Note**
>
> アクセス許可セット名は、IAM アイデンティティセンターインスタンス内で一意である必要があります。

2. (オプション) 説明を入力することもできます。説明は IAM Identity Center コンソールにのみ表示され、AWS アクセスポータルには表示されません。

3. (オプション) Session duration (セッション期間) の値を指定します。この値は、コンソールがユーザーをセッションからログアウトさせるまでのログオン時間の長さを決定します。詳細については、「AWS アカウントのセッション期間を設定する」を参照してください。

4. (オプション) Relay state (リレーステート) の値を指定します。この値は、フェデレーションプロセスにおいて、アカウント内のユーザーをリダイレクトするために使用されます。詳細については、「AWS マネジメントコンソールにすばやくアクセスできるようにリレーステートを設定する」を参照してください。

> **Note**
>
> リレーステート URL は AWS マネジメントコンソール 内にある必要があります。例えば、次のようになります。
> **`https://console.aws.amazon.com/ec2/`**

5. [タグ (オプション)] を拡張して [タグの追加] を選択し、[キー] と [値 (オプション)] () の値を指定します。

タグの詳細についてはAWS IAM アイデンティティセンター リソースのタグ付けを参照してください。

6. [次へ] を選択します。

7. [確認と作成] ページで、選択した内容を確認し、[作成] を選択します。

8. デフォルトでは、権限セットを作成しても、その権限セットはプロビジョニングされません (どの AWS アカウント でも使用されます)。AWS アカウント で権限セットをプロビジョニングするには、アカウント内のユーザーとグループに IAM Identity Center アクセスを割り当て、その権限セットをそれらのユーザーとグループに適用する必要があります。詳細については、「AWS アカウント にユーザーまたはグループアクセスを割り当てる」を参照してください。

権限セットを表示および変更する

アクセス許可セットを使用して、ユーザーに AWS アカウント へのアクセスを許可できます。AWS IAM アイデンティティセンター コンソールを使用して権限セットを確認および変更できます。IAM アイデンティティセンターコンソールでアクセス許可セットを作成できます。IAM アイデンティティセンターでの権限セットの使用方法の詳細については、the section called “権限セット” を参照してください。

アクセス許可セットは、ユーザーにアプリケーションへのアクセスを管理するためには必要はありません。

> **Note**
>
> アクセス許可セットを使用するには、IAM アイデンティティセンターの組織インスタンスを使用する必要があります。詳細については、「IAM アイデンティティセンターの組織インスタンスとアカウントインスタンス」を参照してください。

アクセス許可セットの割り当てを表示する

この手順を使用して、AWS IAM アイデンティティセンター コンソールに適用されたアクセス許可セットを表示します。

All AWS アカウント where a permission set is provisioned

アクセス許可セットのすべての割り当てを表示するには、次の手順を使用します。

1. AWS マネジメントコンソール にサインインし、AWS IAM アイデンティティセンター コンソールを https://console.aws.amazon.com/singlesignon/ で開きます。
2. [マルチアカウント権限] で、[権限セット] を選択します。
3. [権限セット] ページで、見たい権限セットを選択します。
4. 選択したアクセス許可セットページで、[アカウント] タブに、アクセス許可セットが使用されているアカウントが表示されます。アカウントを選択すると、アカウント内でアクセス許可セットがどのようにプロビジョニングされるかを確認できます。ポリシーを削除、編集、およびアクセス許可セットにアタッチできます。

All permission sets for an AWS アカウント

アクセス許可セットのすべての割り当てを表示するには、次の手順を使用します。

1. AWS マネジメントコンソール にサインインし、AWS IAM アイデンティティセンター コンソールを https://console.aws.amazon.com/singlesignon/ で開きます。
2. [マルチアカウント権限] で、[AWS アカウント] を選択します。プロビジョニングされたアクセス許可セットを表示するアカウントを選択します。
3. 選択した AWS アカウント ページに移動したら、[アクセス許可セット] タブで、選択した AWS アカウント に割り当てられたさまざまなアクセス許可セットを表示できます。アクセス許可セットのハイパーリンクを選択すると、アクセス許可セットの詳細を確認できます。

All applied permission sets to users and groups

ユーザーまたはグループに割り当てられたすべてのアクセス許可セットを表示するには、次の手順を使用します。

1. AWS マネジメントコンソール にサインインし、AWS IAM アイデンティティセンター コンソールを https://console.aws.amazon.com/singlesignon/ で開きます。
2. ダッシュボードでユーザーまたはグループを選択して、IAM アイデンティティセンターのユーザーまたはグループを表示します。

    a. [ユーザー] ページで、適用されたアクセス許可セットを表示するユーザーを選択します。次に、[AWS アカウントアクセス] セクションの AWS アカウント タブと AWS アカウント を選択します。選択したユーザーに適用されたアクセス許可セットと AWS アカウント を表示できます。

b. [グループ] ページで、適用されたアクセス許可セットを表示するグループを選択します。次に、 [AWS アカウント アクセス セクションの AWS アカウント タブと AWS アカウント を選択します。選択したグループに適用されたアクセス許可セットと AWS アカウント を表示できます。

権限セットを変更する

IAM アイデンティティセンターコンソールを使用してユーザーからアクセス許可セットを削除するには、この手順を使用します。グループにアクセス許可を追加したり、グループからアクセス許可を削除したりできます。

1. AWS マネジメントコンソール にサインインし、AWS IAM アイデンティティセンター コンソールを https://console.aws.amazon.com/singlesignon/ で開きます。
2. [マルチアカウント権限] で、[AWS アカウント] を選択します。
3. [AWS アカウント] ページに、組織のツリービューリストが表示されます。権限セットを変更したい AWS アカウントの名前を選択します。
4. AWS アカウントの [概要] ページで、[割り当てられたユーザーとグループ] にある、権限セットを変更するユーザー名またはグループ名を選択します。次に、[権限セットの変更] を選択します。
5. 権限セットに必要な変更を加え、[変更の保存] を選択します。
6. [権限セット] タブに移動し、もっとも最近に変更された権限セットを選択し、[更新] を選択します。
7. [権限の更新] ページで、[更新] を選択します。

権限セット管理の委任

IAM Identity Center では、IAM Identity Center リソースの Amazon リソースネーム (ARN) を参照する IAM ポリシーを作成することで、アカウントのアクセス権限セットや割り当ての管理を委任することができます。例えば、特定のタグが付いたアクセス権限セットの特定のアカウントでの割り当てを、異なる管理者が管理できるようなポリシーを作成することができます。

> **Note**
>
> アクセス許可セットを使用するには、IAM アイデンティティセンターの組織インスタンスを使用する必要があります。詳細については、「IAM アイデンティティセンターの組織インスタンスとアカウントインスタンス」を参照してください。

このようなポリシーを作成するには、以下の方法があります。

- (推奨) IAM Identity Center で権限セットを作成し、それぞれに異なるポリシーを設定して、アクセス権限セットを異なるユーザーまたはグループに割り当てます。これにより、選択した IAM Identity Center アイデンティティソースを使用してサインインしたユーザーの管理権限を管理することができます。
- IAM でカスタムポリシーを作成し、管理者が想定する IAM ロールにアタッチします。ロールについては、割り当てられた IAM Identity Center 管理権限を取得するための「IAM ロール」を参照してください。

> **Important**
>
> IAM Identity Center リソースの ARN は、大文字と小文字を区別します。

以下は、IAM Identity Center 権限セットとアカウントリソースタイプを参照する適切なケースです。

リソースタイプ	ARN	コンテキストキー
PermissionSet	`arn:${Partition}:sso:::permissionSet/${InstanceId}/${PermissionSetId}`	`aws:ResourceTag/${TagKey}`
アカウント	`arn:${Partition}:sso:::account/${AccountId}`	該当しません

権限セットに IAM ポリシーを使用する

アクセス権限セットを作成します。 では、カスタマー管理ポリシーや権限境界などのポリシーを権限セットに追加する方法を学習しました。カスタマーが管理するポリシーと権限を権限セットに追加すると、IAM Identity Center はどの AWS アカウント でもポリシーを作成しません。その代わりに、権限セットを割り当てたい各アカウントで事前にそれらのポリシーを作成し、権限セットの名前とパスの指定に一致させる必要があります。権限セットを組織の AWS アカウント に割り当てると、IAM アイデンティティセンターが AWS Identity and Access Management IAM ロールを作成し、IAM ポリシーをそのロールにアタッチします。

考慮事項

- アクセス許可セットを使用するには、IAM アイデンティティセンターの組織インスタンスを使用する必要があります。詳細については、「IAM アイデンティティセンターの組織インスタンスとアカウントインスタンス」を参照してください。
- IAM ポリシーを使用して権限セットを割り当てる前に、メンバーアカウントを準備する必要があります。メンバーアカウントの IAM ポリシー名は、管理アカウントのポリシー名と一致している必要があります。ポリシーがメンバーアカウントに存在しない場合、IAM Identity Center は権限セットを割り当てることができません。

> **Note**
>
> カスタマー管理ポリシーがアクセス許可セットにアタッチされている場合、ポリシーの名前では大文字と小文字は区別されません。

- ポリシーによって付与されるアクセス許可は、アカウント間で完全に一致する必要はありません。

IAM ポリシーを権限セットに割り当てる

1. 権限セットを割り当てる各 AWS アカウント で、IAM ポリシーを作成します。
2. IAM ポリシーにアクセス許可を割り当てます。アカウントごとに異なるアクセス許可を割り当てることができます。一貫した操作性を実現するには、各ポリシーで同じ権限を設定し、維持してください。AWS CloudFormation StackSets などの自動化リソースを使用して、各メンバーアカウントに同じ名前と権限を持つ IAM ポリシーのコピーを作成できます。CloudFormation StackSets の詳細については、「AWS CloudFormation CloudFormation ユーザーガイド」の「AWS CloudFormation StackSets の操作」を参照してください。

3. 管理アカウントに権限セットを作成し、[カスタマー管理ポリシー] または [アクセス許可の境界] に IAM ポリシーを追加します。権限セットの作成方法の詳細については、アクセス権限セットを作成します。 を参照してください。
4. 準備したインラインポリシー、AWS 管理ポリシー、その他の IAM ポリシーを追加します。
5. 権限セットを作成して割り当てます。

IAM アイデンティティセンターでアクセス許可セットを削除する

IAM アイデンティティセンターコンソールで、IAM アイデンティティセンターユーザーとグループからアクセス許可セットを削除できます。AWS アカウント からアクセス許可セットを削除することもできます。IAM アイデンティティセンターでの権限セットの使用方法の詳細については、権限セットを使用して AWS アカウントを管理する を参照してください。

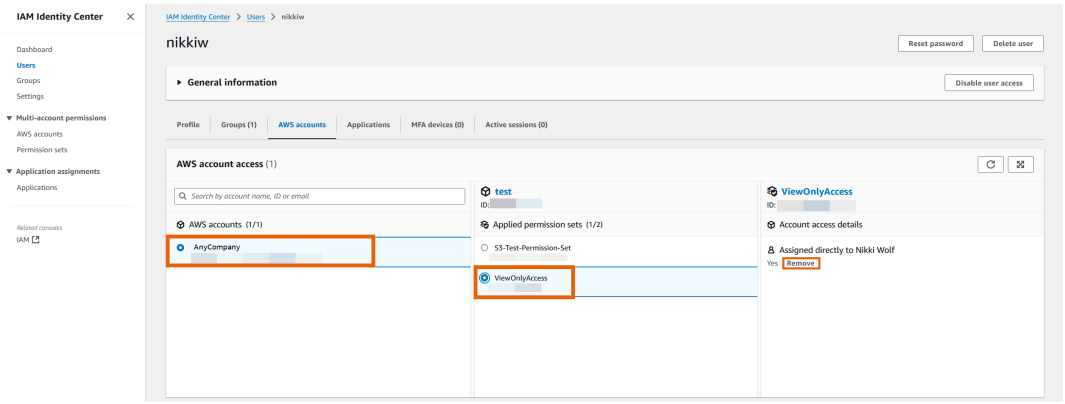
> **Note**
>
> アクセス許可セットを使用するには、IAM アイデンティティセンターの組織インスタンスを使用する必要があります。詳細については、「IAM アイデンティティセンターの組織インスタンスとアカウントインスタンス」を参照してください。

Remove permission set from a user

ユーザーからアクセス許可セットを削除するには

IAM アイデンティティセンターコンソールを使用してユーザーからアクセス許可セットを削除するには、この手順を使用します。

1. AWS マネジメントコンソール にサインインし、AWS IAM アイデンティティセンター コンソールを https://console.aws.amazon.com/singlesignon/ で開きます。
2. [IAM アイデンティティセンター] で、[ユーザー]を選択します。
3. アクセス許可セットを削除するユーザーのユーザー名を選択します。
4. [ユーザーの詳細] ページで、AWS アカウント タブを選択します。AWS アカウント アクセスで、AWS アカウント を選択します。
5. 右側のペインに、選択したユーザーに適用されたアクセス許可が表示されます。削除するアクセス許可セットを選択します。[アカウントアクセスの詳細] で、[削除] を選択します。
6. このアクセス許可セットを削除するかどうかを確認するダイアログボックスが表示されます。[削除] を選択します。

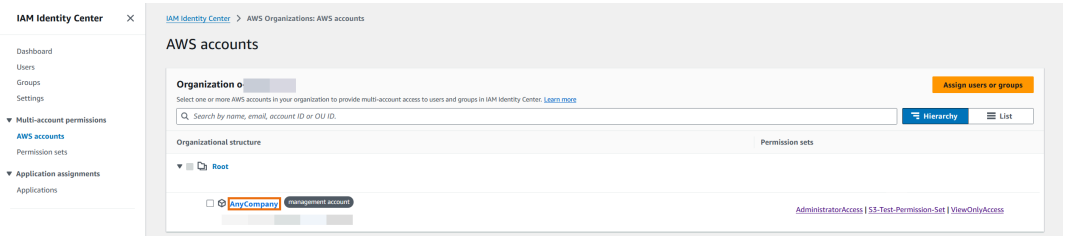


Remove permission set from a group

グループからアクセス許可セットを削除するには

IAM アイデンティティセンターコンソールを使用してグループからアクセス許可セットを削除するには、この手順を使用します。

1. AWS マネジメントコンソール にサインインし、AWS IAM アイデンティティセンター コンソールを https://console.aws.amazon.com/singlesignon/ で開きます。
2. [マルチアカウント許可] で、[AWS アカウント] を選択します。管理アカウントへのリンクを選択します。



3. [割り当てられたユーザーとグループ] タブで、アクセス許可セットを削除するグループを選択し、[アクセス許可セットの変更] を選択します。
4. [アクセス許可セットの変更] ページで、削除するアクセス許可セットをクリアし、[変更の保存] を選択します。

Remove permission set from an AWS アカウント

IAM アイデンティティセンターコンソールを使用して AWS アカウント からアクセス許可セットを削除するには、この手順を使用します。

1. AWS マネジメントコンソール にサインインし、AWS IAM アイデンティティセンター コンソールを https://console.aws.amazon.com/singlesignon/ で開きます。
2. [マルチアカウント許可] で、[AWS アカウント] を選択します。権限セットを削除したい AWS アカウント の名前を選択します。
3. AWS アカウント の [概要] ページで [アクセス許可セット] タブを選択します。削除するアクセス許可セットを選択します。次に、[削除] を選択します。
4. [権限セットの削除] ダイアログボックスで、正しい権限セットが選択されていることを確認し、**Delete** と入力して削除を確認し、[アクセス権の削除] を選択します。

IAM アイデンティティセンターで権限セットを削除する

IAM アイデンティティセンターからアクセス許可セットを削除する前に、アクセス許可セットを使用するすべての AWS アカウント からそれを削除する必要があります。既存のユーザーやグループ向けのアクセスを確認するには、「権限セットを表示および変更する」を参照してください。

考慮事項

- アクセス許可セットを使用するには、IAM アイデンティティセンターの組織インスタンスを使用する必要があります。詳細については、「IAM アイデンティティセンターの組織インスタンスとアカウントインスタンス」を参照してください。
- アクティブな権限セットセッションを取り消す場合は、「the section called “ワークフォースユーザーのアクティブなセッションを終了する”」を参照してください。
- 削除する前に、削除するユーザーまたはグループからアクセス許可セットとアプリケーションの割り当てを削除する必要があります。それ以外の場合は、IAM アイデンティティセンターに未割り当ての未使用のアクセス許可セットとアプリケーションがあります。

1 つ以上の権限セットを削除して、組織のいずれの AWS アカウント でも使用不可になるようにするには、以下の手順を実行します。

> **Important**
>
> この権限セットが割り当てられていたすべてのユーザーおよびグループは、どの AWS アカウント でそのアクセス権限セットが使用されていたかに関係なく、サインインできなくなります。既存のユーザーやグループ向けのアクセスを確認するには、「権限セットを表示および変更する」を参照してください。

AWS アカウント から権限セットを削除するには

1. IAM Identity Center コンソール を開きます。
2. [マルチアカウント権限] で、[権限セット] を選択します。
3. 削除するアクセス権限セットを選択してから、[削除] を選択します。
4. [権限セットの削除] ダイアログボックスで、権限セットの名前を入力して削除を確認し、[削除] を選択します。名前は、大文字と小文字が区別されます。

アクセス権限セットのプロパティを構成する

IAM アイデンティティセンターでは、管理者は以下の構成および管理タスクを行うことで、ユーザーアクセスとセッション期間をコントロールできます。

タスク	詳細情報
管理者は、IAM アイデンティティセンターを介して AWS リソースにアクセスする際のユーザーセッションの最大時間を設定できます。	AWS アカウントのセッション期間を設定する
管理者は、IAM アイデンティティセンターを通じて正常に認証された後に表示されるランディングページの内容をカスタマイズできます。	AWS マネジメントコンソールにすばやくアクセスできるようにリレーステートを設定する
権限が取り消されたユーザーが AWS リソースにアクセスできなくなるようにします。	拒否ポリシーを使用してアクティブなユーザーの権限を取り消す

AWS アカウントのセッション期間を設定する

権限セット毎に、ユーザーが AWS アカウント アカウントにサインインできる期間を制御するためのセッション期間を指定できます。指定された期間が経過すると、AWS によりユーザーがセッションからログアウトされます。

新しいアクセス権限セットを作成すると、デフォルトでセッションの継続時間が 1 時間 (秒単位) に設定されます。セッション時間は、最短で 1 時間、最長で 12 時間まで設定できます。IAM Identity Center では、権限セットごとに割り当てられたアカウントに IAM ロールが自動的に作成され、これらのロールは最大セッション時間が 12 時間になるように構成されています。

ユーザーが AWS アカウント コンソールにフェデレーションするか、AWS Command Line Interface (AWS CLI) を使用する場合、IAM Identity Center は権限セットのセッション期間設定を使用してセッション期間を制御します。デフォルトでは、IAM Identity Center によって生成された権限セットの IAM ロールは、IAM Identity Center ユーザーのみが引き受けることができます。これにより、IAM Identity Center 権限セットで指定されたセッション期間が適用されます。

> **Important**
>
> セキュリティのベストプラクティスとして、ロールを実行するために必要な長さを超えるセッション期間を設定しないことをお勧めします。

権限セットが作成された後、更新して、新しいセッションの有効期間を適用できます。特定の権限セットのセッション期間の長さを変更するには、次の手順を実行します。

セッション期間を設定するには

1. IAM Identity Center コンソール を開きます。
2. [マルチアカウント権限] で、[権限セット] を選択します。
3. セッション継続時間を変更する権限セットの名前を選択します。
4. 権限セットの詳細ページの [一般設定] セクションの見出しの右側で、[編集] を選択します。
5. [一般権限セット設定の編集] ページで、[セッション期間] に新しい値を選択します。
6. 権限セットがどの AWS アカウント でもプロビジョニングされている場合、アカウント名は [AWS アカウント自動的に再ビジョニングする] の下に表示されます。権限セットのセッション期間の値が更新されると、権限セットを使用するすべての AWS アカウント が再プロビジョニングされます。つまり、この設定の新しい値は、権限セットを使用するすべての AWS アカウント に適用されます。
7. [Save changes] (変更の保存) をクリックします。
8. [AWS アカウント] ページの上部に通知が表示されます。
   - 権限セットが 1 つまたは複数の AWS アカウント にプロビジョニングされている場合、通知は、AWS アカウント が正常に再ビジョニングされ、更新された権限セットがアカウントに適用されたことを確認します。
   - 権限セットが AWS アカウント でプロビジョニングされていない場合、通知により権限セットの設定が更新されたことが確認されます。

AWS マネジメントコンソールにすばやくアクセスできるようにリレーステートを設定する

デフォルトでは、ユーザーが AWS アクセスポータルにサインインしてアカウントを選択し、割り当てられた権限セットから AWS が作成するロールを選択すると、IAM Identity Center はユーザのブラウザを AWS マネジメントコンソール にリダイレクトします。リレーステートを別のコンソール URL に設定することで、この動作を変更できます。

リレーステートを設定すると、ユーザーは自分の役割に最も適したコンソールにすばやくアクセスできるようになります。たとえば、Amazon EC2 コンソール URL (**`https://console.aws.amazon.com/ec2/`**) にリレー状態を設定して、ユーザーが Amazon EC2 管理者ロールを選択したときにユーザーをそのコンソールにリダイレクトできます。デフォルト URL またはリレー状態 URL へのリダイレクト中、IAM Identity Center はユーザのブラウザを、ユーザが最後に使用したAWS リージョンのコンソールエンドポイントにルーティングします。たとえば、ユーザーが欧州 (ストックホルム) リージョン (eu-north-1) で最後のコンソールセッションを終了した場合、ユーザーはそのリージョンの Amazon EC2 コンソールにリダイレクトされます。



ユーザーを特定の AWS リージョン のコンソールにリダイレクトするように IAM Identity Center を設定するには、URL の一部にリージョン指定を含めます。たとえば、ユーザーを米国東部 (オハイオ) リージョン (us-east-2) の Amazon EC2 コンソールにリダイレクトするには、そのリージョン (**`https://us-east-2.console.aws.amazon.com/ec2/`**) の Amazon EC2 コンソールの URL を指定します。米国西部 (オレゴン) リージョン (us-west-2) リージョンで IAM Identity Center を有効にし、そのリージョンにユーザを誘導する場合は、**`https://us-west-2.console.aws.amazon.com`** を指定します。

リレーステートを設定する

特定の権限セットのリレーステート URL を変更するには、次の手順を実行します。

1. IAM Identity Center コンソールを開きます。
2. [マルチアカウント権限] で、[権限セット] を選択します。
3. 新しいリレーステート URL を指定するアクセス権限セットの名前を選択します。
4. 権限セットの詳細ページの [一般設定] セクションの見出しの右側で、[編集] を選択します。
5. [一般権限セット設定の編集] ページの [リレーステート] で、任意の AWS サービスのコンソール URL を入力します。例えば、次のようになります。

`https://console.aws.amazon.com/ec2/`

> **Note**
>
> リレーステート URL は AWS マネジメントコンソール 内にある必要があります。

6. 権限セットがどの AWS アカウント でもプロビジョニングされている場合、アカウント名は [AWS アカウント自動的に再ビジョニングする] の下に表示されます。権限セットのリレー状態 URL が更新されると、その権限セットを使用するすべての AWS アカウント が再ビジョニングされます。つまり、この設定の新しい値は、権限セットを使用するすべての AWS アカウントに適用されます。
7. [Save changes] (変更の保存) をクリックします。
8. [AWS 組織] ページの上部に通知が表示されます。

   - 権限セットが 1 つまたは複数の AWS アカウント にプロビジョニングされている場合、通知は、AWS アカウント が正常に再ビジョニングされ、更新された権限セットがアカウントに適用されたことを確認します。
   - 権限セットが AWS アカウント でプロビジョニングされていない場合、通知により権限セットの設定が更新されたことが確認されます。

> **Note**
>
> AWSAPI、AWSSDK、またはAWS Command Line Interface (AWS CLI) を使用してこのプロセスを自動化できます。詳細については、以下を参照してください。
>
> - [IAM Identity Center API リファレンス] の `CreatePermissionSet` または `UpdatePermissionSet` アクション
> - [AWS CLI コマンドリファレンス] の sso-admin セクションにある `create-permission-set` または `update-permission-set` コマンド。

拒否ポリシーを使用してアクティブなユーザーの権限を取り消す

IAM アイデンティティセンターユーザーが権限セットをアクティブに使用している間に、そのユーザーの AWS アカウントへのアクセスを取り消したい場合があります。ユーザーを指定しない拒否ポリシーを事前に実装しておくことで、ユーザーがアクティブな IAM ロールセッションを使用する機

能を削除できます。必要に応じて、拒否ポリシーを更新し、アクセスをブロックするユーザーを指定することができます。このトピックでは、拒否ポリシーを作成する方法と、ポリシーをデプロイする方法に関する注意事項について説明します。

権限セットによって作成されたアクティブな IAM ロールセッションを取り消す準備をする

サービスコントロールポリシーを使用して特定のユーザーに対して「すべてを拒否する」ポリシーを適用することで、ユーザーがアクティブに使用している IAM ロールでアクションを実行できないようにすることができます。また、パスワードを変更するまで、ユーザーが権限セットを使用することを禁止できます。これにより、盗まれた認証情報を不正使用している攻撃者を排除できます。広範囲にわたってアクセスを拒否し、ユーザーが権限セットに再参加したり他の権限セットに参加しようとする行為も阻止したい場合は、すべてのユーザーアクセスを削除してアクティブな AWS アクセスポータルセッションを停止し、かつユーザーのサインインを無効にする必要があるかもしれません。より広範なアクセス取り消しのための追加アクションと併せて拒否ポリシーを発動する方法については、「the section called “ワークフォースユーザーのアクティブなセッションを終了する”」を参照してください。

拒否ポリシー

IAM アイデンティティセンターアイデンティティストア内のユーザー UserID と一致する条件を持つ拒否ポリシーを使用することで、そのユーザーがアクティブに使用中の IAM ロールによるさらなるアクション実行を阻止することができます。こうしたポリシーの使用により、拒否ポリシーのデプロイ時に同じ権限セットを使用している他のユーザーへの影響を回避できます。このポリシーは、アクセスを取り消すユーザー ID で更新される "identitystore:userId" のプレースホルダーユーザー ID として、「*Add user ID here*」を使用します。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "*"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "identitystore:userId": "Add user ID here"
```

```
                }
            }
        }
    ]
}
```

“aws:userId” などの別の条件キーを使用することもできますが、“identitystore:userId” は 1 人のユーザーに関連付けられるグローバルに一意の値であるため、より確実です。条件内での “aws:userId” の使用は、ユーザー属性が ID のソースから同期される方法に影響を受けるため、ユーザーのユーザー名または E メールアドレスが変更された場合に属性が変化する可能性があります。

IAM アイデンティティセンターコンソールから [ユーザー] に移動し、名前でユーザーを検索して [一般情報] セクションを展開し、ユーザー ID をコピーすることで、ユーザーの identitystore:userId を確認することができます。また、ユーザー ID を検索している間にユーザーの AWS アクセスポータルセッションを停止し、同じセクションでサインインアクセスを無効にするのも便利です。ID ストア API に対するクエリによりユーザーのユーザー ID を取得することで、拒否ポリシーを作成するプロセスを自動化できます。

拒否ポリシーをデプロイする

Add user ID here などの無効なプレースホルダーユーザー ID を使用することで、AWS アカウントユーザーにアタッチしたサービスコントロールポリシー (SCP) を使用して事前に拒否ポリシーをデプロイしておくことができます。このアプローチはシンプルかつすばやく影響が発揮されるため、お勧めの方法です。拒否ポリシーを使用してユーザーのアクセス権を取り消す場合、ポリシーを編集して、プレースホルダーユーザー ID をアクセス権を取り消したいユーザーのユーザー ID に置き換えます。これにより、SCP をアタッチしたすべてのアカウントの権限セットで、ユーザーがアクションを起こすことを防ぐことができます。そのユーザーがアクティブな AWS アクセスポータルセッションを使用して異なるアカウントに移動し、異なるロールを引き受けようとしても、そのようなアクションはブロックされます。ユーザーアクセスを SCP によって完全にブロックしたうえで、必要に応じてサインイン能力の無効化、割り当ての取り消し、また必要に応じて AWS アクセスポータルセッションを停止することができます。

SCP を使用する代わりに、権限セットのインラインポリシーと、ユーザーがアクセスできる権限セットで使用されるカスタマー管理ポリシーに拒否ポリシーを含めることもできます。

複数のユーザーのアクセスを取り消す必要がある場合は、以下のような条件ブロックの値のリストを使用できます。

```
        "Condition": {
                "StringEquals": {
                    "identitystore:userId": [" user1 userId", "user2 userId"...]
                    }
    }
```

> **Important**
>
> どのような方法を使用する場合でも、併せてその他の是正措置を講じ、そのユーザーのユーザー ID を拒否ポリシー内に少なくとも 12 時間保持する必要があります。12 時間後にはユーザーが引き受けていたロールはすべて失効しているため、拒否ポリシーからユーザー ID を削除できます。

リソースポリシー、Amazon EKS クラスター構成マップ、および AWS KMS キーポリシーでの権限セットを参照する

AWS アカウントに権限セットを割り当てると、IAM Identity Center は AWSReservedSSO_ で始まる名前のロールを作成します。

ロールのフルネームと Amazon リソースネーム (ARN) は、次の形式を使用します。

名前	ARN
AWSReservedSSO_ *permission-set-name_unique-suffix*	arn:aws:iam:: *aws-account-ID*:role/aws-reserved/sso.amazonaws.com/ *aws-region* /AWSReservedSSO_ *permission-set-name_unique-suffix*

IAM アイデンティティセンターの ID ソースが us-east-1 でホストされている場合、ARN に *aws-region* は含まれません。ロールのフルネームと ARN は、次の形式を使用します。

名前	ARN
AWSReservedSSO_ *permission-set-name_unique-suffix*	arn:aws:iam:: *aws-account-ID* :role/aws-reserved/sso.amazonaws.com/AWSReservedSSO_ *permission-set-name_unique-suffix*

たとえば、データベース管理者に AWS アカウントアクセスを許可する権限セットを作成すると、対応するロールが次の名前と ARN で作成されます。

名前	ARN
AWSReservedSSO_DatabaseAdministrator_1234567890abcdef	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_1234567890abcdef

AWS アカウント内の権限セットへの割り当てをすべて削除すると、IAM Identity Center が作成した対応するロールも削除されます。後で同じ権限セットに新しい割り当てを行うと、IAM Identity Center はその権限セット用の新しいロールを作成します。新しいロールの名前と ARN には、異なる固有のサフィックスが含まれます。この例では、ユニークなサフィックスは「abcdef0123456789」です。

名前	ARN
AWSReservedSSO_DatabaseAdministrator_ **abcdef0123456789**	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_ **abcdef0123456789**

ロールの新しい名前と ARN のサフィックスが変更されると、元の名前と ARN を参照するすべてのポリシーが古くなり、対応する権限セットを使用する個人のアクセスが中断されます。たとえば、以

下の設定で元の ARN が参照されている場合、ロールの ARN を変更すると、権限セットのユーザのアクセスが中断されます。

- クラスターアクセスに `aws-auth ConfigMap` を使用する場合、Amazon Elastic Kubernetes Service (Amazon EKS) クラスター内の `aws-auth ConfigMap` ファイル。
- AWS Key Management Service (AWS KMS) キー用のリソースベースのポリシー内 このポリシーはキーポリシーとも呼ばれます。

> **Note**
>
> Amazon EKS アクセスエントリを使用して、Amazon EKS クラスターへのアクセスを管理することをお勧めします。これにより、IAM 権限を使用して、Amazon EKS クラスターにアクセスできるプリンシパルを管理できます。Amazon EKS アクセスエントリを使用することで、Amazon EKS 権限を持つ IAM プリンシパルを使用して、サポートに連絡せずにクラスターへのアクセスを回復できます。

ほとんどの AWS サービスのリソースベースポリシーを更新して、権限セットに対応するロールの新しい ARN を参照することができますが、ARN が変更された場合は、Amazon EKS および AWS KMS 用の IAM で作成するバックアップロールが必要です。Amazon EKS では、バックアップ IAM ロールが `aws-auth ConfigMap` に存在している必要があります。AWS KMS の場合、それはキーポリシーに存在しなければなりません。`aws-auth ConfigMap` または AWS KMS のキーポリシーを更新する権限を持つバックアップ IAM ロールがない場合は、サポートに連絡して、それらのリソースへのアクセスを回復してください。

アクセスが中断されないようにするための推奨事項

権限セットに対応するロールの ARN の変更によるアクセスの中断を避けるため、次のことを行うことをお勧めします。

- 少なくとも 1 つの権限セット割り当てを維持します。

  Amazon EKS の`aws-auth ConfigMap`、AWS KMS のキーポリシー、または他の AWS のサービス のリソースベースポリシーで参照するロールを含む AWS アカウントで、この割り当てを維持します。

  たとえば、`EKSAccess` 権限セットを作成し、AWS アカウント `111122223333` から対応するロール ARN を参照した場合、そのアカウントの権限セットに管理グループを永続的に割り当てます。

この割り当ては永続的であるため、IAM Identity Center は対応するロールを削除せず、名前を変更するリスクがなくなります。管理グループは、権限昇格のリスクなしにいつでもアクセスできます。

- **`aws-auth ConfigMap`** および AWS KMS を使用する Amazon EKS クラスターの場合: IAMで作成されたロールを含めてください。

  Amazon EKS クラスタの `aws-auth ConfigMap` または AWS KMS キーのキーポリシーで、権限セットにロールの ARN を参照する場合、IAM で作成する少なくとも 1 つのロールも含めることを推奨します。ロールには Amazon EKS クラスターへのアクセスまたは AWS KMS キーポリシーの管理が許可されている必要があります。権限セットがこのロールを引き受けることができる必要があります。そうすれば、権限セットのロール ARN が変更された場合に、`aws-auth ConfigMap` または AWS KMS キーポリシーの ARN への参照を更新できます。次のセクションでは、IAM で作成されたロールの信頼ポリシーを作成する方法の例を示します。このロールは `AdministratorAccess` 権限セットによってのみ引き受けることができます。

カスタム信頼ポリシーの例

以下は、IAM で作成されたロールへの `AdministratorAccess` 権限セットを提供するカスタム信頼ポリシーの例です。この基盤を構成する主な要素には以下が含まれます。

- この信頼ポリシーのプリンシパル要素は AWS アカウントプリンシパルを指定します。このポリシーでは、`sts:AssumeRole` 権限を持つ AWS アカウント `111122223333` のプリンシパルが IAM で作成されたロールを引き受けることができます。
- このトラストポリシーの `Condition element` は、IAM で作成されたロールを引き受けるプリンシパルの追加要件を指定します。このポリシーでは、以下のロール ARN を持つ権限セットがロールを引き受けることができます。

```
arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/
AWSReservedSSO_AdministratorAccess_*"
```

> **Note**
>
> この `Condition` 要素には `ArnLike` 条件演算子が含まれ、権限セットロール ARN の末尾には固有のサフィックスではなくワイルドカードが使用されます。つまり、ポリシーは、権限セットのロール ARN が変更された場合でも、権限セットが IAM で作成されたロールを引き継ぐことを許可します。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/aws-reserved/
sso.amazonaws.com/eu-west-2/AWSReservedSSO_AdministratorAccess_*"
        }
      }
    }
  ]
}
```

IAM で作成したロールをこのようなポリシーに含めると、権限セットまたは権限セットへのすべての割り当てが誤って削除され、再作成された場合に、Amazon EKS クラスタ、AWS KMS keys、またはその他の AWS リソースへの緊急アクセスを提供します。

属性ベースのアクセス制御

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。IAM Identity Center を使用して、任意の IAM Identity Center ID ソースから得られるユーザー属性を使用して、複数の AWS アカウント アカウントにまたがる AWS リソースへのアクセスを管理することができます。AWS では、これらの属性はタグと呼ばれます。AWS でユーザー属性をタグとして使用することで、AWS での細かな権限設定のプロセスを簡素化し、タグが一致した AWS リソースにのみ従業員がアクセスできるようにします。

例えば、2 つの異なるチームに所属する開発者ボブとサリーを IAM Identity Center で同じアクセス権限セット (またはアカウントアクセスマネージャーで同じ IAM ロール) に割り当て、アクセスコントロールにチーム名属性を選択することができます。ボブとサリーが AWS アカウント アカウントにサインインすると、IAM Identity Center は AWS セッションでチーム名属性を送信するため、ボブと

サリーはチーム名の属性がプロジェクトリソースのチーム名タグと一致する場合のみ AWS プロジェクトリソースにアクセスできます。将来、Bob が Sally のチームに移った場合、コーポレートディレクトリのチーム名属性を更新するだけで、Bob のアクセスを変更することができます。次回、ボブがサインインすると、AWS での権限の更新を必要とせず、自動的に新しいチームのプロジェクトリソースにアクセスできるようになります。

このアプローチは、IAM Identity Center で作成したり、管理したりしなければならない個別のアクセス許可の数を減らすのにも役立ちます。これは、同じアクセス権限セットに関連付けられたユーザー (またはアカウントアクセスマネージャーで同じ IAM ロールに関連付けられたユーザー) が、その属性に基づいて独自の権限を持つことができるようになったためです。これらのユーザー属性を IAM Identity Center の権限セット (またはアカウントアクセスマネージャーのロール割り当てを使用する場合は IAM ロール) やリソースベースのポリシーで使用することで、AWS リソースへの ABAC を実装し、大規模な許可管理を簡素化することができます。

利点

IAM Identity Center で ABAC を使用すると、以下のようなメリットがあります。

- ABAC では必要なアクセス許可セットの数が少ない - 職務ごとに異なるポリシーを作成する必要がないため、アクセス許可セット (またはアカウントアクセスマネージャーを使用する場合は IAM ロール) の数も少なくて済みます。これにより、許可管理の複雑さを軽減できます。
- ABAC を使用することで、チームは変化し、急速に成長することができる - リソースの作成時に適切なタグが付けられれば、属性に基づいて新しいリソースの権限が自動的に付与されます。
- ABAC で社内ディレクトリの従業員属性を利用する - IAM Identity Center で構成された任意の ID ソースから既存の従業員属性を使用して、AWS でのアクセスコントロールの決定を行うことができます。
- リソースにアクセスしているユーザーを追跡する — セキュリティ管理者は、AWS CloudTrail でユーザー属性を確認して、AWS でユーザーの活動を追跡することで、セッション ID を容易に割り出すことができます。

IAM Identity Center コンソールを使って ABAC を設定する方法については、「アクセスコントロールの属性」を参照してください。IAM アイデンティティセンター API を使って ABAC を有効にして設定する方法については、「IAM アイデンティティセンター API リファレンスガイド」の「CreateInstanceAccessControlAttributeConfiguration」を参照してください。

トピック

- チェックリスト: IAM Identity Center を使用して AWS で ABAC を設定する

- アクセスコントロールの属性

チェックリスト: IAM Identity Center を使用して AWS で ABAC を設定する

このチェックリストには、AWS リソースを準備し、ABAC アクセス用の IAM Identity Center を設定するために必要な設定作業が含まれています。このチェックリストのタスクを順番に行います。リファレンスリンクからトピックに移動した場合は、このトピックに戻って、チェックリストの残りのタスクを引き続き行うことができます。

ステップ	タスク	リファレンス
1	すべての AWS リソースにタグを追加する方法を確認します。IAM Identity Center に ABAC を実装するには、まず、ABAC を実装したい AWS リソースすべてにタグを追加する必要があります。	• AWS リソースのタグ付け
2	IAM Identity Center の ID ソースを Identity Store で関連するユーザーの ID と属性で設定する方法を確認します。IAM Identity Center では、サポートされている IAM Identity Center ID ソースのユーザー属性を AWS の ABAC に使用できます。	• ID ソースを管理する
3	以下の基準に基づいて、AWS でのアクセスコントロールの決定に使用する属性を決定し、IAM Identity Center に送信します。	• 開始方法
	• 外部の ID プロバイダー (IdP) を使用している場合、IdP から渡された属性を使用するのか、それとも IAM Identity Center 内で属性を選択するのかを決定します。	• 外部 ID プロバイダーを ID ソースとして使用する際の属性を選択する
	• IdP に属性を送信させる場合は、SAML アサーションで属性を送信するように IdP を設定します。お使いの IdP 向けチュートリアルの `Optional` 関連セクションを参照してください。	• IAM アイデンティティセンターの ID ソースに関するチュートリアル

ステップ	タスク	リファレンス
	• ID ソースとして IdP を使用し、IAM Identity Center で属性を選択する場合は、属性値が IdP から来るように SCIM を構成する方法を調べます。IdP で SCIM を使用できない場合は、IAM Identity Center コンソールの [ユーザー] ページでユーザーとその属性を追加します。	• SCIM を使用して外部 ID プロバイダーからユーザーとグループをプロビジョニングする • サポートされている外部 ID プロバイダ属性
	• ID ソースとして Active Directory または IAM Identity Center を使用する場合、または IdP を使用して IAM Identity Center で属性を選択する場合は、設定可能な属性を確認してください。その後、すぐにステップ 4 に進み、IAM Identity Center コンソールを使って ABAC 属性の設定を開始します。	• IAM Identity Center を ID ソースとして使用する際の属性を選択する • AWS Managed Microsoft AD を ID ソースとして使用する際の属性を選択する • IAM アイデンティティセンターと Microsoft AD の間のデフォルトのマッピング
4	IAM Identity Center コンソールの [アクセスコントロールの属性] ページで、ABAC に使用する属性を選択します。このページでは、ステップ 2 で設定した ID ソースから、アクセスコントロールのための属性を選択できます。ID とその属性が IAM Identity Center に登録された後、アクセスコントロールの決定のために AWS アカウント に渡されるキーバリューのペア (マッピング) を作成する必要があります。	• アクセスコントロールのための属性の有効化と設定

ステップ	タスク	リファレンス
5	アクセス権限セット (またはアカウントアクセスマネージャーを使用する場合は IAM ロール) 内にカスタム権限ポリシーを作成し、アクセスコントロール属性を使用して ABAC ルールを作成し、ユーザーが一致するタグを持つリソースにのみアクセスできるようにします。ステップ 4 で設定したユーザー属性は、AWS のタグとしてアクセスコントロールの判断に使用されます。`aws:PrincipalTag/key` 条件を使用して、権限ポリシーのアクセスコントロール属性を参照することができます。	• IAM Identity Center を使用して ABAC の権限セットを作成する
6	さまざまな AWS アカウント で、ステップ 5 で作成した権限セットにユーザーを割り当てます。そうすることで、ユーザーが自分のアカウントと連携して AWS のリソースに、マッチするタグに基づいてアクセスできるようになります。	• AWS アカウント にユーザーまたはグループアクセスを割り当てる

これらの手順を完了すると、シングルサインオンを使用して AWS アカウント にフェデレートしたユーザーは、一致する属性に基づいて AWS リソースにアクセスできるようになります。

アクセスコントロールの属性

[アクセスコントロールの属性] は、IAM Identity Center コンソールのページ名で、リソースへのアクセスコントロールをするためのポリシーで使用するユーザー属性を選択します。管理者は、ユーザーの ID ソースにある既存の属性に基づいて、AWS のワークロードにユーザーを割り当てることができます。

例えば、部署名に基づいて S3 バケットへのアクセスを割り当てたいとします。[Attributes for access control] (アクセスコントロールの属性)では、属性ベースのアクセスコントロール (ABAC) で使用する Department (部署) ユーザー属性を選択します。IAM Identity Center 権限セット (またはアカウントアクセスマネージャーを使用する場合は IAM ロール) では、部署属性が、S3 バケットに割り当てた部門タグと一致した場合にのみ、ユーザーにアクセスを許可するポリシーを書き込みます。IAM Identity Center は、アクセスされるアカウントに、ユーザーの部門属性を渡します。

そして、その属性は、ポリシーに基づいてアクセスを決定するために使用されます。これらの属性は、IAM Identity Center からアカウントに渡ると、セッションタグとして送信されます。セッションタグは、関連するすべての AWS IAM ポリシータイプで `aws:PrincipalTag/tag-key` 条件キーを使用して参照できます。ABAC の詳細については、「属性ベースのアクセス制御」を参照してください。

開始方法

アクセスコントロールの属性設定をどのように始めるかは、使用している ID ソースによって異なります。選択した ID ソースにかかわらず、属性を選択した後、アクセス権限セットのポリシー (またはアカウントアクセスマネージャーを使用する場合は IAM ロールポリシー) を作成または編集する必要があります。これらのポリシーは、ユーザーの ID に AWS リソースへのアクセスを許可する必要があります。

IAM Identity Center を ID ソースとして使用する際の属性を選択する

IAM Identity Center を ID ソースとして設定する場合、まずユーザーを追加し、その属性を設定します。次に、[Attributes for access control] (アクセスコントロールの属性) ページに移動して、ポリシーで使用する属性を選択します。最後に、AWS アカウントのページに移動して、ABAC の属性を使用するための権限セットを作成または編集します。

AWS Managed Microsoft AD を ID ソースとして使用する際の属性を選択する

AWS Managed Microsoft AD を ID ソースとして IAM Identity Center を構成する場合、まず Active Directory の属性セットを IAM Identity Center のユーザー属性にマッピングします。次に、[Attributes for access control] (アクセスコントロールの属性) のページに移動します。次に、アクティブディレクトリからマッピングされた既存の SSO 属性のセットに基づいて、ABAC 構成で使用する属性を選択します。最後に、アクセス権限セット (またはアカウントアクセスマネージャーを使用する場合は IAM ロール) に含まれるアクセスコントロール属性を使用して、AWS リソースへのアクセスをユーザー ID に許可する ABAC ルールを作成します。IAM Identity Center のユーザー属性と AWS Managed Microsoft AD ディレクトリのユーザー属性のデフォルトマッピングの一覧は、「IAM アイデンティティセンターと Microsoft AD の間のデフォルトのマッピング」を参照してください。

外部 ID プロバイダーを ID ソースとして使用する際の属性を選択する

外部 ID プロバイダー (IdP) を ID ソースとして IAM Identity Center を構成する場合、ABAC で属性を使用する方法は 2 つあります。

- IAM Identity Center コンソールで属性マッピングを設定します。IAM Identity Center ディレクトリの属性を、IAM Identity Center コンソールの [アクセスコントロールの属性] ページのセッションタ

グにマッピングできます。ここで選択した属性値は、アイデンティティセンターディレクトリから取得されたもので、SAML アサーションを介して IdP から取得された一致する属性の値を置き換えます。SCIM の使用状況に応じて、次のことを考慮してください。

- SCIM を使用している場合、IdP は属性値を自動的に IAM Identity Center に同期させます。その後、[アクセスコントロールの属性] ページでこれらの同期された属性を選択して、セッションタグとして使用できます。
- SCIM を使用しない場合は、IAM Identity Center を ID ソースとして使用する場合と同様に、手動でユーザーを追加し、属性を設定する必要があります。次に、[Attributes for access control] (アクセスコントロールの属性) ページに移動して、ポリシーで使用する属性を選択します。

- IdP から SAML アサーションを介して属性を渡します。SAML アサーションを通じてセッションタグとして属性を送信するように IdP を設定することができます。これを行うには、属性名を `https://aws.amazon.com/SAML/Attributes/AccessControl:TagKey` に設定したうえで SAML アサーションを送信するように IdP を設定します。*`TagKey`* は、入力するセッションタグキーに置き換えます。この場合、IAM Identity Center はポリシー評価のために IdP から属性名と値を渡します。

  外部 IdP から SAML アサーションを介して属性を渡す場合、[アクセスコントロールの属性] ページで ABAC 属性マッピングを設定する必要はありません。ただし、[アクセスコントロールの属性] ページで同じ属性の ABAC マッピングを設定すると、Identity Center ディレクトリからのマッピングが優先され、SAML アサーションで IdP によって送信された値が置き換えられます。

> **Note**
>
> SAML アサーションの属性は、[Attributes for access control] (アクセスコントロールの属性) ページには表示されません。これらの属性を事前に把握しておき、ポリシー作成時にアクセスコントロールルールに追加する必要があります。属性の外部 IdP を信頼する場合、ユーザーが AWS アカウント にフェデレーションする際に、これらの属性が常に渡されます。SAML アサーションの送信のために IdP 側でアクセス制御用のユーザー属性を構成する方法については、お使いの IdP の IAM アイデンティティセンターの ID ソースに関するチュートリアル を確認してください。

IAM Identity Center のユーザー属性から外部 IdP のユーザー属性まで、サポートされている属性の完全なリストについては、「サポートされている外部 ID プロバイダ属性」を参照してください。

IAM Identity Center で ABAC を使い始めるには、以下のトピックを参照してください。

トピック

- アクセスコントロールのための属性の有効化と設定
- IAM Identity Center を使用して ABAC の権限セットを作成する

アクセスコントロールのための属性の有効化と設定

属性ベースのアクセス制御 (ABAC) を使用するには、まず IAM アイデンティティセンターコンソールの[設定] ページまたは IAM アイデンティティセンター API で有効にする必要があります。ID ソースに関係なく、ABAC で使用するように ID ストアのユーザー属性をいつでも設定できます。コンソールで、[設定] ページの [アクセスコントロールの属性] タブに移動することで、これを行うことができます。ID ソースとして外部 ID プロバイダー (IdP) を使用する場合は、SAML アサーションで外部 IdP から属性を受信するオプションもあります。この場合、目的の属性を送信するように外部 IdP を設定する必要があります。SAML アサーションの属性が IAM アイデンティティセンターの ABAC 属性としても定義されている場合、IAM アイデンティティセンターは、AWS アカウント へのサインイン時のセッションタグとしてアイデンティティストアから値を送信します。

> **Note**
>
> IAM Identity Center コンソールの [アクセスコントロールの属性] ページから、外部 IdP によって構成および送信された属性を表示することはできません。外部 IdP からの SAML アサーションでアクセスコントロール属性を渡している場合は、ユーザーがフェデレーションを行う際に、その属性が AWS アカウント に直接送信されます。その属性は IAM Identity Center でのマッピングには利用できません。

トピック

- アクセスコントロールの属性を有効にする
- アクセス制御用の属性を選択する
- アクセスコントロールの属性を無効にする

アクセスコントロールの属性を有効にする

IAM Identity Center コンソールを使用してアクセス属性 (ABAC) コントロール機能を有効にする場合は、次の手順で行います。

> **Note**
>
> 既存の権限セットがあり、IAM Identity Center インスタンスで ABAC を有効にする予定の場合、まず、追加のセキュリティ制限により、最初に `iam:UpdateAssumeRolePolicy` ポリシーを設定する必要があります。アカウントにアクセス権限セットを作成していない場合は、これらの追加のセキュリティ制限は必要ありません。
> IAM Identity Center インスタンスが 2020 年 12 月より前に作成され、そのインスタンスで ABAC を有効にする場合は、お使いのアカウントでアクセス許可セットが作成されているかどうかにかかわらず、IAM Identity Center 管理ロールに関連付けられた `iam:UpdateAssumeRolePolicy` ポリシーが必要です。

アクセスコントロールの属性を有効にする

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [設定] ページで、[アクセス制御情報の属性] ボックスを探し、[有効化] を選択します。次の手順に進み、設定します。

アクセス制御用の属性を選択する

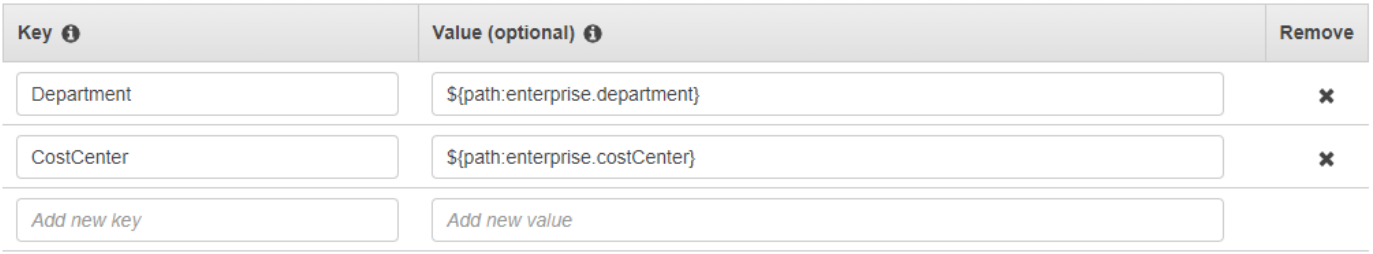
ABAC 構成向け属性設定は、次の手順で行います。

> **Note**
>
> この手順は、セッションタグとして使用するために IAM Identity Center ディレクトリから属性をマッピングする場合にのみ適用されます。SAML アサーションを介して外部 ID プロバイダー (IdP) から属性を渡す場合は、ここで属性マッピングを設定する必要はありません。詳細については、「外部 ID プロバイダーを ID ソースとして使用する際の属性を選択する」を参照してください。Identity Center ディレクトリからマッピングで設定された値は、SAML アサーションで設定された値を上書きします。

IAM Identity Center コンソールを使って属性を選択するには

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。

3. [設定] ページで [アクセス制御用の属性] タブを選択し、[属性の管理] を選択します。
4. [アクセス許可の属性] ページで、[属性を追加] を選択し、[キー] と [値] の詳細を入力します。ここでは、ID ソースから送られてくる属性を、IAM Identity Center がセッションタグとして渡す属性にマッピングします。



キーは、ポリシーで使用するための属性に付ける名前を表します。これは任意の名前で構いませんが、アクセスコントロールのために作成したポリシーでは、その正確な名前を指定する必要があります。例えば、Okta (外部の IdP) を ID ソースとして使用しており、組織のコストセンターのデータをセッションタグとして渡す必要があるとします。キーには、CostCenter のような名前をキーネームとして入力します。重要なのは、ここでどのような名前を設定しても、`aws:PrincipalTag ####` (つまり `"ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"`) で、全く同じ名前を設定する必要があります。

> **Note**
>
> キーには単一値の属性 (例: **`Manager`**) を使用します。IAM Identity Center は ABAC の複数値属性 (例: **`Manager, IT Systems`**) をサポートしていません。

値は、設定された ID ソースから取得される属性のコンテンツを表します。ここでは、IAM アイデンティティセンターと外部 ID プロバイダーディレクトリ間の属性マッピング にリストされている適切な ID ソーステーブルから任意の値を入力できます。例えば、上記の例では、サポートされている IdP 属性リストを確認して最も近い属性である **`${path:enterprise.costCenter}`** を特定し、それを値フィールドに入力します。上記のスクリーンショットを参考にしてください。SAML アサーションで属性を渡すオプションを使用しない限り、このリスト以外の外部 IdP の属性値を ABAC に使用することはできません。

5. [Save changes] (変更の保存) をクリックします。

アクセスコントロール属性のマッピング設定できたので、ABAC 設定プロセスを完了させます。そのためには、ABAC ルールを作成し、権限セットやリソースベースのポリシーに追加します。これは、

ユーザー ID に AWS リソースへのアクセスを許可するために必要です。詳細については、「IAM Identity Center を使用して ABAC の権限セットを作成する」を参照してください。

アクセスコントロールの属性を無効にする

次の手順で、ABAC 機能を無効にし、設定されていた属性マッピングをすべて削除します。

アクセスコントロールの属性を無効にする

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [設定] ページで [アクセス制御用の属性] タブを選択し、[属性の管理] を選択します。
4. [アクセスコントロールの属性の管理] ページで、[無効] を選択します。
5. [アクセスコントロールの属性を無効にする] ダイアログウィンドウで情報を確認し、準備ができたら **DISABLE** と入力し、[確認] を選択します。

> **Important**
>
> このステップでは、外部 ID ソースプロバイダーからの SAML アサーションに属性が存在するかどうかに関係なく、AWS アカウント へのフェデレーション時にすべての属性を削除し、アクセスコントロールの属性の使用を停止します。

IAM Identity Center を使用して ABAC の権限セットを作成する

設定した属性値に基づいて AWS リソースにアクセスできるユーザーを決定するアクセス権限ポリシーを作成できます。ABAC を有効にして属性を指定すると、IAM Identity Center は認証されたユーザーの属性値を IAM に渡し、ポリシー評価で使用できるようにします。

aws:PrincipalTag 条件キー

アクセスコントロール属性は、アクセスコントロールルールを作成するための `aws:PrincipalTag` 条件キーを使用して、アクセス権限セット (またはアカウントアクセスマネージャーを使用する場合は IAM ロール) に使用することができます。例えば、次のポリシーでは、組織内のすべてのリソースに、それぞれのコストセンターをタグ付けすることができます。また、開発者にコストセンターのリソースへのアクセスを許可する単一のアクセス権限セット (またはアカウントアクセスマネージャーを使用する場合は IAM ロール) を使用することもできます。これで、開発者が SSO とコストセンター属性を使ってアカウントに連携すると、それぞれのコストセンターのリソースにしかアクセスで

きなくなります。チームがプロジェクトに開発者やリソースを追加しても、リソースに正しいコストセンターをタグ付けするだけで済みます。そして、開発者が AWS アカウント にフェデレートする際に、AWS セッションでコストセンター情報を渡します。その結果、組織がコストセンターに新しいリソースや開発者を追加しても、開発者は権限の更新を必要とせずに、コストセンターに整合したリソースを管理することができます。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/
CostCenter}"
                }
            }
        }
    ]
}
```

ユーザーが IAM Identity Center を介して AWS アカウント にフェデレーションすると、設定されたアクセスコントロール属性がセッションタグとして渡されます。ポリシー内のこれらのセッションタグを参照するには、aws:PrincipalTag/*tag-key* 条件キーを使用します。この条件キーは、アイデンティティベースのポリシー、リソースベースのポリシー、アクセス許可の境界、サービスコントロールポリシー (SCP)、VPC エンドポイントポリシーなど、条件を使用できるすべての関連する

AWS IAM ポリシータイプでサポートされています。これにより、AWS 環境全体でユーザー属性に基づいてアクセスコントロールをきめ細かく決めることができます。

詳細については、「IAM ユーザーガイド」のaws:PrincipalTag および「EC2: 一致するプリンシパルタグとリソースタグに基づいてインスタンスを開始または停止する」を参照してください。

ポリシーの条件に無効な属性が含まれている場合、ポリシーの条件は失敗し、アクセスは拒否されます。詳細については、「ユーザーが外部の ID プロバイダーを使用してサインインしようとすると、「予期しないエラーが発生しました」というエラーが発生します」を参照してください。

IAM アイデンティティセンターのサービスリンクロールについて

サービスにリンクされたロールは、IAM Identity Center が、組織内の特定の AWS アカウント へのシングルサインオン· アクセスを持つユーザーを AWS Organizations に委譲し、実施できるようにするための事前定義された権限を提供します。このサービスでは、サービスにリンクされたロールを組織内のすべての AWS アカウント でプロビジョニングすることで、この機能を有効にします。それにより、IAM Identity Center などの他の AWS サービスがサービス関連のタスクを実行するためにこれらのロールを活用できるようになります。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。

IAM Identity Center を有効にすると、IAM Identity Center は AWS Organizations の組織内のすべてのアカウントにサ ービスにリンクされたロールを作成します。また、IAM Identity Center では、その後組織に追加されるすべてのアカウントに、同じサービスにリンクしたロールが作成されます。このロールは、IAM Identity Center が顧客に代わって各アカウントのリソースにアクセスすることを可能にします。詳細については、「AWS アカウント へのアクセスを設定する」を参照してください。

各 AWS アカウント に作成されるサービスにリンクされたロール名は `AWSServiceRoleForSSO` です。詳細については、「IAM Identity Center のサービスリンクロールの使用」を参照してください。

> **注意事項**
>
> - AWS Organizations 管理アカウントにサインインしている場合、サービスリンクロールではなく、現在サインインしているロールが使用されます。これにより、権限の昇格を防ぐことができます。
> - IAM Identity Center が AWS Organizations 管理アカウントで IAM 操作を実行すると、すべての操作は IAM プリンシパルの認証情報を使用して行われます。これにより、CloudTrail のログから、管理アカウントのすべての権限変更を誰が行ったかがわかります。

AWS アクセスポータルのセットアップと使用

AWS アクセスポータルは、IAM アイデンティティセンターを通じてワークフォースを AWS アカウント およびクラウドアプリケーションに接続します。管理者はポータルを設定し、ユーザーアクセスを管理します。エンドユーザーは一度サインインして、承認されたすべてのリソースにシームレスにアクセスします。

AWS アクセスポータルは、以下へのシングルサインオンアクセスを提供します。

- AWS アカウント組織内の 。
- AWS Amazon Quick や Kiro などのマネージドアプリケーション。
- Office 365、Concur、Salesforce などのクラウドアプリケーション。

ユーザーがポータルにサインインすると、追加のサインインなしでアクセスが許可されている AWS アカウント およびアプリケーションが見つかります。

AWS アクセスポータルは、AWS アカウントアクセスアプリケーションへのアクセスも提供します。ユーザーは、アカウントアクセスマネージャーを介して自身に割り当てられた IAM ロールを表示してアクセスできます。

AWS アクセスポータルの開始方法

管理者向け:

AWS アクセスポータルを設定し、ユーザーアクセスを管理するには、IAM アイデンティティセンターの組織インスタンスまたはアカウントインスタンスへの管理アクセスが必要です。

1. 必要に応じて、 AWS アクセスポータル URL をカスタマイズします。
2. AWS アカウント とアプリケーションへのユーザーアクセスを割り当てる。割り当てられた AWS リソースがポータルに表示されます。

エンドユーザーの場合:

管理者は AWS アクセスポータルのセットアップを完了し、ポータル URL とサインイン認証情報を提供している必要があります。

1. 管理者からポータル URL を取得します (通常は `https://your-company.awsapps.com/start`)。

2. 管理者から提供された認証情報を使用してサインインします。
3. ポータルの リソースにアクセスします。

AWS アクセスポータルを設定する

管理者は、組織のニーズに合わせて AWS アクセスポータルをカスタマイズし、ユーザーが承認されたリソースに簡単にアクセスできるようにします。

設定できる内容

AWS アクセスポータルのアクティベーション: ユーザー認証情報のアクティベーションや初回サインインプロセスなど、 AWS アクセスポータルへの最初のユーザーアクセスを設定します。

カスタム AWS アクセスポータル URL (オプション): 組織の AWS アクセスポータル URL をデフォルトの形式 (`d-xxxxxxxxxx.awsapps.com/start`) からより認識しやすいサブドメイン (`your-company.awsapps.com/start`) にパーソナライズします。

開始する前に

IAM アイデンティティセンターへの管理アクセス権があることを確認し、IAM アイデンティティセンターが組織インスタンスまたはアカウントインスタンスとして設定されていることを確認し、カスタムサブドメイン名を計画します (これは後で変更できない 1 回限りの設定です)。

設定が完了すると、ユーザーはカスタム URL を使用して AWS アクセスポータルにアクセスし、組織用に確立したアクティベーションプロセスに従うことができます。

トピック

- IAM アイデンティティセンターを初めて使用するユーザー向けに、AWS アクセスポータルを有効化する
- AWS アクセスポータル URL のカスタマイズ
- ユーザーが AWS アクセスポータルにサインインできることを確認する

IAM アイデンティティセンターを初めて使用するユーザー向けに、AWS アクセスポータルを有効化する

AWS アクセスポータルに初回サインインする場合は、ユーザー認証情報を有効にする手順が記載された電子メールを確認してください。

ユーザー認証情報を有効にするには

1. 会社から送られてきたメールに応じて次のいずれかの方法を選択し、AWS アクセスポータルを使用し始めることができるように、ユーザー認証情報をアクティブ化します。

   a. 「Invitation to join AWS IAM Identity Center」という件名のメールを受信したら、メールを開いて [招待を受け入れる] を選択します。「新規ユーザー登録」ページで、パスワードを入力して確認し、「新しいパスワードを設定」を選択します。このパスワードは、ポータルにサインインするたびに使用します。

   b. 貴社の IT サポートまたは IT 管理者から E メールを送信された場合は、ユーザー認証情報をアクティブ化するために伝えられた指示事項に従います。

2. 新しいパスワードを指定してユーザー認証情報を有効にすると、AWS アクセスポータルにより自動的にサインインされます。されない場合は、AWS アクセスポータルにサインインします。で説明されている指示事項に従って、手動で AWS アクセスポータルにサインインできます。

AWS アクセスポータル URL のカスタマイズ

デフォルトでは、AWS 形式の URL を使用して d-*xxxxxxxxxx*.awsapps.com/start アクセスポータルにアクセスできます。プラグインは次のようにカスタマイズできます: *your_subdomain*.awsapps.com/start

> **Important**
>
> AWS アクセスポータル URL を変更した場合、後で編集することはできません。

URL をカスタマイズするには

1. https://console.aws.amazon.com/singlesignon/ で AWS IAM アイデンティティセンター コンソールを開きます。
2. IAM アイデンティティセンターコンソールのナビゲーションペイン内で、[ダッシュボード] > [設定の概要] を選択します。
3. AWS アクセスポータル URL の下にある [カスタマイズ] ボタンを選択します。

> **Note**
>
> [カスタマイズ] ボタンが表示されない場合は、AWS アクセスポータルがすでにカスタマイズされていることを意味します。AWS アクセスポータル URL のカスタマイズは 1 回限りの操作であり、一度実行すると取り消しできません。

4. 希望するドメイン名を入力し、[保存] をクリックします。

これで、カスタマイズした URL を使って、AWS アクセスポータルから AWS コンソールにサインインできるようになりました。

ユーザーが AWS アクセスポータルにサインインできることを確認する

次の手順は、IAM アイデンティティセンターユーザーが AWS アクセスポータルにサインインし、AWS アカウント にアクセスできることを確認するためのものです。

AWS アクセスポータルにサインインします。

1. 以下のいずれかを行って、AWS マネジメントコンソール にサインインします。
   - 新規の AWS (ルートユーザー) – [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、アカウント所有者としてサインインします。次のページでパスワードを入力します。
   - すでに使用している AWS (IAM 認証情報) — IAM 認証情報を使用してサインインし、管理者ロールを選択します。
2. IAM Identity Center コンソール を開きます。
3. ナビゲーションペインで、ダッシュボードを選択してください。
4. 「ダッシュボード」ページの「設定概要」で、AWSアクセスポータル URL を選択します。
5. 次のいずれかを使用してサインインします。
   - Active Directory または外部 ID プロバイダー (IdP) を ID ソースとして使用している場合は、Active Directory または IdP ユーザーの認証情報でサインインします。
   - ID ソースとしてデフォルトの Identity Center ディレクトリを使用している場合は、ユーザーを作成したときに指定したユーザー名と、そのユーザーに指定した新しいパスワードを使用してサインインします。
6. [アカウント] タブ内で、見たい AWS アカウントを展開します。

7. 使用可能なロールが表示されます。例えば、[AdministratorAccess] 権限セットと [Billing] 権限セットの両方を割り当てられている場合、それらのロールはいずれも AWS アクセスポータルに表示されます。セッションに使用する IAM ロール名を選択します。
8. AWS 管理コンソールにリダイレクトされれば、AWS アカウント へのアクセスの設定は正常に完了しています。

> **Note**
>
> AWS アカウント一覧に何も表示されない場合は、そのユーザはそのアカウントのアクセス権限セットにまだ割り当てられていない可能性があります。アクセス権限セットにユーザを割り当てる手順については、AWS アカウント にユーザーまたはグループアクセスを割り当てる を参照してください。

IAM アイデンティティセンターの認証情報を使用してサインインできることを確認したら、AWS マネジメントコンソールへのサインインに使用したブラウザに切り替えて、ルートユーザーまたは IAM ユーザーの認証情報からサインアウトします。

> **Important**
>
> AWS アクセスポータルにサインインして管理タスクを実行するときは、IAM ユーザーまたはルートユーザーの認証情報を使用する代わりに IAM アイデンティティセンター管理ユーザーの認証情報を使用することを強くお勧めします。ルートユーザー資格情報は保護し、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。他のユーザーがアカウントやアプリケーションにアクセスできるようにし、IAM Identity Center を管理できるようにするには、IAM Identity Center を通じてのみアクセス権限セットを作成して割り当ててください。

AWS アクセスポータルを使用する

ポータル内から、AWS アカウント またはアプリケーションのアイコンを選択すると、複数のアプリケーションを起動できます。AWS アクセスポータル内にアプリケーションアイコンがあるということは、組織の管理者がそれらの AWS アカウントまたはアプリケーションへのアクセスを許可していることを意味します。つまり、AWS アクセスポータルからこれらのアカウントまたはアプリケーションには、サインインのプロンプトが表示されることなくアクセスできるということです。

AWS アクセスポータルの使用方法

AWS アクセスポータルを使用するには:

1. 管理者からポータル URL を取得します (通常は `https://your-company.awsapps.com/start` のようになります)。
2. 管理者から提供された認証情報を使用してサインインします。
3. ポータルでアクセスするアカウントとアプリケーションを選択します。

管理者は、ロールとアクセス許可に基づいてポータルに表示される内容をコントロールします。以下の状況では、管理者に連絡して追加のアクセスをリクエストしてください。

- アクセスする必要のある AWS アカウント またはアプリケーションが表示されていない。
- 特定のアカウントまたはアプリケーションに対するアクセス権限が想定されるものと異なっている。

トピック

- AWS アクセスポータルにサインインします。
- AWS アクセスポータルのユーザーパスワードをリセットする
- AWS CLI または AWS SDK の IAM Identity Center のユーザー認証情報を取得します。
- AWS マネジメントコンソール 宛先へのショートカットリンクの作成
- MFA 用デバイスの登録
- アクティブなセッションの表示と終了

AWS アクセスポータルにサインインします。

AWS アクセスポータルは、IAM アイデンティティセンターユーザーに、ウェブポータルを介して割り当てられたすべての AWS アカウント およびアプリケーションへのシングルサインオンアクセスを提供します。AWS アクセスポータルにサインインする方法、サインインのヒント、および AWS アクセスポータルからサインアウトする方法について説明します。

前提条件

AWS アクセスポータルを使用するには、IAM アイデンティティセンターを有効にする必要があります。詳細については、「IAM Identity Center を有効にする」を参照してください。

> **Note**
>
> サインイン後、AWS アクセスポータルのセッション有効時間はデフォルトで 8 時間です。管理者はこのセッションの有効時間を変更できます。

AWS アクセスポータルにサインインします。

AWS アクセスポータルにサインインします。

1. ブラウザウィンドウで、提供されたサインイン URL を貼り付け、 Enter キーを押します。URL は `d-xxxxxxxxxx.awsapps.com/start` または `your_subdomain.awsapps.com/start` のようになります。ポータルへのこのリンクをブックマークに追加して後ですばやくアクセスできるようにすることをお勧めします。
2. 標準の会社のサインイン認証情報を使用してサインインします。

   > **Note**
   >
   > 管理者から E メールでワンタイムパスワード (OTP) が送信され、初めてサインインする場合は、そのパスワードを入力します。サインインしたら、今後のサインイン用に新しいパスワードを作成する必要があります。

   [Verification code] (確認コード) の入力を指示された場合は、E メールを確認してコードをコピーしてサインインページに貼り付けてください。

   > **Note**
   >
   > 確認コードは通常、E メールで送信されますが、その送信方法はさまざまです。詳細については、管理者に確認してください。
3. サインインしたら、ポータルに表示される AWS アカウント とアプリケーションにアクセスできます。

信頼されたデバイス

サインインページで [これは信頼できるデバイスです] というオプションを選択すると、IAM Identity Center はそのデバイスからの今後のすべてのサインインを承認されたものとみなします。つまり、

その信頼できるデバイスを使用している限り、 IAM アイデンティティセンターは、MFA コードを入力する指示を出しません。ただし、新しいブラウザからサインインした場合や、お客様のデバイスに未知の IP アドレスが発行された場合などは例外となります。

AWS アクセスポータルにサインインします。

AWS アクセスポータルの操作を管理するのに役立つヒントをいくつか紹介します。

- 場合によっては、サインアウトして AWS アクセスポータルにサインインしなおす必要があります。この手順は、管理者から最近割り当てられた新しいアプリケーションにアクセスするために必要になります。ただし、すべての新しいアプリケーションは 1 時間ごとに更新されるため、この手順は必須ではありません。
- AWS アクセスポータルにサインインすると、ポータルに表示されているアプリケーションのアイコンを選択して、そのアプリケーションを開くことができます。アプリケーションを使用し終わったら、アプリケーションを閉じるか、AWS アクセスポータルからサインアウトします。アプリケーションを閉じると、そのアプリケーションからのみサインアウトされます。AWS アクセスポータルから開いた他のアプリケーションは開いたままで実行されています。
- 別のユーザーとしてサインインするには、最初に AWS アクセスポータルからサインアウトする必要があります。ポータルからログアウトすると、ブラウザセッションから認証情報が完全に削除されます。
- AWS アクセスポータルにサインインすると、ロールに切り替えることができます。切り替えることで元のユーザーアクセス権限が一時的に無効になり、そのロールに割り当てられたアクセス権限が代わりに付与されます。 詳細については、「ロールの切り替え (コンソール)」を参照してください。

AWS アクセスポータルからサインアウトする

ポータルからログアウトすると、認証情報がブラウザセッションから完全に削除されます。詳細については、AWS サインイン ガイドの「AWS アクセスポータルからサインアウトする方法」を参照してください。

AWS アクセスポータルからサインアウトするには

- AWS アクセスポータルのナビゲーションバーから「サインアウト」を選択します。

> **Note**
>
> 別のユーザーとしてサインインする場合は、最初に AWS アクセスポータルからサインアウトする必要があります。

AWS アクセスポータルのユーザーパスワードをリセットする

AWS アクセスポータルは、IAM アイデンティティセンターユーザーに対し、すべての割り当て済み AWS アカウントおよびクラウドアプリケーションへのシングルサインオンアクセスを Web ポータルを介して提供するソリューションです。AWS アクセスポータルは、AWS リソースを管理するためのサービスコンソールの集合体である AWS マネジメントコンソール とは異なります。

この手順を使用して、AWS アクセスポータルの IAM Identity Center ユーザーパスワードをリセットします。ユーザータイプの詳細については、「AWS サインイン ユーザーガイド」をご覧ください。

考慮事項

AWS アクセスポータルのパスワードリセット機能は、Identity Center ディレクトリまたは AWS Managed Microsoft AD を ID ソースとして使用している Identity Center インスタンスのユーザーのみが使用できます。ユーザーが外部 ID プロバイダーまたは AD Connector に接続されている場合、ユーザーパスワードのリセットは外部 ID プロバイダーまたは接続された Active Directory から行う必要があります。

- ID ソースが IAM アイデンティティセンターディレクトリである場合は、「IAM Identity Center で ID を管理する際のパスワード要件」を参照してください。
- ID ソースが AWS Managed Microsoft AD である場合は、「Password requirements when resetting a password in AWS Managed Microsoft AD」を参照してください。

AWS アクセスポータルのパスワードをリセットするには

1. ブラウザを開き、AWS アクセスポータルのサインインページに移動します。

   AWS アクセスポータル URL がお持ちでない場合は、Eメールを確認してください。AWS アクセスポータルへの特定のサインイン URL が記載された AWS IAM Identity Center への招待状がメールで送信されているはずです。あるいは、ワンタイムパスワードと AWS アクセスポータル URL を管理者が直接提供している場合もあります。この情報が見つからない場合は、管理者に連絡して送信してもらってください。

AWS アクセスポータルへのサインインについて詳しくは、「AWS サインイン ユーザーガイド」の「AWS アクセスポータルへのサインイン」を参照してください。

2. [ユーザー名] を入力し、[次へ] を選択します。
3. [パスワード] で [パスワードを忘れた場合] を選択します。

   [ユーザー名] を入力し、提供されたイメージの文字を入力してロボットではないことを確認します。次に、[次へ] を選択します。文字を入力できない場合は、広告ブロックソフトウェアを無効にする必要がある場合があります。
4. パスワードリセットの E メールが送信されたことを確認するメッセージが表示されます。[続行] をクリックしてください。
5. no-reply@signin.aws から、「パスワードのリセットがリクエストされました」という件名のメールが届きます。メールで「パスワードのリセット」を選択します。
6. [パスワードのリセット] ページで、[ユーザー名] を確認し、AWSアクセスポータルの新しいパスワードを指定して、[新しいパスワードの設定] を選択します。
7. no-reply@signin.awsから「パスワードが更新されました」という件名のメールが届きます。

> **Note**
>
> 管理者は、パスワードのリセット手順を記載したメールを送信するか、ワンタイムパスワードを生成してユーザーと共有することで、パスワードをリセットできます。管理者の場合は、「エンドユーザーの IAM Identity Center ユーザーパスワードをリセットします。」を参照してください。

AWS CLI または AWS SDK の IAM Identity Center のユーザー認証情報を取得します。

IAM Identity Center のユーザー認証情報を使用して、AWS Command Line Interface または AWS Software Development Kit (SDK) を使用することにより、プログラムで AWS サービスにアクセスできます。このトピックでは、IAM Identity Center のユーザーの一時的な認証情報を取得する方法について説明します。

AWS アクセスポータルは、IAM Identity Center のユーザーに AWS アカウント やクラウドアプリケーションへのシングルサインオンアクセスを提供します。IAM Identity Center ユーザーとして

AWS アクセスポータルにサインインすると、一時的な認証情報を取得できます。その後、AWS CLI または AWS SDK 内の認証情報 (IAM Identity Center ユーザー認証情報とも呼ばれます) を使用して、AWS アカウント 内のリソースにアクセスできます。

AWS CLI を使用してプログラムから AWS サービスにアクセスする場合は、このトピックの手順を使用して AWS CLI へのアクセスを開始できます。AWS CLI の詳細については、「AWS Command Line Interface ユーザーガイド」を参照してください。

AWSSDK を使用してプログラムでAWSサービスにアクセスする場合は、このトピックの手順に従うことでAWS SDK の認証も直接確立されます。AWSSDK について詳しくは、「AWS SDK およびツールリファレンスガイド」を参照してください。

> **Note**
>
> IAM Identity Center のユーザーは「IAM ユーザー」とは異なります。IAM ユーザーには、AWS リソースへの長期的な認証情報が付与されます。IAM Identity Center のユーザーには一時的な認証情報が付与されます。一時的な認証情報は、ログインするたびに生成されるため、AWS アカウント にアクセスするための安全なベストプラクティスとして、一時的な認証情報を使用することをお勧めします。

前提条件

IAM Identity Center ユーザーの一時認証情報を取得するには、以下が必要です。

- IAM Identity Center ユーザー — このユーザーとして AWS アクセスポータルにサインインします。ユーザーまたは管理者がこのユーザーを作成できます。IAM Identity Center を有効化して IAM Identity Center ユーザーを作成する方法については、IAM アイデンティティセンターを使用した開始方法 を参照してください。
- AWS アカウント へのユーザーアクセス — IAM Identity Center ユーザーに一時的な認証情報を取得する権限を付与するには、管理者または管理者が IAM Identity Center ユーザーを「権限セット」に割り当てる必要があります。権限セットは IAM Identity Center に保存され、IAM Identity Center ユーザーが AWS アカウント に対して持つアクセスレベルを定義します。管理者が IAM Identity Center ユーザーを作成した場合は、このアクセス権を追加してもらうよう依頼してください。詳細については、「AWS アカウント にユーザーまたはグループアクセスを割り当てる」を参照してください。

- AWS CLI インストール済み — 一時的な認証情報を使用するには、AWS CLI をインストールする必要があります。手順については、「AWS CLI ユーザーガイド」にある「AWS CLI の最新バージョンのインストールまたは更新」を参照してください。

考慮事項

IAM Identity Center ユーザーの一時的な認証情報を取得する手順を完了する前に、以下の考慮事項に注意してください。

- IAM Identity Center は IAM ロールを作成する — IAM Identity Center のユーザーを権限セットに割り当てると、IAM Identity Center はその権限セットから対応する IAM ロールを作成します。権限セットによって作成される IAM ロールは、AWS Identity and Access Managementで作成される IAM ロールとは以下の点で異なります。
  - IAM Identity Center は、権限セットによって作成されたロールを所有し、保護します。IAM Identity Center のみがこれらのロールを変更できます。
  - IAM Identity Center のユーザーのみが、割り当てられた権限セットに対応するロールを引き受けることができます。権限セットへのアクセスを IAM ユーザー、IAM フェデレーティッドユーザー、またはサービスアカウントに割り当てることはできません。
  - これらのロールのロール信頼ポリシーを変更して IAM Identity Center 外の「プリンシパル」へのアクセスを許可することはできません。

  IAM で作成したロールの一時的な認証情報を取得する方法については、「AWS Identity and Access Management ユーザーガイド」の「AWS CLI で一時的なセキュリティ認証情報を使用する」を参照してください。
- 権限セットのセッション期間を設定可能 — AWS アクセスポータルにサインインすると、IAM Identity Center ユーザーが割り当てられている権限セットが使用可能なロールとして表示されます。IAM Identity Center は、このロール用に別のセッションを作成します。このセッションは、権限セットに設定されているセッション時間に応じて 1 時間から 12 時間まで可能です。デフォルトでは、セッションの有効期間は 1 時間です。詳細については、「AWS アカウントのセッション期間を設定する」を参照してください。

一時的な認証情報の取得と更新

IAM Identity Center ユーザーの一時認証情報は、自動または手動で取得および更新できます。

トピック

- 認証情報の自動更新 (推奨)
- 認証情報の手動更新

認証情報の自動更新 (推奨)

認証情報の自動更新は、Open IdConnect Center (OIDC) デバイスコード認可標準を使用します。この方法では、AWS CLI の `aws configure sso` コマンドを使用して直接アクセスを開始します。このコマンドを使用すると、どの AWS アカウント でも、自分が割り当てられている権限セットに関連付けられているロールに自動的にアクセスすることができます。

IAM Identity Center ユーザーに作成されたロールにアクセスするには、`aws configure sso` コマンドを実行し、ブラウザのウィンドウから AWS CLI を承認します。AWS アクセスポータルのセッションがアクティブである限り、AWS CLI は一時認証情報を自動的に取得し、認証情報を自動的に更新します。

詳細については、AWS Command Line Interface ユーザーガイドの「`aws configure sso wizard` を使用したプロフィール設定」を参照してください。

自動的に更新される一時的な認証情報を取得するには

1. 管理者から提供された特定のサインイン URL を使用して AWS アクセスポータルにサインインします。IAM Identity Center ユーザーを作成した場合は、AWS はサインイン URL を含む招待メールを送信しました。アクセスポータルへのサインインについて詳しくは、「AWS Sign-In User Guide」の「Sign in to the AWS access portal」を参照してください。
2. [アカウント] タブ内で、認証情報を取得する AWS アカウントを選択します。アカウントを選択すると、そのアカウントに関連付けられているアカウント名、アカウント ID、および E メールアドレスが表示されます。

   > **Note**
   >
   > AWS アカウントが一覧表示されていない場合は、そのアカウントの権限セットに割り当てられていない可能性があります。この場合は、管理者に連絡して、このアクセス権を追加してもらうよう依頼してください。詳細については、「AWS アカウント にユーザーまたはグループアクセスを割り当てる」を参照してください。

3. アカウントの下に、IAM Identity Center ユーザーに割り当てられている権限セットの名前が使用可能なロールとして表示されます。たとえば、IAM アイデンティティセンターユーザーがア

カウントの [PowerUserAccess] 権限セットに割り当てられている場合、ロールはAWSアクセスポータルに [PowerUserAccess] として表示されます。

4. ロール名の横にあるオプションに応じて、[アクセスキー] を選択するか、[コマンドラインまたはプログラムによるアクセス] を選択します。
5. [認証情報の取得]ダイアログボックスで、AWS CLIをインストールしたオペレーティングシステムに応じて、「macOS と Linux」、「Windows」、または「PowerShell」のいずれかを選択します。
6. 「AWSIAM Identity Center の認証情報 (推奨)」に、`SSO Start URL` と `SSO Region` が表示されます。これらの値は、IAM Identity Center で有効化されたプロファイルおよび `sso-session` を AWS CLI に対して設定する必要があります。この設定を完了するには、「AWS Command Line Interfaceユーザーガイド」の「`aws configure sso wizard` でプロファイルを設定」の指示に従います。

認証情報が期限切れになるまで、AWS アカウント で必要に応じて AWS CLI を使用できます。

認証情報の手動更新

特定の AWS アカウント の特定の権限セットに関連付けられたロールの一時的な認証情報を取得するには、認証情報の手動更新を使用できます。そのためには、一時的な認証情報に必要なコマンドをコピーして貼り付けます。この方法では、一時的な認証情報を手動で更新する必要があります。

一時的な認証情報の有効期限が切れるまで AWS CLI コマンドを実行できます。

手動で更新する認証情報を取得するには

1. 管理者から提供された特定のサインイン URL を使用して AWS アクセスポータルにサインインします。IAM Identity Center ユーザーを作成した場合は、AWS はサインイン URL を含む招待メールを送信しました。アクセスポータルへのサインインについて詳しくは、「AWS Sign-In User Guide」の「Sign in to the AWS access portal」を参照してください。
2. [アカウント] タブ内で、アクセス認証情報を取得したい AWS アカウントを展開し、IAM ロール名 (Administrator など) を表示させます。IAM ロール名の横にあるオプションに応じて、[アクセスキー] を選択するか、[コマンドラインまたはプログラムによるアクセス] を選択します。

> **Note**
>
> AWS アカウントが一覧表示されていない場合は、そのアカウントの権限セットに割り当てられていない可能性があります。この場合は、管理者に連絡して、このアクセス権

を追加してもらうよう依頼してください。詳細については、「AWS アカウント にユーザーまたはグループアクセスを割り当てる」を参照してください。

3. [認証情報の取得]ダイアログボックスで、AWS CLIをインストールしたオペレーティングシステムに応じて、「MacOS と Linux」、「Windows」、または「PowerShell」のいずれかを選択します。
4. 次のいずれかのオプションを選択します。

   - オプション 1: AWS 環境変数を設定する

     このオプションを選択すると、`credentials` ファイルや `config` ファイル内の設定を含むすべての認証情報が上書きされます。詳細については、「AWS CLIユーザガイド」の「AWS CLIを設定するための環境変数」を参照してください。

     このオプションを使用するには、コマンドをクリップボードにコピーし、AWS CLI ターミナルウィンドウに貼り付け、[Enter] を押して必要な環境変数を設定します。

   - オプション 2: AWS 認証情報ファイルにプロファイルを追加する

     このオプションを選択すると、さまざまな認証情報を使用してコマンドを実行できます。

     このオプションを使用するには、コマンドをクリップボードにコピーし、そのコマンドを共有AWS`credentials` ファイルに貼り付けて、新しい名前付きプロファイルを設定します。詳細については、「AWS SDK とツールのリファレンスガイド」の「共有設定ファイルおよび認証情報ファイル」を参照してください。この認証情報を使用するには、AWS CLI コマンドで `--profile` オプションを指定します。このことは、この同じ認証情報ファイルを使用するすべての環境にも当てはまります。

   - オプション 3: AWS サービスクライアントで個別の値を使用する

     AWS サービスクライアントから AWS リソースにアクセスするには、このオプションを選択します。詳細については、「AWS での構築ツール」を参照してください。

     このオプションを使用するには、値をクリップボードにコピーし、その値をコードに貼り付け、SDK の適切な変数に割り当てます。詳細については、お使いの SDK API 固有のドキュメントを参照してください。

AWS マネジメントコンソール 宛先へのショートカットリンクの作成

AWS アクセスポータルで作成するショートカットリンクを利用すると、IAM アイデンティティセンターのユーザーは、特定の AWS アカウント内にある特定のアクセス許可セットを備えた AWS マネジメントコンソール内のアクセス先にジャンプできます。

ショートカットリンクは、ユーザーとコラボレーターの操作時間を短縮する効果があります。AWS アクセスポータルを含む複数のページを経由して AWS マネジメントコンソール内のアクセス先 URL (例: Amazon S3 バケットインスタンスページなど) に移動する代わりに、ショートカットリンクを使用して同じアクセス先に自動的にジャンプできます。

ショートカットリンクのリンク先オプション

ショートカットリンクには、以下に示すように、優先度別に 3 つのリンク先オプションが用意されています。

- (オプション) ショートカットリンクで指定される AWS マネジメントコンソール内の任意のリンク先 URL。例えば、Amazon S3 バケットインスタンスページなどです。
- (オプション) 許可セット内で管理者が設定するリレーステート URL。リレーステート設定の詳細については、「AWS マネジメントコンソールにすばやくアクセスできるようにリレーステートを設定する」を参照してください。
- AWS マネジメントコンソールホーム。指定しない場合は、これがデフォルトのリンク先になります。

> **Note**
>
> リンク先への自動ナビゲーションは、ユーザーが IAM アイデンティティセンターで認証済みで、AWS アカウントとリンク先 URL 向けへのアクセスに必要なアクセス許可セットが割り当てられている場合のみ成功します。

AWS アクセスポータルには、共有可能なショートカットリンクの作成に使用できる [ショートカットの作成] ボタンが含まれています。リンク先 URL (直前のリストの最初のオプション) を指定する場合は、URL をクリップボードにコピーして共有できます。

AWS アクセスポータルでショートカットリンクを作成する

1. AWS アクセスポータルにサインインした状態で、[アカウント] タブを選択し、[ショートカットの作成] ボタンを選択します。
2. ダイアログボックスで、次の操作を行います。

   a. アカウント ID またはアカウント名を使用して AWS アカウントを選択します。入力すると、ドロップダウンメニューに、入力内容に一致するアクセス可能なアカウント ID と名前が表示されます。アクセス可能なアカウントのみを選択できます。

   b. または、ドロップダウンリストから IAM ロールを選択します。これらは、選択したアカウントに対して割り当てられたアクセス許可セットです。ロールの選択を省略すると、ショートカットリンクを使用する際に、選択したアカウントに対して割り当てられたロールを選択するように求められます。

   > **Note**
   >
   > ショートカットリンクを使用して、新しいアクセスを許可することはできません。ショートカットリンクは、そのユーザーに割り当て済みのアクセス許可セットでのみ機能します。アカウントとリンク先 URL へのアクセスに必要なアクセス許可セットがユーザーに割り当てられていない場合、アクセスは拒否されます。

   c. 必要に応じて、AWS アクセスポータルのリンク先 URL を入力します。URL 入力を省略すると、ショートカットリンクの使用時に、前述のリンク先オプションに基づいてリンク先が自動的に設定されます。

   d. 入力に基づいて、ダイアログボックスの下部にショートカットリンクが生成されます。[URL のコピー] ボタンを選択します。これで、コピーされたショートカットリンクを使用してブックマークを作成したり、あるいは同じアカウントに対する同じアクセス許可セットまたは別の十分なアクセス許可セットを持つコラボレーターとブックマークを共有できるようになりました。

URL エンコーディングを使用した安全な AWS マネジメントコンソールショートカットリンクの作成

アカウント ID、アクセス許可セット名、リンク先 URL を含むすべての URL パラメータ値は、URL エンコードされている必要があります。

ショートカットリンクは、次のパスを使用して、AWS アクセスポータル URL を拡張します。

/#/console?
account_id=*[account_ID]*&role_name=*[permission_set_name]*&destination=*[destination*

従来の AWS パーティションでの完全な URL は、次のパターンに従います。

IPv4 エンドポイント:

https://*[your_subdomain]*.awsapps.com/start/#/console?
account_id=*[account_ID]*&role_name=*[permission_set_name]*&destination=*[destination*

デュアルスタックエンドポイント

https://*[identity_center_instance_id]*.portal.*[region]*.app.aws/#/console?
account_id=*[account_ID]*&role_name=*[permission_set_name]*&destination=*[destination*

以下は、S3FullAccess アクセス許可セットを使用して、ユーザーをアカウント 123456789012 にサインインさせ、S3 コンソールのホームページにジャンプさせるショートカットリンクの例です。

- IPv4 エンドポイント: https://example.awsapps.com/start/#/console?
  account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F
  %2Fconsole.aws.amazon.com%2Fs3%2Fhome
- デュアルスタックエンドポイント: https://ssoins-1234567890abcdef.portal.us-
  east-1.app.aws/#/console?
  account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F
  %2Fconsole.aws.amazon.com%2Fs3%2Fhome
- (AWS GovCloud (US) Region) IPv4 エンドポイント: https://start.us-gov-
  west-1.us-gov-home.awsapps.com/directory/example/#/console?
  account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F
  %2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome
- (AWS GovCloud (US) Region) デュアルスタックエンドポイント: https://
  ssoins-1234567890abcdef.portal.us-gov-west-1.app.aws/#/console?
  account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F
  %2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome

MFA 用デバイスの登録

アイデンティティセンターディレクトリ内のユーザーの場合は、新しいデバイスを多要素認証 (MFA) に登録するには、AWS アクセスポータル内で次の手順で行います。

> **Important**
>
> IAM Identity Center の MFA は、現在、外部 ID プロバイダー による使用はサポートされていません。

開始する前に

この手順を開始する前に、まず適切な認証システムアプリケーションをデバイスにダウンロードすることをお勧めします。MFA デバイスに使用できるアプリケーションの一覧については、「仮想認証アプリ」を参照してください。

デバイスの登録

MFA を使用するデバイスを登録するには

1. AWS アクセスポータルにサインインします。詳細については、「AWS アクセスポータルにサインインします。」を参照してください。
2. ページの右上近くにある [MFA devices] (MFA デバイス) をクリックします。
3. [Multi-factor authentication (MFA) devices] (多要素認証 (MFA) デバイス) ページで、[Register device] (デバイスの登録) をクリックします。

   > **Note**
   >
   > [MFA デバイスの登録] オプションがグレーアウトしている場合は、管理者に連絡してデバイスの登録をサポートしてもらう必要があります。

4. [MFA デバイスの登録] ページで、次の MFA デバイスタイプを選択し、指示に従います。

   - 認証システムアプリケーション
     1. [Set up the authenticator app] (認証システムアプリケーションの設定) ページで、QR コードのグラフィックを含む新しい MFA デバイスの設定情報を表示します。図は、QR コードに対応していないデバイスのマニュアル入力に利用できるシークレットキーを示しています。
     2. 物理的に MFA デバイスを使用して、次の操作を行います。
        a. 互換性のある MFA 認証システムアプリケーションを開きます。MFA デバイスで使用できるテスト済みアプリケーションのリストについては、「仮想認証アプリ」を参照してください。MFA アプリケーションが複数のアカウント (複数の MFA デバイス) をサポー

トしている場合は、新しいアカウント (新しい MFA デバイス) を作成するオプションを選択します。

b. MFA アプリケーションが QR コードをサポートしているかどうかを判断し、[Set up the authenticator app] (認証アプリケーションの設定) ページで以下のいずれかの操作を行います。

i. [Show QR code] (QR コードの表示) を選択し、アプリケーションを使用して QR コードをスキャンします。例えば、カメラアイコンまたは スキャンコード に似たオプションを選択します。次に、デバイスのカメラでコードをスキャンします。

ii. [show secret key] (シークレットキーを表示する) をクリックし、そのシークレットキーを MFA アプリケーションに入力します。

> **Important**
>
> MFA デバイスを IAM アイデンティティセンターに設定する際には、QR コードやシークレットキーのコピーを安全な場所に保存することをお勧めします。これは、携帯電話を紛失した場合や、MFA 認証システムアプリケーションを再インストールしなければならない場合に役立ちます。いずれの場合も、すぐにアプリケーションを再設定して同じ MFA 設定を使用することができます。

3. [Set up the authenticator app] (認証システムアプリケーションをセットアップする) ページで、[Authenticator code] (認証コード) で、物理的な MFA デバイスに現在表示されているワンタイムパスワードを入力します。

> **Important**
>
> コードを生成したら、即時にリクエストを送信します。コードを生成した後にリクエストを送信するまで時間がかかりすぎる場合、MFA デバイスは ユーザーとは正常に関連付けられますが、その MFA デバイスは同期しません。これは、タイムベースドワンタイムパスワード (TOTP) の有効期間が短いために起こります。その場合は、デバイスの再同期ができます。

4. [Assign MFA] (MFA の割り当て) を選択します。これで、MFA デバイスはワンタイムパスワードの生成を開始し、AWS で使用できるようになります。

- セキュリティキーと内蔵認証システム

1. [ユーザーのセキュリティキーの登録] ページでは、お使いのブラウザやプラットフォームの指示に従ってください。

> **Note**
>
> エクスペリエンスは、ブラウザまたはプラットフォームによって異なります。デバイスが正常に登録されると、登録したデバイスに識別しやすい表示名を付けるオプションが表示されます。変更する場合は、[名前の変更] を選択し、新しい名前を入力してから [保存] を選択します。

アクティブなセッションの表示と終了

AWS アクセスポータルを使用して、アクティブなセッションのリストを表示し、必要に応じて 1 つ以上のセッションを終了できます。

AWS アクセスポータルを使用してアクティブなセッションを終了する

1. AWS アクセスポータルにサインインします。詳細については、「AWS アクセスポータルにサインインします。」を参照してください。
2. ページの右上近くにある [セキュリティ] を選択します。
3. [セキュリティ] ページで、[アクティブセッション]の横にある括弧内の数字は、アクティブなセッションの数を示します。終了する各セッションの横にあるチェックボックスをオンにし、[セッションの終了] を選択します。

> **Tip**
>
> ユーザーバックグラウンドセッションでは、セッションを使用しているジョブの Amazon リソースネーム (ARN) でセッションを検索できます。セッションタイプリストで、[ユーザーバックグラウンドセッション]を選択し、検索ボックスにジョブ ARN を入力します。

ロードされたアクティブなセッションのみを終了できます。セッションが多い場合は、「アクティブなセッションをロードして追加のセッションを表示する」を選択します。

4. 終了する各セッションの横にあるチェックボックスをオンにし、[セッションの終了] を選択します。

5. アクティブなセッションを終了することを確認するダイアログボックスが表示されます。情報を確認し、続行する場合は、「confirm」と入力し、[セッションの終了] を選択します。
6. アクティブなセッションのリストに戻ります。選択したセッションが正常に終了したことを示す緑色の通知メッセージが表示されます。

複数の 間で IAM アイデンティティセンターを使用するAWS リージョン

このトピックでは、複数の AWS リージョンで AWS IAM アイデンティティセンター を使用する方法について説明します。インスタンスを追加のリージョンにレプリケートする方法、ワークフォースアクセスとセッションを管理する方法、アプリケーションをデプロイする方法、およびサービスの中断時にアカウントアクセスを維持する方法について説明します。

IAM Identity Center の組織インスタンスを有効にする場合は、単一の AWS リージョン (プライマリリージョン) を選択します。特定の前提条件を満たしている場合、このインスタンスをインスタンスの作成時または作成後に、追加の AWS リージョンにレプリケートできます。IAM Identity Center は、ワークフォース ID、アクセス許可セット、ユーザーとグループの割り当て、セッション、およびその他のメタデータをプライマリリージョンから選択した追加リージョンに自動的にレプリケートします。

マルチリージョンサポートの利点

IAM Identity Center を追加の AWS リージョンにレプリケートすると、以下の 2 つの主な利点があります。

- AWS アカウントアクセスの回復性の向上 – IAM Identity Center インスタンスのプライマリリージョンでサービスの中断が発生した場合でも、ワークフォースは AWS アカウントにアクセスできます。これは、中断前にプロビジョニングされたアクセス許可によるアクセスに適用されます。
- AWS マネージドアプリケーションのデプロイリージョン選択の柔軟性の向上 – AWS マネージドアプリケーションを任意のリージョンにデプロイして、アプリケーションデータレジデンシー要件を満たし、ユーザーとの近接性によってパフォーマンスを向上させることができます。追加のリージョンにデプロイされたアプリケーションは、レプリケートされたワークフォース ID にローカルにアクセスして、最適なパフォーマンスと信頼性を実現します。

前提条件と考慮事項

IAM Identity Center インスタンスをレプリケートする前に、以下の要件が満たされていることを確認してください。

- インスタンスタイプ - IAM Identity Center インスタンスは組織インスタンスである必要があります。マルチリージョンサポートは、アカウントインスタンスでは使用できません。

- ID ソース - IAM Identity Center インスタンスは、Okta などの外部 ID プロバイダー (IdP) に接続されているか、Identity Center ディレクトリを ID ソースとして使用する必要があります。マルチリージョンのサポートは、Active Directory を ID ソースとして使用するインスタンスでは使用できません。
- AWS リージョン - マルチリージョンのサポートは、AWS アカウントにおいてデフォルトで有効になっている商用リージョンで利用できます。オプトインリージョンは現在サポートされていません。
- 保管時の暗号化用の KMS キータイプ - IAM Identity Center インスタンスは、マルチリージョンのカスタマーマネージド KMS キーで設定する必要があります。KMS キーは、IAM Identity Center と同じ AWS アカウントに配置する必要があります。詳細については、「AWS IAM アイデンティティセンター でのカスタマーマネージド KMS キーの実装」を参照してください。
- AWS マネージドアプリケーションの互換性 - 「the section called “IAM アイデンティティセンターで使用できるアプリケーション”」のアプリケーションテーブルにアクセスして、以下の 2 つのアプリケーション要件を確認します。
  - 組織で使用されているすべての AWS マネージドアプリケーションは、カスタマーマネージド KMS キーで設定された IAM Identity Center をサポートしている必要があります。
  - 追加のリージョンにデプロイする AWS マネージドアプリケーションは、このタイプのデプロイをサポートしている必要があります。
- 外部 IdP の互換性 (外部 ID プロバイダーのみ) - 外部 ID プロバイダーを使用する場合、マルチリージョンのサポートを最大限に活用するには、IdP が複数のアサーションコンシューマーサービス (ACS) URL をサポートする必要があります。これは、Okta、Microsoft Entra ID、PingFederate、PingOne、JumpCloud などの IdP でサポートされている SAML 機能です。

  Google Workspace などの複数の ACS URL をサポートしていない IdP を使用する場合は、IdP ベンダーと連携してこの機能を有効にすることをお勧めします。この前提条件は、Identity Center ディレクトリを ID ソースとして使用する場合には適用されません。複数の ACS URL を使用しない場合に利用可能なオプションについては、「the section called “複数の ACS URL なしで AWS マネージドアプリケーションを使用する”」および「the section called “複数の ACS URL を使用しない AWS アカウントアクセス回復性”」を参照してください。

追加のリージョンの選択

デフォルトで有効になっている商用リージョンの中から追加のリージョンを選択する場合は、以下の要素を考慮してください。

- コンプライアンス要件 – コンプライアンス上の理由から、特定のリージョンに限定されたデータセットにアクセスする AWS マネージドアプリケーションを実行する必要がある場合は、データセットが存在するリージョンを選択します。
- パフォーマンスの最適化 – データレジデンシーが要因でない場合は、アプリケーションユーザーに最も近いリージョンを選択して、エクスペリエンスを最適化します。
- アプリケーションサポート – 選択したリージョンで必要な AWS アプリケーションが使用可能であることを確認します。
- AWS アカウントアクセスの回復性 – AWS アカウントへのアクセスを継続するには、IAM Identity Center インスタンスのプライマリリージョンから地理的に離れたリージョンを選択します。

> **Note**
>
> IAM Identity Center には、AWS リージョンの数に対するクォータがあります。詳細については、「the section called “追加のクォータ”」を参照してください。

IAM Identity Center を追加のリージョンにレプリケートする

マルチリージョンのカスタマーマネージド KMS キーを使用して IAM Identity Center を設定するなど、環境が前提条件を満たしている場合は、以下の手順を実行して IAM Identity Center インスタンスを追加のリージョンにレプリケートします。プライマリリージョンは、これらの手順の実行中および実行後も正常に動作し続けます。

> **Note**
>
> 新しい組織インスタンスを作成する場合は、インスタンスの作成時にマルチリージョンを有効にできます。詳細については、「IAM Identity Center を有効にする」を参照してください。

手順 1: 追加のリージョンにレプリカキーを作成する

IAM Identity Center をリージョンにレプリケートする前に、まずそのリージョンでカスタマーマネージド KMS キーのレプリカキーを作成し、IAM Identity Center のオペレーションに必要なアクセス許可をレプリカキーに設定する必要があります。マルチリージョンレプリカキーの作成手順については、「マルチリージョンレプリカキーの作成」を参照してください。

KMS キーアクセス許可の推奨アプローチは、プライマリキーからキーポリシーをコピーすることです。これにより、プライマリリージョンの IAM Identity Center に対して既に確立されているものと同じアクセス許可が付与されます。または、リージョン固有のキーポリシーを定義することもできますが、このアプローチではリージョン間のアクセス許可管理が複雑になり、将来的にポリシーを更新する際に追加の調整が必要になる場合があります。

> **Note**
>
> AWS KMS は、マルチリージョン KMS キーのリージョン間で KMS キーポリシーを同期しません。KMS キーポリシーを KMS キーのリージョン間で同期させるには、各リージョンに変更を個別に適用する必要があります。

手順 2: IAM Identity Center にリージョンを追加する

IAM Identity Center にリージョンを追加すると、そのリージョンへの IAM Identity Center データの自動レプリケーションがトリガーされます。レプリケーションは非同期で、結果整合性を持ちます。以下のタブでは、AWS マネジメントコンソールおよび AWS CLI でこれを行う手順について説明します。

Console

リージョンを追加するには

1. IAM Identity Center コンソールを開きます。
2. ナビゲーションペインで [設定] を選択します。
3. [管理] タブを選択します。
4. [IAM Identity Center のリージョン] セクションで、[リージョンを追加] を選択します。
5. [レプリケーション用に利用可能な AWS リージョン] セクションで、任意の AWS リージョンを選択します。リージョンがリストに表示されない場合、KMS キーがそのリージョンにレプリケートされていないため、レプリケーションには使用できません。詳細については、「the section called “カスタマーマネージド KMS キーの実装”」を参照してください。
6. [リージョンの追加] を選択します。
7. [IAM Identity Center のリージョン] セクションで、リージョンのステータスをモニタリングします。[更新] ボタン (円形の矢印) を使用して、必要に応じて最新のリージョンのステータスを確認します。レプリケーションが完了したら、手順 3 に進みます。

AWS CLI

リージョンを追加するには

```
aws sso-admin add-region \
    --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
    --region-name eu-west-1
```

現在のリージョンのステータスを確認するには

```
aws sso-admin describe-region \
    --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
    --region-name eu-west-1
```

リージョンのステータスが ACTIVE の場合、手順 3 に進むことができます。

追加のリージョンへの初回レプリケーションにかかる時間は、IAM Identity Center インスタンスのデータ量によって異なります。後続の増分変更は、ほとんどの場合、数秒以内にレプリケートされます。

手順 3 (外部 ID プロバイダーのみ): 外部 IdP 設定を更新する

この手順は、外部 ID プロバイダー (IdP) を使用する場合にのみ適用されます。Identity Center ディレクトリを ID ソースとして使用する場合は、手順 4 に進みます。

以下の手順については、「ID ソースのチュートリアル」の外部 IdP のチュートリアルに従ってください。

手順 3.a: アサーションコンシューマーサービス (ACS) URL を外部 IdP に追加する

この手順により、追加の各リージョンへの直接サインインが有効になります。また、それらのリージョンにデプロイされた AWS マネージドアプリケーションへのサインインを有効にし、それらのリージョンを経由して AWS アカウントにアクセスするために必要です。ACS URL の確認方法については、「プライマリおよび追加の AWS リージョンの ACS エンドポイント」を参照してください。

手順 3.b (オプション): AWS アクセスポータルを外部 IdP ポータルで使用できるようにする

追加のリージョンの AWS アクセスポータルを、外部 IdP ポータルのブックマークアプリとして利用できるようにします。ブックマークアプリには、目的の宛先へのリンク (URL) のみが含まれてお

り、ブラウザのブックマークに似ています。AWS アクセスポータル URL をコンソールで確認するには、[IAM Identity Center のリージョン] セクションの [すべての AWS アクセスポータル URL を表示] を選択します。詳細については、「the section called “プライマリおよび追加の AWS リージョンの AWS アクセスポータルエンドポイント”」を参照してください。

IAM Identity Center は、追加の各リージョンで IdP 開始 SAML SSO をサポートしていますが、外部 IdP は通常、単一の ACS URL でのみこれをサポートします。継続性を確保するために、IdP 開始 SAML SSO にはプライマリリージョンの ACS URL を引き続き使用し、追加のリージョンへのアクセスにはブックマークアプリとブラウザのブックマークを利用することをお勧めします。

手順 4: ファイアウォールとゲートウェイの許可リストを確認する

ファイアウォールまたはゲートウェイのドメイン許可リストを確認し、「ドキュメントに記載された許可リスト」に基づいて更新します。

ステップ 5: ユーザーに情報を提供する

追加のリージョンの AWS アクセスポータル URL や追加のリージョンの使用方法など、新しいセットアップに関する情報をユーザーに提供します。関連する詳細については、以下のセクションを参照してください。

- the section called “追加のリージョンを介したワークフォースアクセス”
- the section called “AWS アカウントアクセスのための追加リージョンへのフェイルオーバー”
- the section called “複数の AWS リージョンにまたがるアプリケーションのデプロイと管理”

最初のリージョンの追加後のリージョン変更

追加のリージョンを追加または削除できます。IAM Identity Center インスタンス全体を削除しない限り、プライマリリージョンを削除することはできません。リージョンの削除の詳細については、「the section called “IAM Identity Center からリージョンを削除する”」を参照してください。

追加リージョンをプライマリに昇格させたり、プライマリリージョンを追加リージョンに降格させたりすることはできません。

レプリケーション対象のデータ

IAM Identity Center は、以下のデータをレプリケートします。

データ	レプリケーションのソースとターゲット
ワークフォース ID (ユーザー、グループ、グループメンバーシップ)	プライマリリージョンから追加リージョンへ
アクセス許可セットとそのユーザーおよびグループへの割り当て	プライマリリージョンから追加リージョンへ
設定 (外部 IdP SAML 設定など)	プライマリリージョンから追加リージョンへ
アプリケーションメタデータおよびユーザーとグループへのアプリケーション割り当て	アプリケーションが接続されている IAM Identity Center リージョンから他の有効なリージョンへ
信頼できるトークン発行者	プライマリリージョンから追加リージョンへ
セッション	セッションの送信元リージョンから他の有効なリージョンへ

> **Note**
>
> IAM Identity Center は、AWS マネージドアプリケーションに保存されているデータをレプリケートしません。また、アプリケーションデプロイのリージョンフットプリントは変更されません。例えば、米国東部 (バージニア北部) に IAM Identity Center インスタンスがあり、Amazon Redshift が同じリージョンにデプロイされている場合、IAM Identity Center を米国西部 (オレゴン) にレプリケートしても、Amazon Redshift のデプロイリージョンとそれが保存するデータには影響しません。

考慮事項:

- 有効なリージョン全体のグローバルリソース識別子 - ユーザー、グループ、アクセス許可セット、およびその他のリソースは、有効なリージョン全体で同じ識別子を持ちます。

- レプリケーションはプロビジョニングされた IAM ロールには影響しません - アクセス許可セットの割り当てからプロビジョニングされた既存の IAM ロールは、有効なリージョンからのアカウントサインイン時に使用されます。

追加のリージョンを介したワークフォースアクセス

このセクションでは、複数のリージョンで IAM Identity Center を有効にしている場合に、ワークフォースが AWS アクセスポータル、AWS アカウント、およびアプリケーションにアクセスする方法について説明します。

追加のリージョンの AWS アクセスポータルには、ワークフォースがアクセスできる AWS アカウントとアプリケーションが、プライマリリージョンと同じ方法で表示されます。ワークフォースは、リージョンポータルエンドポイントへの直接リンク (`https://ssoins-111111h2222j33pp.eu-west-1.portal.amazonaws.com` など) を使用して、追加のリージョンの AWS アクセスポータルにサインインできます。外部 ID プロバイダーを使用する場合、ワークフォースは外部 IdP で設定したブックマークアプリを使用してサインインすることもできます。

追加のリージョンの AWS アクセスポータルエンドポイントを使用して、IAM Identity Center ユーザーとして API へのアクセスを AWS CLI に許可できます。この機能は、プライマリリージョンと同じ方法で動作します。ただし、CLI 認可は有効なリージョン間でレプリケートされません。したがって、各リージョンで CLI を個別に承認する必要があります。

複数の AWS リージョンにまたがるユーザーセッション

IAM Identity Center は、ユーザーセッションを元のリージョンから他の有効なリージョンにレプリケートします。1 つのリージョンでのセッションの失効とサインアウトも、他のリージョンにレプリケートされます。

IAM Identity Center 管理者によるセッションの取り消し

IAM Identity Center 管理者は、追加のリージョンでユーザーセッションを取り消すことができます。セッションはリージョン間でレプリケートされるため、通常の状況では、1 つのリージョンでセッションを取り消し、その変更が IAM Identity Center によって他の有効なリージョンにレプリケートされるようにするだけで十分です。IAM Identity Center のプライマリリージョンに障害が発生した場合、管理者は追加のリージョンでこのオペレーションを実行できます。

プライマリおよび追加の AWS リージョンの AWS アクセスポータルエンドポイント

有効なリージョンの AWS アクセスポータル URL を検索する必要がある場合は、以下の手順に従います。

1. IAM Identity Center コンソールを開きます。
2. ナビゲーションペインで [設定] を選択します。
3. [管理] タブを選択します。
4. [IAM Identity Center のリージョン] セクションで、[すべての AWS アクセスポータル URL を表示] を選択します。

以下の表は、IAM Identity Center インスタンスのプライマリリージョンと追加のリージョンにわたる AWS アクセスポータルエンドポイントを示しています。

AWS アクセスポータルエンドポイント	プライマリリージョン	追加のリージョン	URL パターンと例
Classic IPv4 専用[1]	はい	いいえ	パターン: `https://[Identity Store ID].awsapps.com/start` 例: `https://d-12345678.awsapps.com/start`
カスタムエイリアス IPv4 専用[1]	はい (オプション)	いいえ	パターン: `https://[custom alias].awsapps.com/start` 例: `https://mycompany.awsapps.com/start`
代替 IPv4 専用[2]	可能	はい	パターン: `https://[Identity Center instance ID].[Region].portal.amazonaws.com`

AWS アクセスポータルエンドポイント	プライマリリージョン	追加のリージョン	URL パターンと例
			例: `https://ssoins-111111h2222j33pp.eu-west-1.portal.amazonaws.com`
デュアルスタック[2]	可能	はい	パターン: `https://[Identity Center instance ID].portal.[Region].app.aws` 例: `https://ssoins-111111h2222j33pp.portal.eu-west-1.app.aws`

[1] 追加のリージョンでは、カスタム エイリアスはサポートされておらず、awsapps.com 親ドメインは使用できません。

[2] 代替 IPv4 専用およびデュアルスタックのポータルエンドポイントの URL には、末尾に /start がありません。

プライマリおよび追加の AWS リージョンのアサーションコンシューマーサービス (ACS) エンドポイント

> **Note**
>
> このセクションは、外部 ID プロバイダー (IdP) を使用するインスタンスにのみ適用されます。ID ソースとして Identity Center ディレクトリを使用する場合、ACS URL の設定は必要ありません。

ACS URL を検索したり、SAML メタデータの一部としてダウンロードしたりする必要がある場合は、以下の手順に従います。

1. IAM Identity Center コンソールを開きます。
2. ナビゲーションペインで [設定] を選択します。

3. [アイデンティティソース] タブを選択します。
4. [アクション] ドロップダウンメニューで、[認証の管理] を選択します。
5. [サービスプロバイダーのメタデータ] セクションには、有効な各リージョンの AWS アクセスポータルと ACS URL が表示されます。IPv4 専用 URL とデュアルスタック URL は、別々のタブに表示されます。IdP が SAML メタデータファイルのアップロードをサポートしている場合は、[メタデータファイルをダウンロード] を選択して、すべての ACS URL を含む SAML メタデータファイルをダウンロードできます。IdP がメタデータファイルのアップロードをサポートしていない場合、または ACS URL を個別に追加する場合は、コンソールのテーブルから個々の URL をコピーするか、[ACS の URL を表示] を選択してから [すべての URL をコピー] を選択します。プライマリリージョンに既に設定されている ACS URL を保持して、プライマリリージョンからサービスプロバイダーが開始した SAML シングルサインオンが機能し続けるようにします。

以下の表は、IAM Identity Center インスタンスのプライマリリージョンと追加リージョンにわたる SAML Assertion Consumer Service (ACS) エンドポイントを示しています。

ACS エンドポイント	プライマリリージョン	追加のリージョン	URL パターンと例
IPv4 のみ	可能	はい	パターン: `https://[Region].signin.aws/platform/saml/acs/ [Tenant ID]` 例: `https://us-west-2.signin.aws/platform/saml/acs/1111111111111111-aaee-ffff-dddd-11111111111`
代替 IPv4 専用*	はい	いいえ	パターン: `https://[Region].signin.aws.amazon.com/platform/saml/acs/ [Tenant ID]` 例: `https://us-west-2.signin.aws.amazon.com/platform/saml/acs/11111111111111`

ACS エンドポイント	プライマリリージョン	追加のリージョン	URL パターンと例
			11-aaee-ffff-dddd-111111111 11
デュアルスタック	可能	はい	パターン: https://*[Region]*.sso.signin.aws/platform/saml/acs/*[Tenant ID]* 例: https://us-west-2.sso.signin.aws/platform/saml/acs/1111111111111111-aaee-ffff-dddd-11111111111

* 2026 年 2 月より前に有効化されたインスタンスの場合、サービスプロバイダーが開始したプライマリリージョンへの SAML シングルサインオンに必要なため、このエンドポイントを保持してください。IAM Identity Center は、2026 年 2 月以降に有効化されたインスタンスにはこのエンドポイントを使用しません。

複数の ACS URL なしで AWS マネージドアプリケーションを使用する

> **Note**
>
> このセクションは、外部 ID プロバイダー (IdP) を使用するインスタンスにのみ適用されます。ID ソースとして Identity Center ディレクトリを使用する場合、この制限は適用されません。

一部の外部 ID プロバイダー (IdP) は、IAM Identity Center アプリケーションで複数のアサーションコンシューマーサービス (ACS) URL をサポートしていません。複数の ACS URL は、マルチリージョン IAM Identity Center の特定のリージョンへの直接サインインに必要な SAML 機能です。

例えば、アプリケーションリンクを介して AWS マネージドアプリケーションを起動すると、システムはアプリケーションの接続された IAM Identity Center リージョンを介してサインインをトリガーします。ただし、そのリージョンの ACS URL が外部 IdP で設定されていない場合、サインインは失敗します。

この問題を解決するには、IdP ベンダーと協力して、複数の ACS URL のサポートを有効にします。その間も、追加のリージョンで AWS マネージドアプリケーションを使用できます。まず、外部 IdP で ACS URL が設定されているリージョン (デフォルトではプライマリリージョン) にサインインします。IAM Identity Center でアクティブなセッションを作成したら、有効な任意のリージョンの AWS アクセスポータルから、またはアプリケーションリンクからアプリケーションを起動できます。

AWS アカウントアクセスのための追加リージョンへのフェイルオーバー

IAM Identity Center を介した AWS アカウントアクセスのトピックについては、「AWS アカウントアクセス」で詳しく説明します。このセクションでは、プライマリリージョンでサービスが中断した場合に、複数の AWS リージョンにわたる AWS アカウントアクセスを維持するための追加の詳細について説明します。

IAM Identity Center インスタンスがプライマリリージョンで中断した場合 (プライマリリージョンの AWS アクセスポータルが使用できないなど)、ワークフォースは追加のリージョンに切り替えて、AWS アカウントや影響を受けないアプリケーションへのアクセスを継続できます。詳細については、「the section called “追加のリージョンを介したワークフォースアクセス”」を参照してください。

「the section called “IAM Identity Center を追加のリージョンにレプリケートする”」のセットアップが完了したらすぐに、追加のリージョンの AWS アクセスポータルエンドポイントをワークフォースに伝えることをお勧めします。外部 ID プロバイダーを使用する場合は、IdP の設定 (追加のリージョンのブックマークアプリなど) も伝えてください。これにより、必要に応じて追加のリージョンへのフェイルオーバーに備えることができます。

同様に、AWS CLI ユーザーはプライマリリージョンのプロファイルごとに、追加のリージョン用の AWS CLI プロファイルを作成することをお勧めします。その後、プライマリリージョンでサービス中断が発生した場合に、そのプロファイルに切り替えることができます。

> **Note**
>
> AWS アカウントへのアクセスの継続性は、サービス中断前にプロビジョニングおよびレプリケートされる、アクセス許可セットの割り当てやグループメンバーシップなどのアクセス許可によって異なります。外部 ID プロバイダーを使用する場合、継続性は外部 IdP の状態にも依存します。また、ID ソースのサービスが中断した場合に少人数の特権ユーザーグルー

プへの AWS アクセスを維持するために、AWS ブレークグラスアクセスを設定することをお勧めします。緊急アクセスは、外部 IdP を必要とする同様のオプションです。

複数の ACS URL を使用しない AWS アカウントアクセス回復性

> **Note**
>
> このセクションは、外部 ID プロバイダー (IdP) を使用するインスタンスにのみ適用されます。ID ソースとして Identity Center ディレクトリを使用する場合、この制限は適用されません。

一部の外部 ID プロバイダー (IdP) は、IAM Identity Center アプリケーションで複数のアサーションコンシューマーサービス (ACS) URL をサポートしていません。複数の ACS URL は、マルチリージョン IAM Identity Center の特定のリージョンへの直接サインインに必要な SAML 機能です。

ユーザーが複数の IAM Identity Center リージョンを介して AWS アカウントにアクセスできるようにするには、外部 IdP でそれぞれのリージョン ACS URL を設定する必要があります。ただし、外部 IdP が IAM Identity Center アプリケーションで 1 つの ACS URL のみをサポートしている場合、ユーザーは 1 つの IAM Identity Center リージョンに直接サインインできます。

この問題を解決するには、IdP ベンダーと協力して、複数の ACS URL のサポートを有効にします。その間、AWS アカウントにアクセスするためのバックアップとして追加のリージョンを使用できます。

プライマリリージョンで IAM Identity Center サービスの中断が発生した場合は、外部 IdP の ACS URL を追加のリージョンの ACS URL で更新する必要があります。この更新後、ユーザーは外部 IdP ポータルの既存の IAM Identity Center アプリケーションを使用するか、共有している直接リンクを使用して、追加のリージョンの AWS アクセスポータルにアクセスできます。

必要なときに機能するように、この設定を定期的にテストし、このフェイルオーバープロセスを組織に伝えることをお勧めします。

> **Note**
>
> この設定で AWS アカウントへのアクセスに追加のリージョンを使用する場合、ユーザーはプライマリリージョンに接続されている AWS マネージドアプリケーションにアクセスでき

ない場合があります。したがって、これは AWS アカウントへのアクセスを維持するための一時的な対策としてのみお勧めします。

複数の AWS リージョンにまたがるアプリケーションのデプロイと管理

IAM Identity Center を介したアプリケーションアクセスのトピックについては、「アプリケーションアクセス」で詳しく説明します。このセクションでは、複数の AWS リージョンにまたがるアプリケーションのデプロイと管理に関連する追加の詳細を提供します。

複数の AWS リージョンにまたがる AWS マネージドアプリケーションのデプロイと管理

単一リージョンの IAM Identity Center インスタンスを使用すると、AWS マネージドアプリケーションをインスタンスと同じリージョンにデプロイできます。Amazon Q Business などの一部のアプリケーションは、IAM Identity Center へのクロスリージョン接続をサポートしています。これにより、対象のアプリケーションが利用可能な場合は、IAM Identity Center のリージョン外にデプロイできます。ただし、クロスリージョン呼び出しはアプリケーションのパフォーマンスを低下させる可能性があり、ほとんどの AWS マネージドアプリケーションはこのタイプの接続をサポートしていません。

マルチリージョン IAM Identity Center インスタンスを使用すると、同じリージョンの IAM Identity Center への接続 (「リージョンローカル接続」) を使用して、有効な任意のリージョンに AWS マネージドアプリケーションをデプロイできます。プライマリリージョンへのデプロイは、すべての統合 AWS マネージドアプリケーションでサポートされています。IAM Identity Center の追加リージョンでのデプロイをサポートする AWS マネージドアプリケーションを確認するには、「the section called “IAM アイデンティティセンターで使用できるアプリケーション”」のアプリケーションテーブルを参照してください。いずれの場合も、AWS マネージドアプリケーションはデプロイするリージョンで利用できる必要があります。

IAM Identity Center へのリージョンローカル接続により、AWS マネージドアプリケーションは同じリージョンのワークフォース ID にアクセスして、最適なパフォーマンスと信頼性を実現します。前提条件が満たされている場合は、AWS マネージドアプリケーションをデプロイする際に、リージョンローカル接続を選択することをお勧めします。

AWS マネージドアプリケーションを IAM Identity Center の追加リージョンにデプロイするには、プライマリリージョンにデプロイするのと同じ方法で、アプリケーションコンソールまたは API を使用してそのリージョンでデプロイを開始します。

考慮事項:

- IAM Identity Center をそのリージョンにまだレプリケートしていない場合は、アプリケーションのデプロイをすぐに完了できるように、最初にレプリケートすることをお勧めします。
- AWS マネージドアプリケーションは、IAM Identity Center をリージョンにレプリケート済みである場合、多くの場合、リージョンローカル接続を自動的に確立します。
- 前提条件が満たされている限り、AWS マネージドアプリケーションが IAM Identity Center へのクロスリージョン接続を提供する場合は、リージョンローカル接続を選択することをお勧めします。
- アプリケーションが追加のリージョンでのデプロイをサポートしていない場合は、アプリケーションがプライマリリージョンで使用可能であれば、プライマリリージョンにデプロイできます。

> **Important**
>
> IAM Identity Center インスタンスがマルチリージョンの場合、組織で使用されているすべての AWS マネージドアプリケーションは、アプリケーションのデプロイリージョンに関係なく、カスタマーマネージド KMS キーで設定された IAM Identity Center をサポートする必要があります。アプリケーションをデプロイする前、および IAM Identity Center でカスタマーマネージド KMS キーを設定する前に、「the section called “IAM アイデンティティセンターで使用できるアプリケーション”」でこれを確認してください。

アプリケーションの管理リージョン

リージョンローカル接続を使用して IAM Identity Center の追加リージョンに AWS マネージドアプリケーションをデプロイした後、同じリージョンでアプリケーションとそのユーザーおよびグループへの割り当てを管理します。IAM Identity Center は、ユーザーやグループへの割り当てを含むアプリケーションメタデータを他の有効なリージョンにレプリケートし、ワークフォースが有効な任意のリージョンからアプリケーションを起動できるようにします。

AWS マネージドアプリケーションが IAM Identity Center へのクロスリージョン接続を使用している場合、接続されたリージョンの IAM Identity Center コンソールと API を使用して、名前や説明などのアプリケーションの詳細、およびユーザーとグループへのアプリケーション割り当てを管理できます。接続タイプに関係なく、デプロイリージョンのコンソールを使用してアプリケーションを管理できます。

信頼できる ID の伝播

IAM Identity Center インスタンスの有効な任意のリージョンで、信頼できる ID 伝達をサポートする AWS マネージドアプリケーションで信頼できる ID 伝達を使用できます。

ID コンテキストを相互に伝達するすべてのアプリケーションは、同じリージョンに存在する必要があります。

接続された IAM Identity Center リージョンへのアプリケーションの依存関係

各 AWS マネージドアプリケーションは、デプロイ時に特定の IAM Identity Center リージョンに接続します。その後、IAM Identity Center が複数のリージョンで有効になっている場合でも、アプリケーションはユーザーのサインインのためにそのリージョンに依存します。そのリージョンで IAM Identity Center に中断が発生している場合、ユーザーはそのリージョンに接続されている AWS マネージドアプリケーションにアクセスできない可能性があります。

複数の AWS リージョンにまたがるカスタマーマネージドアプリケーションのデプロイと管理

IAM Identity Center は、SAML および OAuth2 カスタマーマネージドアプリケーションをサポートしています。IAM Identity Center インスタンスの有効な任意のリージョンで作成できます。作成後は、同じリージョンでアプリケーションとユーザーおよびグループへの割り当てを管理します。

IAM Identity Center からリージョンを削除する

IAM Identity Center インスタンスから追加のリージョンを削除するには、以下の手順に従います。

手順 1: 外部 IdP 設定を更新する (該当する場合)

外部 ID プロバイダーを使用する場合は、このリージョンの ACS URL を外部 IdP から削除するか、後でこのリージョンを再度追加する場合に備えて保持するかを選択できます。このリージョンの AWS アクセスポータル用に作成したブックマークアプリを削除または非表示にすることをお勧めします。Identity Center ディレクトリを ID ソースとして使用する場合は、手順 2 に進みます。

手順 2: リージョンを削除する

Console

リージョンを削除するには

1. IAM Identity Center コンソールを開きます。
2. ナビゲーションペインで [設定] を選択します。
3. [管理] タブを選択します。
4. [IAM Identity Center のリージョン] セクションで、削除する追加のリージョンを選択します。
5. [を削除] を選択します。
6. [リージョンを削除] を選択して削除を確認する前に、この IAM Identity Center リージョンで作成されたアプリケーションへのアクセスが失われる可能性があるという警告に注意してください。このようなアプリケーションがあるかどうかわからない場合は、ナビゲーションペインで [アプリケーション] を選択し、各 AWS マネージドアプリケーションとカスタマーマネージドアプリケーションの [作成元] 列で接続されたリージョンを確認します。

   > **Note**
   >
   > これらのアプリケーションへのアクセスを失っても、削除されたリージョンにまだ接続されている AWS マネージドアプリケーションのデプロイに対して引き続き料金が発生する場合があります。これを防ぐには、IAM Identity Center でリージョンを削除する前に、アプリケーションコンソールまたは API を使用してこれらの AWS マネージドアプリケーションのデプロイを削除する必要があります。IAM Identity Center リージョンを既に削除している場合、リージョンを再度追加することで、アプリケーションへのアクセスを復元できます。

7. [IAM Identity Center のリージョン] セクションで、リージョンのステータスをモニタリングします。[更新] ボタン (円形の矢印) を使用して、必要に応じて最新のリージョンステータスを確認します。リージョンが削除されると、そのリージョンはリージョンリストに表示されなくなります。

AWS CLI

リージョンを削除するには

```
aws sso-admin remove-region \
    --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
    --region-name eu-west-1
```

現在のリージョンのステータスを確認するには

```
aws sso-admin describe-region \
    --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
    --region-name eu-west-1
```

リージョンが削除されたら、手順 3 に進みます。

手順 3: レプリカキーを削除する

KMS ストレージ料金が発生しないように、このリージョンからレプリカキーを削除することもできます。詳細については、「AWS KMS キーの削除」を参照してください。

> **Important**
>
> この特定のリージョンのレプリカキーのみを削除してください。他の IAM Identity Center リージョンは、通常のオペレーションで引き続き他の有効なリージョンの KMS キーに依存します。

追加の AWS リージョンでサポートされている IAM Identity Center サービス API

API	追加のリージョンの機能
Identity Center API	サポート対象: • アプリケーション管理の読み取り/書き込みオペレーション • インスタンスの読み取りオペレーション サポート外: • アプリケーション関連以外の書き込みオペレーション • アクセス許可セットとアカウント割り当ての読み取りオペレーション
ID ストア Auth	読み込み操作

API	追加のリージョンの機能
OIDC API	すべてのオペレーションがサポートされています
アクセスポータル API	すべてのオペレーションがサポートされています
SCIM API	オペレーションはサポートされていません

プライマリリージョンと追加のリージョンにおける IAM Identity Center の AWS CloudTrail イベント

AWS CloudTrail では、IAM Identity Center ユーザーと管理者が IAM Identity Center インスタンスの有効になっているすべての AWS リージョンに対して実行するアクションを監査できます。AWS CloudTrail イベントが出力され、アクションが実行されるリージョンに記録されます。詳細については、「the section called “ログ記録とモニタリング”」を参照してください。

プライマリリージョンと追加のリージョンでの IAM Identity Center ユースケースの可用性

機能	リージョン別の可用性
ユーザーポータルを使用するワークフォースディレクトリ	
ポータルサインインおよびグローバルセッションを含む AWS アクセスポータルへのユーザーアクセス (すべてのリージョンに 1 つのサインイン)	有効なすべてのリージョン
割り当てられたすべてのアカウントの表示	有効なすべてのリージョン
割り当てられたすべてのアプリケーションの表示 (アプリケーションが作成された場所に関係なく)	有効なすべてのリージョン
AWS コンソールまたは Identity Store API を介したユーザー、グループ、メンバーシップへの読み取りアクセス	有効なすべてのリージョン

機能	リージョン別の可用性
ユーザーセッションの取り消し	有効なすべてのリージョン
外部 ID ソース (SCIM API または Identity Store API を介した外部 IdP など) からのユーザーとグループの自動同期。この行は、外部 ID プロバイダーにのみ適用されます。	プライマリリージョンのみ
SCIM を使用した自動 ID プロビジョニングの設定	プライマリリージョンのみ
外部 IdP を使用した SAML SSO の設定	プライマリリージョンのみ - 有効なすべてのリージョンでコンソールからの読み取りアクセス
コンソールまたは Identity Store API を使用して、ユーザー、グループ、グループメンバーシップに対する作成/更新/削除オペレーションを実行します。	プライマリリージョンのみ。Identity Center ディレクトリを使用する場合、これらのオペレーションはプライマリリージョンの IAM Identity Center コンソールと Identity Store API を通じて使用できます。SCIM プロビジョニングで外部 IdP を使用する場合、書き込みオペレーションはコンソールでブロックされます (ユーザーアクセスの無効化/有効化とユーザーの削除を除く)。その他のリージョン: 読み取り専用アクセス。
AWS アクセスポータルを介したユーザーデータプレーンオペレーション (パスワードリセット、MFA デバイス管理) (Identity Center ディレクトリのみ)	有効なすべてのリージョン (Identity Center ディレクトリを ID ソースとして使用する場合にのみ適用)
マルチアカウントアクセス	
AWS アクセスポータル、AWS CLI、およびショートカットリンクから割り当てられたアカウントにアクセスする	有効なすべてのリージョン

機能	リージョン別の可用性
コンソールと API でマルチアカウントアクセス許可セットとその割り当てを管理する (一時的な昇格アクセスを含む)	プライマリリージョンのみ
アプリケーションと AWS サービスへのアクセス	
アプリケーションコンソールと API を使用して AWS マネージドアプリケーションをデプロイする	有効なすべてのリージョン – アプリケーションのリージョン可用性と追加リージョンでのデプロイのサポートの対象となります。
Identity Center コンソールと API を使用してカスタマーマネージドアプリケーションを作成する	有効なすべてのリージョン
コンソールと API でアプリケーションのメタデータと割り当てを管理する	アプリケーションの接続先 IAM Identity Center リージョン
AWS アクセスポータルから、またはアプリケーションリンクやブックマークを使用して直接アプリケーションを起動する	有効なすべてのリージョン
Amazon EC2 インスタンスへの SSO	有効なすべてのリージョン
信頼できる ID の伝播	
信頼できるトークン発行者を作成します。	プライマリリージョンのみ
AWS マネージドアプリケーションでの信頼できる ID の伝播	有効なすべてのリージョン – ID コンテキストを相互に伝達するアプリケーションは、同じリージョンに存在する必要があります
その他の管理機能	

機能	リージョン別の可用性
リージョン管理、KMS キー管理、インスタンス管理、セッション管理 (セッション失効を除く) などのその他すべての管理機能	プライマリリージョンのみ - 一部のデータについては有効なすべてのリージョンで読み取りアクセスが利用可能 (アクセス許可セットの割り当てを除く)

復元力設計とリージョンごとの動作

IAM Identity Center サービスはフルマネージド型で、Amazon S3 や Amazon EC2 などの可用性と耐久性に優れた AWS サービスを使用します。アベイラビリティーゾーンに障害が発生した場合でも可用性を確保するため、IAM Identity Center は複数のアベイラビリティーゾーンにわたって運用されています。リージョンの中断が発生した場合には、IAM Identity Center インスタンスを追加リージョンにレプリケートして、アクセス許可が既にプロビジョニングされているアカウントアクセスを維持できます。詳細については、「複数の 間で IAM アイデンティティセンターを使用するAWS リージョン」を参照してください。

AWS Organizations 管理アカウントで IAM Identity Center を有効にします。これは、IAM Identity Center がすべての AWS アカウント のロールをプロビジョニング、プロビジョニング解除、更新できるようにするために必要です。IAM Identity Center を有効にすると、現在選択されている AWS リージョン にデプロイされます。これは「プライマリリージョン」と呼ばれます。特定の AWS リージョン にデプロイする場合は、IAM Identity Center を有効にする前にリージョンの選択を変更してください。IAM Identity Center を有効にした後ではプライマリリージョンを変更できないためです。

IAM Identity Center は、ほとんどの管理機能をプライマリリージョンからのみサポートします。こうした機能には、外部 ID プロバイダーへの接続、ユーザーとグループの同期、ユーザーとグループに対するアクセス許可セットの作成と割り当てなどがあります。一方、アプリケーションとその割り当ての管理は、アプリケーションが作成された IAM Identity Center リージョンで行う必要があります。

> **Note**
>
> IAM Identity Center が追加リージョンにレプリケートされている場合でも、AWS ブレークグラスアクセスをセットアップすることをお勧めします。これにより、外部 IdP でのサービス中断といったイベントの発生時に、少数の特権ユーザーの AWS アクセスを維持できます。緊急アクセスは、IAM ユーザーではなく外部 IdP の ID を使用するもう 1 つの選択肢ですが、外部 IdP の中断からは保護されません。

IAM Identity Center はサービスを有効にしたリージョンからのアクセスを決定しますが、AWS アカウント はグローバルです。つまり、ユーザーが IAM Identity Center にサインインした後は、IAM Identity Center を介してアクセスすればAWS アカウント、どのリージョンでも操作できるようになります。ただし、Amazon SageMaker AI などのほとんどの AWS マネージドアプリケーション

は、ユーザーが認証してこれらのアプリケーションへのアクセスを割り当てるために、IAM Identity Center インスタンスのリージョンにインストールする必要があります。IAM Identity Center でアプリケーションを使用する場合のリージョンの制約については、アプリケーションのドキュメントおよび「the section called “複数の AWS リージョンにまたがる AWS マネージドアプリケーションのデプロイと管理”」を参照してください。

IAM Identity Center を使用して、アプリケーションが構築されているプラットフォームやクラウドに関係なく、パブリック URL を介してアクセス可能な SAML ベースのカスタマーマネージドアプリケーションへのアクセスを認証および認可することもできます。

AWS アカウントアクセスをサポートせず、組織インスタンスに接続されていない 2 番目の分離されたコントロールポイントが作成されるため、復元性を実装する手段として IAM アイデンティティセンターのアカウントインスタンス を使用することはお勧めしません。

可用性を考慮した設計

次の表は、シングル AWS リージョンで IAM Identity Center が達成するように設計された可用性を示しています。これらの値は、サービスレベルアグリーメントや保証を表すものではなく、むしろソリューションの設計目標を示すものと考えてください。可用性のパーセンテージは、データまたは機能へのアクセス性の目安であり、耐久性 (データの長期保持など) を示す数値ではありません。

サービスコンポーネント	可用性の設計目標
データプレーン (サインインを含む)	99.95%
コントロールプレーン	99.90%

AWS マネジメントコンソール への緊急アクセスを設定する

IAM Identity Center は可用性の高い AWS インフラストラクチャを基盤として構築されており、Availability Zone アーキテクチャを使用して単一障害点を排除しています。IAM アイデンティティセンターまたは AWS リージョンに障害が発生する万一の場合に備えて、保護の強化として AWS マネジメントコンソールに一時的にアクセスできる設定を用意しておくことをお勧めします。

AWS により以下ができます。

- サードパーティ IdP を IAM Identity Center に接続します。

- SAML 2.0 ベースのフェデレーション を使用して、サードパーティーの IdP を個人 AWS アカウント に接続します。

IAM Identity Center を使用している場合は、これらの機能を使用して、以下のセクションで説明する緊急アクセス設定を作成できます。この設定により、IAM Identity Center を AWS アカウント アクセスのメカニズムとして使用できるようになります。IAM Identity Center が停止した場合、緊急時の操作を行うユーザーは、アカウントへのアクセスに使用するのと同じ認証情報を使用して、ダイレクトフェデレーションを通じて AWS マネジメントコンソール にサインインできます。この設定は、IAM Identity Center は使用できないが、IAM データプレーンと外部 ID プロバイダー (IdP) は使用できる場合に機能します。外部 IdP に依存しないようにする場合は、AWS ブレークグラスアクセスのセットアップを検討してください。

> **Important**
>
> 必要な IAM ロールを作成するためのアクセスも中断されると設定を作成できないため、中断が発生する前にこの設定をデプロイすることをお勧めします。また、この設定を定期的にテストして、IAM Identity Center が中断された場合の対処方法をチームが理解できるようにしてください。

トピック

- 緊急アクセス設定の概要
- 重要な運用上の役割を設計する方法
- アクセスモデルを計画する方法
- 緊急時のロール、アカウント、グループのマッピングを設計する方法
- 緊急アクセス設定の作成方法
- 緊急事態に備えたタスク
- 緊急フェイルオーバープロセス
- 通常の運用に戻る
- Okta でダイレクト IAM フェデレーションアプリケーションの 1 回限りの設定を行う
- ADFS でダイレクト IAM フェデレーションアプリケーションの 1 回限りの設定を行う

緊急アクセス設定の概要

緊急アクセスを設定するには、次のタスクを完了する必要があります。

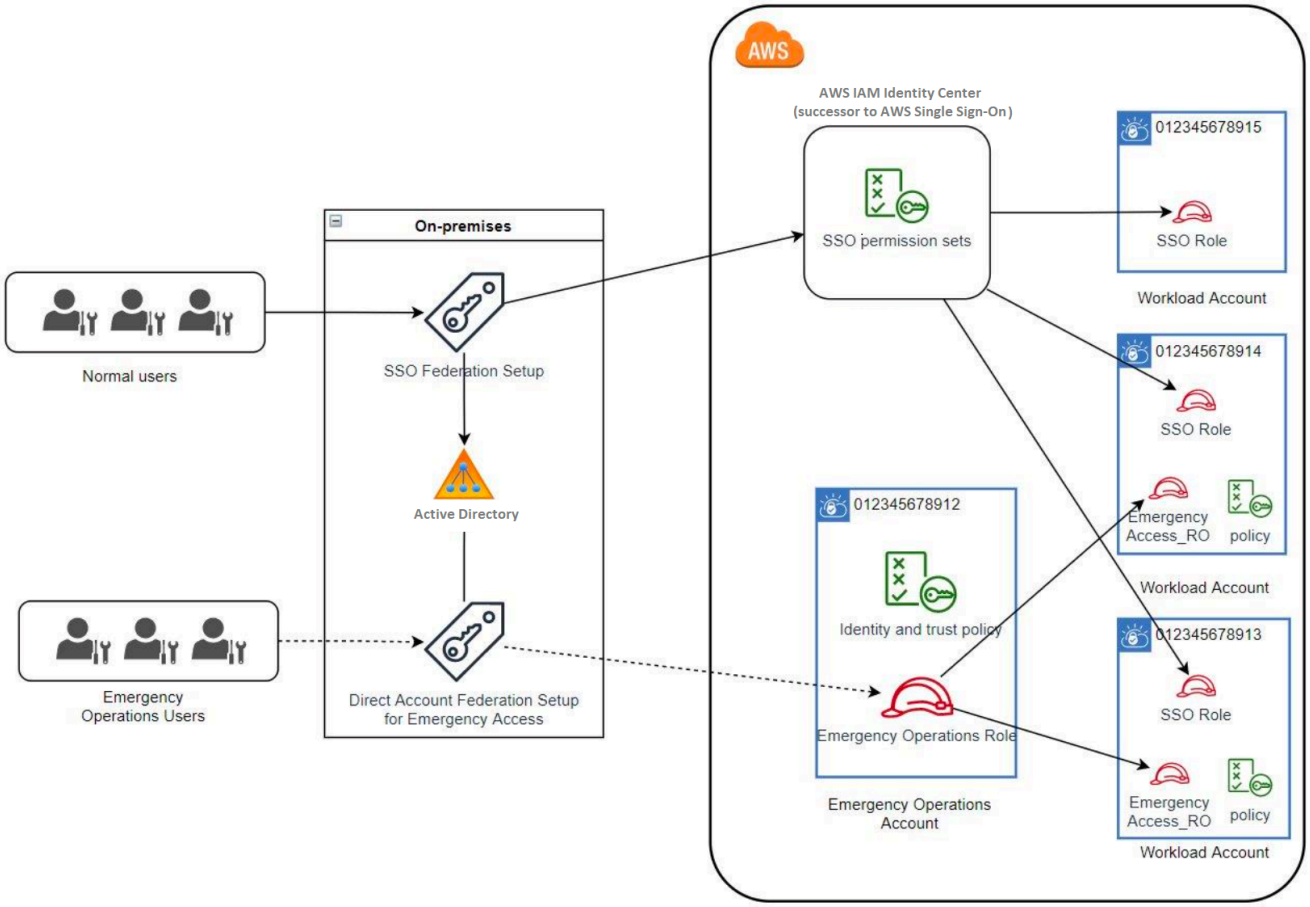
1. で、組織の緊急対応アカウントを作成してください。AWS Organizationsこのアカウントは緊急作業用のアカウントになります。
2. SAML 2.0 ベースのフェデレーションを使用して IdP を緊急対応アカウントに接続します。
3. 緊急対応アカウントで、サードパーティーの ID プロバイダーフェデレーション用のロールを作成します。また、各ワークロードアカウントに、必要な権限を持つ緊急対応ロールを作成します。
4. 緊急対応アカウントで作成した IAM ロールに、ワークロードアカウントへのアクセスを委任します。緊急対応アカウントへのアクセスを許可するには、メンバーなしで IdP に緊急対応グループを作成します。
5. IdP に SAML 2.0 フェデレーションのAWS マネジメントコンソールへのアクセスを有効にするルールを作成して、IdP 内の緊急対応グループが、緊急対応ロールを使用できるようにします。

IdP の緊急対応グループにはメンバーがいないため、通常の運用中は誰も緊急対応アカウントにアクセスできません。IAM Identity Center に障害が発生した場合は、IdP を使用して信頼できるユーザーを IdP の緊急対応グループに追加します。その後、これらのユーザーは IdP にサインインして AWS マネジメントコンソール に移動し、緊急対応アカウントの緊急対応ロールを引き受けることができます。そこから、これらのユーザーは、運用作業を行う必要があるワークロードアカウントの緊急アクセスロールにロールを切り替える ことができます。

重要な運用上の役割を設計する方法

この設計では、IAM を介して連携する単一 AWS アカウント の役割を設定して、ユーザーが重要な運用ロールを引き受けられるようにします。重要な運用ロールには、ユーザーがワークロードアカウントで対応するロールを引き受けることを許可する信頼ポリシーがあります。ワークロードアカウントのロールは、ユーザーが重要な作業を行うために必要な権限を提供します。

次の図は、設計の概要を示しています。



アクセスモデルを計画する方法

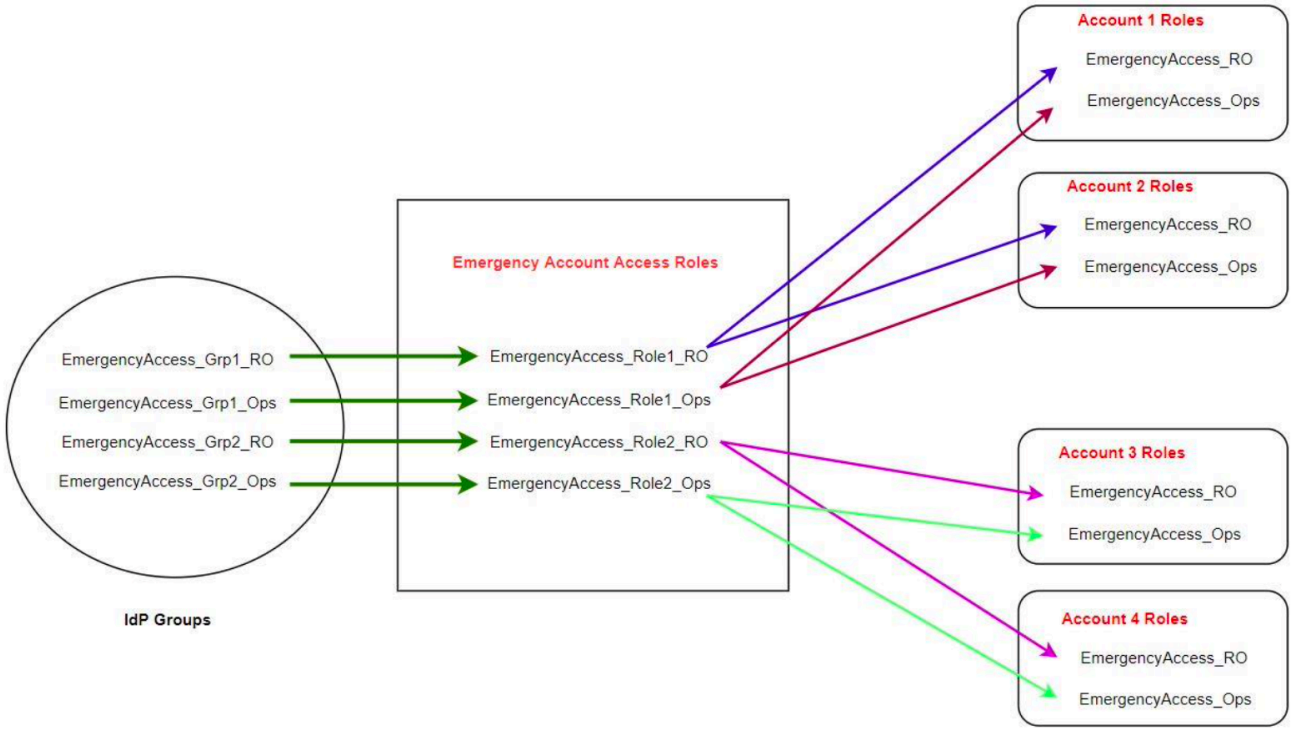
緊急アクセスを設定する前に、アクセスモデルがどのように機能するかについての計画を立ててください。このプランを作成するには、次の手順に従います。

1. IAM Identity Center の障害発生時にオペレーターによる緊急アクセスが不可欠な場所 AWS アカウント を特定します。例えば、本番アカウントはおそらく必要ですが、開発用アカウントとテスト用アカウントはそうではない場合があります。
2. このようなアカウントのコレクションに関して、アカウントに必要な具体的な重要な役割を特定してください。これらのアカウント全体で、それぞれのロールで何ができるかを一貫して定義してください。これにより、クロスアカウントロールを作成する緊急アクセスアカウントでの作業が簡素化されます。これらのアカウントでは、読み取り専用 (RO) と運用 (Ops) という 2 つの異なるロールから始めることをお勧めします。必要に応じて、さらに役割を作成し、これらの役割をセットアップ内のより明確な緊急アクセスユーザーのグループにマッピングできます。

3. IdP で緊急アクセスグループを特定して作成します。グループメンバーは、緊急アクセスロールへのアクセスを委任しているユーザーです。
4. これらのグループが緊急アクセスアカウントで引き受けることができるロールを定義します。そのためには、グループがアクセスできるロールを一覧表示するクレームを生成するルールを IdP で定義します。その後、これらのグループが緊急アクセスアカウントの「読み取り専用」または「オペレーション」のロールを引き受けることができます。これらのロールから、ワークロードアカウントの対応するロールを引き受けることができます。

緊急時のロール、アカウント、グループのマッピングを設計する方法

次の図は、緊急アクセス グループを緊急アクセスアカウントのロールにマップする方法を示しています。この図には、緊急アクセスアカウントロールがワークロードアカウント内の対応するロールにアクセスできるようにする、アカウント間ロールの信頼関係も示されています。緊急時対応計画の設計では、これらのマッピングを出発点として使用することをお勧めします。



緊急アクセス設定の作成方法

次のマッピング テーブルを使用して、緊急アクセス設定を作成します。この表は、ワークロードアカウントにおける読み取り専用 (RO) と運用 (Ops) の 2 つのロールと、対応する信頼ポリシーと権限

ポリシーを含む計画を反映しています。信頼ポリシーにより、緊急アクセスアカウントロールが個々のワークロードのアカウントロールにアクセスできるようになります。個々のワークロードアカウントロールには、そのロールが、アカウント内で実行できる操作に関するアクセス権限ポリシーもあります。アクセス権限ポリシーは、AWSマネージドポリシー でも カスタマー管理ポリシー でもかまいません。

アカウント	作成するロール	信頼ポリシー	アクセス権限ポリシー
アカウント 1	Emergency Access_RO	Emergency Access_Role1_RO	arn:aws:iam::aws:policy/ReadOnlyAccess
アカウント 1	Emergency Access_Ops	Emergency Access_Role1_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator
アカウント 2	Emergency Access_RO	Emergency Access_Role2_RO	arn:aws:iam::aws:policy/ReadOnlyAccess
アカウント 2	Emergency Access_Ops	Emergency Access_Role2_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator
緊急アクセスアカウント	Emergency Access_Role1_RO Emergency Access_Role1_Ops Emergency Access_Role2_RO Emergency Access_Role2_Ops	IdP	アカウント内のロールリソースの AssumeRole

このマッピングプランでは、緊急アクセスアカウントには 2 つの読み取り専用ロールと 2 つの操作ロールが含まれています。これらのロールは IdP を信頼して、アサーションでロールの名前を渡すことにより、選択したグループがロールにアクセスすることを認証および認可します。ワークロー

ドのアカウント 1 とアカウント 2 には、対応する読み取り専用ロールと運用ロールがあります。ワークロードアカウント 1 の場合、EmergencyAccess_RO ロールは緊急アクセスアカウントにある EmergencyAccess_Role1_RO ロールを信頼します。この表では、ワークロードアカウントの読み取り専用ロール、運用ロール、および対応する緊急アクセスロール間の類似の信頼パターンを示しています。

緊急事態に備えたタスク

緊急アクセス設定を準備するために、緊急事態が発生する前に次のタスクを実行するようお勧めします。

1. IdP でダイレクト IAM フェデレーションアプリケーションを設定します。ID ソースとして Okta または他の外部 IdP を使用している場合は、「Okta でダイレクト IAM フェデレーションアプリケーションの 1 回限りの設定を行う」を参照してください。Active Directory を ID ソースとして使用している場合は、「ADFS でダイレクト IAM フェデレーションアプリケーションの 1 回限りの設定を行う」を参照してください。
2. イベント中にアクセス可能な緊急アクセスアカウントに IdP 接続を作成します。
3. 上記のマッピング表で説明されているように、緊急アクセスアカウントに緊急アクセスロールを作成します。
4. 各ワークロードアカウントに、信頼ポリシーと権限ポリシーを含む一時的な運用ロールを作成します。
5. IdP に一時的な運用グループを作成します。グループ名は、一時的な運用ロールの名前によって異なります。
6. 直接 IAM フェデレーションをテストします。
7. IdP の IdP フェデレーションアプリケーションを無効にして、通常の使用を防止します。

緊急フェイルオーバープロセス

IAM Identity Center インスタンスが使用できず、AWS 管理コンソールへの緊急アクセスを提供する必要があると判断した場合は、以下のフェイルオーバープロセスをお勧めします。

1. IdP 管理者は IdP でダイレクト IAM フェデレーションアプリケーションを有効にします。
2. ユーザーは、E メールリクエスト、Slack チャネル、その他の通信手段など、既存のメカニズムを通じて一時的運用グループへのアクセスをリクエストします。
3. 緊急アクセスグループに追加したユーザーは IdP にサインインし、緊急アクセスアカウントを選択すると、ユーザーは緊急アクセスアカウントで使用するロールを選択します。これらのロール

から、緊急アカウントロールと相互に信頼されている、対応するワークロードアカウントのロールを引き受けることができます。

通常の運用に戻る

AWS Health Dashboard をチェックして、IAM Identity Center サービスの状態がいつ回復したかを確認します。通常の運用に戻すには、次のステップを実行します。

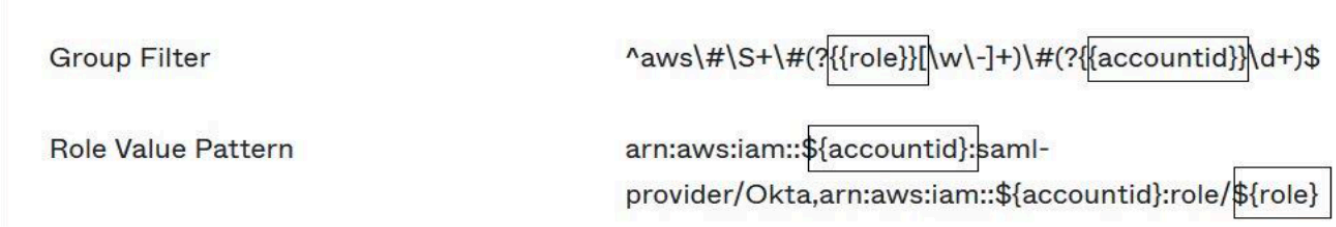
1. IAM Identity Center サービスのステータスアイコンにサービスが正常であることが示されたら、IAM Identity Center にサインインします。
2. IAM Identity Center に正常にサインインできたら、IAM Identity Center が利用可能であることを緊急アクセスユーザーに伝えてください。これらのユーザーに、サインアウトし、AWS アクセスポータルを使用して IAM Identity Center にサインインし直すよう指示します。
3. すべての緊急アクセスユーザーがサインアウトしたら、IdP で IdP フェデレーションアプリケーションを無効にします。このタスクは勤務時間後に実行することをお勧めします。
4. IdP の緊急アクセスグループからすべてのユーザーを削除します。

緊急アクセスロールのインフラストラクチャはバックアップアクセスプランとしては残っていますが、現在は無効になっています。

Okta でダイレクト IAM フェデレーションアプリケーションの 1 回限りの設定を行う

1. 管理者アクセス権限を持つユーザーとしてご自身のOktaアカウントにサインインします。
2. Okta 管理コンソールの [アプリケーション] で、[アプリケーション] を選択します。
3. [アプリカタログを参照] を選択します。[AWS アカウントフェデレーション] を検索して選択します。それから[統合の追加] を選択します。
4. 「AWSアカウントフェデレーション用の SAML 2.0 の設定方法」の手順に従って、AWS で直接 IAM フェデレーションを設定します。リージョン障害のシナリオに対処するには、サインインエンドポイントを設定する際に、フェデレーションの回復力を向上させるため、運用しているすべてのリージョンで非リージョンエンドポイントと複数のリージョンエンドポイントの両方を有効にすることをお勧めします。この緊急アクセス用に ACS URL を設定する際は、IAM Identity Center がデプロイされているリージョンとは異なるリージョンのリージョンエンドポイントを使用することをお勧めします。リージョンエンドポイントのリストについては、「AWS 全般リファレンス」の「サインインエンドポイント」を参照してください。

5. [サインオンオプション] タブで [SAML 2.0] を選択し、[グループフィルター] と [ロール値パターン] の設定を入力します。ユーザーディレクトリのグループ名は、設定するフィルターによって異なります。



上の図では、role 変数は緊急アクセスアカウントの緊急運用のロール用です。例えば、(マッピング表で説明されているように) EmergencyAccess_Role1_RO ロールを AWS アカウント 123456789012 で作成し、グループフィルター設定が上の図のように構成されている場合、グループ名は aws#EmergencyAccess_Role1_RO#123456789012 になります。

6. ディレクトリ (Active Directory 内のディレクトリなど) に緊急アクセスグループを作成し、ディレクトリの名前 (例:aws#EmergencyAccess_Role1_RO#123456789012) を指定します。既存のプロビジョニングメカニズムを使用して、ユーザーをこのグループに割り当てます。

7. 緊急アクセスアカウントで、中断中に緊急アクセスの役割を引き受けるのに必要なアクセス許可を提供するカスタム信頼ポリシーを設定します。EmergencyAccess_Role1_RO ロールに添付されているカスタム 信頼ポリシー のステートメントの例を以下に示します。図については、緊急時のロール、アカウント、グループのマッピングを設計する方法 の図の緊急アカウントを参照してください。サンプルの SAML プロバイダー ARN を、緊急アクセスアカウントで作成した正しい ARN に置き換えます。例のリージョンエンドポイントを、選択したリージョンのものに置き換えます。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
      {
         "Effect":"Allow",
         "Principal":{
            "Federated":"arn:aws:iam::123456789012:saml-provider/[SAML
 PROVIDER NAME]"
         },
         "Action":[
            "sts:AssumeRoleWithSAML",
            "sts:TagSession"
```

```
            ],
            "Condition":{
               "StringEquals":{
                  "SAML:aud": [
                           "https://signin.aws.amazon.com/saml",
                           "https://us-west-2.signin.aws.amazon.com/saml",
                           "https://us-west-1.signin.aws.amazon.com/saml",
                           "https://us-east-2.signin.aws.amazon.com/saml"
                  ]
               }
            }
         },
         {
            "Effect":"Allow",
            "Principal":{
            "Federated":"arn:aws:iam::123456789012:saml-provider/Okta"
            },
            "Action":"sts:SetSourceIdentity"
          }
      ]
}
```

8. 以下は、EmergencyAccess_Role1_RO ロールに適用されているアクセス 権限ポリシー のステートメントの例です。図については、緊急時のロール、アカウント、グループのマッピングを設計する方法 の図の緊急アカウントを参照してください。

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": [
                "arn:aws:iam::111122223333:role/EmergencyAccess_RO",
                "arn:aws:iam::444455556666:role/EmergencyAccess_RO"
            ]
        }
    ]
}
```

9. ワークロードアカウントで、カスタム信頼ポリシーを設定します。EmergencyAccess_RO ロールに添付されている 信頼ポリシー のステートメントの例を以下に示します。この例では、アカウント 123456789012 は緊急アクセスアカウントです。図については、緊急時のロール、アカウント、グループのマッピングを設計する方法の図の「ワークロードアカウント」を参照してください。

   JSON

```
{
    "Version":"2012-10-17",
    "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::123456789012:root"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

> **Note**
>
> ほとんどの IdPs では、必要になるまでアプリケーション統合を無効にしておくことができます。緊急アクセスが必要となるまで、IdP のダイレクト IAM フェデレーションアプリケーションを無効にしたままにしておくことをお勧めします。

ADFS でダイレクト IAM フェデレーションアプリケーションの 1 回限りの設定を行う

このガイドでは、IAM Identity Center が利用できない場合に AWS アカウント への緊急アクセスを有効にするために、ADFS との直接 IAM フェデレーションを設定する 1 回限りのセットアッププロセスについて説明します。

前提条件

AWS Managed Microsoft AD で ADFS を設定する場合は、まずマルチリージョンレプリケーションを設定し、回復力確保のためにプライマリリージョンではなく追加リージョンで次の手順に進むことをお勧めします。

Active Directory グループの命名規則を計画する

グループ名と AWS IAM ロールの自動マッチングを可能にする特定の命名パターンを使用して AD グループを作成します。

グループ命名形式: `AWS-<AccountNumber>-<RoleName>`

図については、緊急時のロール、アカウント、グループのマッピングを設計する方法 の図の緊急アカウントを参照してください。ユーザーは、このグループに割り当てられると、アカウント `123456789012` の `EmergencyAccess_Role1_RO` ロールへのアクセス権が付与されます。ユーザーが複数のグループに関連付けられている場合、AWS アカウント で使用可能なロールのリストが表示され、ユーザーはどのロールを引き受けるかを選択できます。

AWS の設定

完全なセットアップには、緊急アクセスアカウントとワークロードアカウントの設定が含まれます。セットアップ全体の図については、「緊急時のロール、アカウント、グループのマッピングを設計する方法」を参照してください。

1. SAML ID プロバイダーを作成する
2. 緊急アクセスロールを作成する
3. ワークロードアカウントロールを設定する

SAML ID プロバイダーを作成する

緊急アクセスアカウントで、「IAM で SAML ID プロバイダーを作成する」の手順に従って、IAM に SAML ID プロバイダーを作成します。ADFS サーバーから必要なメタデータをダウンロードします。

```
https://<yourADFSserverFQDN>/FederationMetadata/2007-06/
FederationMetadata.xml
```

緊急アクセスロールを作成する

信頼できるエンティティタイプとして SAML 2.0 フェデレーションを使用して、緊急アカウントに緊急アクセスロールを作成します。前のステップで作成した SAML 2.0 プロバイダーを選択します。

考慮事項:

- 運用しているすべてのリージョンを含める — アクティブなワークロードがあるすべてのリージョンを選択して、リージョンが中断しても引き続きフェデレーションを利用できるようにします。
- 1 つのリージョンで運用している場合でも、少なくとも 1 つの追加リージョンエンドポイントを設定する — 例えば、us-east-1 でのみ運用している場合は、us-west-2 をセカンダリエンドポイントとして追加します。IdP を us-west-2 SAML サインインエンドポイントにフェイルオーバーすることで、us-west-2 にワークロードがない場合でも us-east-1 リソースにアクセスできます。
- 非リージョンエンドポイントとリージョンエンドポイントの両方を有効にする — 非リージョンエンドポイント (https://signin.aws.amazon.com/saml) は高可用性ですが、単一の AWS リージョン、us-east-1 でホストされます。一方、リージョンエンドポイント (https://<region>.signin.aws.amazon.com/saml) は、単一のグローバルエンドポイントへの依存を減らすことで回復力を高めます。

信頼ポリシーを設定する

複数のサインインリージョンエンドポイントを持つ信頼ポリシーの例については、「Okta でダイレクト IAM フェデレーションアプリケーションの 1 回限りの設定を行う」を参照してください。例のリージョンエンドポイントと SAML プロバイダー ARN を自分のものに置き換えます。

アクセス許可ポリシーを設定する

緊急アクセスロールにアタッチするアクセス許可ポリシーの例については、「Okta でダイレクト IAM フェデレーションアプリケーションの 1 回限りの設定を行う」を参照してください。

ワークロードアカウントロールを設定する

ワークロードアカウントロールにカスタムの信頼ポリシーを設定して、そのロールを緊急アクセスアカウントの緊急アクセスロールが引き受けられるようにします。アカウント 123456789012 が緊急アクセスアカウントである信頼ポリシーの例については、「Okta でダイレクト IAM フェデレーションアプリケーションの 1 回限りの設定を行う」を参照してください。

アクティブディレクトリの設定

次の手順では、緊急アクセス用に Active Directory と ADFS を設定する方法について説明します。

1. グループの作成
2. 証明書利用者を作成する
3. クレームルールを作成する

グループの作成

前述の命名規則 (例えば `AWS-123456789012-EmergencyAccess_Role1_R0`) に従って、Active Directory に緊急グループを作成します。既存のプロビジョニングメカニズムを使用して、ユーザーをこれらのグループに割り当てます。

証明書利用者を作成する

ADFS フェデレーションには、証明書利用者の設定が必要です。証明書利用者は AWS Security Token Service (AWS STS) であり、ID プロバイダーとして ADFS に認証を外部委託します。

1. ADFS マネジメントコンソールで、[アクション] メニューを使用し、[証明書利用者の信頼を追加] を選択します。証明書利用者を追加するときに [クレーム対応] を選択します。
2. フェデレーションメタデータには、IAM コンソールの ID プロバイダーメタデータ情報からメタデータ URL を入力します。例えば、次のようになります。

   ```
   https://signin.aws.amazon.com/static/saml/SAMLSPXXXXXX/saml-metadata.xml
   ```
3. 証明書利用者の表示名 (例えば AWS アカウントアクセス) を設定し、[次へ] を選択します。
4. AWS へのアクセスを有効にするユーザーを選択します。特定のグループを選択し、MFA などの要件を定義できます。
5. [完了] ページで [閉じる] を選択して、証明書利用者信頼の追加ウィザードを完了します。これで AWS が証明書利用者として設定されます。

クレームルールを作成する

ADFS は、クレームルール言語を使用して、クレームプロバイダーと証明書利用者との間でクレームを発行および変換します。クレームルールを 4 つ作成する必要があります。NameId、RoleSessionName、Get AD Groups、および Roles for AWS Access です。

証明書利用者を右クリックし、[クレーム発行ポリシーの編集] を選択します。ルールを追加するには、[ルールの追加] を選択します。

1. NameId

a. [受信クレームの変換] を選択し、[次へ] を選択します。

b. 以下の設定を使用します。

- クレームルール名: `NameId`
- 受信クレームタイプ: `Windows Account Name`
- 送信クレームタイプ: `Name ID`
- 送信名 ID 形式: `Persistent Identifier`
- [すべてのクレーム値を渡す]: オン

c. [OK] を選択してください。

2. RoleSessionName

a. [ルールの追加] を選択します。

b. クレームルールテンプレートリストで、[LDAP 属性をクレームとして送信] を選択します。

c. 以下の設定を使用します。

- クレームルール名: `RoleSessionName`
- 属性ストア: `Active Directory`
- LDAP 属性: `E-Mail-Addresses`
- 送信クレームタイプ: `https://aws.amazon.com/SAML/Attributes/RoleSessionName`

d. [OK] を選択してください。

3. AD グループを取得する

a. [ルールの追加] を選択します。

b. クレームルールテンプレートリストで、[カスタムルールを使用してクレームを送信] を選択し、[次へ] を選択します。

c. [クレームルール名] に `Get AD Groups` と入力し、[カスタムルール] に次のように入力します。

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/
windowsaccountname", Issuer == "AD AUTHORITY"]
```

```
=> add(store = "Active Directory", types = ("http://temp/variable"), query =
 ";tokenGroups;{0}", param = c.Value);
```

このカスタムルールでは、クレームルール言語によるスクリプトを使用し、認証ユーザーがメンバーになっているグループをすべて取得して、http://temp/variable という名前の一時的なクレームに配置します。

> **Note**
>
> 予期しない結果を避けるため、末尾に空白がないことを確認します。

4. [ロール属性]

a. [ルールの追加] を選択します。

b. クレームルールテンプレートリストで、[カスタムルールを使用してクレームを送信] を選択し、[次へ] を選択します。

c. [クレームルール名] に Roles と入力し、[カスタムルール] に次のように入力します。

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([\d]{12})"]
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-([\d]{12})-", "arn:aws:iam::$1:saml-provider/
<ADFS>,arn:aws:iam::$1:role/"));
```

このカスタムルールでは、正規表現を使用して、フォーム AWS-<Account Number>-<Role Name> の各グループメンバーシップを、AWS が想定する IAM ロール ARN および IAM フェデレーションプロバイダー ARN の形式に変換します。

> **Note**
>
> 上記のルール言語の例では、ADFS は AWS ID プロバイダーのセットアップ時に SAML ID プロバイダーに付与された論理名を表します。これを、ID プロバイダーの IAM コンソールで選択した論理名に基づいて変更します。

設定をテストする

https://<yourADFSserverFQDN>/adfs/ls/IdpInitiatedSignOn.aspx で認証して、ソリューションが機能することをテストします。サイトのドロップダウンリストから、作成した証明書利用者の名前を選択します。

ADFS でデフォルトの SAML アサーションエンドポイントを更新する

> **Important**
>
> ADFS で証明書利用者の信頼を設定すると、SAML アサーションエンドポイントはデフォルトで https://signin.aws.amazon.com/ に設定されます。これはグローバルエンドポイントではなく、us-east-1 にあります。回復力確保のため、デフォルトのエンドポイントを、IAM Identity Center が設定されているリージョンとは異なるリージョンエンドポイントに変更することをお勧めします。例えば、IAM Identity Center を us-east-1 にデプロイしていて、us-west-2 でも運用している場合は、デフォルトの SAML アサーションコンシューマーエンドポイントを https://us-west-2.signin.aws.amazon.com/saml に変更します。

1. 証明書利用者信頼の [プロパティ] を選択し、[モニタリング] タブに移動します。[証明書利用者を自動的に更新] チェックボックスをオフにします。
2. [エンドポイント] タブに移動し、任意にサインインエンドポイントを選択して、[編集] を選択します。
3. [信頼できる URL をデフォルトに設定] チェックボックスをオンにします。[OK] を選択し、[適用] を選択して設定を有効にします。

> **Note**
>
> ほとんどの IdPs では、必要になるまでアプリケーション統合を無効にしておくことができます。緊急アクセスが必要となるまで、IdP のダイレクト IAM フェデレーションアプリケーションを無効にしたままにしておくことをお勧めします。

AWS IAM アイデンティティセンター でのセキュリティ

AWS ではクラウドセキュリティが最優先事項です。セキュリティを最も重視する組織の要件を満たすために構築された 「AWS」 のデータセンターとネットワークアーキテクチャは、お客様に大きく貢献します。

セキュリティは、「AWS」 と顧客の間の責任共有です。責任共有モデルでは、この責任が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されています。

- クラウドのセキュリティ - 「AWS」は、「AWS」クラウドで「AWS」のサービスを実行するインフラストラクチャを保護する責任を負います。また、「AWS」は、使用するサービスを安全に提供します。「AWS」 コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。「AWS IAM アイデンティティセンター」 に適用されるコンプライアンスプログラムの詳細については、「コンプライアンスプログラムによる対象範囲内の 「AWS」 のサービス」を参照してください。
- クラウド内のセキュリティ - ユーザーの責任は、使用する 「AWS」 のサービスに応じて異なります。また、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、IAM Identity Center が使用する際の責任共有モデルの適用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 IAM Identity Center を設定する方法について説明します。また、IAM Identity Center リソースのモニタリングや保護に役立つ他の AWS のサービスの使用方法についても説明します。

トピック

- IAM Identity Center の ID とアクセス管理
- IAM Identity Center コンソールと API 認可
- AWS STSIAM アイデンティティセンターの 条件コンテキストキー
- IAM Identity Center でのロギングとモニタリング
- IAM Identity Center のコンプライアンス検証
- IAM Identity Center の障害への耐性
- IAM Identity Center でのインフラストラクチャのセキュリティ

IAM Identity Center の ID とアクセス管理

IAM Identity Center へのアクセスには、AWS によってリクエストの認証に使用される認証情報が必要です。これらの認証情報には、AWS マネージドアプリケーションなどの AWS リソースに対するアクセス許可が必要です。

AWS アクセスポータルに対する認証は、IAM Identity Center に接続したディレクトリによって制御されます。ただし、AWS アクセスポータル内でエンドユーザーが利用できる AWS アカウント に対する権限付与は、以下の 2 つの要因によって決まります。

1. IAM Identity Center コンソールでそれらの AWS アカウント に対するアクセス権限が誰に割り当てられているか。詳細については、「AWS アカウント へのシングルサインオン・ アクセス」を参照してください。
2. それらの AWS アカウント に適切なアクセス権を付与するために、 IAM Identity Center コンソールでエンドユーザーにどのレベルのアクセス権限が付与されているか。詳細については、「アクセス許可セットの作成、管理と削除」を参照してください。

以下のセクションでは、管理者が IAM Identity Center コンソールへのアクセスを制御する方法や、IAM Identity Center コンソールから日常のタスクの管理アクセスを委任する方法について説明します。

- 認証
- アクセスコントロール

認証

IAM ID を使用して AWS にアクセスする方法をご覧ください。

アクセスコントロール

有効な認証情報があればリクエストを認証できますが、アクセス許可が付与されている場合を除き、IAM アイデンティティセンターリソースの作成やアクセスはできません。例えば、IAM Identity Center 接続先ディレクトリを作成するためのアクセス権限が必要です。

> **Note**
>
> IAM アイデンティティセンターインスタンスにカスタマーマネージド KMS キーが設定されている場合、IAM アイデンティティセンター管理者および KMS キーへのアクセスを必要

とするその他のアクターには、追加のアクセス許可が必要です。「AWS IAM アイデンティティセンター でのカスタマーマネージド KMS キーの実装」を参照してください。

次のセクションでは、IAM Identity Center の権限を管理する方法について説明します。最初に概要のセクションを読むことをお勧めします。

- IAM Identity Center リソースへのアクセス権限の管理の概要
- IAM Identity Center の ID ベースのポリシーの例
- IAM Identity Center のリソースベースのポリシーの例
- IAM Identity Center のサービスリンクロールの使用

IAM Identity Center リソースへのアクセス権限の管理の概要

すべての AWS リソースは AWS アカウント によって所有され、リソースの作成またはアクセスの許可は、許可ポリシーによって管理されます。アクセスを提供するには、アカウント管理者は、IAM ID (つまり、ユーザー、グループ、ロール) に権限ポリシーを追加します。一部のサービス (AWS Lambda など) は、アクセス権限ポリシーをリソースに追加することができます。

> **Note**
>
> アカウント管理者 (または管理者ユーザー) は、管理者権限を持つユーザーです。詳細については、「IAM ユーザーガイド」の「IAM ベストプラクティス」を参照してください。

トピック

- IAM Identity Center リソースと運用
- リソース所有権についての理解
- リソースへのアクセスの管理
- ポリシー要素の指定 : アクション、効果、リソース、プリンシパル
- ポリシーの条件の指定

IAM Identity Center リソースと運用

IAM Identity Center で、主なリソースはアプリケーションのインスタンス、プロファイル、アクセス権限セットです。

リソース所有権についての理解

リソース所有者は、リソースを作成した AWS アカウント です。つまり、リソース所有者とは、リソースの作成リクエストを認証するプリンシパルエンティティ (アカウント、ユーザー、または IAM ロール) の AWS アカウント です。次の例は、この仕組みを示しています。

- AWS アカウントのルートユーザー がアプリケーションのインスタンスやアクセス権限セットなどの IAM Identity Center リソースを作成する場合、AWS アカウント はそのリソースの所有者です。
- AWS アカウントにユーザーを作成し、そのユーザーに IAM Identity Center を作成する権限を付与すると、そのユーザーは IAM Identity Center リソースを作成できます。ただし、そのリソースを所有しているのは、ユーザーが属する AWS アカウントです。
- IAM Identity Center リソースを作成するためのアクセス権限を持つ AWS アカウントに IAM ロールを作成すると、ロールを引き受けるすべてのユーザーが IAM Identity Center リソースを作成できます。ロールが属する AWS アカウント は、IAM Identity Center リソースを所有しています。

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、IAM Identity Center のコンテキストでの IAM の使用について説明します。ここでは、IAM サービスに関する詳細情報を提供しません。IAM に関する詳細なドキュメントについては、「IAM ユーザーガイド」の「What is IAM?」(IAM とは？) 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「AWS IAM 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。IAM Identity Center では、ID ベースのポリシー (IAM ポリシー) のみがサポートされます。

トピック

- ID ベースのポリシー (IAM ポリシー)
- リソースベースのポリシー

ID ベースのポリシー (IAM ポリシー)

IAM ID にアクセス権限を追加できます。例えば、次のオペレーションを実行できます。

- AWS アカウント のユーザーまたはグループにアクセス権限ポリシーをアタッチする - アカウント管理者は、特定のユーザーに関連付けられる権限ポリシーを使用して、そのユーザーに IAM Identity Center リソース (新しいアプリケーションなど) を追加するためのアクセス権限を付与できます。
- アクセス権限ポリシーをロールにアタッチする (クロスアカウントの許可を付与) - ID ベースのアクセス権限ポリシーを IAM ロールにアタッチして、クロスアカウントの権限を付与することができます。

  IAM を使用したアクセス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。

次のアクセス権限ポリシーは、`List` で始まるすべてのアクションを実行するためのアクセス権限をユーザーに付与します。これらのアクションは、アプリケーションインスタンスやアクセス権限セットなどの IAM Identity Center リソースに関する情報を表示します。`Resource` 要素内のワイルドカード文字 (*) は、アカウントによって所有されるすべての IAM Identity Center リソースに対してそれらのアクションが許可されることを示します。

JSON

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

IAM Identity Center で ID ベースのポリシーを使用する場合の詳細については、 IAM Identity Center の ID ベースのポリシーの例 を参照してください。ユーザー、グループ、ロール、アクセス権限の詳細については、「IAM ユーザーガイド」の「ID (ユーザー、グループ、ロール)」を参照してください。

リソースベースのポリシー

Simple Storage Service (Amazon S3) などの他のサービスでは、リソースベースの許可ポリシーもサポートされています。例えば、ポリシーを S3 バケットにアタッチして、そのバケットに対するアクセス許可を管理できます。IAM Identity Center では、リソースベースのポリシーはサポートされていません。

ポリシー要素の指定 : アクション、効果、リソース、プリンシパル

IAM Identity Center のリソースごとに (「IAM Identity Center リソースと運用」参照)、このサービスは、一連の API オペレーションを定義します。こうした API 操作の権限を付与するために、IAM Identity Center はポリシーに特定できる一連のアクションを定義します。API オペレーションを実行する場合には、複数のアクションに対するアクセス許可が必要になることがあります。

以下は、基本的なポリシーの要素です。

- リソース – ポリシーで Amazon リソースネーム (ARN) を使用して、ポリシーを適用するリソースを識別します。
- アクション - アクションのキーワードを使用して、許可または拒否するリソースの操作を識別します。例えば、`sso:DescribePermissionsPolicies` 権限では、IAM アイデンティティセンター `DescribePermissionsPolicies` の操作を行うためのユーザー権限が与えられています。
- 効果 – ユーザーが特定のアクションを要求する際の効果を指定します。許可または拒否のいずれかになります。リソースへのアクセスを明示的に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、明示的にリソースへのアクセスを拒否すると、別のポリシーによってアクセスが許可されている場合でも、ユーザーはそのリソースにアクセスできなくなります。
- プリンシパル - ID ベースのポリシー (IAM ポリシー) で、ポリシーがアタッチされているユーザーが黙示的な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 Identity Center では、リソースベースのポリシーはサポートされていません。

IAM ポリシーの構文と説明の詳細はこちら IAM ユーザーガイドの AWS IAM ポリシーリファレンス。

ポリシーの条件の指定

アクセス権限を付与するとき、アクセスポリシー言語を使用して、ポリシーを有効にするために必要な条件を指定できます。例えば、特定の日付の後にのみ適用されるポリシーが必要になる場合があります。ポリシー言語での条件の指定の詳細については、「IAM ユーザーガイド」の「条件」を参照してください。

条件を表すには、あらかじめ定義された条件キーを使用します。IAM Identity Center に固有の条件キーはありません。ただし、AWS の条件キーを必要に応じて使用できます。AWS キーの完全なリストについては、「IAM ユーザーガイド」の「利用可能なグローバル条件キー」を参照してください。

IAM Identity Center の ID ベースのポリシーの例

このトピックでは、IAM Identity Center を管理する権限をユーザーとロールに付与するために作成できる IAM ポリシーの例を紹介します。

> **Important**
>
> 初めに、IAM Identity Center のリソースへのアクセスを管理するための基本概念と使用可能なオプションについて説明する概要トピックをお読みになることをお勧めします。詳細については、「IAM Identity Center リソースへのアクセス権限の管理の概要」を参照してください。

このセクションでは、次のトピックを対象としています。

- カスタムポリシーの例
- IAM Identity Center コンソールの使用に必要な権限

カスタムポリシーの例

このセクションでは、カスタム IAM ポリシーを必要とする一般的なユースケースの例を示します。これらのポリシーの例は ID ベースのポリシーであり、プリンシパル要素を指定しません。これは、ID ベースのポリシーでは、権限を取得するプリンシパルを指定しないためです。代わりに、ポリシーをプリンシパルにアタッチします。IAM ロールに ID ベースの権限ポリシーをアタッチすると、ロールの信頼ポリシーで識別されたプリンシパルが許可を得ることになります。IAM で ID ベースのポリシーを作成し、ユーザー、グループ、ロールにアタッチできます。IAM Identity Center でア

クセス権限セットを作成するときに、これらのポリシーを IAM Identity Center のユーザーに適用することもできます。

> **Note**
>
> お使いの環境用のポリシーを作成するときにこれらの例を使用し、これらのポリシーを本番環境に展開する前に、肯定的な (「アクセス許可」) テストケースと否定的な (「アクセス拒否」) テストケースの両方をテストしてください。IAM ポリシーシミュレーターの詳細については、「IAM ユーザーガイド」の「Testing IAM policies with the IAM policy simulator」(IAM Policy Simulator を使用した IAM ポリシーのテスト) を参照してください。

トピック

- 例 1: ユーザーに IAM Identity Center の表示を許可する
- 例 2: ユーザーが IAM Identity Center で AWS アカウント へのアクセス権限を管理できるようにする
- 例 3: IAM Identity Center でのアプリケーション管理をユーザーに許可する
- 例 4: Identity Center ディレクトリのユーザーとグループの管理をユーザーに許可する

例 1: ユーザーに IAM Identity Center の表示を許可する

次のアクセス権限ポリシーは、ユーザーに読み取り権限を付与し、IAM Identity Center 内で設定されたすべての設定やディレクトリ情報を閲覧できるようにします。

> **Note**
>
> このポリシーは、例示のみを目的として提供されています。本番環境では、IAM Identity Center の `ViewOnlyAccess` AWS マネージドポリシーを使用することをお勧めします。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
```

```
            "Effect": "Allow",
            "Action": [
                "ds:DescribeDirectories",
                "ds:DescribeTrusts",
                "iam:ListPolicies",
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:ListAccountsForParent",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListOrganizationalUnitsForParent",
                "sso:ListManagedPoliciesInPermissionSet",
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListPermissionSets",
                "sso:DescribePermissionSet",
                "sso:GetInlinePolicyForPermissionSet",
                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

例 2: ユーザーが IAM Identity Center で AWS アカウント へのアクセス権限を管理できるようにする

以下のアクセス権限ポリシーでは、ユーザーが AWS アカウント アカウントのアクセス権限セットを作成、管理、デプロイできる許可を付与しています。

JSON

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

```
            "Action": [
                "sso:AttachManagedPolicyToPermissionSet",
                "sso:CreateAccountAssignment",
                "sso:CreatePermissionSet",
                "sso:DeleteAccountAssignment",
                "sso:DeleteInlinePolicyFromPermissionSet",
                "sso:DeletePermissionSet",
                "sso:DetachManagedPolicyFromPermissionSet",
                "sso:ProvisionPermissionSet",
                "sso:PutInlinePolicyToPermissionSet",
                "sso:UpdatePermissionSet"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMListPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:ListPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AccessToSSOProvisionedRoles",
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:GetRole",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy",
                "iam:UpdateRole",
                "iam:UpdateRoleDescription"
            ],
            "Resource": "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "iam:GetSAMLProvider"
            ],
            "Resource": "arn:aws:iam::*:saml-provider/AWSSSO_*_DO_NOT_DELETE"
        }
    ]
}
```

> **Note**
>
> "Sid": "IAMListPermissions"、および "Sid": "AccessToSSOProvisionedRoles" セクションに記載されている追加の権限は、ユーザーが AWS Organizations 管理アカウントで割り当てを作成できるようにするために必要です。場合によっては、これらのセクションに iam:UpdateSAMLProvider を追加する必要もあります。

例 3: IAM Identity Center でのアプリケーション管理をユーザーに許可する

以下のアクセス権限ポリシーは、IAM Identity Center カタログ内から事前に統合された SaaS アプリケーションを含む IAM Identity Center のアプリケーションをユーザーが表示および設定できるようにするための許可を付与するものです。

> **Note**
>
> 以下のポリシー例で使用されている sso:AssociateProfile 操作は、ユーザーおよびグループのアプリケーションへの割り当てを管理するために必要です。また、既存のアクセス権限セットを利用して、ユーザーやグループを AWS アカウント アカウントに割り当てることもできます。ユーザーが IAM Identity Center 内でAWS アカウントアクセスを管理する必要があり、アクセス権限セットの管理に権限が必要な場合は、「例 2: ユーザーが IAM Identity Center で AWS アカウント へのアクセス権限を管理できるようにする」を参照してください。

2020 年 10 月時点で、これらの運用の多くは AWS コンソールからのみ利用可能です。この例のポリシーには、リスト、取得、検索などの「読み取り」アクションが含まれており、この場合のコンソールエラーのないオペレーションに関連します。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:ImportApplicationInstanceServiceProviderMetadata",
                "sso:DeleteApplicationInstance",
                "sso:DeleteProfile",
                "sso:DisassociateProfile",
                "sso:GetApplicationTemplate",
                "sso:UpdateApplicationInstanceServiceProviderConfiguration",
                "sso:UpdateApplicationInstanceDisplayData",
                "sso:DeleteManagedApplicationInstance",
                "sso:UpdateApplicationInstanceStatus",
                "sso:GetManagedApplicationInstance",
                "sso:UpdateManagedApplicationInstanceStatus",
                "sso:CreateManagedApplicationInstance",
                "sso:UpdateApplicationInstanceSecurityConfiguration",
                "sso:UpdateApplicationInstanceResponseConfiguration",
                "sso:GetApplicationInstance",
                "sso:CreateApplicationInstanceCertificate",
                "sso:UpdateApplicationInstanceResponseSchemaConfiguration",
                "sso:UpdateApplicationInstanceActiveCertificate",
                "sso:DeleteApplicationInstanceCertificate",
                "sso:ListApplicationInstanceCertificates",
                "sso:ListApplicationTemplates",
                "sso:ListApplications",
                "sso:ListApplicationInstances",
                "sso:ListDirectoryAssociations",
                "sso:ListProfiles",
                "sso:ListProfileAssociations",
                "sso:ListInstances",
                "sso:GetProfile",
                "sso:GetSSOStatus",
                "sso:GetSsoConfiguration",
                "sso-directory:DescribeDirectory",
                "sso-directory:DescribeUsers",
                "sso-directory:ListMembersInGroup",
```

```
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

例 4: Identity Center ディレクトリのユーザーとグループの管理をユーザーに許可する

以下のアクセス権限ポリシーは、ユーザーが IAM Identity Center でユーザーとグループを作成、表示、修正、削除するための許可を付与します。

場合によっては、IAM Identity Center のユーザーやグループを直接変更することが制限されている場合もあります。例えば、アクティブディレクトリや、自動プロビジョニングが有効になっている外部の ID プロバイダーが ID ソースとして選択されている場合などです。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso-directory:ListGroupsForUser",
                "sso-directory:DisableUser",
                "sso-directory:EnableUser",
                "sso-directory:SearchGroups",
                "sso-directory:DeleteGroup",
                "sso-directory:AddMemberToGroup",
                "sso-directory:DescribeDirectory",
                "sso-directory:UpdateUser",
                "sso-directory:ListMembersInGroup",
                "sso-directory:CreateUser",
                "sso-directory:DescribeGroups",
                "sso-directory:SearchUsers",
                "sso:ListDirectoryAssociations",
                "sso-directory:RemoveMemberFromGroup",
                "sso-directory:DeleteUser",
                "sso-directory:DescribeUsers",
```

```
                "sso-directory:UpdateGroup",
                "sso-directory:CreateGroup"
            ],
            "Resource": "*"
        }
    ]
}
```

IAM Identity Center コンソールの使用に必要な権限

ユーザーが IAM Identity Center コンソールをエラーなく使用するためには、追加の権限が必要です。これらの最小限必要なアクセス許可よりも制限された IAM ポリシーを作成している場合、そのポリシーを使用するユーザーに対してコンソールは意図したとおりには機能しません。以下の例では、IAM Identity Center コンソール内でエラーのない運用を行うために必要となる権限のセットを示しています。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:DescribeAccountAssignmentCreationStatus",
                "sso:DescribeAccountAssignmentDeletionStatus",
                "sso:DescribePermissionSet",
                "sso:DescribePermissionSetProvisioningStatus",
                "sso:DescribeRegisteredRegions",
                "sso:GetApplicationInstance",
                "sso:GetApplicationTemplate",
                "sso:GetInlinePolicyForPermissionSet",
                "sso:GetManagedApplicationInstance",
                "sso:GetMfaDeviceManagementForDirectory",
                "sso:GetPermissionSet",
                "sso:GetProfile",
                "sso:GetSharedSsoConfiguration",
                "sso:GetSsoConfiguration",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:ListAccountAssignmentCreationStatus",
```

```
                "sso:ListAccountAssignmentDeletionStatus",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListApplicationInstanceCertificates",
                "sso:ListApplicationInstances",
                "sso:ListApplications",
                "sso:ListApplicationTemplates",
                "sso:ListDirectoryAssociations",
                "sso:ListInstances",
                "sso:ListManagedPoliciesInPermissionSet",
                "sso:ListPermissionSetProvisioningStatus",
                "sso:ListPermissionSets",
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListProfileAssociations",
                "sso:ListProfiles",
                "sso:ListTagsForResource",
                "sso-directory:DescribeDirectory",
                "sso-directory:DescribeGroups",
                "sso-directory:DescribeUsers",
                "sso-directory:ListGroupsForUser",
                "sso-directory:ListMembersInGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

IAM Identity Center のリソースベースのポリシーの例

IAM アイデンティティセンターと連携し、OAuth 2.0 を使用するすべてのアプリケーションには、リソースベースのポリシーが必要です。アプリケーションはカスタマーマネージドでも AWS マネージドでもかまいません。アプリケーションポリシー (または API の ActorPolicy) と呼ばれる必要なリソースベースポリシーは、`CreateTokenWithIAM` などの IAM 認証メソッド API アクションを呼び出すことを許可されている IAM プリンシパルを定義します。IAM 認証方法を使用すると、IAM ロールや AWS サービスなどの IAM プリンシパルは、IAM 認証情報を提示して IAM アイデンティティセンターの OIDC サービスに対して認証を行い、/token?aws_iam=t エンドポイントでアクセストークンをリクエストまたは管理できます。

アプリケーションポリシーは、トークンの発行オペレーションを管理します (CreateTokenWithIAM)。このポリシーは、トークンの検証 (IntrospectTokenWithIAM) およびトークンの取り消し (RevokeTokenWithIAM) のためにAWSマネージドアプリケーションによってのみ使用されるアクセス許可のみのアクションも管理します。カスタマーマネージドアプリケーションの場合、CreateTokenWithIAM を呼び出す権限がある IAM プリンシパルを指定して、このポリシーを設定します。承認されたプリンシパルがこの API アクションを呼び出すと、プリンシパルはアプリケーションのアクセストークンと更新トークンを受け取ります。

IAM アイデンティティセンターコンソールを使用して信頼できる ID の伝播用にカスタマーマネージドアプリケーションをセットアップする場合、アプリケーションポリシーの設定方法の詳細については、「カスタマーマネージド OAuth 2.0 アプリケーションのセットアップ」のステップ 4 を参照してください。例となるポリシーについては、このトピックの後方にある「ポリシーの例: アクセストークンの作成と更新を IAM ロールに許可する」を参照してください。

ポリシーの要件

ポリシーは次の要件を満たしている必要があります。

- ポリシーには、「2012-10-17」に設定された Version 要素を含める必要があります。
- 各ポリシーには、少なくとも 1 つの Statement 要素が含まれている必要があります。
- 各ポリシー Statement には、Effect、Principal、Action、および Resource の要素を含める必要があります。

ポリシーの要素

ポリシーには以下の要素が含まれます。

バージョン

ポリシードキュメントのバージョンを指定します。バージョンを 2012-10-17 (最新バージョン) に設定します。

Statement

ポリシー Statements が含まれます。ポリシーには、少なくとも 1 つの Statement が含まれている必要があります。

各ポリシー Statement は以下の要素で構成されています。

Effect

(必須) ポリシーステートメント内の許可を許容するか拒否するかを決定します。有効な値は `Allow` または `Deny` です。

Principal

(必須) プリンシパルは、ポリシーステートメントで指定されている許可を取得するアイデンティティです。IAM ロールまたは AWS サービスプリンシパルを指定できます。

アクション

(必須) 許可または拒否する IAM アイデンティティセンター OIDC サービス API オペレーション。有効なアクションは以下のとおりです。

- `sso-oauth:CreateTokenWithIAM`: `CreateTokenWithIAM` API オペレーションに対応するこのアクションは、AWS サービスロールやユーザーなどの IAM エンティティを使用して認証された承認済みクライアントアプリケーションのアクセストークンと更新トークンを作成および返すアクセス許可を付与します。これらのトークンには、 `read:profile` や `write:data` などのアクセス許可を指定する定義済みのスコープが含まれる場合があります。
- `sso-oauth:IntrospectTokenWithIAM` [アクセス許可のみ]: アクティブな OAuth 2.0 アクセストークンと更新トークンに関する情報を検証および取得するアクセス許可を付与します。これには、関連するスコープとアクセス許可が含まれます。このアクセス許可は AWS マネージドアプリケーションでのみ使用され、「IAM アイデンティティセンター OIDC API リファレンス」には記載されていません。
- `RevokeTokenWithIAM` [アクセス許可のみ]: OAuth 2.0 アクセストークンと更新トークンを取り消し、通常の有効期限が切れる前に無効にするアクセス許可を付与します。このアクセス許可は AWS マネージドアプリケーションでのみ使用され、「IAM アイデンティティセンター OIDC API リファレンス」には記載されていません。

リソース

(必須) このポリシーでは、`Resource` 要素の値は `"*"` です。これは「このアプリケーション」を意味します。

AWS ポリシー構文の詳細については、IAM ユーザーガイドの AWS IAM ポリシーリファレンスを参照してください。

ポリシーの例: アクセストークンの作成と更新を IAM ロールに許可する

次のアクセス許可ポリシーは、ワークロードが引き受ける IAM ロールである ExampleAppClientRole にアクセストークンを作成して返すアクセス許可と更新トークンを付与します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRoleToCreateTokens",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/ExampleAppClientRole"
            },
            "Action": "sso-oauth:CreateTokenWithIAM",
            "Resource": "*"
        }
    ]
}
```

AWS IAM Identity Center のマネージドポリシー

チームが必要とする権限のみを提供する IAM カスタマーマネージメントポリシーを作成するには、時間と専門知識が必要です。AWS マネージドポリシーを使用することで、すぐに使用を開始できます。これらのポリシーは、一般的なユースケースをターゲット範囲に含めており、AWS アカウントで利用できます。AWS マネージドポリシーの詳細については、「IAMユーザーガイド」の「AWS マネージドポリシー」を参照してください。

AWS のサービスはAWS マネージドポリシーを維持および更新します。AWS マネージドポリシーの許可を変更することはできません。サービスでは新しい機能を利用できるようにするために、AWS マネージドポリシーに権限が追加されることがあります。この種類の更新はポリシーがアタッチされている、すべてのアイデンティティ (ユーザー、グループおよびロール) に影響を与えます。新しい機能が立ち上げられた場合や、新しいオペレーションが使用可能になった場合に、各サービスが AWS マネージドポリシーを更新する可能性が最も高くなります。サービスは AWS マネージドポリシーから権限を削除しないため、ポリシーの更新によって既存の権限が破棄されることはありません。

さらに、AWS は複数のサービスにまたがるジョブ機能の特徴に対するマネージドポリシーもサポートしています。例えば、ReadOnlyAccess AWS マネージドポリシーではすべての AWS のサービ

スおよびリソースへの読み取り専用アクセスを許可します。サービスが新しい機能を起動する場合、AWS は新たなオペレーションとリソース用に、読み取り専用の許可を追加します。ジョブ機能ポリシーのリストと説明については、IAM ユーザーガイド の「AWSジョブ機能のマネージドポリシー」を参照してください。

ユーザーセッションを一覧表示したり削除したりできる新しいアクションが、新しい名前スペース identitystore-auth で利用できるようになりました。この名前スペースのアクションに対する追加の権限は、このページで更新されます。カスタム IAM ポリシーを作成するときは、identitystore-auth の後に * を使用しないでください。これは、現在または将来名前スペースに存在するすべてのアクションに適用されるためです。

AWS マネージドポリシー: AWSSSOMasterAccountAdministrator

AWSSSOMasterAccountAdministrator ポリシーは、プリンシパルに必要な管理上のアクションを提供するものです。このポリシーは、AWS IAM アイデンティティセンター 管理者のジョブのロールを遂行するプリンシパルを対象とします。時間の経過とともに、提供されるアクションのリストは、IAM Identity Center の既存の機能と管理者として必要なアクションに一致するように更新されます。

AWSSSOMasterAccountAdministrator ポリシーを IAM IDにアタッチできます。AWSSSOMasterAccountAdministrator ポリシーを ID にアタッチすると、管理者用 AWS IAM アイデンティティセンター の許可が付与されます。このポリシーを持つプリンシパルは、 AWS Organizations 管理アカウントおよびすべてのメンバーアカウント内の IAM Identity Center にアクセスできます。このプリンシパルは、IAM Identity Center インスタンス、ユーザー、アクセス権限セット、割り当てを作成する機能を含む、すべての IAM Identity Center の運用を完全に管理することができます。また、プリンシパルは、AWS 組織のメンバーアカウント全体でこれらの割り当てをインスタンス化し、 AWS Directory Service マネージドディレクトリと IAM Identity Center の間の接続を確立することができます。新しい管理機能がリリースされると、アカウント管理者にはこれらの権限が自動的に付与されます。

このポリシーには、暗号化にカスタマーマネージドキーを使用する IAM アイデンティティセンターインスタンスに必要な AWS Key Management Service アクセス許可も含まれています。

アクセス権限のグループ化

このポリシーは、提供された一連の許可に基づくステートメントごとにグループ化されます。

- AWSSSOMasterAccountAdministrator – IAM Identity Center が AWSServiceRoleforSSO という名前の サービスロール を IAM Identity Center に渡すことを許可します。これにより、後でそ

のロールを引き受けて、代わりにアクションを実行できるようになります。これは、ユーザーやアプリケーションが IAM Identity Center を有効にするときに必要です。詳細については、「AWS アカウント へのアクセスを設定する」を参照してください。

- `AWSSSOMemberAccountAdministrator` - マルチアカウントの AWS 環境で IAM Identity Center がアカウント管理者のアクションを実行できるようにします。詳細については、「AWS マネージドポリシー: AWSSSOMemberAccountAdministrator」を参照してください。
- `AWSSSOManageDelegatedAdministrator` — IAM Identity Center が組織の委任管理者を登録および登録解除できるようにします。
- `AllowKMSKeyUseViaService` および `AllowKMSKeyDiscovery` – IAM アイデンティティセンターインスタンスで使用されるカスタマーマネージドキーの AWS Key Management Service オペレーションを許可します。

このポリシーに対するアクセス権限を確認するには、「AWS Managed Policy Reference」の「AWSSSOMasterAccountAdministrator」を参照してください。

ポリシーに関する追加情報。

IAM Identity Center が初めて有効になると、IAM Identity Center サービスは AWS Organizations マネージドアカウント (以前のマスターアカウント) にサービスリンクロール を作成し、IAM Identity Center がアカウントのリソースを管理できるようにします。このアクションには `iam:CreateServiceLinkedRole` と `iam:PassRole` が必要です。

AWS マネージドポリシー: AWSSSOMemberAccountAdministrator

`AWSSSOMemberAccountAdministrator` ポリシーは、プリンシパルに必要な管理上のアクションを提供するものです。このポリシーは、IAM Identity Center 管理者のジョブのロールを遂行するプリンシパルを対象とします。時間の経過とともに、提供されるアクションのリストは、IAM Identity Center の既存の機能と管理者として必要なアクションに一致するように更新されます。

`AWSSSOMemberAccountAdministrator` ポリシーを IAM IDにアタッチできます。`AWSSSOMemberAccountAdministrator` ポリシーを ID にアタッチすると、管理者用 AWS IAM アイデンティティセンター の許可が付与されます。このポリシーを持つプリンシパルは、 AWS Organizations 管理アカウントおよびすべてのメンバーアカウント内の IAM Identity Center にアクセスできます。このプリンシパルは、ユーザー、アクセス権限セット、および割り当てを作成する機能を含む、すべての IAM Identity Center の運用を完全に管理することができます。また、プリンシパルは、AWS 組織のメンバーアカウント全体でこれらの割り当てをインスタンス化し、 AWS Directory Service マネージドディレクトリと IAM Identity Center の間の接続を確立することができま

す。新しい管理機能がリリースされると、アカウント管理者にはこれらの権限が自動的に付与されます。

このポリシーには、暗号化にカスタマーマネージドキーを使用する IAM アイデンティティセンターインスタンスに必要な AWS Key Management Service アクセス許可も含まれています。

このポリシーに対するアクセス権限を確認するには、「AWS Managed Policy Reference」の「AWSSSOMemberAccountAdministrator」を参照してください。

ポリシーに関する追加情報。

IAM Identity Center 管理者は、IAM Identity Center ディレクトリストア (sso-directory) でユーザー、グループ、パスワードを管理します。アカウント管理者ロールには、以下のアクションの権限が含まれます。

- `"sso:*"`
- `"sso-directory:*"`

IAM Identity Center 管理者は、日常業務を行うために、以下の Directory Service アクションに対する限定的な権限が必要です。

- `"ds:DescribeTrusts"`
- `"ds:UnauthorizeApplication"`
- `"ds:DescribeDirectories"`
- `"ds:AuthorizeApplication"`
- `“ds:CreateAlias”`

これらの権限により、IAM Identity Center の管理者は、既存のディレクトリを特定し、アプリケーションを管理して、IAM Identity Center で使用できるように設定することができます。各アクションの詳細については、「Directory Service API 権限：アクション、リソース、参照する条件」を参照してください。

IAM Identity Center は、IAM ポリシーを使用して、IAM Identity Center ユーザーにアクセス許可を付与します。IAM Identity Center 管理者は、アクセス権限セットを作成し、それにポリシーをアタッチします。IAM Identity Center 管理者は、作成または更新するアクセス権限セットで使用するポリシーを選択できるように、既存のポリシーを一覧表示するには以下の権限が必要です。安全で機能的な権限を設定するには、IAM Identity Center の管理者が IAM Access Analyzer ポリシー検証を実行する権限を持っている必要があります。

- "iam:ListPolicies"
- "access-analyzer:ValidatePolicy"

IAM Identity Center の管理者は、日常業務を行うために、以下の AWS Organizations アクションに対する限定的なアクセスが必要です。

- "organizations:EnableAWSServiceAccess"
- "organizations:ListRoots"
- "organizations:ListAccounts"
- "organizations:ListOrganizationalUnitsForParent"
- "organizations:ListAccountsForParent"
- "organizations:DescribeOrganization"
- "organizations:ListChildren"
- "organizations:DescribeAccount"
- "organizations:ListParents"
- "organizations:ListDelegatedAdministrators"
- "organizations:RegisterDelegatedAdministrator"
- "organizations:DeregisterDelegatedAdministrator"

これらの権限により、IAM Identity Center の管理者は、組織リソース (アカウント) を操作して、以下のような基本的な IAM Identity Center 管理タスクを行うことができます。

- 組織に属する管理アカウントの特定
- 組織に属するメンバーアカウントの識別
- アカウントに対する AWS サービスアクセスの有効化
- 代理管理者の設定と管理

IAM Identity Center での委任管理者の使用の詳細については、「委任された管理」を参照してください。これらの権限が AWS Organizations でどのように使用されるかの詳細については、他の AWS サービスでの AWS Organizations の使用 を参照してください

AWS マネージドポリシー: AWSSSODirectoryAdministrator

AWSSSODirectoryAdministrator ポリシーを IAM IDにアタッチできます。

このポリシーは、IAM Identity Center のユーザーとグループに対する管理権限を付与します。このポリシーが適用されたプリンシパルは、IAM Identity Center のユーザーとグループを更新することができます。このポリシーには、暗号化にカスタマーマネージドキーを使用する IAM アイデンティティセンターインスタンスに必要な AWS Key Management Service アクセス許可も含まれています。

このポリシーには、以下のアクセス許可が含まれています。

- IAM アイデンティティセンターディレクトリ - IAM アイデンティティセンターディレクトリオペレーションへの完全な管理アクセス。
- ID ストア - ID ストアのオペレーションと認証への完全な管理アクセス。
- IAM アイデンティティセンター - ディレクトリの関連付けを一覧表示するアクセス許可。
- AWS Key Management Service - IAM アイデンティティセンターインスタンスで使用されるカスタマーマネージドキーの復号、キーの説明、データキーの生成を行うアクセス許可。

このポリシーに対するアクセス権限を確認するには、「AWS Managed Policy Reference」の「AWSSSODirectoryAdministrator」を参照してください。

AWS マネージドポリシー: AWSSSOReadOnly

`AWSSSOReadOnly` ポリシーを IAM IDにアタッチできます。

このポリシーは、ユーザーが IAM Identity Center の情報を閲覧するための読み取り専用の権限を付与します。このポリシーが適用されたプリンシパルは、IAM Identity Center のユーザーやグループを直接表示できません。IAM Identity Center では、このポリシーが適用されたプリンシパルを更新できません。例えば、これらの権限を持つプリンシパルは、IAM Identity Center 設定を閲覧することはできますが、設定値を変更することはできません。

このポリシーには、暗号化にカスタマーマネージドキーを使用する IAM アイデンティティセンターインスタンスに必要な AWS Key Management Service アクセス許可も含まれています。

このポリシーに対するアクセス権限を確認するには、「AWS Managed Policy Reference」の「AWSSSOReadOnly」を参照してください。

AWS マネージドポリシー: AWSSSODirectoryReadOnly

`AWSSSODirectoryReadOnly` ポリシーを IAM IDにアタッチできます。

このポリシーは、ユーザーが IAM Identity Center のユーザーとグループを閲覧するための読み取り専用の権限を付与します。このポリシーが適用されたプリンシパルは、IAM Identity Center の割り当て、アクセス権限セット、アプリケーション、または設定を表示できません。IAM Identity Center で

は、このポリシーが適用されたプリンシパルを更新できません。例えば、これらのアクセス許可を持つプリンシパルは、IAM アイデンティティセンターユーザーを表示できますが、ユーザー属性の変更や MFA デバイスの割り当てはできません。

このポリシーには、暗号化にカスタマーマネージドキーを使用する IAM アイデンティティセンターインスタンスに必要な AWS Key Management Service アクセス許可も含まれています。

このポリシーに対するアクセス権限を確認するには、「AWS Managed Policy Reference」の「AWSSSODirectoryReadOnly」を参照してください。

AWS マネージドポリシー: AWSIdentitySyncFullAccess

`AWSIdentitySyncFullAccess` ポリシーを IAM IDにアタッチできます。

このポリシーが適用されたプリンシパルには、同期プロファイルの作成と削除、同期プロファイルと同期ターゲットとの関連付けまたは更新、同期フィルターの作成、一覧表示、削除、同期の開始または停止を行う完全なアクセス権があります。

アクセス許可の詳細

このポリシーに対するアクセス権限を確認するには、「AWS Managed Policy Reference」の「AWSIdentitySyncFullAccess」を参照してください。

AWS マネージドポリシー: AWSIdentitySyncReadOnlyAccess

`AWSIdentitySyncReadOnlyAccess` ポリシーを IAM IDにアタッチできます。

このポリシーは、ユーザーが ID 同期プロファイル、フィルター、およびターゲット設定に関する情報を確認できるようにする読み取り専用の権限を付与します。このポリシーが適用されているプリンシパルは、同期設定を更新できません。例えば、これらのアクセス許可を持つプリンシパルは ID 同期設定を表示できますが、プロファイルやフィルターの値を変更することはできません。

このポリシーに対するアクセス権限を確認するには、「AWS Managed Policy Reference」の「AWSIdentitySyncReadOnlyAccess」を参照してください。

AWS マネージドポリシー: AWSSSOServiceRolePolicy

`AWSSSOServiceRolePolicy` ポリシーを IAM アイデンティティにアタッチできません。

このポリシーは、IAM Identity Center がどのユーザーに AWS Organizations 内の特定の AWS アカウント へのシングルサインオンアクセス権を委任および施行できるようにするサービスにリンクされたロールに適用されます。IAM を有効にすると、サービスにリンクされたロールが AWS アカウン

ト 組織内のすべてに作成されます。また、IAM Identity Center では、その後組織に追加されるすべてのアカウントに、同じサービスにリンクしたロールが作成されます。このロールは、IAM Identity Center が顧客に代わって各アカウントのリソースにアクセスすることを可能にします。各 AWS アカウント に作成されるサービスにリンクされたロール名は AWSServiceRoleForSSO です。詳細については、「IAM Identity Center のサービスリンクロールの使用」を参照してください。

AWS マネージドポリシー: AWSIAMIdentityCenterAllowListForIdentityContext

IAM アイデンティティセンターID コンテキストでロールを引き受けると、AWS Security Token Service (AWS STS) によって AWSIAMIdentityCenterAllowListForIdentityContext ポリシーが自動的にロールにアタッチされます。

このポリシーは、IAM アイデンティティセンターID コンテキストで引き受けられるロールで信頼できる ID の伝播を使用する場合に許可されるアクションのリストを提供します。このコンテキストで呼び出される他のすべてのアクションはブロックされます。ID コンテキストは ProvidedContext として渡されます。

このポリシーに対するアクセス権限を確認するには、「AWS Managed Policy Reference」の「AWSIAMIdentityCenterAllowListForIdentityContext」を参照してください。

AWS マネージドポリシー: AWSIdentityCenterExternalManagementPolicy

AWSIdentityCenterExternalManagementPolicy ポリシーを IAM IDにアタッチできます。

このポリシーにより、外部プロバイダーから IAM Identity Center ユーザーを管理するためのアクセスが提供されます。

このポリシーのアクセス許可を確認するには、「AWS マネージドポリシーリファレンス」の「AWSIdentityCenterExternalManagementPolicy」を参照してください。

IAM Identity Center は AWS マネージドポリシーを更新します

次の表は、IAM アイデンティティセンター の AWS マネージドポリシーについて、このサービスが変更の追跡を開始して以降に行われた更新を示しています。このページの変更に関する自動通知については、[IAM Identity Center ドキュメントの履歴] ページの RSS フィードを購読してください。

変更	説明	日付
AWSIdentityCenterExternalManagementPolicy	プロビジョニングテナントの ARN への変更が反映されるよ	2025 年 12 月 5 日

変更	説明	日付
	うにマネージドポリシーを更新しました。	
AWSIdentityCenterExternalManagementPolicy	このポリシーにより、外部プロバイダーから IAM Identity Center ユーザーを管理するためのアクセスが提供されます。	2025 年 11 月 21 日
AWSSSOMasterAccountAdministrator、AWSSSOMemberAccountAdministrator、AWSSSOReadOnly、AWSSSODirectoryAdministrator、AWSSSODirectoryReadOnly	マネージドポリシーを更新し、暗号化にカスタマーマネージドキーを使用する IAM アイデンティティセンターインスタンスに必要な AWS KMS アクセス許可を追加しました。	2025 年 9 月 17 日
AWSSSOServiceRolePolicy	このポリシーには、`identity-sync:DeleteSyncProfile` を呼び出すための新しいアクセス許可が含まれるようになりました。	2025 年 2 月 11 日
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーには、ID 拡張コンソールセッションをサポートする AWS マネージドアプリケーション向けにそれらのセッションをサポートする `qapps:ListQAppSessionData` と `qapps:ExportQAppSessionData` のアクションが含まれるようになりました。	2024 年 10 月 2 日

変更	説明	日付
AWSSSOMasterAccountAdministrator	IAM アイデンティティセンターに、DeleteSyncProfile 権限を付与する新しいアクションが追加され、このポリシーを使用して同期プロファイルを削除できるようになりました。これは DeleteInstance API に関連するアクションです。	2024 年 9 月 26 日
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーには、ID 拡張コンソールセッションをサポートする AWS マネージドアプリケーション向けにそれらのセッションをサポートする `s3:ListCallerAccessGrants` のアクションが含まれるようになりました。	2024 年 9 月 4 日
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーには、ID 拡張コンソールセッションをサポートする AWS マネージドアプリケーション向けにそれらのセッションをサポートする `aoss:APIAccessAll` 、`es:ESHttpHead` 、`es:ESHttpPost` 、`es:ESHttpGet` 、`es:ESHttpPatch` 、`es:ESHttpDelete` および `es:ESHttpPut` アクションが含まれるようになりました。	2024 年 7 月 12 日

変更	説明	日付
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーには、ID 拡張コンソールセッションをサポートする AWS マネージドアプリケーション向けにそれらのセッションをサポートする qapps:PredictQApp 、qapps:ImportDocument 、qapps:AssociateLibraryItemReview 、qapps:DisassociateLibraryItemReview 、qapps:GetQAppSession 、qapps:UpdateQAppSession 、qapps:GetQAppSessionMetadata 、qapps:UpdateQAppSessionMetadata および qapps:TagResource アクションが含まれるようになりました。	2024 年 6 月 27 日

変更	説明	日付
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーには、Amazon EMR で信頼できる ID の伝播をサポートするための elasticmapreduce:AddJobFlowSteps 、elasticmapreduce:DescribeCluster 、elasticmapreduce:CancelSteps 、elasticmapreduce:DescribeStep および elasticmapreduce:ListSteps アクションが含まれるようになりました。	2024 年 5 月 17 日

変更	説明	日付
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーには、ID 拡張コンソールセッションをサポートする AWS マネージドアプリケーション向けにそれらのセッションをサポートする qapps:CreateQApp 、qapps:PredictProblemStatementFromConversation 、qapps:PredictQAppFromProblemStatement 、qapps:CopyQApp 、qapps:GetQApp 、qapps:ListQApps 、qapps:UpdateQApp 、qapps:DeleteQApp 、qapps:AssociateQAppWithUser 、qapps:DisassociateQAppFromUser 、qapps:ImportDocumentToQApp 、qapps:ImportDocumentToQAppSession 、qapps:CreateLibraryItem 、qapps:GetLibraryItem 、qapps:UpdateLibraryItem 、qapps:CreateLibraryItemReview 、qapps:ListLibraryI	2024 年 4 月 30 日

変更	説明	日付
	tems 、qapps:CreateSubscriptionToken 、qapps:StartQAppSession および qapps:StopQAppSession アクションが含まれるようになりました。	
AWSSSOMasterAccountAdministrator	このポリシーには、ID 拡張コンソールセッションをサポートする AWS マネージドアプリケーション向けにそれらのセッションをサポートする signin:CreateTrustedIdentityPropagationApplicationForConsole と signin:ListTrustedIdentityPropagationApplicationsForConsole のアクションが含まれるようになりました。	2024 年 4 月 26 日

変更	説明	日付
AWSSSOMemberAccountAdministrator	このポリシーには、ID 拡張コンソールセッションをサポートする AWS マネージドアプリケーション向けにそれらのセッションをサポートする `signin:CreateTrustedIdentityPropagationApplicationForConsole` と `signin:ListTrustedIdentityPropagationApplicationsForConsole` のアクションが含まれるようになりました。	2024 年 4 月 26 日
AWSSSOReadOnly	このポリシーには、ID 拡張コンソールセッションをサポートする AWS マネージドアプリケーション向けにそれらのセッションをサポートする `signin:ListTrustedIdentityPropagationApplicationsForConsole` のアクションが含まれるようになりました。	2024 年 4 月 26 日
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーには、ID 拡張コンソールセッションをサポートする AWS マネージドアプリケーション向けにそれらのセッションをサポートする `qbusiness:PutFeedback` のアクションが含まれるようになりました。	2024 年 4 月 26 日

変更	説明	日付
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーには、ID 拡張コンソールセッションをサポートする AWS マネージドアプリケーション向けにそれらのセッションをサポートする q:StartConversation 、q:SendMessage 、q:ListConversations 、q:GetConversation 、q:StartTroubleshootingAnalysis 、q:GetTroubleshootingResults 、q:StartTroubleshootingResolutionExplanation および q:UpdateTroubleshootingCommandResult アクションが含まれるようになりました。	2024 年 4 月 24 日
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーには、ID 拡張コンソールセッションをサポートする AWS マネージドアプリケーション向けにそれらのセッションをサポートする sts:SetContext のアクションが含まれるようになりました。	2024 年 4 月 19 日

変更	説明	日付
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーには、ID 拡張コンソールセッションをサポートする AWS マネージドアプリケーション向けにそれらのセッションをサポートする qbusiness:Chat 、qbusiness:ChatSync 、qbusiness:ListConversations 、 qbusiness:ListMessages および qbusiness:DeleteConversation アクションが含まれるようになりました。	2024 年 4 月 11 日
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーには現在 s3:GetAccessGrantsInstanceForPrefix および s3:GetDataAccess アクションが含まれます。	2023 年 11 月 26 日
AWSIAMIdentityCenterAllowListForIdentityContext	このポリシーは、IAM アイデンティティセンターID コンテキストで引き受けられるロールで信頼できる ID の伝播を使用する場合に許可されるアクションのリストを提供します。	2023 年 11 月 15 日
AWSSSODirectoryReadOnly	このポリシーには、ユーザーがセッションを一覧表示して取得できるようにする新たな権限を付与された新しい名前スペース identitystore-auth が含まれました。	2023 年 2 月 21 日

変更	説明	日付
AWSSSOServiceRolePolicy	このポリシーにより、管理アカウントに対して UpdateSAMLProvider アクションを実行できるようになりました。	2022 年 10 月 20 日
AWSSSOMasterAccountAdministrator	このポリシーには、管理者がユーザーのセッションを一覧表示したり削除したりできるようにする新しい権限を持つ新しいネームスペース identitystore-auth が含まれるようになりました。	2022 年 10 月 20 日
AWSSSOMemberAccountAdministrator	このポリシーには、管理者がユーザーのセッションを一覧表示したり削除したりできるようにする新しい権限を持つ新しいネームスペース identitystore-auth が含まれるようになりました。	2022 年 10 月 20 日
AWSSSODirectoryAdministrator	このポリシーには、管理者がユーザーのセッションを一覧表示したり削除したりできるようにする新しい権限を持つ新しいネームスペース identitystore-auth が含まれるようになりました。	2022 年 10 月 20 日

変更	説明	日付
AWSSSOMasterAccountAdministrator	このポリシーには、AWS Organizations 内の ListDelegatedAdministrators を呼び出すための新しいアクセス許可が含まれるようになりました。このポリシーには、RegisterDelegatedAdministrator および DeregisterDelegatedAdministrator を呼び出すためのアクセス許可 AWSSSOManageDelegatedAdministrator を含むアクセス許可のサブセットも含まれるようになりました。	2022 年 8 月 16 日
AWSSSOMemberAccountAdministrator	このポリシーには、AWS Organizations 内の ListDelegatedAdministrators を呼び出すための新しいアクセス許可が含まれるようになりました。このポリシーには、RegisterDelegatedAdministrator および DeregisterDelegatedAdministrator を呼び出すためのアクセス許可 AWSSSOManageDelegatedAdministrator を含むアクセス許可のサブセットも含まれるようになりました。	2022 年 8 月 16 日

変更	説明	日付
AWSSSOReadOnly	このポリシーには、AWS Organizations 内の ListDelegatedAdministrators を呼び出すための新しいアクセス許可が含まれるようになりました。	2022 年 8 月 11 日
AWSSSOServiceRolePolicy	このポリシーには、DeleteRolePermissionsBoundary 内の PutRolePermisionsBoundary を呼び出すための新しいアクセス許可が含まれるようになりました。	2022 年 7 月 14 日
AWSSSOServiceRolePolicy	このポリシーには、AWS Organizations 内の ListAWSServiceAccessForOrganization and ListDelegatedAdministrators を呼び出すための新しいアクセス権が含まれました。	2022 年 5 月 11 日
AWSSSOMasterAccountAdministrator AWSSSOMemberAccountAdministrator AWSSSOReadOnly	プリンシパルが検証のためにポリシー チェックを使用できるようにする IAM Access Analyzer 権限を追加します。	2022 年 4 月 28 日

変更	説明	日付
AWSSSOMasterAccountAdministrator	このポリシーにより、IAM ID Center ID Store のすべてのサービスアクションが許可されるようになりました。 IAM ID センター ID Store サービスで使用できるアクションについては、IAM Identity Center Identity Store API Reference を参照してください。	2022 年 3 月 29 日
AWSSSOMemberAccountAdministrator	このポリシーにより、IAM ID Center ID Store のすべてのサービスアクションが許可されるようになりました。	2022 年 3 月 29 日
AWSSSODirectoryAdministrator	このポリシーにより、IAM ID Center ID Store のすべてのサービスアクションが許可されるようになりました。	2022 年 3 月 29 日
AWSSSODirectoryReadOnly	このポリシーは、IAM Identity Center Identity Store サービスの読み取りアクションへのアクセスを許可するようになりました。このアクセスは、IAM Identity Center Identity Store サービスからユーザーとグループの情報を取得するために必要です。	2022 年 3 月 29 日
AWSIdentitySyncFullAccess	このポリシーは、ID 同期許可への全アクセスを許可します。	2022 年 3 月 3 日

変更	説明	日付
AWSIdentitySyncReadOnlyAccess	このポリシーは、プリンシパルが ID 同期設定を閲覧するための読み取り専用の権限を付与します。	2022 年 3 月 3 日
AWSSSOReadOnly	このポリシーは、プリンシパルがすべての IAM Identity Center 構成設定を閲覧できる読み取り専用の権限を付与します。	2021 年 8 月 4 日
IAM Identity Center が変更の追跡を開始	IAM Identity Center で、AWS のマネージドポリシーの変更の追跡ができるようになりました。	2021 年 8 月 4 日

IAM Identity Center のサービスリンクロールの使用

AWS IAM アイデンティティセンター では AWS Identity and Access Management (IAM) のサービスリンクロールを使用します。サービスリンクロールは、IAM Identity Center に直接リンクされた特殊なタイプの IAM ロールです。これは IAM Identity Center によって事前に定義され、その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権限が含まれます。詳細については、「IAM アイデンティティセンターのサービスリンクロールについて」を参照してください。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がないため、IAM Identity Center の設定が簡単になります。サービスリンクロールの許可は IAM Identity Center が定義し、特に定義されない限り、IAM Identity Center のみがそのロールを引き受けることができます。定義されたアクセス許可には、信頼ポリシーとアクセス権限ポリシーが含まれ、そのアクセス権限ポリシーを他の IAM エンティティに適用することはできません。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連携する AWS のサービス」を参照して、「サービスにリンクされたロール」列が「はい」になっているサービスを確認してください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには [はい] リンクを選択してください。

IAM Identity Center のサービスリンクロールの権限

IAM Identity Center は、AWSServiceRoleForSSO という名称のサービスリンクロールを使用して、ユーザーに代わって IAM ロール、ポリシー、SAML IdP などの AWS リソースを管理するためのアクセス権限を IAM Identity Center に付与します。

AWSServiceRoleForSSO サービスリンクロールは、ロールの引き受けに以下のサービスを信頼します。

- IAM アイデンティティセンター(サービスプレフィックス: sso)

AWSSSOServiceRolePolicy サービスリンクロールのアクセス許可ポリシーでは、IAM アイデンティティセンターは「/aws-reserved/sso.amazonaws.com/」パスにあり、名前のプレフィックスが「AWSReservedSSO_」であるロールで以下のことを実行することができます。

- iam:AttachRolePolicy
- iam:CreateRole
- iam:DeleteRole
- iam:DeleteRolePermissionsBoundary
- iam:DeleteRolePolicy
- iam:DetachRolePolicy
- iam:GetRole
- iam:ListRolePolicies
- iam:PutRolePolicy
- iam:PutRolePermissionsBoundary
- iam:ListAttachedRolePolicies

AWSSSOServiceRolePolicy サービスリンクロールのアクセス許可ポリシーでは、IAM アイデンティティセンターは名前のプレフィックスが「AWSSSO_」である SAML プロバイダーで以下のことを実行することができます。

- iam:CreateSAMLProvider
- iam:GetSAMLProvider
- iam:UpdateSAMLProvider
- iam:DeleteSAMLProvider

AWSSSOServiceRolePolicy サービスリンクロールのアクセス許可ポリシーでは、IAM アイデンティティセンターはすべての組織で以下のことを実行することができます。

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`
- `organizations:ListAccounts`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:ListDelegatedAdministrators`

AWSSSOServiceRolePolicy サービスリンクロールのアクセス許可ポリシーでは、IAM アイデンティティセンターはすべての IAM ロール (*) で以下のことを実行することができます。

- `iam:listRoles`

AWSSSOServiceRolePolicy サービスリンクロールのアクセス許可ポリシーでは、IAM アイデンティティセンターは「arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO」で以下のことを実行することができます。

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam:DeleteServiceLinkedRole`

AWSSSOServiceRolePolicy サービスリンクロールのアクセス許可ポリシーでは、IAM アイデンティティセンターは「arn:aws:identity-sync:*:*:profile/*」で以下を完了できます。

- `identity-sync:DeleteSyncProfile`

AWSSSOServiceRolePolicy サービスリンクロールのアクセス許可ポリシーの更新の詳細については、「IAM Identity Center は AWS マネージドポリシーを更新します」を参照してください。

JSON

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

```
            "Effect":"Allow",
            "Action":[
               "iam:AttachRolePolicy",
               "iam:CreateRole",
               "iam:DeleteRolePermissionsBoundary",
               "iam:PutRolePermissionsBoundary",
               "iam:PutRolePolicy",
               "iam:UpdateRole",
               "iam:UpdateRoleDescription",
               "iam:UpdateAssumeRolePolicy"
            ],
            "Resource":[
               "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
            ],
            "Condition":{
               "StringNotEquals":{
                  "aws:PrincipalOrgMasterAccountId":"${aws:PrincipalAccount}"
               }
            }
         },
         {
            "Sid":"IAMRoleReadActions",
            "Effect":"Allow",
            "Action":[
               "iam:GetRole",
               "iam:ListRoles"
            ],
            "Resource":[
               "*"
            ]
         },
         {
            "Sid":"IAMRoleCleanupActions",
            "Effect":"Allow",
            "Action":[
               "iam:DeleteRole",
               "iam:DeleteRolePolicy",
               "iam:DetachRolePolicy",
               "iam:ListRolePolicies",
               "iam:ListAttachedRolePolicies"
            ],
            "Resource":[
               "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
            ]
```

```
      },
      {
         "Sid":"IAMSLRCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteServiceLinkedRole",
            "iam:GetServiceLinkedRoleDeletionStatus",
            "iam:DeleteRole",
            "iam:GetRole"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO"
         ]
      },
      {
        "Sid": "IAMSAMLProviderCreationAction",
        "Effect": "Allow",
        "Action": [
          "iam:CreateSAMLProvider"
      ],
      "Resource": [
         "arn:aws:iam::*:saml-provider/AWSSSO_*"
       ],
      "Condition": {
         "StringNotEquals": {
            "aws:PrincipalOrgMasterAccountId": "${aws:PrincipalAccount}"
          }
        }
      },
      {
        "Sid": "IAMSAMLProviderUpdateAction",
        "Effect": "Allow",
        "Action": [
          "iam:UpdateSAMLProvider"
        ],
        "Resource": [
           "arn:aws:iam::*:saml-provider/AWSSSO_*"
        ]
      },
      {
         "Sid":"IAMSAMLProviderCleanupActions",
         "Effect":"Allow",
         "Action":[
```

```
            "iam:DeleteSAMLProvider",
            "iam:GetSAMLProvider"
         ],
         "Resource":[
            "arn:aws:iam::*:saml-provider/AWSSSO_*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "organizations:DescribeAccount",
            "organizations:DescribeOrganization",
            "organizations:ListAccounts",
            "organizations:ListAWSServiceAccessForOrganization",
            "organizations:ListDelegatedAdministrators"
         ],
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"AllowUnauthAppForDirectory",
         "Effect":"Allow",
         "Action":[
            "ds:UnauthorizeApplication"
         ],
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"AllowDescribeForDirectory",
         "Effect":"Allow",
         "Action":[
            "ds:DescribeDirectories",
            "ds:DescribeTrusts"
         ],
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"AllowDescribeAndListOperationsOnIdentitySource",
         "Effect":"Allow",
```

```
            "Action":[
               "identitystore:DescribeUser",
               "identitystore:DescribeGroup",
               "identitystore:ListGroups",
               "identitystore:ListUsers"
            ],
            "Resource":[
               "*"
            ]
         },
         {
            "Sid":"AllowDeleteSyncProfile",
            "Effect":"Allow",
            "Action":[
               "identity-sync:DeleteSyncProfile"
            ],
            "Resource":[
               "arn:aws:identity-sync:*:*:profile/*"
            ]
         }
      ]
}
```

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

IAM Identity Center のサービスリンクロールの作成

サービスリンクロールを手動で作成する必要はありません。IAM Identity Center を有効にすると、AWS Organizations の組織内のすべてのアカウントに、サービスリンクロールが作成されます。また、IAM Identity Center では、その後組織に追加されるすべてのアカウントに、同じサービスにリンクしたロールが作成されます。このロールは、IAM Identity Center が顧客に代わって各アカウントのリソースにアクセスすることを可能にします。

注意事項

- AWS Organizations 管理アカウントにサインインしている場合、サービスリンクロールではなく、現在サインインしているロールが使用されます。これにより、権限の昇格を防ぐことができます。

- IAM Identity Center が AWS Organizations 管理アカウントで IAM 操作を実行すると、すべての操作は IAM プリンシパルの認証情報を使用して行われます。これにより、CloudTrail のログから、管理アカウントのすべての権限変更を誰が行ったかがわかります。

Important

サービスリンクロールのサポートを開始した 2017 年 12 月 7 日以前に IAM Identity Center サービスを利用していた場合、IAM Identity Center はお客様のアカウントに AWSServiceRoleForSSO ロールを作成しています。詳細については、「IAM アカウントに新しいロールが表示される」を参照してください。

このサービスにリンクされたロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。

IAM Identity Center のサービスリンクロールの編集

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

IAM Identity Center のサービスリンクロールの削除

AWSServiceRoleForSSO ロールを手動で削除する必要はありません。AWS アカウント が AWS 組織から削除されると、IAM Identity Center は自動的にリソースをクリーンアップし、AWS アカウント からサービスリンクロールを削除します。

サービスにリンクされたロールは、IAM コンソール、IAM CLI、または IAM API を使用して手動で削除することもできます。そのためにはまず、サービスリンクロールのリソースをクリーンアップする必要があります。その後で、手動で削除できます。

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

AWSServiceRoleForSSO が使用する IAM Identity Center リソースを削除するには

1. AWS アカウントへのユーザーおよびグループのアクセスを削除する へのアクセス権を持つすべてのユーザーとグループの AWS アカウント。
2. IAM アイデンティティセンターでアクセス許可セットを削除する に関連付けられている AWS アカウント。

サービスリンクロールを IAM で手動削除するには

IAM コンソール、IAM CLI、または IAM API を使用して、AWSServiceRoleForSSO サービスにリンクされたロールを削除します。詳細については、「IAM User Guide」(IAM ユーザーガイド) の「Deleting a Service-Linked Role」(サービスにリンクされたロールの削除) を参照してください。

IAM Identity Center コンソールと API 認可

既存の IAM アイデンティティセンターコンソール API は二重認可をサポートしているため、新しい API が利用可能になっても既存の API オペレーションを引き続き使用できます。2023 年 11 月 15 日および 2020 年 10 月 15 日より前に作成された IAM アイデンティティセンターの既存のインスタンスがある場合は、次の表を使用して、どの API オペレーションがそれらの日付以降にリリースされた新しい API オペレーションにマップされているかを判断できます。

トピック

- 2023 年 11 月以降の API アクション
- 2020 年 10 月以降の API アクション

2023 年 11 月以降の API アクション

2023 年 11 月 15 日より前に作成された IAM アイデンティティセンターのインスタンスは、いずれかのアクションに対して明示的な拒否がない限り、新旧両方の API アクションを受け入れま

す。2023 年 11 月 15 日以降に作成されたインスタンスは、IAM アイデンティティセンターコンソールでの認可に新しい API アクションを使用します。

2023 年 11 月 15 日以前に使用されたコンソールオペレーション名	2023 年 11 月 15 日以降に使用された API アクション
AssociateProfile	CreateApplicationAssignment
CreateManagedApplicationInstance | CreateApplicationInstance	CreateApplication
CreateManagedApplicationInstance	PutApplicationAuthenticationMethod
DeleteApplicationInstance | DeleteManagedApplicationInstance	DeleteApplication
DeleteSSO	DeleteInstance
DisassociateProfile	DeleteApplicationAssignment
GetApplicationTemplate	DescribeApplicationProvider
GetManagedApplicationInstance	DescribeApplication
GetSharedSsoConfiguration	DescribeInstance
ListApplicationInstances	ListApplications
ListApplicationTemplates	ListApplicationProviders
ListDirectoryAssociations	DescribeInstance
ListProfileAssociations	ListApplicationAssignments
UpdateApplicationInstanceDisplayData | UpdateApplicationInstanceStatus | UpdateManagedApplicationInstanceStatus	UpdateApplication

2020 年 10 月以降の API アクション

2020 年 10 月 15 日以前に作成された IAM アイデンティティセンターのインスタンスは、いずれかのアクションに明示的な拒否がない限り、新旧両方の API アクションを受け入れます。2020 年 10 月 15 日以降に作成されたインスタンスは、IAM アイデンティティセンターコンソールでの認可に新しい API アクションを使用します。

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
AssociateProfile	AssociateProfile	CreateAccountAssignment
AttachManagedPolicy	PutPermissionsPolicy	AttachManagedPolicyToPermissionSet
CreatePermissionSet	CreatePermissionSet	CreatePermissionSet
DeleteApplicationInstanceForAWsAccount	DeleteApplicationInstance | DeleteTrust	DeleteAccountAssignment
DeleteApplicationProfileForAwsAccount	DeleteProfile	DeleteAccountAssignment
DeletePermissionsPolicy	DeletePermissionsPolicy	DeleteInlinePolicyFromPermissionSet
DeletePermissionSet	DeletePermissionSet	DeletePermissionSet
DescribePermissionsPolicies	DescribePermissionsPolicies	ListManagedPoliciesInPermissionSet
DetachManagedPolicy	DeletePermissionsPolicy	DetachManagedPolicyFromPermissionSet
DisassociateProfile	DisassociateProfile	DeleteAccountAssignment
GetApplicationInstanceForAWSAccount	GetApplicationInstance	ListAccountAssignments

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
GetAWSAccountProfileStatus	GetProfile	ListPermissionSetsProvisionedToAccount
GetPermissionSet	GetPermissionSet	DescribePermissionSet
GetPermissionsPolicy	GetPermissionsPolicy	GetInlinePolicyForPermissionSet
ListAccountsWithProvisionedPermissionSet	ListApplicationInstances | GetApplicationInstance	ListAccountsForProvisionedPermissionSet
ListAWSAccountProfiles	ListProfiles | GetProfile	ListPermissionSetsProvisionedToAccount
ListPermissionSets	ListPermissionSets	ListPermissionSets
ListProfileAssociations	ListProfileAssociations	ListAccountAssignments
ProvisionApplicationInstanceForAWSAccount	GetApplicationInstance | CreateApplicationInstance	CreateAccountAssignment
ProvisionApplicationProfileForAWSAccountInstance	GetProfile | CreateProfile | UpdateProfile	CreateAccountAssignment
ProvisionSAMLProvider	GetTrust | CreateTrust | UpdateTrust	CreateAccountAssignment
PutPermissionsPolicy	PutPermissionsPolicy	PutInlinePolicyToPermissionSet
UpdatePermissionSet	UpdatePermissionSet	UpdatePermissionSet

AWS STSIAM アイデンティティセンターの 条件コンテキストキー

特定のプリンシパルが AWS にリクエストを行うと、AWS は、リクエスト情報をリクエストコンテキストに集約し、そのコンテキストを利用してリクエストを評価し承認します。JSON ポリシーの

Condition 要素を使用して、リクエストコンテキストのキーを、ポリシーで指定したキーバリューと比較できます。リクエスト情報は、リクエストを行うプリンシパル、リソース、リクエストの対象、リクエスト自体に関するメタデータなど、さまざまなソースから提供されます。サービス固有の条件キーは、個々の AWS サービスで使用するように定義されています。

IAM アイデンティティセンターには、AWS マネージドアプリケーションやサードパーティーアプリケーションが IAM アイデンティティセンターで定義された条件キーに値を追加できるようにする AWS STS コンテキストプロバイダーが含まれています。これらのキーは、IAM ロールに含まれています。アプリケーションがトークンを AWS STS に渡す際に、キー値が設定されます。アプリケーションは、次のいずれかの方法で AWS STS に渡されるトークンを取得します。

- IAM アイデンティティセンターでの認証中。
- 信頼できる ID の伝播のために信頼できるトークン発行者とトークンを交換した後。この場合、アプリケーションは信頼できるトークン発行者からトークンを取得し、そのトークンを IAM アイデンティティセンターからのトークンと交換します。

これらのキーは、通常、信頼できる ID の伝播機能を統合したアプリケーションで使用されます。場合によっては、キー値が存在するため、作成する IAM ポリシーでこれらのキーを使用して、アクセス権限の許可や拒否ができます。

例えば、UserId の値に基づいてリソースへの条件付きアクセスを提供したい場合があるでしょう。この値は、どの IAM アイデンティティセンターユーザーがロールを使用しているかを示します。この例は、SourceId を使用する場合に似ています。ただし SourceId とは異なり、UserId の値は、ID ストア由来の特定の検証済みユーザーを表します。この値は、アプリケーションが取得し、AWS STS に渡すトークンに含まれます。任意の値を格納できる汎用文字列ではありません。

トピック

- identitystore:UserId
- identitystore:IdentityStoreArn
- identitycenter:ApplicationArn
- identitycenter:CredentialId
- identitycenter:InstanceArn

identitystore:UserId

このコンテキストキーは、IAM アイデンティティセンターによって発行されるコンテキストアサーションの対象である IAM アイデンティティセンターユーザーの UserId です。コンテキストアサーションは AWS STS に渡されます。このキーを使用して、リクエストの送信元である IAM アイデンティティセンターユーザーの UserId を、ポリシーで指定したユーザーの識別子と比較できます。

- 可用性 – このキーは、AWS CLI または AWS STS AssumeRole API オペレーションで任意の AWS STS assume-role コマンドを使用してロールを引き受ける際に、IAM アイデンティティセンターが発行するコンテキストアサーションの設定後にリクエストコンテキストに含まれます。
- データ型 – 文字列
- 値タイプ — 単一値

identitystore:IdentityStoreArn

このコンテキストキーは、コンテキストアサーションを発行した IAM アイデンティティセンターのインスタンスにアタッチされた ID ストアの ARN です。また、identitystore:UserID の属性を検索できる ID ストアでもあります。このキーをポリシーで使用して、identitystore:UserID が想定される ID ストアの ARN から取得されたものかを判断できます。

- 可用性 – このキーは、AWS CLI または AWS STS AssumeRole API オペレーションで任意の AWS STS assume-role コマンドを使用してロールを引き受ける際に、IAM アイデンティティセンターが発行するコンテキストアサーションの設定後にリクエストコンテキストに含まれます。
- データ型 – Arn、文字列
- 値タイプ — 単一値

identitycenter:ApplicationArn

このコンテキストキーは、IAM アイデンティティセンターがコンテキストアサーションを発行したアプリケーションの ARN です。このキーをポリシーで使用して、identitycenter:ApplicationArn が想定されるアプリケーションから取得されたものであるかを判断できます。このキーを使用するころで、予期しないアプリケーションによる IAM ロールへのアクセスを防止できます。

- 可用性 – このキーは、AWS STS AssumeRole API オペレーションのリクエストコンテキストに含まれています。リクエストコンテキストには、IAM アイデンティティセンターによって発行されたコンテキストアサーションが含まれます。
- データ型 – Arn、文字列
- 値タイプ — 単一値

identitycenter:CredentialId

このコンテキストキーは、アイデンティティ強化ロール認証情報のランダム ID であり、ログ記録のみに使用されます。このキー値は予測できないため、ポリシーのコンテキストアサーションには使用しないことをお勧めします。

- 可用性 – このキーは、AWS STS AssumeRole API オペレーションのリクエストコンテキストに含まれています。リクエストコンテキストには、IAM アイデンティティセンターによって発行されたコンテキストアサーションが含まれます。
- データ型 – 文字列
- 値タイプ — 単一値

identitycenter:InstanceArn

このコンテキストキーは、identitystore:UserID のコンテキストアサーションを発行した IAM アイデンティティセンターのインスタンスの ARN です。このキーを使用して、identitystore:UserID と コンテキストアサーションが、想定される IAM アイデンティティセンターインスタンスの ARN から取得されたものであるかを判断できます。

- 可用性 – このキーは、AWS STS AssumeRole API オペレーションのリクエストコンテキストに含まれています。リクエストコンテキストには、IAM アイデンティティセンターによって発行されたコンテキストアサーションが含まれます。
- データ型 – Arn、文字列
- 値タイプ — 単一値

IAM Identity Center でのロギングとモニタリング

ベストプラクティスとして、組織をモニタリングして、変更がログに記録されていることを確認することが推奨されます。モニタリングにより、確実に予期しない変更を調査することができ、不要

な変更をロールバックできます。現在 IAM アイデンティティセンターでは、組織および組織内で発生するアクティビティを監視することができる 2 つの AWS サービス、AWS CloudTrail と Amazon EventBridge.のサービスをサポートしています。

トピック

- AWS CloudTrail を使用した IAM Identity Center API コールのログ記録
- AWS CloudTrail を使用した IAM アイデンティティセンター SCIM API コールのログ記録
- アプリケーションコンポーネントを Amazon EventBridge に接続する
- 設定可能な AD 同期エラーのログ記録

AWS CloudTrail を使用した IAM Identity Center API コールのログ記録

AWS IAM アイデンティティセンター は、IAM Identity Center のユーザー、ロール、または AWS サービスによって実行されたアクションの記録を提供するサービスである AWS CloudTrail と統合されています。CloudTrail は、IAM Identity Center に対する API コールをイベントとしてキャプチャします。キャプチャされた呼び出しには、IAM Identity Center コンソールからの呼び出しと、IAM Identity Center の API 運用へのコードの呼び出しが含まれます。証跡を作成する場合は、IAM アイデンティティセンターのイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。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 で収集された情報を使用して、IAM Identity Center に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時など追加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。

次の表は、IAM アイデンティティセンターの CloudTrail イベント、その CloudTrail イベントソース、および一致する API をまとめたものです。API の詳細については、「IAM アイデンティティセンター API リファレンス」を参照してください。

> **Note**
>
> サインインと呼ばれる CloudTrail イベントの追加のグループがあり、IAM アイデンティティセンター ユーザーとして AWS にサインインするために AWS が出力します。これらのイベントには一致するパブリック API がないため、API リファレンスには表示されません。

CloudTrail のイベント	パブリック API	説明	CloudTrail イベントソース
IAM アイデンティティーセンター	IAM アイデンティティセンター	IAM アイデンティティセンター API を使用すると、アクセス許可セット、アプリケーション、信頼できるトークン発行者、アカウントとアプリケーションの割り当て、IAM アイデンティティセンターインスタンス、タグを管理できます。	sso.amazonaws.com
Identity Store	Identity Store	ID ストア API を使用すると、ワークフォースのユーザーとグループのライフサイクル、およびユーザーのグループメンバーシップを管理できます。また、ユーザーの MFA デバイスの管理もサポートしています。	sso-directory.amazonaws.com , identitystore.amazonaws.com
OIDC	OIDC	OIDC API、信頼できる ID の伝播と、既に認証された IAM アイデンティティセンターユーザーとしての AWS CLI および IDE ツールキットへの	sso.amazonaws.com , sso-oauth.amazonaws.com

CloudTrail のイベント	パブリック API	説明	CloudTrail イベントソース
		サインインをサポートしています。	
AWS アクセスポータル	AWS アクセスポータル	AWS アクセスポータル API、 AWS アクセスポータルのオペレーションと、AWS CLI を通じてアカウント認証情報を取得するユーザーをサポートします。	sso.amazonaws.com
– SCIM	– SCIM	SCIM API、SCIM プロトコルを介したユーザー、グループ、グループメンバーシップのプロビジョニングをサポートします。詳細については「AWS CloudTrail を使用した IAM アイデンティティセンター SCIM API コールのログ記録」を参照してください。	identitystore-scim.amazonaws.com
AWS サインイン	パブリック API がない	AWS は、ユーザー認証とフェデレーションフローのサインイン CloudTrail イベントを IAM アイデンティティセンターに出力します。	signin.amazon.com

トピック

- IAM アイデンティティセンターの CloudTrail ユースケース
- CloudTrail での IAM Identity Center の情報

IAM アイデンティティセンターの CloudTrail ユースケース

IAM アイデンティティセンターが発行する CloudTrail イベントは、さまざまなユースケースで役立ちます。組織は、これらのイベントログを使用して、AWS 環境内のユーザーアクセスとアクティビティをモニタリングおよび監査できます。これにより、ログは誰がいつどのリソースにアクセスするかの詳細をキャプチャするため、コンプライアンスのユースケースに役立ちます。CloudTrail データをインシデント調査に使用して、チームがユーザーのアクションを分析し、疑わしい動作を追跡できるようにすることもできます。さらに、イベント履歴はトラブルシューティング作業をサポートし、時間の経過とともにユーザーのアクセス許可と設定に加えられた変更を可視化できます。

以下のセクションでは、監査、インシデント調査、トラブルシューティングなどのワークフローに役立つ基本的なユースケースについて説明します。

IAM アイデンティティセンターのユーザーが開始した CloudTrail イベントでユーザーを特定する

IAM アイデンティティセンターは、IAM または AWS CLI へのサインイン、MFA デバイスの管理を含む AWS アクセスポータルの使用など、CloudTrail イベントの背後にある IAM アイデンティティセンターユーザーを識別できる 2 つの CloudTrail フィールドを出力します。

- `userId` – IAM アイデンティティセンターインスタンスの ID ストアからの一意でイミュータブルなユーザー識別子。
- `identityStoreArn` – ユーザーを含む ID ストアの Amazon リソースネーム (ARN)。

`userID` および `identityStoreArn` フィールドは、次の CloudTrail イベントログの例に示すように、`onBehalfOf` 要素内にネストされた `userIdentity` 要素に表示されます。このイベントログには、`userIdentity` タイプが「`IdentityCenterUser`」であるイベントのこれら 2 つのフィールドが表示されます。これらのフィールドは、`userIdentity` タイプが「Unknown」である認証済み IAM アイデンティティセンターユーザーのイベントでも確認できます。ワークフローは両方の型値を受け入れる必要があります。

```
"userIdentity":{
  "type":"IdentityCenterUser",
  "accountId":"111122223333",
```

```
  "onBehalfOf": {
    "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "90e292de-5eb8-446e-9602-90f7c45044f7"
  }
```

> **Tip**
>
> IAM Identity Center CloudTrail イベントの背後にあるユーザーを特定するには、 `userId` と `identityStoreArn` を使用することをお勧めします。`userIdentity` 要素の `userName` および `principalId` フィールドは使用できなくなりました。監査やインシデント対応などのワークフローが `username` へのアクセスに依存している場合は、次の 2 つのオプションがあります。
>
> - 「サインイン CloudTrail イベントのユーザー名」の説明に従って、IAM アイデンティティセンターディレクトリからユーザー名を取得します。
> - サインインの `additionalEventData` 要素で IAM アイデンティティセンターが出力する `UserName` を取得します。このオプションは、IAM アイデンティティセンターディレクトリへのアクセスを必要としません。詳細については、「サインイン CloudTrail イベントのユーザー名」を参照してください。

`username` フィールドを含むユーザーの詳細を取得するには、ユーザー ID と ID ストア ID をパラメータとして ID ストアにクエリを実行します。このアクションは、`DescribeUser` API リクエストまたは CLI を使用して実行できます。以下にサンプル CLI コマンドを示します。IAM アイデンティティセンターインスタンスが CLI のデフォルトリージョンにある場合は、 `region` パラメータを省略できます。

```
aws identitystore describe-user \
--identity-store-id  d-1234567890 \
--user-id  544894e8-80c1-707f-60e3-3ba6510dfac1 \
--region your-region-id
```

前の例の CLI コマンドの ID ストア ID 値を決定するには、 `identityStoreArn`値から ID ストア ID を抽出します。ARN の例では `arn:aws:identitystore::111122223333:identitystore/d-1234567890`、ID ストア ID は `d-1234567890` です。または、IAM アイデンティティセンター

コンソールの設定セクションの [ID ストア] タブに移動して、ID ストア ID を見つけることもできます。

IAM アイデンティティセンタディレクトリ内のユーザーの検索を自動化する場合は、ユーザー検索の頻度を見積もり、ID ストア API の IAM アイデンティティセンターのスロットル制限を検討することをお勧めします。取得したユーザー属性をキャッシュすると、スロットル制限内に収まるようになります。

同じユーザーセッション内のユーザーイベントの関連付け

サインインイベントで出力される `AuthWorkflowID` フィールドを使用すると、IAM アイデンティティセンターユーザーセッションを開始する前に、サインインシーケンスに関連付けられたすべての CloudTrail イベントを追跡できます。

AWS アクセスポータル内のユーザーアクションの場合、`credentialId`値はアクションのリクエストに使用される IAM アイデンティティセンターユーザーのセッションの ID に設定されます。この値を使用して、 AWS アクセスポータルの同じ認証済み IAM アイデンティティセンターユーザーセッション内で開始された CloudTrail イベントを識別できます。

> **Note**
>
> `credentialId` を使用して、サインインイベントを AWS アクセスポータルの使用などの後続のイベントに関連付けることはできません。サインインイベントで出力される `credentialId` フィールドの値は内部的に使用されるため、依存しないことをお勧めします。OIDC で呼び出されるAWS アクセスポータルイベントに対して出力される `credentialId` フィールドの値は、アクセストークンの ID と等しくなります。

IAM アイデンティティセンターのユーザーが開始した CloudTrail イベントでのユーザーバックグラウンドセッションの詳細の特定

次の CloudTrail イベントは、OAuth 2.0 トークン交換のプロセスをキャプチャします。このプロセスでは、ユーザーのインタラクティブセッションを表す既存のアクセストークン (`subjectToken`) が更新トークン (`requestedTokenType`) と交換されます。更新トークンを使用すると、ユーザーが長時間実行ジョブを開始した場合でも、ユーザーがサインアウトした後でも、ユーザーのアクセス許可を使用して実行を継続できます。

IAM アイデンティティセンターユーザーバックグラウンドセッションの場合、CloudTrail イベントには `requestParameters` 要素に `resource` という追加要素が含まれます。`resource` パ

ラメータには、バックグラウンドで実行されるジョブの Amazon リソースネーム (ARN) が含まれます。この要素は CloudTrail イベントレコードにのみ存在し、IAM アイデンティティセンター CreateTokenWithIAM API または SDK レスポンスには含まれません。

```
{
  "clientId": "EXAMPLE-CLIENT-ID",
  "grantType": "urn:ietf:params:oauth:grant-type:token-exchange",
  "code": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "redirectUri": "https://example.com/callback",
  "assertion": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "subjectToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "subjectTokenType": "urn:ietf:params:oauth:token-type:access_token",
  "requestedTokenType": "urn:ietf:params:oauth:token-type:refresh_token",
  "resource": "arn:aws:sagemaker:us-west-2:123456789012:training-job/my-job"
}
```

IAM アイデンティティセンターと外部ディレクトリ間のユーザーの関連付け

IAM アイデンティティセンターには、ディレクトリ内のユーザーを外部ディレクトリ内の同じユーザー (Microsoft Active Directory や Okta Universal Directory など) に関連付けるために使用できる 2 つのユーザー属性が用意されています。

- `externalId` – IAM アイデンティティセンターユーザーの外部識別子。この識別子は、外部ディレクトリのイミュータブルなユーザー識別子にマッピングすることをお勧めします。IAM アイデンティティセンターは CloudTrail でこの値を出力しないことに注意してください。
- `username` – ユーザーが通常サインインする、お客様が指定した値。値は変更できます (SCIM 更新など)。ID ソースが Directory Service の場合、IAM アイデンティティセンターが CloudTrail で出力するユーザー名は、認証のために入力したユーザー名と一致することに注意してください。ユーザー名は、IAM アイデンティティセンターディレクトリのユーザー名と完全に一致する必要はありません。

  CloudTrail イベントにアクセスできるが、IAM アイデンティティセンターディレクトリにはアクセスできない場合は、サインイン時に `additionalEventData` 要素の下に出力されるユーザー名を使用できます。`additionalEventData` のユーザー名の詳細については、「サインイン CloudTrail イベントのユーザー名」を参照してください。

ID ソースが Directory Service の場合、これら 2 つのユーザー属性と外部ディレクトリ内の対応するユーザー属性のマッピングは IAM アイデンティティセンターで定義されます。詳細については、「IAM アイデンティティセンターと外部 ID プロバイダーディレクトリ間の属性マッピング」を参

照してください。SCIM でユーザーをプロビジョニングする外部 IdP には、独自のマッピングがあります。ID ソースとして IAM アイデンティティセンターディレクトリを使用している場合でも、externalId 属性を使用してセキュリティプリンシパルを外部ディレクトリに相互参照できます。

次のセクションでは、ユーザーの username と externalId を考慮して IAM アイデンティティセンターユーザーを検索する方法について説明します。

ユーザー名と externalId による IAM アイデンティティセンターユーザーの表示

GetUserId API リクエストを使用して対応する userId をリクエストし、前の例に示すように DescribeUser API リクエストを発行することで、既知のユーザー名の IAM アイデンティティセンターディレクトリからユーザー属性を取得できます。次の例は、特定のユーザー名の を ID ストア userIdから取得する方法を示しています。IAM アイデンティティセンターインスタンスが CLI を使用した場合のデフォルトリージョンにあるなら、 region パラメータを省略できます。

```
aws identitystore get-user-id \
    --identity-store d-9876543210 \
    --alternate-identifier '{
      "UniqueAttribute": {
      "AttributePath": "username",
      "AttributeValue": "anyuser@example.com"
        }
          }' \
    --region your-region-id
```

同様に、externalId がわかっている場合も、同じメカニズムを使用できます。前の例の属性パスを externalId 値で更新し、属性値を検索対象の特定の externalId で更新します。

Microsoft Active Directory (AD) と externalId でのユーザーの Secure Identifier (SID) の表示

場合によっては、IAM Identity Center は、AWS アクセスポータルや OIDC API が出力するイベントなど、CloudTrail イベントの principalId フィールドでユーザーの SID を出力します。これらのケースは段階的に廃止されています。AD から一意のユーザー識別子が必要な場合は、ワークフローで AD 属性 objectguid を使用することをお勧めします。この値は、IAM アイデンティティセンターディレクトリの externalId 属性にあります。ただし、ワークフローで SID を使用する必要がある場合は、IAM アイデンティティセンター API では使用できないため、AD から値を取得します。

同じユーザーセッション内のユーザーイベントの関連付け では、 フィールドexternalIdとusernameフィールドを使用して、IAM アイデンティティセンターユーザーと外部ディレクトリ内の一致するユーザーを関連付ける方法について説明します。デフォルトでは、IAM アイデンティティ

センターは AD の objectguid 属性 externalId にマッピングされ、このマッピングは修正されています。IAM アイデンティティセンターを使用すると、管理者は AD の userprincipalname へのデフォルトのマッピングとは異なる方法で柔軟に username にマッピングできます。

これらのマッピングは、IAM アイデンティティセンターコンソールで表示できます。[設定] の [ID ソース] タブに移動し、[アクション] メニューで [同期の管理] を選択します。[同期の管理] セクションで、[属性マッピングの表示] ボタンを選択します。

IAM アイデンティティセンターで使用可能な一意の AD ユーザー識別子を使用して AD のユーザーを検索できますが、変更不可能な識別子であるため、クエリで objectguid を使用することをお勧めします。次の例は、Powershell で Microsoft AD をクエリして、ユーザーの 16809ecc-7225-4c20-ad98-30094aefdbca の objectguid 値を使用してユーザーを取得する方法を示しています。このクエリへの正常なレスポンスには、ユーザーの SID が含まれます。

```
Install-WindowsFeature -Name  RSAT-AD-PowerShell

  Get-ADUser `
  -Filter {objectGUID -eq  [GUID]::Parse("16809ecc-7225-4c20-ad98-30094aefdbca")} `
  -Properties *
```

CloudTrail での IAM Identity Center の情報

CloudTrail は、AWS アカウント を作成すると、その中で有効になります。IAM Identity Center でアクティビティが発生すると、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。最近のイベントは、AWS アカウント で表示、検索、ダウンロードできます。詳細については、「CloudTrail Event 履歴でのイベントの表示」を参照してください。

> **Note**
>
> CloudTrail イベントでのユーザーアクションのユーザー識別と追跡がどのように進化しているかの詳細については、「AWS セキュリティブログ」の「IAM アイデンティティセンターの CloudTrail イベントに対する重要な変更」を参照してください。

IAM Identity Center のイベントなど、AWS アカウント のイベントの継続記録のための証跡を作成します。証跡により、ログファイルを CloudTrail で Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成すると、すべての AWS リージョンに証跡が適用されます。証跡は、AWS パーティションのすべてのリージョンからのイベントを口グに記録し、指定した Amazon

S3 バケットにログファイルを配信します。さらに、CloudTrail· ログで収集したイベントデータをより詳細に分析し、それに基づく対応するためにその他の AWS サービスを設定できます。詳細については、『AWS CloudTrail ユーザーガイド:』の以下のトピックを参照してください。

- 証跡作成の概要
- CloudTrail がサポートされているサービスと統合
- CloudTrail の Amazon SNS 通知の設定
- CloudTrail ログファイルを複数のリージョンから受け取る、複数のアカウントから CloudTrail ログファイルを受け取る

AWS アカウント で CloudTrail のログ記録を有効にすると、IAM Identity Center アクションに対して行った API コールがログファイルに記録されます。IAM Identity Center の記録は、他の AWS のサービス記録と一緒にログファイルに記録されます。CloudTrail は、期間とファイルサイズに基づいて、新しいファイルをいつ作成して書き込むかを決定します。

サポートされている IAM アイデンティティセンター API CloudTrail イベント

以下のセクションでは、IAM アイデンティティセンターがサポートする以下の API に関連付けられた CloudTrail イベントについて説明します。

- IAM アイデンティティセンター API
- ID ストア Auth
- OIDC API
- AWS アクセスポータル API
- SCIM API

IAM アイデンティティセンター API オペレーションの CloudTrail イベント

次のリストには、パブリック IAM アイデンティティセンター オペレーションが `sso.amazonaws.com` イベントソースで出力する CloudTrail イベントが含まれています。IAM アイデンティティセンター API オペレーションの詳細については、「IAM アイデンティティセンター API レファレンスガイド」を参照してください。

コンソールが依存する IAM アイデンティティセンターコンソール API オペレーションの追加のイベントが CloudTrail に表示される場合があります。これらのコンソール API に関する詳細については、「サービス認可リファレンス」を参照してください。

- AttachCustomerManagedPolicyReferenceToPermissionSet
- AttachManagedPolicyToPermissionSet
- CreateAccountAssignment
- CreateApplication
- CreateApplicationAssignment
- CreateInstance
- CreateInstanceAccessControlAttributeConfiguration
- CreatePermissionSet
- CreateTrustedTokenIssuer
- DeleteAccountAssignment
- DeleteApplication
- DeleteApplicationAccessScope
- DeleteApplicationAssignment
- DeleteApplicationAuthenticationMethod
- DeleteApplicationGrant
- DeleteInlinePolicyFromPermissionSet
- DeleteInstance
- DeleteInstanceAccessControlAttributeConfiguration
-

DeletePermissionsBoundaryFromPermissionSet

- DeletePermissionSet
- DeleteTrustedTokenIssuer
- DescribeAccountAssignmentCreationStatus
- DescribeAccountAssignmentDeletionStatus
- DescribeApplication
- DescribeApplicationAssignment
- DescribeApplicationProvider
- DescribeInstance
- DescribeInstanceAccessControlAttributeConfiguration
- DescribePermissionSet
- DescribePermissionSetProvisioningStatus
- DescribeTrustedTokenIssuer
- DetachCustomerManagedPolicyReferenceFromPermissionSet
- DetachManagedPolicyFromPermissionSet
-

- GetApplicationAccessScope
- GetApplicationAssignmentConfiguration
- GetApplicationAuthenticationMethod
- GetApplicationGrant
- GetInlinePolicyForPermissionSet
- GetPermissionsBoundaryForPermissionSet
- ListAccountAssignmentCreationStatus
- ListAccountAssignmentDeletionStatus
- ListAccountAssignments
- ListAccountAssignmentsForPrincipal
- ListAccountsForProvisionedPermissionSet
- ListApplicationAccessScopes
- ListApplicationAssignments
- ListApplicationAssignmentsForPrincipal
- ListApplicationAuthenticationMethods
- ListApplicationGrants

- ListApplicationProviders
- ListApplications
- ListCustomerManagedPolicyReferencesInPermissionSet
- ListInstances
- ListManagedPoliciesInPermissionSet
- ListPermissionSetProvisioningStatus
- ListPermissionSets
- ListPermissionSetsProvisionedToAccount
- ListTagsForResource
- ListTrustedTokenIssuers
- ProvisionPermissionSet
- PutApplicationAccessScope
- PutApplicationAssignmentConfiguration
- PutApplicationAuthenticationMethod
- PutApplicationGrant

- PutInlinePolicyToPermissionSet
- PutPermissionsBoundaryToPermissionSet
- TagResource
- UntagResource
- UpdateApplication
- UpdateInstance
- UpdateInstanceAccessControlAttributeConfiguration
- UpdatePermissionSet
- UpdateTrustedTokenIssuer

ID ストア API オペレーションの CloudTrail イベント

次のリストには、パブリック ID ストアオペレーションがイベントソースで出力する CloudTrail `identitystore.amazonaws.com`イベントが含まれています。IAM アイデンティティセンターのパブリック API オペレーションの詳細については、「IAM アイデンティティセンター API レファレンスガイド 」を参照してください。

`sso-directory.amazonaws.com` イベントソースを使用した ID ストアコンソール API オペレーションの追加イベントが CloudTrail に表示される場合があります。これらの API、 コンソールと AWS アクセスポータルをサポートしています。グループにメンバーを追加するなど、特定のオペレーションの発生を検出する必要がある場合は、パブリック API オペレーションとコンソール API オペレーションの両方を検討することをお勧めします。これらのコンソール API に関する詳細については、「サービス認可リファレンス」を参照してください。

- CreateGroup
- CreateGroupMembership

- CreateUser
- DeleteGroup
- DeleteGroupMembership
- DeleteUser
- DescribeGroup
- DescribeGroupMembership
- DescribeUser
- GetGroupId
- GetGroupMembershipId
- GetUserId
- IsMemberInGroups
- ListGroupMemberships
- ListGroupMembershipsForMember
- ListGroups
- ListUsers
- UpdateGroup
- UpdateUser

OIDC API オペレーションの CloudTrail イベント

次のリストには、パブリック OIDC オペレーションが出力する CloudTrail イベントが含まれています。使用可能な OIDC API オペレーションの詳細については、「OIDC API リファレンス」を参照してください。

- CreateToken (イベントソース)`sso.amazonaws.com`
- CreateTokenWithIAM (イベントソース)`sso-oauth.amazonaws.com`

AWS アクセスポータル API オペレーションの CloudTrail イベント

次のリストには、 AWS アクセスポータル API オペレーションが `sso.amazonaws.com` イベントソースで出力する CloudTrail イベントが含まれています。パブリック API で使用できないと記録された API オペレーションは、AWS アクセスポータルのオペレーションをサポートします。AWS CLI を使用すると、パブリック AWS アクセスポータル API オペレーションとパブリック API で使用できないオペレーションの両方の CloudTrail イベントが発生する可能性があります。パブリック AWS

アクセスポータル API オペレーションの詳細については、「AWS アクセスポータル API リファレンス」を参照してください。

- Authenticate (パブリック API では使用できません。 AWS アクセスポータルへのログインを提供します。)
- Federate (パブリック API では使用できません。 アプリケーションへのフェデレーションを提供します。)
- ListAccountRoles
- ListAccounts
- ListApplications (パブリック API では使用できません。 AWS アクセスポータルに表示するユーザーに割り当てられたリソースを提供します。)
- ListProfilesForApplication (パブリック API では使用できません。 AWS アクセスポータルに表示するアプリケーションメタデータを提供します。)
- GetRoleCredentials
- Logout

SCIM API オペレーションの CloudTrail イベント

パブリック SCIM API オペレーションの詳細については、「AWS アクセスポータル API リファレンス」を参照してください。

IAM アイデンティティセンター CloudTrail の ID 情報

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストが、ルートユーザーまたは AWS Identity and Access Management (IAM) ユーザーのどちらかの認証情報を使用して送信された場合。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用し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。
- リクエストが IAM アイデンティティセンターによって行われたかどうか。その場合は、CloudTrail イベントで `userId` および `identityStoreArn` フィールドを使用して、リクエストを開始した IAM アイデンティティセンターユーザーを識別できます。詳細については、「IAM アイデンティティセンターのユーザーが開始した CloudTrail イベントでユーザーを特定する」を参照してください。

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

> **Note**
>
> 現在、IAM アイデンティティセンターは、OIDC API を使用して AWS マネージドウェブアプリケーション (Amazon SageMaker AI Studio など) にユーザーサインインするための CloudTrail イベントを出力しません。これらのウェブアプリケーションは、より広範な the section called “AWS マネージドアプリケーション” のセットのサブセットであり、Amazon Athena SQL や Amazon S3 Access Grants などのウェブ以外のアプリケーションも含まれます。

IAM アイデンティティセンターの CloudTrail イベントの概要

証跡は、指定した Amazon S3 バケットにイベントを配信できる設定です。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 イベントは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。詳細については、「 ユーザーガイド」の「CloudTrail レコードコンテンツ」を参照してください。

この例では、IAM アイデンティティセンターを操作する IAM ユーザー (samadams) によって実行された `DescribePermissionsPolicies` アクションをキャプチャする CloudTrail ログエントリを示します。

```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDAJAIENLMexample",
            "arn":"arn:aws:iam::08966example:user/samadams",
            "accountId":"111122223333",
            "accessKeyId":"AKIAIIJM2K4example",
            "userName":"samadams"
         },
         "eventTime":"2017-11-29T22:39:43Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"DescribePermissionsPolicies",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
```

```
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":{
            "permissionSetId":"ps-79a0dde74b95ed05"
         },
         "responseElements":null,
         "requestID":"319ac6a1-d556-11e7-a34f-69a333106015",
         "eventID":"a93a952b-13dd-4ae5-a156-d3ad6220b071",
         "readOnly":true,
         "resources":[

         ],
         "eventType":"AwsApiCall",
         "recipientAccountId":"111122223333"
      }
   ]
}
```

この例では、 AWS アクセスポータル内の IAM アイデンティティセンターユーザーが実行したListApplicationsアクションをキャプチャする CloudTrail ログエントリを示します。

```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"IdentityCenterUser",
            "accountId":"111122223333",
            "onBehalfOf": {
              "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
              "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
            },
            "credentialId" : "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
         },
         "eventTime":"2017-11-29T18:48:28Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"ListApplications",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":null,
```

```
         "responseElements":null,
         "requestID":"de6c0435-ce4b-49c7-9bcc-bc5ed631ce04",
         "eventID":"e6e1f3df-9528-4c6d-a877-6b2b895d1f91",
         "eventType":"AwsApiCall",
         "recipientAccountId":"111122223333"
      }
   ]
}
```

この例では、IAM アイデンティティセンター OIDC サービスで認証する IAM アイデンティティセンターユーザーが実行したCreateTokenアクションをキャプチャする CloudTrail ログエントリを示します。

```
{
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IdentityCenterUser",
        "accountId": "111122223333",
        "onBehalfOf": {
          "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
          "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
        },
        "credentialId" : "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
      },
      "eventTime": "2020-06-16T01:31:15Z",
      "eventSource": "sso.amazonaws.com",
      "eventName": "CreateToken",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "203.0.113.0",
      "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
      "requestParameters": {
        "clientId": "clientid1234example",
        "clientSecret": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "grantType": "urn:ietf:params:oauth:grant-type:device_code",
        "deviceCode": "devicecode1234example"
      },
      "responseElements": {
        "accessToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "tokenType": "Bearer",
        "expiresIn": 28800,
        "refreshToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
```

```
        "idToken": "HIDDEN_DUE_TO_SECURITY_REASONS"
      },
      "eventID": "09a6e1a9-50e5-45c0-9f08-e6ef5089b262",
      "readOnly": false,
      "resources": [
        {
          "accountId": "111122223333",
          "type": "IdentityStoreId",
          "ARN": "d-1234567890"
        }
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
}
```

IAM Identity Center サインインイベントの概要

AWS CloudTrail は、すべての IAM アイデンティティセンターの ID ソースに関する、サインインイベントの成功と失敗を記録します。IAM アイデンティティセンターおよび Active Directory (AD Connector およびAWS Managed Microsoft AD) をソースとする ID には、ユーザーが特定の資格情報のチャレンジや要素を解決するよう求められるたびにキャプチャされるサインインイベントに加えて、その特定の認証情報の検証リクエストのステータスが含まれます。必要な認証情報のチャレンジをすべて完了したユーザーだけがサインインを許可され、`UserAuthentication` イベントが記録されます。

次の表は、IAM Identity Center サインインの各 CloudTrail イベント名、その目的、および異なる ID ソースへの適用性を示しています。

イベント名	イベントの目的	ID ソースの適用性
`CredentialChallenge`	IAM Identity Center がユーザーに特定の認証課題の解決を要求したことを通知するために使用され、要求されている `CredentialType` を指定します (例として、PASSWORD または TOTP)。	ネイティブ IAM Identity Center ユーザー、AD Connector、および AWS Managed Microsoft AD
`CredentialVerification`	ユーザーが特定の `CredentialChallenge` リクエストの	ネイティブ IAM Identity Center ユーザー、AD

イベント名	イベントの目的	ID ソースの適用性
	解決を試みたことを通知するために使用され、その認証情報が成功したか失敗したかを指定します。	Connector、および AWS Managed Microsoft AD
`UserAuthentication`	要求されたすべての認証要件をユーザーが正常に完了し、正常にサインインしたことを通知するために使用されます。ユーザーが必要な認証情報のチャレンジを正常に完了できなかった場合、*`UserAuthentication`* イベントはログに記録されません。	すべての ID ソース

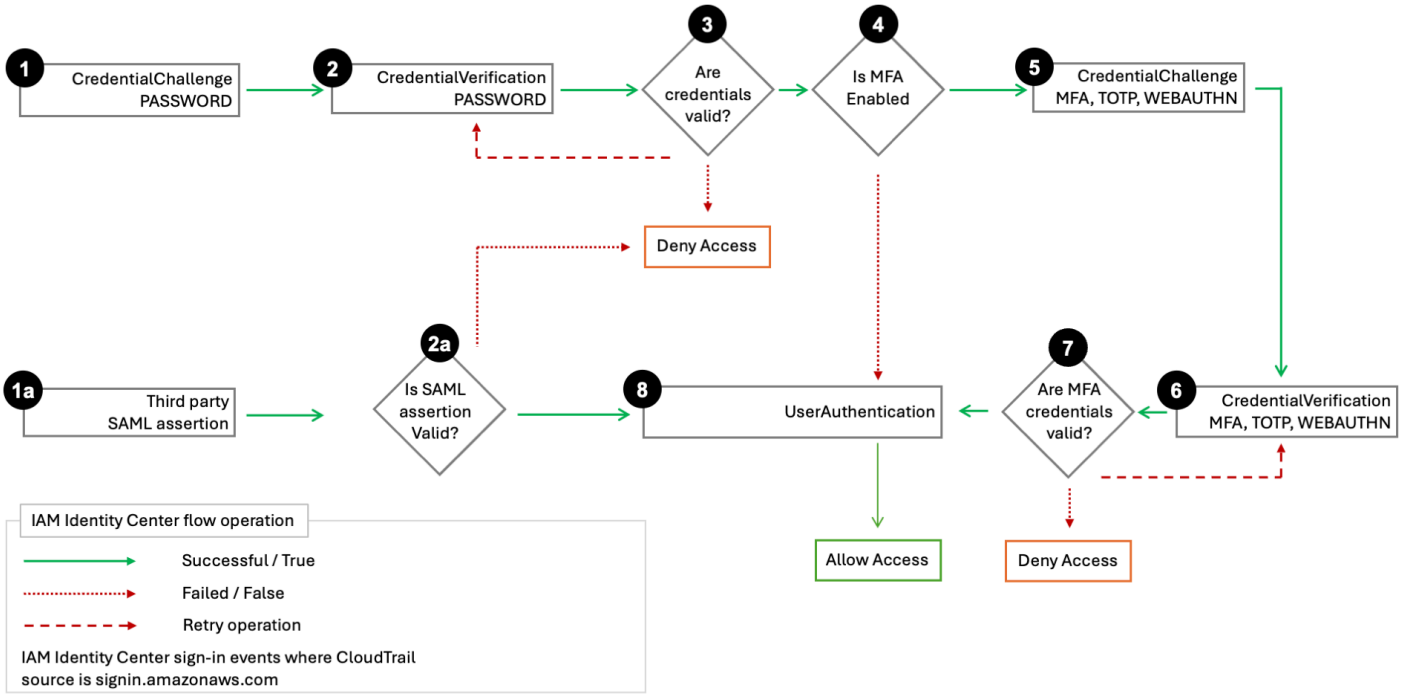
次の表は、特定のサインイン CloudTrail イベント内に含まれる追加の有用なイベントデータフィールドを示します。

フィールド	イベントの目的	サインインイベントの適用性	値の例
`AuthWorkflowID`	サインインシーケンス全体で発生するすべてのイベントを相関させるために使用されます。各ユーザーのサインインに対して、IAM Identity Center は複数のイベントを発行することができます。	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	"AuthWorkflowID": "9de74b32-8362-4a01-a524-de21df59fd83"
`CredentialType`	チャレンジされた認証またはファ	`CredentialChalleng`	「CredentialType」:「PASSWORD」ま

フィールド	イベントの目的	サインインイベントの適用性	値の例
	クターを指定するために使用されます。UserAuthentication イベントには、ユーザーのサインインーケンスで正常に検証された CredentialType 値がすべて含まれます。	e , CredentialVerification , UserAuthentication	たは「CredentialType」:「PASSWORD,TOTP」(可能な値は以下の通り: PASSWORD, TOTP, WEBAUTHN, EXTERNAL_IDP, RESYNC_TOTP, EMAIL_OTP)
DeviceEnrollmentRequired	サインイン時に MFA デバイスの登録が要求され、ユーザーがその要求を正常に完了したことを示すために使用されます。	UserAuthentication	「DeviceEnrollmentRequired」:「true」
LoginTo	サインインに成功した後のリダイレクト先を指定するために使用します。	UserAuthentication	「ログイン」:「https://mydirectory.awsapps.com/start/.....」

IAM アイデンティティセンターのサインインフローの CloudTrail イベント

次の図は、サインインフローとサインインが出力する CloudTrail イベントを示しています。



この図は、パスワードサインインフローとフェデレーションサインインフローを示しています。

ステップ 1~8 で構成されるパスワードサインインフローは、ユーザー名とパスワードのサインインプロセス中のステップを示しています。IAM アイデンティティセンターは `userIdentity.additionalEventData.CredentialType` を「`PASSWORD`」に設定し、IAM アイデンティティセンターは認証情報のチャレンジ-レスポンスサイクルを実行し、必要に応じて再試行します。

ステップの数は、ログインのタイプと多要素認証 (MFA) の有無によって異なります。初期プロセスでは、3 つまたは 5 つの CloudTrail イベントが生成され、`UserAuthentication` がシーケンスが終了することで認証が成功します。パスワード認証の試行に失敗すると、IAM アイデンティティセンターが通常の MFA 認証、または有効になっている場合は MFA 認証のために `CredentialChallenge` を再発行するため、追加の CloudTrail イベントが生成されます。

パスワードサインインフローでは、`CreateUser` API コールで新しく作成された IAM アイデンティティセンターユーザーがワンタイムパスワード (OTP) でサインインするシナリオについても説明します。このシナリオの認証情報タイプは「`EMAIL_OTP`」です。

ステップ 1a、2a、および 8 で構成されるフェデレーティッドサインインフローは、ID プロバイダーによって SAML アサーションが提供され、IAM アイデンティティセンターによって検証され、成功

すると UserAuthentication になるフェデレーティッド認証プロセスの主なステップを示しています。IAM アイデンティティセンターはステップ 3~7 で内部 MFA 認証シーケンスを呼び出しません。これは、外部のフェデレーティッド ID プロバイダーがすべてのユーザー認証情報認証を担当するためです。

サインイン CloudTrail イベントのユーザー名

IAM アイデンティティセンターは、IAM アイデンティティセンターユーザーのサインインに成功するたびに additionalEventData 要素の UserName フィールドを 1 回出力します。次のリストでは、範囲内の 2 つのサインインイベントと、これらのイベントが発生する条件について説明します。ユーザーがサインインしているときは、いずれかの条件のみが当てはまります。

- CredentialChallenge
  - CredentialType が「PASSWORD」の場合 — Directory Service または IAM アイデンティティセンターディレクトリ を使用したパスワード認証に適用されます。
  - CredentialType が「EMAIL_OTP」の場合 - CreateUser API コールで作成したユーザーが初めてサインインを試み、そのパスワードでサインインするためのワンタイムパスワードを 1 回受け取った場合にのみ IAM アイデンティティセンターディレクトリ に適用されます。
- UserAuthentication
  - CredentialType が「EXTERNAL_IDP」の場合 — 外部 IdP による認証に適用されます。

認証が成功した場合の UserName の値は次のとおりです。

- ID ソースが外部 IdP の場合、値は受信 SAML アサーションの nameID 値と等しくなります。この値は、IAM アイデンティティセンターディレクトリ の UserName フィールドと等しくなります。
- ID ソースが IAM アイデンティティセンターディレクトリ の場合、出力される値はこのディレクトリの UserName フィールドと等しくなります。
- ID ソースが Directory Service の場合、出力される値は、認証中にユーザーが入力したユーザー名と等しくなります。たとえば、ユーザー名が のユーザーはanyuser@company.com、anyuser、anyuser@company.com、または company.com/anyuser で認証できます。いずれの場合も、入力された値は CloudTrail でそれぞれ出力されます。

誤ったユーザー名試行のセキュリティマスキング

UserName フィールドには、記録されたイベントが正しくないユーザー名の入力によって引き起こされたコンソールサインインの失敗である場合、文字列 HIDDEN_DUE_TO_SECURITY_REASONS が

入ります。次の例のように、テキストに機密情報が含まれている可能性があるため、CloudTrail は、この場合コンテンツを記録しません。

- ユーザーが誤ってユーザー名フィールドにパスワードを入力した。
- ユーザーが、個人の E メールアカウント、銀行のサインイン ID、その他のプライベート ID のアカウント名を誤って入力した。

> **Tip**
>
> IAM Identity Center CloudTrail イベントの背後にあるユーザーを特定するには、`userId` と `identityStoreArn` を使用することをお勧めします。`userName` フィールドを使用する必要がある場合は、サインインに成功するたびに 1 回出力される `additionalEventData` 要素で `userName` を使用できます。

`UserName` フィールドの使用方法の詳細については、「同じユーザーセッション内のユーザーイベントの関連付け」を参照してください。

IAM Identity Center サインインシナリオのイベント例

次の例は、さまざまな AWS サインインシナリオで生成される一般的な CloudTrail イベントシーケンスを示しています。これらの例は、認証ログの解釈、セキュリティの問題の特定、認証ポリシーが正しく機能していることの確認に役立つ参照パターンとして機能します。

トピック

- パスワードのみで認証した場合のサインインの成功
- 外部の ID プロバイダーで認証した場合のサインインの成功
- パスワードとタイムベースドワンタイムパスワード (TOTP) 認証アプリケーションで認証した場合のサインインの成功
- 強制的な MFA の登録が必要な場合にパスワードと認証したサインインの成功
- パスワード認証が正しくないためにサインインに失敗しました

パスワードのみで認証した場合のサインインの成功

次の一連のイベントは、正常に完了したパスワードのみのサインインの例を示します。

CredentialChallenge (パスワード)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-07T20:33:58Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "UserName":"bobsmith@example.com",
      "CredentialType":"PASSWORD"
   },
   "requestID":"5be44ffb-6946-4f47-acaf-1adebd4afead",
   "eventID":"27ea7725-c1fd-4355-bdba-d0e628e0e604",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


正常に完了した CredentialVerification (パスワード)


```
{
   "eventVersion":"1.08",
```

```
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"c49640f6-0c8a-43d3-a6e0-900e3bb188d4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```


正常に完了した UserAuthentication (パスワードのみ)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
```

```
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```

外部の ID プロバイダーで認証した場合のサインインの成功

以下の一連のイベントは、外部の ID プロバイダを使用して SAML プロトコルで認証された場合のサインインの成功例を示しています。

正常に完了した UserAuthentication (外部 ID プロバイダ)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"EXTERNAL_IDP",
      "UserName":"bobsmith@example.com"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
```

```
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```

パスワードとタイムベースドワンタイムパスワード (TOTP) 認証アプリケーションで認証した場合のサインインの成功

次の一連のイベントは、サインイン時に多要素認証が必要で、ユーザーがパスワードと TOTP 認証アプリケーションを使ってサインインに成功した例を示しています。

CredentialChallenge (パスワード)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-08T20:40:13Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD",
      "UserName":"bobsmith@example.com"
```

```
   },
   "requestID":"e454ea66-1027-4d00-9912-09c0589649e1",
   "eventID":"d89cc0b5-a23a-4b88-843a-89329aeaef2e",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

正常に完了した CredentialVerification (パスワード)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-08T20:40:20Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
```

```
   "eventID":"4533fd49-6669-4d0b-b272-a0b2139309a8",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```


CredentialChallenge (TOTP)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-08T20:40:20Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
   "eventID":"29202f08-f240-40cc-b789-c0cea8a27847",
   "readOnly":false,
```

```
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

正常に完了した CredentialVerification (TOTP)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"e889ff1d-fcaf-454f-805d-7132cf2362a4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
```

```
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

正常に完了した UserAuthentication (パスワード + TOTP)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVLeFhWeDRmZFJmMmxHcWYwdzhZck5RQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11Fir1mCVJ-4Y5UY6RI10UCXvRePCHd6195xvYg1rwo1Pj7B-7UGIGlYUUVe31Nkzd7ihxKn6DMdnFfO01O8qc3RF
Sx-pjBXKG_jUcvBk_UILdGytV4o1u97h42B-
TA_6uwdmJiw1dcCz_Rv44d_BS0PkulW-5LVJy1oeP1H0FPPMeheyuk5Uy48d5of9-c\u0026wdc_csrf_token
\u003dNMlui44guoVnxRd0qu2tYJIdyyFPX6SDRNTspIScfMM0AgFbho1nvvCaxPTghHbgHCRIXdffFtzH0sL1ow419Bobn
\u0026organization\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD,TOTP"
```

```
   },
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"7a8c8725-db2f-488d-a43e-788dc6c73a4a",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```

強制的な MFA の登録が必要な場合にパスワードと認証したサインインの成功

次の一連のイベントは、ユーザーがサインインプロセスを確定する前に多要素認証 (MFA) を登録して正常に完了する必要があるパスワード認証の成功を示しています。

CredentialChallenge (パスワード)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-09T01:24:02Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
```

```
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD",
      "UserName":"bobsmith@example.com"
   },
   "requestID":"321f4b13-42b5-4005-a0f7-826cad26d159",
   "eventID":"8c707b0f-e45a-4a9c-bee2-ff68638d2f1b",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

正常に完了した CredentialVerification (パスワード)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-09T01:24:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
```

```
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD"
   },
   "requestID":"12b57efa-0a92-4479-91a3-5b6641817c21",
   "eventID":"783b0c89-7142-4942-8b84-6ee0de1b992e",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

正常に完了した UserAuthentication (パスワード + MFA 登録が必要)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"IdentityCenterUser",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "onBehalfOf": {
         "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
         "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
   },
   "eventTime":"2020-12-09T01:24:14Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
```

```
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVGQ3VqdHF5aW9CUDdrNXRTVTJUaWNnQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11eZ80S_maUsZ7ABETjeQhyWfvIHYz52rgR28sYAKN1oEk2G07czrwzXvE9HLlN2K9De8LyBEV83SFeDQfrWpkwXf
FJyJqkoGrt_w6rm_MpAn0uyrVq8udY EgU3fhOL3QWvWiquYnDPMyPmmy_qkZgR9rz__BI
\u0026wdc_csrf_token
\u003dJih9U62o5LQDtYLNqCK8a6xj0gJg5BRWq2tbl75y8vAmwZhAqrgrgbxXat2M646UZGp93krw7WYQdHIgi5OYI9QSc
\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD",
      "DeviceEnrollmentRequired":"true"
   },
   "requestID":"74d24604-a365-4237-8c4a-350795494b92",
   "eventID":"a15bf257-7f37-46c0-b67c-fea5fa6166be",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


パスワード認証が正しくないためにサインインに失敗しました

次の一連のイベントは、ユーザーがユーザー名を正常に入力したがパスワード検証ステップに失敗したため、サインインに失敗した認証試行を示しています。

CredentialChallenge (パスワード)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
   },
   "eventTime":"2020-12-08T18:56:15Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
```

```
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
      "CredentialType":"PASSWORD",
      "UserName":"bobsmith@example.com"
   },
   "requestID":"f54848ea-b1aa-402f-bf0d-a54561a2ffcc",
   "eventID":"d96f1d6c-dbd9-4a0b-9a45-6a2b66078c78",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

失敗した CredentialVerification (パスワード)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
   },
   "eventTime":"2020-12-08T18:56:21Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
      "CredentialType":"PASSWORD"
```

```
    },
    "requestID":"04528c82-a678-4a1f-a56d-ea2c6445a72a",
    "eventID":"9160fe06-fc2a-474f-9b78-000ee067a09d",
    "readOnly":false,
    "eventType":"AwsServiceEvent",
    "managementEvent":true,
    "eventCategory":"Management",
    "recipientAccountId":"111122223333",
    "serviceEventDetails":{
       "CredentialVerification":"Failure"
    }
}
```


AWS CloudTrail を使用した IAM アイデンティティセンター SCIM API コールのログ記録

IAM アイデンティティセンター SCIM は、ユーザー、ロール、または AWS のサービス によって実行されるアクションの記録を提供するサービスである AWS CloudTrail と統合されています。CloudTrail は、SCIM の API コールをイベントとしてキャプチャします。CloudTrail によって収集される情報を使用することで、リクエストされたアクション、アクションの日付と時刻、リクエストパラメータなどに関する情報を確認できます。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。

> **Note**
>
> CloudTrail は、AWS アカウント を作成すると、その中で有効になります。ただし、トークンが 2024 年 9 月より前に作成された場合は、SCIM からのイベントを確認するためにアクセストークンをローテーションする必要がある場合があります。
> 詳細については、「アクセストークンをローテーションする」を参照してください。

SCIM は、以下のオペレーションを CloudTrail のイベントとして記録する口グをサポートしています。

- CreateGroup
- CreateUser
- DeleteGroup
- DeleteUser

- GetGroup
- GetSchema
- GetUser
- ListGroups
- ListResourceTypes
- ListSchemas
- ListUsers
- PatchGroup
- PatchUser
- PutUser
- ServiceProviderConfig

の CloudTrail イベントの例

次の例は、IAM アイデンティティセンターでの SCIM オペレーション中に生成される一般的な CloudTrail イベントログを示しています。これらの例は、成功したオペレーションと一般的なエラーシナリオのイベントの構造と内容を示し、SCIM プロビジョニングの問題をトラブルシューティングするときに CloudTrail ログを解釈する方法を理解するのに役立ちます。

正常な **CreateUser** オペレーション

この CloudTrail イベントは、SCIM API を通じて正常に実行された `CreateUser` オペレーションを示します。イベントは、リクエストパラメータ (機密情報がマスクされている) と、新しく作成されたユーザーの ID を含むレスポンス要素の両方をキャプチャします。このタイプのイベントは、ID プロバイダーが SCIM プロトコルを使用して IAM アイデンティティセンターに新しいユーザーを正常にプロビジョニングしたときに生成されます。

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "WebIdentityUser",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "CreateUser",
```

```
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "requestParameters": {
    "httpBody": {
      "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "schemas" : [
        "urn:ietf:params:scim:schemas:core:2.0:User"
      ],
      "name": {
        "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
      },
      "active": true,
      "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "tenantId": "xxxx"
  },
  "responseElements": {
    "meta" : {
      "created" : "Oct 10, 2024, 1:23:45 PM",
      "lastModified" : "Oct 10, 2024, 1:23:45 PM",
      "resourceType" : "User"
    },
    "displayName" : "HIDDEN_DUE_TO_SECURITY_REASONS",
    "schemas" : [
      "urn:ietf:params:scim:schemas:core:2.0:User"
    ],
    "name": {
      "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "active": true,
    "id" : "c4488478-a0e1-700e-3d75-96c6bb641596",
    "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "requestID": "xxxx",
  "eventID": "xxxx",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
```

```
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
  }
}
```

失敗した **PatchGroup** オペレーション: 必須のパス属性がありません

この CloudTrail イベントは、失敗した PatchGroup オペレーションがValidationException を引き起こし、エラーメッセージ "Missing path in PATCH request" が発生したことを示します。PATCH オペレーションで、変更するグループ属性を指定するためのパス属性が必要なため、エラーが発生しましたが、この属性がリクエストにありませんでした。

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchGroup",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ValidationException",
  "errorMessage": "Missing path in PATCH request",
  "requestParameters": {
    "httpBody": {
      "operations": [
        {
          "op": "REMOVE",
          "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
        }
      ],
      "schemas": [
        "HIDDEN_DUE_TO_SECURITY_REASONS"
      ]
    },
    "tenantId": "xxxx",
    "id": "xxxx"
  },
  "responseElements": null,
  "requestID": "xxxx",
```

```
  "eventID": "xxxx",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
  }
}
```

失敗した **CreateGroup** オペレーション: グループ名は既に存在します

この CloudTrail イベントは、失敗した CreateGroup オペレーションがConflictException を引き起こし、エラーメッセージ "Duplicate GroupDisplayName" が発生したことを示します。このエラーは、IAM アイデンティティセンターに既に存在する表示名を持つグループを作成しようとすると発生します。ID プロバイダーは、新しいグループを作成する代わりに、一意のグループ名を使用するか、既存のグループを更新する必要があります。

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "CreateGroup",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ConflictException",
  "errorMessage": "Duplicate GroupDisplayName",
  "requestParameters": {
    "httpBody": {
      "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "tenantId": "xxxx"
  },
  "responseElements": null,
  "requestID": "xxxx",
  "eventID": "xxxx",
```

```
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
  }
}
```

失敗した **PatchUser** オペレーション: 複数の E メールアドレスはサポートされていません

この CloudTrail イベントは、失敗した PatchUser オペレーションがValidationException を引き起こし、エラーメッセージ "List attribute emails exceeds allowed limit of 1" が発生したことを示します。このエラーは、IAM アイデンティティセンターがユーザーごとに 1 つの E メールアドレスのみをサポートしているため、ユーザーに複数の E メールアドレスを割り当てるときに発生します。ID プロバイダーは、ユーザーごとに 1 つの E メールアドレスのみを送信するように SCIM マッピングを設定する必要があります。

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ValidationException",
  "errorMessage": "List attribute emails exceeds allowed limit of 1",
  "requestParameters": {
    "httpBody": {
      "operations": [
        {
          "op": "REPLACE",
          "path": "emails",
          "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
        }
      ],
```

```
      "schemas": [
        "HIDDEN_DUE_TO_SECURITY_REASONS"
      ]
    },
    "tenantId": "xxxx",
    "id": "xxxx"
  },
  "responseElements": null,
  "requestID": "xxxx",
  "eventID": "xxxx",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
  }
}
```


IAM アイデンティティセンターでの一般的な SCIM API 検証エラー

IAM アイデンティティセンターで SCIM API を使用する場合、CloudTrail イベントには一般的に次の検証エラーメッセージが表示されます。これらの検証エラーは通常、ユーザーおよびグループのプロビジョニングオペレーション中に発生します。

これらのエラーを解決し、SCIM プロビジョニングを適切に設定するための詳細なガイダンスについては、このAWS re:Post 記事を参照してください。

- 「リスト属性の E メールが 1 件の上限を超えています」
- 「リスト属性のアドレスは、1 つまでに制限されています」
- 「1 つの検証エラーが検出されました: '*name.familyName*' の値が制約を満たしませんでした: メンバー名は次の正規表現パターンを満たす必要があります: [\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r]+」
- 「2 つの検証エラーが検出されました: 'name.familyName' の値が制約を満たしませんでした: メンバー名の長さは 1 以上である必要があります。 'name.familyName' の値が制約を満たしませんでした: メンバー名は次の正規表現パターンを満たす必要があります: [\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r]+」
- 「2 つの検証エラーが検出されました: 'urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.manager.value' の値

が制約を満たしませんでした: メンバー名の長さは 1 以上である必要があります。'urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.manager.value' の値が制約を満たしませんでした: メンバー名は次の正規表現パターンを満たす必要があります: [\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r]+"、」

- RequestBody からの無効な JSON
- 無効なフィルター形式

アプリケーションコンポーネントを Amazon EventBridge に接続する

IAM アイデンティティセンターを Amazon EventBridge と統合すると、CloudTrail イベントに記録された特定の IAM アイデンティティセンターアクションに応じて、管理通知を開始するイベントを発生させたり、自動ワークフローを呼び出すイベントを生成したりできます。

たとえば、ユーザーがアプリケーションを削除したとき、または IAM アイデンティティセンターが新しいグループを作成するときに検出するように EventBridge ルールを設定できます。ユースケースに応じて、これらのイベントを Amazon SNS トピックにルーティングして管理者に通知するか、AWS Lambda、Step Functions、またはその他の EventBridge がサポートするサービスを使用して追加のオートメーションを呼び出すことができます。

設定可能な AD 同期エラーのログ記録

設定可能な Active Directory (AD) 同期設定でログ記録を有効にして、同期プロセス中に発生する可能性のあるエラーに関する情報を含むログを得られます。これらのログを使用することで、設定可能な AD 同期に問題があるかどうかをモニタリングし、必要に応じてアクションを実行できます。Amazon S3 バケットと Firehose では、アカウント間の配信がサポートされており、Amazon CloudWatch Logs ロググループ、Amazon Simple Storage Service (Amazon S3) バケット、Amazon Data Firehose にログを送信できます。

制限、権限、Vended Logs の詳細については、「Enabling logging from AWS のサービス」を参照してください。

> **Note**
>
> ログ記録には料金がかかります。詳細については、「Amazon CloudWatch Pricing」ページの「Vended Logs」を参照してください。

設定可能な AD 同期エラーログを有効にするには

1. IAM アイデンティティセンターコンソールにサインインします。
2. [設定] を選択します。
3. [設定] ページで [ID ソース] タブを選択して [アクション] を選択し、次に [ログの管理] を選択します。
4. [ログ配信の追加] と、次のいずれかの送信先タイプを選択します。
   a. [Amazon CloudWatch Logs へ] を選択します。次に、送信先ロググループを選択または入力します。
   b. [Amazon S3 へ] を選択します。次に、送信先バケットを選択または入力します。
   c. [Firehose へ] を選択します。次に、送信先配信ストリームを選択または入力します。
5. [Submit] を選択してください。

設定可能な AD 同期エラーログを無効にするには

1. IAM アイデンティティセンターコンソールにサインインします。
2. [設定] を選択します。
3. [設定] ページで [ID ソース] タブを選択して [アクション] を選択し、次に [ログの管理] を選択します。
4. 削除したい送信先について [削除] を選択します。
5. [Submit] を選択してください。

設定可能な AD 同期エラーログフィールド

発生する可能性のあるエラーログフィールドについては、次のリストを参照してください。

`sync_profile_name`

同期プロファイルの名前。

`error_code`

発生したエラーのタイプを表すエラーコード。

`error_message`

発生したエラーに関する詳細情報を含むメッセージ。

`sync_source`

同期ソースは、エンティティが同期される場所を示します。IAM アイデンティティセンターの場合、これは Directory Service によって管理される Active Directory (AD) です。同期ソースには、影響を受けるディレクトリのドメインと ARN が含まれます。

`sync_target`

同期ターゲットは、エンティティが保存される送信先です。IAM アイデンティティセンターの場合、これは ID ストアです。同期ターゲットには、影響を受ける Identity Store ARN が含まれます。

`source_entity_id`

エラーの原因となったエンティティを表す一意の識別子。IAM アイデンティティセンターの場合、これはエンティティの SID です。

`source_entity_type`

エラーの原因となったエンティティのタイプ。ここには、`USER` または `GROUP` が表示されます。

`eventTimestamp`

エラー発生時のタイムスタンプ。

設定可能な AD 同期エラーログの例

例 1: AD ディレクトリのパスワード期限切れのエラーログ

```
{
    "sync_profile_name": "EXAMPLE-PROFILE-NAME",
    "error" : {
        "error_code": "InvalidDirectoryCredentials",
        "error_message": "The password for your AD directory has expired. Please reset
 the password to allow Identity Sync to access the directory."
    },
    "sync_source": {
        "arn": "arn:aws:ds:us-east-1:123456789:directory/d-123456",
        "domain": "EXAMPLE.com"
    },
    "eventTimestamp": "1683355579981"
}
```

例 2: 一意でないユーザー名を持つユーザーのエラーログ

```
{
    "sync_profile_name": "EXAMPLE-PROFILE-NAME",
    "error" : {
        "error_code": "ConflictError",
        "error_message": "The source entity has a username conflict with the sync
 target. Please verify that the source identity has a unique username in the target."
    },
    "sync_source": {
        "arn": "arn:aws:ds:us-east-1:111122223333:directory/d-123456",
        "domain": "EXAMPLE.com"
    },
    "sync_target": {
        "arn": "arn:aws:identitystore::111122223333:identitystore/d-123456"
    },
    "source_entity_id": "SID-1234",
    "source_entity_type": "USER",
    "eventTimestamp": "1683355579981"
}
```

IAM Identity Center のコンプライアンス検証

サードパーティーの監査人は、AWS IAM アイデンティティセンター のような複数の AWS コンプライアンスプログラムの一環として AWS のサービス のセキュリティとコンプライアンスを評価します。

新しい AWS サインアップエクスペリエンスは、規制対象ワークロード向けには設計されていません。新しい AWS サインアップエクスペリエンスを使用しているものの、規制対象ワークロードに AWS を使用する場合は、AWS (高度) にサインアップしたり、AWS 環境の高度な機能をアクティブ化したりできます。

AWS のサービスが特定のコンプライアンスプログラムの対象であるかどうかを確認するには、「コンプライアンスプログラムによる対象範囲内の AWS のサービス」を参照して、関心のあるコンプライアンスプログラムを選択してください。一般的な情報については、AWSコンプライアンスプログラム を参照してください。

AWS Artifact を使用して、サードパーティの監査レポートをダウンロードできます。詳細については、「AWS Artifact でレポートをダウンロードする」「」を参照してください。

AWS のサービスを使用する際のお客様のコンプライアンス責任は、お客様のデータの機密性や貴社のコンプライアンス目的、適用可能な法律および規制によって決定されます。AWS のサービス を使

用する際のコンプライアンス責任の詳細については、「AWS セキュリティドキュメント」を参照してください。

サポートされるコンプライアンス標準

IAM Identity Center は、以下の標準について監査済みであり、コンプライアンスの認定を取得する必要があるソリューションの一部として使用できます。



AWS は、医療保険の相互運用性と説明責任に関する法令 (HIPAA) のコンプライアンスプログラムを拡張し、HIPAA 対応サービス として IAM Identity Center を含めています。

AWS では、医療情報の処理や保存に AWS のサービス の活用を検討する顧客向けに、HIPAA 関連のホワイトペーパーも用意しています。詳細については、「HIPAA コンプライアンス」を参照してください。



オーストラリア政府の顧客は、情報セキュリティ登録評価プログラム (IRAP) を使用して、適切なコンプライアンス管理が行われていることを検証し、オーストラリアサイバーセキュリティセンター (ACSC) が作成したオーストラリア政府情報セキュリティマニュアル (ISM) の要件に対応する適切な責任モデルを決定することができます。詳細については、IRAP リソースを参照してください。



IAM Identity Center は、支払いカード業界 (PCI) のデータセキュリティ標準 (DSS) バージョン 3.2、サービスプロバイダーレベル 1 で準拠証明書を取得しています。

AWS の製品やサービスを使用してカード所有者のデータを保存、処理、転送するユーザーは、各自の PCI DSS 準拠認定の管理に IAM Identity Center を使用できます。

- Active Directory
- 外部 ID プロバイダー

	IAM Identity Center の ID ソースは、現在 PCI DSS に準拠していません。 PCI DSS の詳細 (AWS PCI Compliance Package のコピーをリクエストする方法など) については、「PCI DSS level 1」を参照してください。
	System and Organization Control (SOC) レポートとは、重要なコンプライアンスの統制および目標を IAM Identity Center がどのように達成したかを実証する、独立した第三者による審査報告書です。これらのレポートは、管理者と監査人が、運用とコンプライアンスの管理をどのようにサポートしているかを理解するのに役立ちます。SOC レポートには、次の 3 つのタイプがあります。 • AWS SOC 1 レポート - AWSアーティファクト付きダウンロード • AWS SOC 2: セキュリティ、可用性、機密性レポート - AWSアーティファクト付きダウンロード • AWS SOC 3: セキュリティ、可用性、機密保持に関するレポート IAM Identity Center は、AWS SOC 1、SOC 2、および SOC 3 レポートの対象範囲内です。詳細については、「SOC Compliance」(SOC コンプライアンス) を参照してください。

IAM Identity Center の障害への耐性

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

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

AWS IAM アイデンティティセンター の耐性については、「復元力設計とリージョンごとの動作」を参照してください。

IAM Identity Center でのインフラストラクチャのセキュリティ

マネージドサービスである AWS IAM アイデンティティセンター 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 AWS がインフラストラクチャを保護する方法については、「AWSクラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、セキュリティの柱 - AWS Well-Architected Framework の インフラストラクチャ保護 を参照してください。

AWS が公開した API コールを使用して、ネットワーク経由で IAM Identity Center にアクセスします。クライアントは次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。

IAM アイデンティティセンターでのデータ保護

AWS IAM アイデンティティセンター でのデータ保護に AWS 責任共有モデルを適用する方法について説明します。このモデルで定義されるように、AWS は、すべての AWS クラウドを実行するグローバルなインフラストラクチャの保護に責任を負います。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービスのセキュリティ設定と管理タスクにも責任があります。データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログ に投稿された「AWS 責任共有モデルおよび GDPR」ブログを参照してください。

次の方法でデータを保護することをお勧めします。

- IAM アイデンティティセンターで多要素認証 (MFA) を使用します。
- TLS を使用して AWS リソースと通信します。TLS 1.2 は必須ですが、TLS 1.3 を推奨します。
- AWS CloudTrail で API とユーザーアクティビティロギングを設定します。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「AWS CloudTrail ユーザーガイド」の「CloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションを AWS のサービス内のすべてのデフォルトのセキュリティ管理と一緒に使用します。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、API、AWS CLI、または AWS SDK で AWS IAM アイデンティティセンター または他の AWS のサービスを使用する場合も同様です。タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、診断ログに使用される場合があります。

転送中の暗号化

IAM アイデンティティセンターは、Transport Layer Security (TLS) 1.2 または TLS 1.3 暗号化プロトコルを使用してすべてのネットワーク間データを自動的に暗号化することにより、サービスに出入りする転送中のデータを保護します。IAM で認証され、IAM アイデンティティセンター API、アイデンティティセンター API、または OIDC API に送信される直接 HTTPS リクエストは、AWS 署名バージョン 4 アルゴリズムを使用して署名され、安全な接続を確立します。

データプライバシー

IAM アイデンティティセンターを利用すれば、組織のデータを常に管理できます。IAM アイデンティティセンターに保存されているユーザー ID とグループ ID は、IAM アイデンティティセンターで有効にし、かつそれらの AWS サービスで必要な場合に限り、AWS マネージドアプリケーションなどの他のサービスと共有されます。

詳細については、「AWS データプライバシーのよくある質問」を参照してください。

データ保持

IAM アイデンティティセンターは、ユーザーとグループの ID、メタデータなどのデータを、サービスから削除するまで保存します。IAM アイデンティティセンターインスタンスを削除すると、それに含まれるデータも削除されます。

保管中の暗号化

IAM アイデンティティセンターは、次のキータイプを使用して保管中の顧客データを保護するための暗号化を提供します。

- AWS 所有のキー (デフォルトキータイプ) — IAM アイデンティティセンターは、デフォルトでこれらのキーを使用してデータを自動的に暗号化します。AWS 所有キーの使用状況を表示、管理、監査したり、他の目的で使用したりすることはできません。IAM アイデンティティセンターは、ユーザーがアクションを実行することなく、データの安全性を維持するためにキー管理を完全に処理します。詳細については、「AWS Key Management Service デベロッパーガイド」の「AWS 所有キー」を参照してください。
- カスタマーマネージドキー — IAM アイデンティティセンターの組織インスタンスでは、ユーザー属性やグループ属性などのワークフォース ID データの保管時の暗号化用に対称カスタマーマネージドキーを選択できます。これらの暗号化キーを作成、所有、管理します。この暗号化層はユーザーが完全に制御できるため、次のようなタスクを実行できます。
  - キーへのアクセスを、IAM アイデンティティセンターや 同じ AWS Organizations 内の AWS マネージドアプリケーション など、アクセスを必要とする IAM プリンシパルとその管理者のみに制限するキーポリシーを確立および維持します。
  - クロスアカウントアクセスを含むキーへのアクセスのための IAM ポリシーの確立と維持
  - キーポリシーの有効化と無効化
  - キー暗号化マテリアルのローテーション
  - キーアクセスを必要とするデータへのアクセスの監査
  - タグの追加

- キーエイリアスの作成
- 削除のためのキースケジューリング

IAM アイデンティティセンターでカスタマーマネージド KMS キーを実装する方法については、「AWS IAM アイデンティティセンター でのカスタマーマネージド KMS キーの実装」を参照してください。カスタマーマネージドキーの詳細については、「AWS Key Management Service デベロッパーガイド」の「カスタマーマネージドキー」を参照してください。

> **Note**
>
> IAM アイデンティティセンターでは、AWS 所有の KMS キーを使用した保管中の暗号化が自動的に有効になり、顧客データを無料で保護します。ただし、カスタマーマネージドキーを使用する際には AWS KMS 料金が適用されます。料金の詳細については、「AWS Key Management Service 料金」を参照してください。

カスタマーマネージドキーの実装に関する考慮事項:

- 専用キー: 既存のキーを再利用するのではなく、IAM アイデンティティセンターインスタンスごとに新しいカスタマーマネージド KMS キーを作成することをお勧めします。このアプローチは、職務の分離を明確にし、アクセスコントロール管理を簡素化し、セキュリティ監査をより簡単にします。専用キーを使用すると、キー変更の影響を単一の IAM アイデンティティセンターインスタンスに制限することで、リスクも軽減されます。
- 複数の AWS リージョンにまたがる IAM Identity Center を使用する: IAM Identity Center インスタンスを追加の AWS リージョンにレプリケートする場合は、保管中の暗号化にカスタマーマネージド KMS キーを使用する必要があります。デフォルトの AWS 所有 KMS キータイプは、マルチリージョン IAM Identity Center ではサポートされていません。詳細については、「複数の 間で IAM アイデンティティセンターを使用するAWS リージョン」を参照してください。

> **Note**
>
> IAM アイデンティティセンターは、従業員 ID データの暗号化にエンベロープ暗号化を使用します。KMS キーは、データの暗号化に実際に使用されるデータキーを暗号化するラッピングキーの役割を果たします。

AWS KMS の詳細については、「 AWS Key Management Service とは」を参照してください。

IAM アイデンティティセンターの暗号化コンテキスト

暗号化コンテキストとは、データに関する追加のコンテキスト情報を含むオプションの非秘密のキーと値のペアのセットです。AWS KMS は、暗号化コンテキストを追加の認証済みデータとして使用し、暗号化の認証をサポートします。データの暗号化リクエストに暗号化コンテキストを組み込むと、AWS KMS は暗号化コンテキストを暗号化後のデータにバインドします。データを復号化するには、そのリクエストに (暗号化時と) 同じ暗号化コンテキストを含めます。暗号化の詳細については、「AWS KMS デベロッパーガイド」を参照してください。

IAM アイデンティティセンターは、aws:sso:instance-arn、aws:identitystore:identitystore-arn、tenant-key-id の暗号化コンテキストキーを使用します。例えば、次の暗号化コンテキストは、IAM アイデンティティセンター API によって呼び出される AWS KMS API オペレーションに表示されます。

```
"encryptionContext": {
    "tenant-key-id": "ssoins-1234567890abcdef",
    "aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-1234567890abcdef"
}
```

次の暗号化コンテキストは、アイデンティティセンター API によって呼び出される AWS KMS API オペレーションに表示されます。

```
"encryptionContext": {
    "tenant-key-id": "12345678-1234-1234-1234-123456789012",
    "aws:identitystore:identitystore-arn":
 "arn:aws:identitystore::123456789012:identitystore/d-1234567890"
}
```

暗号化コンテキストを使用して顧客マネージドキーへのアクセスを制御する

対称カスタマーマネージドキー (CMK) へのアクセスを制御するための条件として、キーポリシーと IAM ポリシー内の暗号化コンテキストを使用することもできます。高度な KMS キーポリシーステートメント の一部のキーポリシーテンプレートには、キーが特定の IAM アイデンティティセンターインスタンスでのみ使用されるように、このような条件が含まれています。

IAM アイデンティティセンターの暗号化キーのモニタリング

カスタマーマネージド KMS キーを IAM アイデンティティセンターインスタンスで使用する場合、AWS CloudTrail または Amazon CloudWatch Logs を使用して、IAM アイデンティティセンターから AWS KMS に送信されたリクエストを追跡できます。IAM アイデンティティセンターが呼び出す KMS API オペレーションは、ステップ 2: KMS キーポリシーステートメントを準備する に記載されています。これらの API オペレーションの CloudTrail イベントには暗号化コンテキストが含まれており、IAM アイデンティティセンターインスタンスによって呼び出された AWS KMS API オペレーションをモニタリングして、カスタマーマネージドキーによって暗号化されたデータにアクセスできます。

AWS KMS API オペレーションの CloudTrail イベントの暗号化コンテキストの例:

```
{
"requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "encryptionContext": {
            "aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-xxxxxxxxxxxxxxxx",
            "tenant-key-id": "ssoins-xxxxxxxxxxxxxxxx"
        }
    }
}
```

AWS マネージドアプリケーションの IAM アイデンティティセンター ID 属性のストレージ、暗号化、削除

AWS Systems Manager や Amazon CodeCatalyst など、AWS IAM アイデンティティセンター でデプロイする一部の AWS マネージドアプリケーションは、IAM アイデンティティセンターの特定のユーザー属性とグループ属性を独自のデータストアに保存します。IAM アイデンティティセンターのカスタマーマネージド KMS キーによる保管時の暗号化は、AWS マネージドアプリケーションに保存されている IAM アイデンティティセンターのユーザー属性とグループ属性には適用されません。 AWS マネージドアプリケーションは、保存するデータに対してさまざまな暗号化方法をサポートしています。最後に、IAM アイデンティティセンター内のユーザー属性とグループ属性を削除すると、これらの AWS マネージドアプリケーションは、削除後にこの情報を IAM アイデンティティセンターに引き続き保存することがあります。アプリケーションに保存されているデータの暗号化とセキュリティについては、AWS マネージドアプリケーションのユーザーガイドを参照してください。

AWS IAM アイデンティティセンター でのカスタマーマネージド KMS キーの実装

カスタマーマネージドキーは AWS Key Management Service のキーで、その作成、所有、管理をユーザーが行います。AWS IAM アイデンティティセンターで保管時の暗号化用のカスタマーマネージド KMS キーを実装するには、次の手順に従います。

> **Important**
>
> 一部の AWS マネージドアプリケーションは、カスタマーマネージド AWS KMS キーで設定された IAM アイデンティティセンターでは使用できません。「AWSIAM アイデンティティセンターで使用できる マネージドアプリケーション」を参照してください。

1. ステップ 1: 組織のユースケースを特定する - KMS キーを使用するための正しいアクセス許可を定義するには、組織全体の関連するユースケースを特定する必要があります。KMS キーのアクセス許可は、適切な IAM プリンシパルが特定のユースケースで KMS キーを使用できるように連携する KMS キーポリシーステートメントと ID ベースのポリシーで構成されます。
2. ステップ 2: KMS キーポリシーステートメントを準備する - ステップ 1 で特定したユースケースに基づいて関連する KMS キーポリシーステートメントテンプレートを選択し、必要な識別子と IAM プリンシパル名を入力します。ベースライン KMS キーポリシーステートメントから開始し、セキュリティポリシーで必要な場合は、「アドバンスト KMS キーポリシーステートメント」の説明に従って絞り込みます。
3. ステップ 3: カスタマーマネージド KMS キーを作成する - IAM Identity Center 要件を満たす AWS KMS で KMS キーを作成し、ステップ 2 で準備した KMS キーポリシーステートメントを KMS キーポリシーに追加します。
4. ステップ 4: KMS キーをクロスアカウントで使用するように IAM ポリシーを設定する - ステップ 1 で特定したユースケースに基づいて関連する IAM ポリシーステートメントテンプレートを選択し、キー ARN を入力して使用できるように準備します。次に、準備された IAM ポリシーステートメントをプリンシパルの IAM ポリシーに追加することで、特定ユースケースそれぞれの IAM プリンシパルがアカウント間で KMS キーを使用できるようにします。
5. ステップ 5: IAM アイデンティティセンターで KMS キーを設定する - IAM アイデンティティセンターインスタンスのカスタマーマネージド KMS キーを有効にして、保管時の暗号化に使用します。

ステップ 1: 組織のユースケースを特定する

カスタマーマネージド KMS キーを作成して設定する前に、ユースケースを特定し、必要な KMS キーのアクセス許可を準備します。KMS キーポリシーの詳細については、「AWS KMS デベロッパーガイド」を参照してください。

IAM アイデンティティセンターサービス API を呼び出す IAM プリンシパルには、 アクセス許可が必要です。たとえば、委任管理者は、アクセス許可セットポリシーを使用してこれらの API を使用するアクセス許可を付与できます。IAM アイデンティティセンターがカスタマーマネージドキーで設定されている場合、IAM プリンシパルには、IAM アイデンティティセンターサービス API を介して KMS API を使用するアクセス許可も必要です。これらの KMS API アクセス許可は、KMS キーポリシーと IAM プリンシパルに関連付けられた IAM ポリシーの 2 つの場所で定義します。

KMS キーのアクセス許可は、以下で構成されます。

1. ステップ 3: カスタマーマネージド KMS キーを作成する での作成時に KMS キーで指定した KMS キーポリシーステートメント。
2. KMS キーの作成後に ステップ 4: KMS キーをクロスアカウントで使用するように IAM ポリシーを設定する で指定した IAM プリンシパルの IAM ポリシーステートメント。

次の表は、KMS キーを使用するためのアクセス許可を必要とする関連するユースケースと IAM プリンシパルを示しています。

ユースケース	KMS キーを使用するためのアクセス許可が必要な IAM プリンシパル	必須/オプション
AWS IAM アイデンティティセンターの使用	• AWS IAM アイデンティティセンターの管理者 • IAM アイデンティティセンターサービスおよび関連する ID ストアサービス	必須
IAM アイデンティティセンターによる AWS マネージドアプリケーションの使用	• AWS マネージドアプリケーションの管理者 • AWS マネージドアプリケーション • AWS マネージドアプリケーションが IAM アイデンティティセンター	オプションです。

ユースケース	KMS キーを使用するためのアクセス許可が必要な IAM プリンシパル	必須/オプション
	サービス API を呼び出すために引き受けるサービスロール	
有効化された AWS IAM アイデンティティセンターインスタンスでの AWS Control Tower の使用	• AWS Control Tower 管理者	オプションです。
AWS IAM Identity Center を使用した Amazon EC2 インスタンスへの SSO	• Amazon EC2 インスタンスへの SSO の実行を許可された IAM プリンシパル	オプションです。
カスタマーマネージドアプリケーション、アクセス許可セットプロビジョニングワークフロー、AWS Lambda 関数など、IAM プリンシパルを使用して IAM アイデンティティセンターサービス API を呼び出すその他のユースケース	• これらのワークフローで IAM アイデンティティセンターサービス API を呼び出すために使用される IAM プリンシパル	オプションです。

> **Note**
>
> テーブルにリストされている複数の IAM プリンシパルには、AWS KMS API アクセス許可が必要です。ただし、IAM アイデンティティセンターでユーザーとグループのデータを保護するために、IAM アイデンティティセンターと ID ストアのサービスのみが AWS KMS API を直接呼び出します。

ステップ 2: KMS キーポリシーステートメントを準備する

「ベースライン KMS キーポリシー」から始めて、組織に合わせてカスタマイズします。セキュリティ要件に基づいてより具体的なポリシーが必要な場合は、「高度な KMS キーポリシーステートメント」の例を使用してポリシーステートメントを変更できます。この決定に関するガイダンスについては、「ベースラインとアドバンスト KMS キーポリシーステートメントの選択に関する考慮事項」を参照してください。

1. ベースラインポリシーをエディタにコピーし、必要な識別子と IAM プリンシパル名を KMS キーポリシーステートメントに挿入します。参照される識別子の値を見つける方法については、「必要な識別子の検索場所」を参照してください。
2. セキュリティ要件で求められている場合は、「高度な KMS キーポリシーステートメント」の例を使用してポリシーステートメントを微調整します。

> **Important**
>
> IAM アイデンティティセンターで既に使用されているキーの KMS キーポリシーを変更するときは注意が必要です。IAM アイデンティティセンターは、最初に KMS キーを設定するときに暗号化と復号のアクセス許可を検証しますが、それ以降のポリシー変更を検証することはできません。必要なアクセス許可を誤って削除すると、IAM アイデンティティセンターの通常のオペレーションが中断される可能性があります。IAM アイデンティティセンターのカスタマーマネージドキーに関連する一般的なエラーのトラブルシューティングのガイダンスについては、「AWS IAM アイデンティティセンター でのカスタマーマネージドキーのトラブルシューティング」を参照してください。

> **Note**
>
> IAM および関連する ID ストアには、カスタマーマネージド KMS キーを使用するためのサービスレベルのアクセス許可が必要です。この要件は、サービス認証情報を使用して IAM アイデンティティセンターサービス API を呼び出す AWS マネージドアプリケーションにも適用されます。転送アクセスセッションで IAM アイデンティティセンターサービス API が呼び出されるその他のユースケースでは、開始する IAM プリンシパル (管理者など) にのみ KMS キーのアクセス許可が必要です。特に、 AWS アクセスポータルと AWS マネージドアプリケーションを使用するエンドユーザーは、それぞれのサービスを通じて付与されるため、直接 KMS キーのアクセス許可を必要としません。

ステップ 3: カスタマーマネージド KMS キーを作成する

AWS 管理コンソールまたは AWS KMS API を使用して、カスタマーマネージドキーを作成できます。キーの作成中に、ステップ 2 で準備した KMS キーポリシーステートメントを KMS キーポリシーに追加します。デフォルトの KMS キーポリシーに関するガイダンスを含む詳細な手順については、「AWS Key Management Service デベロッパーガイド」を参照してください。

キーは次の要件を満たしている必要があります。

- KMS キーは IAM アイデンティティセンターインスタンスと同じ AWS リージョンに存在する必要があります。
- マルチリージョンキーまたは単一リージョンキーのいずれかを選択できます。ただし、複数の AWS リージョンで IAM Identity Center を使用する場合は、マルチリージョン KMS キーを作成する必要があります。シングルリージョン KMS キーをマルチリージョン KMS キーに変換することはできないため、特にシングルリージョン KMS キーを使用する要件がない限り、マルチリージョン KMS キーから始めることをお勧めします。
- KMS キーは、「暗号化と復号」の用途に設定された対称キーである必要があります
- KMS キーは、IAM アイデンティティセンターの組織インスタンスと同じ AWS Organizations 管理アカウントに存在する必要があります

> **Note**
>
> IAM Identity Center をレプリケートするリージョンにこの KMS キーをレプリケートする場合は、まずこのセクションのセットアップを完了してから、「the section called “IAM Identity Center を追加のリージョンにレプリケートする”」のガイダンスに従うことをお勧めします。

ステップ 4: KMS キーをクロスアカウントで使用するように IAM ポリシーを設定する

IAM アイデンティティセンター委任管理者など、別の AWS アカウントの IAM アイデンティティセンターサービス API を使用する IAM プリンシパルには、これらの API を介した KMS キーの使用を許可する IAM ポリシーステートメントも必要です。

ステップ 1 で特定した各ユースケースについて:

1. ベースライン KMS キーと IAM ポリシーステートメントで、関連する IAM ポリシーステートメントテンプレートを見つけます。
2. テンプレートをエディタにコピーし、キー ARN を入力します。この ARN は、ステップ 3 の KMS キーの作成後に使用可能になりました。キー ARN 値を見つける方法については、「必要な識別子の検索場所」を参照してください。
3. AWS マネジメントコンソール で、ユースケースに関連付けられている IAM プリンシパルの IAM ポリシーを見つけます。このポリシーの場所は、ユースケースとアクセス許可の付与方法によって異なります。

- IAM で直接付与されるアクセスについては、IAM コンソールで IAM ロールなどの IAM プリンシパルを見つけることができます。
- IAM アイデンティティセンターを通じて付与されたアクセスについては、IAM アイデンティティセンターコンソールで関連するアクセス許可セットを見つけることができます。

4. ユースケース固有の IAM ポリシーステートメントを IAM ロールに追加し、変更を保存します。

> **Note**
>
> ここで説明する IAM ポリシーは、ID ベースのポリシーです。このようなポリシーは IAM ユーザー、グループ、ロールにアタッチできますが、可能な場合は IAM ロールを使用することをお勧めします。IAM ロールと IAM ユーザーの詳細については、「IAM ユーザーガイド」を参照してください。

一部の AWS マネージドアプリケーションの追加設定

一部の AWS マネージドアプリケーションでは、アプリケーションが IAM アイデンティティセンターサービス API を使用できるようにサービスロールを設定する必要があります。組織が IAM アイデンティティセンターで AWS マネージドアプリケーションを使用している場合は、デプロイされたアプリケーションごとに次の手順を実行します。

1. IAM アイデンティティセンターでアプリケーションを使用するための KMS キー関連のアクセス許可を含めるようにアクセス許可が更新されているかどうかを確認するには、アプリケーションのユーザーガイドを参照してください。
2. その場合は、アプリケーションのユーザーガイドの指示に従ってアクセス許可を更新し、アプリケーションのオペレーションが中断されないようにします。

> **Note**
>
> AWS マネージドアプリケーションがこれらのアクセス許可を使用しているかどうか不明な場合は、デプロイされたすべての AWS マネージドアプリケーションのユーザーガイドを確認することをお勧めします。この設定を実行する必要があるのは、設定が必要なアプリケーションごとに 1 回だけです。

ステップ 5: IAM アイデンティティセンターで KMS キーを設定する

Important

このステップに進む前に:

- AWS マネージドアプリケーションがカスタマーマネージド KMS キーと互換性があることを確認します。互換性のあるアプリケーションのリストについては、「AWS IAM アイデンティティセンターで使用できるマネージドアプリケーション」を参照してください。互換性のないアプリケーションがある場合は、続行しないでください。
- KMS キーを使用するために必要なアクセス許可を設定します。適切なアクセス許可がない場合、このステップは IAM アイデンティティセンターの管理、AWS マネージドアプリケーションの使用、および KMS キーアクセス許可を必要とするその他のユースケースに失敗または中断する可能性があります。詳細については、「ステップ 1: 組織のユースケースを特定する」を参照してください。
- IAM ロールを使用して IAM アイデンティティセンターサービス API を呼び出す AWS マネージドアプリケーションとカスタマーマネージドアプリケーションのアクセス許可でも、IAM アイデンティティセンターサービス API を介して KMS キーの使用が許可されていることを確認します。一部の AWS マネージドアプリケーションでは、これらの API を使用するためのサービスロールなどのアクセス許可を設定する必要があります。特定の KMS キーアクセス許可を追加する必要があるかどうかを確認するには、デプロイされた各 AWS マネージドアプリケーションのユーザーガイドを参照してください。

IAM アイデンティティセンターの新しい組織インスタンスを有効にするときに KMS キーを指定する

Note

デフォルトで有効になっている AWS リージョンでは、インスタンス作成の一環としてカスタマーマネージドキーを設定できます。詳細については、「IAM Identity Center を有効にする」を参照してください。

インスタンス設定オプションを使用できないリージョンで IAM Identity Center の新しい組織インスタンスを有効にする場合、セットアップ時にカスタマーマネージド KMS キーを指定できます。これにより、インスタンスは最初から保管時の暗号化にキーを使用します。開始する前に、「カスタマーマネージド KMS キーと高度な KMS キーポリシーに関する考慮事項」を参照してください。

1. [IAM アイデンティティセンターの有効化] ページで、[保管時の暗号化] セクションを展開します。
2. [暗号化の管理] を選択します。
3. [カスタマーマネージドキー] を選択します。
4. [新規の KMS キーの作成] で、次のいずれかの操作を行います。
   a. [KMS キーから選択] を選択し、ドロップダウンリストから作成したキーを選択します。
   b. [KMS キー ARN を入力] を選択し、キーの完全な ARN を入力します。
5. [保存] を選択します。
6. [有効化] を選択してセットアップを完了します。

詳細については、「IAM Identity Center の有効化」を参照してください。

IAM アイデンティティセンターの既存の組織インスタンスのキー設定を変更する

カスタマーマネージド KMS キーは、いつでも別のキーに変更したり、AWS 所有キーに切り替えることができます。

Console

KMS キー設定を変更するには

1. https://console.aws.amazon.com/singlesignon/ で IAM Identity Center のコンソールを開きます。
2. ナビゲーションペインで [設定] を選択します。
3. [追加の設定] タブを選択します。
4. [暗号化の管理] を選択します。
5. 次のいずれかを選択します。
   a. カスタマーマネージドキー - ドロップダウンから別のカスタマーマネージドキーを選択するか、新しいキー ARN を入力します。
   b. AWS 所有キー - デフォルトの暗号化オプションに切り替えます。
6. [保存] を選択します。

AWS CLI

KMS カスタマーマネージドキーを使用するように IAM アイデンティティセンターの既存の組織インスタンスを変更するには

```
aws sso-admin update-instance \
    --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
    --encryption-configuration \
        KeyType=CUSTOMER_MANAGED_KEY,KmsKeyArn=arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

AWS所有キーを使用するように IAM アイデンティティセンターの既存の組織インスタンスを変更するには

```
aws sso-admin update-instance \
    --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
    --encryption-configuration KeyType=AWS_OWNED_KMS_KEY
```

カスタマーマネージドキーに関する考慮事項

- IAM アイデンティティセンターオペレーションの KMS キー設定を更新しても、IAM アイデンティティセンターのアクティブなユーザーセッションには影響しません。このプロセス中は、 AWS アクセスポータル、IAM アイデンティティセンターコンソール、IAM アイデンティティセンターサービス API を引き続き使用できます。
- 新しい KMS キーに切り替えると、IAM アイデンティティセンターはキーを暗号化と復号に正常に使用できることを検証します。キーポリシーまたは IAM ポリシーの設定中にエラーが発生した場合、コンソールに説明エラーメッセージが表示され、以前の KMS キーは引き続き使用されます。
- デフォルトの年間 KMS キーローテーションは自動的に行われます。キーローテーション、AWS KMS キーのモニタリング、キー削除へのアクセスのコントロールなどのトピックについては、「AWS KMSデベロッパーガイド」を参照してください。

> **Important**
>
> IAM アイデンティティセンターインスタンスで使用されているカスタマーマネージド KMS キーが、KMS キーポリシーが正しくないために削除、無効化、またはアクセスできない場合、ワークフォースユーザーと IAM アイデンティティセンター管理者は IAM アイデンティティセンターを使用できません。アクセスの喪失は、状況に応じて、一時的 (キーポリシー

を修正できる) または永続的 (削除されたキーを復元できない) にすることができます。KMS キーの削除や無効化など、重要なオペレーションへのアクセスを制限することをお勧めします。また、特権ユーザーが万一 IAM Identity Center にアクセスできなくなった場合に AWS にアクセスできるように、組織でAWSブレークグラスアクセス手順を設定することをお勧めします。

必要な識別子の検索場所

カスタマーマネージド KMS キーのアクセス許可を設定する場合、キーポリシーと IAM ポリシーステートメントテンプレートを完了するには、特定の AWS リソース識別子が必要です。必要な識別子 (組織 ID など) と IAM プリンシパル名を KMS キーポリシーステートメントに挿入します。

以下は、 AWS 管理コンソールでこれらの識別子を見つけるためのガイドです。

IAM アイデンティティセンター Amazon リソースネーム (ARN) と ID ストア ARN

IAM アイデンティティセンターインスタンスは、arn:aws:sso:::instance/ssoins-1234567890abcdef などの独自の ARN を持つ AWS リソースです。ARN は、「サービス認可リファレンス」の「IAM アイデンティティセンターリソースタイプ」セクションに記載されているパターンに従います。

すべての IAM アイデンティティセンターインスタンスには、ユーザー ID とグループ ID を保存する ID ストアが関連付けられています。ID ストアには、ID ストア ID と呼ばれる一意の識別子 (例: d-123456789a) があります。ARN は、「サービス認可リファレンス」の「ID ストアリソースタイプ」セクションに記載されているパターンに従います。

ARN と ID ストア ID の両方の値は、IAM アイデンティティセンターの設定ページで確認できます。ID ストア ID は ID ソースタブにあります。

AWS Organizations ID

キーポリシーで組織 ID (o-exampleorg1 など) を指定する場合は、IAM アイデンティティセンターと組織コンソールの設定ページでその値を確認できます。ARN は、「サービス認可リファレンス」の「組織リソースタイプ」セクションに記載されているパターンに従います。

KMS キー ARN

KMS キーの ARN は、AWS KMS コンソールで確認できます。左側のカスタマーマネージドキーを選択し、ARN を検索するキーをクリックすると、全般設定セクションに表示されます。ARN は、「サービス認可リファレンス」の「AWS KMS リソースタイプ」セクションに記載されているパターンに従います。

AWS KMS のキーポリシーと AWS KMS アクセス許可のトラブルシューティングの詳細については、「AWS Key Management Service デベロッパーガイド」を参照してください。IAM ポリシーとその JSON 表現の詳細については、IAM ユーザーガイドを参照してください。

ベースライン KMS キーポリシー

次の KMS キーポリシーは、よく使用されるデプロイシナリオに対応しています。委任管理者と AWS マネージドアプリケーション (AWS Control Tower、Amazon EC2 インスタンスへの SSO、カスタムワークフローなど) を持つ IAM Identity Center インスタンスです。IAM Identity Center のカスタマーマネージド KMS キーを作成するときは、このポリシーを出発点として使用します。キーを特定の IAM Identity Center インスタンスまたはアプリケーションに制限するなど、アクセスを細かく制御する必要がある場合は、「高度な KMS キーポリシーステートメント」を参照してください。マルチリージョンキーを使用する場合は、一貫した認可を確保するために、すべてのレプリカで同じポリシーを使用する必要があります。

このポリシーを使用するには、以下のプレースホルダ値を自身の値に置き換えます。

- *111122223333* — IAM Identity Center インスタンスの AWS アカウント ID (AWS Organizations 管理アカウント)。
- *444455556666* — 委任管理アカウントの AWS アカウント ID。委任管理を使用しない場合は、このプリンシパルを削除します。

AWS IAM Identity Center では、KMS キーがサービスと同じ AWS アカウントにある必要があるため、次のステートメントではリテラル値ではなく `${aws:ResourceOrgID}` 変数と `${aws:ResourceAccount}` 変数を使用しています。これらの変数は、必要に応じて AWS 組織 ID と AWS アカウント ID に置き換えることができます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIdentityCenterAdminAccounts",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::444455556666:root"
        ]
      },
      "Action": "kms:*",
```

```
      "Resource": "*"
    },
    {
      "Sid": "AllowIdentityCenterAndIdentityStoreToDescribeKey",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "identitystore.amazonaws.com",
          "sso.amazonaws.com"
        ]
      },
      "Action": "kms:DescribeKey",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid": "AllowIdentityCenterAndIdentityStoreToUseKey",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "identitystore.amazonaws.com",
          "sso.amazonaws.com"
        ]
      },
      "Action": [
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "${aws:ResourceAccount}"
        },
        "ForAnyValue:StringEquals": {
          "kms:EncryptionContextKeys": [
            "aws:sso:instance-arn",
            "aws:identitystore:identitystore-arn"
          ]
```

```
        }
      }
    },
    {
      "Sid": "AllowOrgPrincipalsViaIdentityCenterAndIdentityStore",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
        },
        "StringLike": {
          "kms:ViaService": [
            "sso.*.amazonaws.com",
            "identitystore.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals": {
          "kms:EncryptionContextKeys": [
            "aws:sso:instance-arn",
            "aws:identitystore:identitystore-arn"
          ]
        }
      }
    },
    {
      "Sid": "AllowManagedApps",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        },
        "StringEquals": {
          "aws:SourceOrgID": "${aws:ResourceOrgID}"
        },
        "StringLike": {
          "kms:ViaService": [
            "identitystore.*.amazonaws.com",
            "sso.*.amazonaws.com"
```

```
          ]
        },
        "ForAnyValue:StringEquals": {
          "kms:EncryptionContextKeys": [
            "aws:sso:instance-arn",
            "aws:identitystore:identitystore-arn"
          ]
        }
      }
    }
  ]
}
```

このポリシーには、ステートメントが 5 つ含まれています。次の表に、各ステートメントの内容を示します。

ステートメント	目的
AllowIdentityCenterAdminAccounts	IAM Identity Center 管理アカウントと委任管理アカウントに完全な KMS キーアクセス許可を付与します。これには、キーポリシーの変更やキー削除のスケジュールなどのキー管理アクションが含まれます。これらのアカウントの管理者は、アイデンティティベースのポリシーで必要なアクセス許可を持っていれば、キーを管理および使用できます。
AllowIdentityCenterAndIdentityStoreToDescribeKey	IAM Identity Center および Identity Store サービスプリンシパルが、キーメタデータを取得できるようになります。これは、暗号化や復号を実行せずにキーを検証するサービスオペレーションに必要です。この `aws:SourceAccount` 条件により、KMS キーを使用できるのはお使いの IAM Identity Center インスタンスに限られます。
AllowIdentityCenterAndIdentityStoreToUseKey	IAM Identity Center および Identity Store サービスプリンシパルが、データの暗号化、復号、再暗号化などの暗号化オペレーションにキーを使用できるようになります。この `aws:SourceAccount` 条件により、KMS キーを使用できるのはお使いの IAM Identity Center インスタンスに限られます。

ステートメント	目的
AllowOrgPrincipalsViaIdentityCenterAndIdentityStore	AWS Organization の IAM プリンシパルが、IAM Identity Center および Identity Store サービスを通じてデータを復号できるようになります。これには、Forward Access Sessions (FAS) を使用して IAM Identity Center 統合 AWS サービスとやり取りするアプリケーション管理者が含まれます。
AllowManagedApps	AWS マネージドアプリケーションが、IAM Identity Center と Identity Store を通じて KMS キーで保護されたデータを復号できるようになります。

ステップ 4: KMS キーをクロスアカウントで使用するように IAM ポリシーを設定する で次の IAM ポリシーステートメントを使用して、委任管理者が IAM Identity Center サービス API を通じて KMS キーを使用できるようにします。キー ARN の例を実際の KMS キー ARN に置き換えます。この例のワイルドカードリージョンは、マルチリージョン KMS キーのすべてのレプリカに対応します。

Amazon EC2 インスタンスへの SSO や AWS マネージドアプリケーションの管理など、IAM Identity Center の管理以外のクロスアカウントユースケースでは、スコープ `AllowCrossAccountKMSKeyUse` を `kms:Decrypt` のみに絞り込み、`AllowListKMSKeyAliases` ステートメントを削除します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCrossAccountKMSKeyUse",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:*:111122223333:key/mrk-1234abcd-12ab-34cd-56ef-1234567890ab"
      ]
    },
    {
      "Sid": "AllowListKMSKeyAliases",
```

```
      "Effect": "Allow",
      "Action": "kms:ListAliases",
      "Resource": "*"
    }
  ]
}
```

高度な KMS キーポリシーステートメント

高度な KMS キーポリシーステートメントを使用して、カスタマーマネージド KMS キーのより詳細なアクセスコントロールを実装します。これらのポリシーは、暗号化コンテキスト条件とサービス固有の制限を追加することで、ベースライン KMS キーポリシー 上に構築されます。高度な KMS キーポリシーステートメントを使用するかどうかを決定する前に、関連する考慮事項を確認してください。

暗号化コンテキストを使用してアクセスを制限する

ベースライン KMS キーポリシー 内の `AllowOrgPrincipalsViaIdentityCenterAndIdentityStore` および `AllowManagedApps` ステートメントに暗号化コンテキスト条件を追加することで、 KMS キーの使用を特定の IAM Identity Center インスタンスに制限できます。特定のアイデンティティセンターインスタンス ARN と Identity Store ARN を使用して、次の条件を追加します。KMS キーのクロスアカウント使用のために設定された IAM ポリシーに同じ暗号化コンテキスト条件を追加することもできます。

アイデンティティセンター

```
"StringEquals": {
    "kms:EncryptionContext:aws:sso:instance-arn":
 "arn:aws:sso:::instance/ssoins-1234567890abcdef"
}
```

ID ストア

```
"StringEquals": {
    "kms:EncryptionContext:aws:identitystore:identitystore-arn":
 "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
}
```

これらの識別子の検索に関するヘルプが必要な場合は、「必要な識別子の検索場所」を参照してください。

> **Note**
>
> カスタマーマネージド KMS キーは、IAM アイデンティティセンターの組織インスタンスでのみ使用できます。カスタマーマネージドキーは AWS 組織の管理アカウントに配置する必要があります。これにより、キーが 1 つの IAM アイデンティティセンターインスタンスで使用されるようになります。ただし、暗号化コンテキストメカニズムは、単一インスタンスの使用に対する独立した技術的保護を提供します。アイデンティティセンターおよび ID ストアサービスプリンシパル向けの KMS キーポリシーステートメントで `aws:SourceArn` 条件キーを使用することもできます。

暗号化コンテキスト条件を実装する際の考慮事項

暗号化コンテキスト条件を実装する前に、以下の要件を確認してください。

- DescribeKey アクション。暗号化コンテキストは、IAM アイデンティティセンター管理者が使用できる「kms:DescribeKey」アクションに適用できません。KMS キーポリシーを設定するときは、この特定のアクションの暗号化コンテキストを除外して、IAM アイデンティティセンター インスタンスの適切なオペレーションを確保します。
- 新しいインスタンスのセットアップ。カスタマーマネージド KMS キーを使用して新しい IAM アイデンティティセンターインスタンスを有効にする場合は、「カスタマーマネージド KMS キーと高度な KMS キーポリシーに関する考慮事項」を参照してください。
- ID ソースの変更。Active Directory との間で ID ソースを変更する場合、暗号化コンテキストには特別な注意が必要です。「ID ソースの変更に関する注意事項」を参照してください。

ポリシーテンプレート

セキュリティ要件に基づいて、これらの高度なポリシーテンプレートから選択します。きめ細かなアクセスコントロールと、導入する管理オーバーヘッドのバランスを取ります。

ここで説明するトピックは以下の通りです。

- 特定の IAM アイデンティティセンターインスタンスの読み取り専用使用のための KMS ポリシーステートメント. このセクションでは、IAM アイデンティティセンターへの読み取り専用アクセスに暗号化コンテキストを使用する方法を示します。

- AWS マネージドアプリケーションを使用するための改良された KMS キーポリシーステートメント. このセクションでは、アプリケーションサービスプリンシパル、アプリケーション ARN、AWSアカウント ID などの暗号化コンテキストとアプリケーション情報を使用して、AWS マネージドアプリケーションの KMS キーポリシーを絞り込む方法を示します。

特定の IAM アイデンティティセンターインスタンスの読み取り専用使用のための KMS ポリシーステートメント

このポリシーは、IAM アイデンティティセンターへの読み取りアクセスのみを必要とするセキュリティ監査担当者やその他の担当者が KMS キーを使用することを許可します。

このポリシーを使用するには以下を実行します。

1. 読み取り専用管理者 IAM プリンシパルの例を実際の管理者 IAM プリンシパルに置き換えます。
2. IAM アイデンティティセンターインスタンス ARN の例を実際のインスタンス ARN に置き換えます。
3. サンプルの ID ストア ARN を実際の ID ストア ARN に置き換える
4. 委任管理を使用している場合は、ステップ 4: KMS キーをクロスアカウントで使用するように IAM ポリシーを設定する を参照してください

これらの識別子の値の検索に関するヘルプが必要な場合は、「必要な識別子の検索場所」を参照してください。

テンプレートを値で更新したら、 ステップ 2: KMS キーポリシーステートメントを準備する に戻り、必要に応じて追加の KMS キーポリシーステートメントを準備します。

kms:Decrypt アクションだけでは、読み取り専用オペレーションへのアクセスは制限されません。IAM ポリシーは、IAM アイデンティティセンターサービス API に読み取り専用アクセスを適用する必要があります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReadOnlyAccessToIdentityCenterAPI",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
```

```
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn":
 "arn:aws:sso:::instance/ssoins-1234567890abcdef"
        }
      }
    },
    {
      "Sid": "AllowReadOnlyAccessToIdentityStoreAPI",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn":
 "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        }
      }
    }
  ]
}
```

AWS マネージドアプリケーションを使用するための改良された KMS キーポリシーステートメント

これらのポリシーテンプレートにより、KMS キーを使用できる AWS マネージドアプリケーションをより詳細にコントロールできます。

> **Note**
>
> 一部の AWS マネージドアプリケーションは、カスタマーマネージド KMS キーで設定された IAM アイデンティティセンターでは使用できません。「AWS IAM アイデンティティセンターで使用できるマネージドアプリケーション」を参照してください。

ベースライン KMS キーポリシー は、同じ AWS 組織内の任意のアカウントの任意の AWS マネージドアプリケーションに KMS キーの使用を許可します。これらの洗練されたポリシーを使用して、以下によってアクセスを制限します。

- アプリケーションサービスプリンシパル
- アプリケーションインスタンス ARN
- AWS アカウント ID
- 特定の IAM アイデンティティセンターインスタンスの暗号化コンテキスト

> **Note**
>
> サービスプリンシパルは、 AWSサービスの一意の識別子で、通常は servicename.amazonaws.com (Amazon EMR の場合は elasticmapreduce.amazonaws.com など) の形式です。

アカウントによる制限

この KMS キーポリシーステートメントテンプレートにより、特定の AWS アカウントの AWS マネージドアプリケーションは、特定の IAM アイデンティティセンターインスタンスを使用して KMS キーを使用できます。

このポリシーを使用するには以下を実行します。

1. サンプルサービスプリンシパルを実際のアプリケーションサービスプリンシパルに置き換える
2. サンプルアカウント ID を、AWS マネージドアプリケーションをデプロイする実際のアカウント ID に置き換えます。
3. サンプルの ID ストア ARN を実際の ID ストア ARN に置き換える
4. IAM アイデンティティセンターインスタンス ARN の例を実際のインスタンス ARN に置き換えます。

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

```
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": [
            "111122223333",
            "444455556666"
          ]
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        }
      }
    },
    {
      "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": [
            "111122223333",
            "444455556666"
          ]
        },
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn":
 "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
```

```
        }
      }
    }
  ]
}
```

アプリケーションインスタンスによる制限

この KMS キーポリシーステートメントテンプレートは、特定の AWS マネージドアプリケーションインスタンスが特定の IAM アイデンティティセンターインスタンスを使用して KMS キーを使用できるようにします。

このポリシーを使用するには以下を実行します。

1. サンプルサービスプリンシパルを実際のアプリケーションサービスプリンシパルに置き換える
2. サンプルアプリケーション ARN を実際のアプリケーションインスタンス ARN に置き換える
3. サンプルの ID ストア ARN を実際の ID ストア ARN に置き換える
4. IAM アイデンティティセンターインスタンス ARN の例を実際のインスタンス ARN に置き換えます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-
application"
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
        },
```

```
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        }
      }
    },
    {
      "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-
application"
        },
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn":
 "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        }
      }
    }
  ]
}
```

カスタマーマネージド KMS キーと高度な KMS キーポリシーに関する考慮事項

IAM アイデンティティセンターでカスタマーマネージド KMS キーを実装する場合は、暗号化設定の設定、セキュリティ、継続的なメンテナンスに影響するこれらの要因を考慮してください。

ベースラインとアドバンスト KMS キーポリシーステートメントの選択に関する考慮事項

高度な KMS キーポリシーステートメント を使用して KMS キーのアクセス許可をより具体的にするかどうかを決定するときは、組織の管理オーバーヘッドとセキュリティニーズを考慮してください。より具体的なポリシーステートメントでは、キーを使用できるユーザーと目的をよりきめ細かく制御できます。ただし、IAM アイデンティティセンターの設定が進化するにつれて、継続的なメンテナンスが必要になります。例えば、KMS キーの使用を特定の AWS マネージドアプリケーションのデ

プロイに制限する場合は、組織がアプリケーションをデプロイまたはデプロイ解除するたびにキーポリシーを更新する必要があります。制限の少ないポリシーは管理上の負担を軽減しますが、セキュリティ要件に必要なよりも広範なアクセス許可を付与する可能性があります。

カスタマーマネージド KMS キーを使用して新しい IAM アイデンティティセンターインスタンスを有効にする際の考慮事項

ここでの考慮事項は、「高度な KMS キーポリシーステートメント」で説明されている暗号化コンテキストを使用して、KMS キーの使用を特定の IAM アイデンティティセンター インスタンスに制限する場合に適用されます。

カスタマーマネージド KMS キーを使用して新しい IAM アイデンティティセンターインスタンスを有効にする場合、IAM アイデンティティセンターと ID ストア ARN はセットアップ後まで使用できません。次のオプションがあります。

- 一時的に汎用 ARN パターンを使用し、インスタンスが有効になったら、 完全な ARN に置き換えます。必要に応じて、StringEquals 演算子と StringLike 演算子を切り替えてください。
  - IAM アイデンティティセンター SPN の場合: "arn:${Partition}:sso:::instance/*"。
  - ID ストア SPN の場合: "arn:${Partition}:identitystore::${Account}:identitystore/*"。
- ARN で一時的に「purpose:KEY_CONFIGURATION」を使用します。これはインスタンスの有効化にのみ機能し、IAM アイデンティティセンターインスタンスが正常に機能するには、実際の ARN に置き換える必要があります。このアプローチの利点は、インスタンスが有効になった後にこれを置き換えることを忘れないことです。
  - IAM アイデンティティセンター SPN の場合は、「arn:${Partition}:sso:::instance/purpose:KEY_CONFIGURATION」を使用します。
  - ID ストア SPN の場合は、「arn:${Partition}:identitystore::${Account}:identitystore/purpose:KEY_CONFIGURATION」を使用します。

> **Important**
>
> この設定は、既存の IAM アイデンティティセンターインスタンスで既に使用されている KMS キーに適用しないでください。通常のオペレーションが中断される可能性があります。

- インスタンスが有効になるまで、KMS キーポリシーから暗号化コンテキスト条件を省略します。

AWS IAM アイデンティティセンター リソースのタグ付け

タグは、AWS リソースに追加して、リソースの識別、整理、検索を容易にでき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。

タグは、AWS リソースの識別や整理に役立ちます。多くの AWS のサービスではタグ付けがサポートされるため、さまざまなサービスからリソースに同じタグを割り当てて、リソースの関連を示すことができます。例えば、IAM アイデンティティセンターのインスタンスの特定のアクセス許可セットに同じタグを割り当てることができます。タグ付け方法の詳細については、「AWS 全般のリファレンスガイド」の「AWS リソースのタグ付け」と「タグ付けのベストプラクティス」を参照してください。

IAM Identity Center リソースの特定、整理、追跡に加え、IAM ポリシーのタグを使って、AWS リソースを表示および操作できるユーザーを制御することもできます。アクセスをコントロールするためのタグの使用については、「IAM ユーザーガイド」の「タグを使用した AWS リソースへのアクセスのコントロール」を参照してください。たとえば、ユーザが IAM Identity Center 権限セットを更新することを許可できるが、それは、IAM Identity Center 権限セットにそのユーザ名の値を持つ `owner` タグがある場合に限られます。

タグは権限セットにのみ適用できます。IAM アイデンティティセンターが AWS アカウント で作成した対応するロールにはタグを適用できません。IAM Identity Center コンソール、AWS CLI、または IAM Identity Center API を使用して、権限セットのタ グを追加、編集、または削除できます。

以下のセクションでは、IAM Identity Center のタグに関する詳細を示します。

トピック

- タグの制限
- IAM Identity Center コンソールを使用してタグを管理する
- AWS CLI の例

- IAM Identity Center API を使用してタグを管理する

タグの制限

IAM Identity Center リソースのタグには、以下のような基本制限があります。

- リソースに割り当てることができるタグの最大数は 50 個です。
- キーの最大長は Unicode 文字で 128 文字です。
- 値の最大長は Unicode 文字で 256 文字です。
- タグのキーと値の有効な文字は次のとおりです。

  a-z、A-Z、0-9、スペース、および以下の文字： _ . : / = + -と@
- キーと値は大文字と小文字が区別されます。
- `aws:` をキーのプレフィックスとして使用しないでください。AWS 用に予約済みです

IAM Identity Center コンソールを使用してタグを管理する

IAM アイデンティティセンターコンソールを使用して、インスタントまたはアクセス許可セットに関連付けられたタグを追加、編集、削除することができます。

IAM アイデンティティセンターコンソールの許可セットタグを管理するには

1. IAM アイデンティティセンターコンソールを開きます。
2. [アクセス許可セット] を選択します。
3. 管理するタグを含むアクセス権限セットの名前を選択します。
4. [権限] タブの [タグ] で以下のいずれかを行い、次のステップに進みます。

   a. このアクセス権限セットに既にタグが割り当てられている場合は、[タグの編集] を選択します。

   b. このアクセス権限セットにタグが割り当てられていない場合は、[タグの追加] を選択します。
5. それぞれの新しいタグについて、[Key] (キー) と [Value (optional)] (値 (オプション)) の列に値を入力します。完了したら、[Save changes] (変更の保存) を選択します。

タグを削除するには、削除したいタグの横にある [削除] 列の [X] をクリックします。

IAM アイデンティティセンターのインスタンスのタグを管理するには

1. IAM アイデンティティセンターコンソールを開きます。
2. [設定] を選択します。
3. [タグ] タブを選択します。
4. それぞれのタグについて、[キー] と [値 (オプション)] のフィールドに値を入力します。完了したら、[新しいタグを追加] ボタンを選択します。

タグを削除するには、削除したいタグの横にある [削除] ボタンを選択します。

AWS CLI の例

AWS CLI には、アクセス権限セットに割り当てたタグを管理するためのコマンドが用意されています。

タグの割り当て

アクセス権限セットにタグを割り当てるには、以下のコマンドを使用します。

Example **`tag-resource`** アクセス権限セットのコマンド

sso セットのコマンドの中で `tag-resource` を使って、アクセス権限セットにタグを割り当てます。

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test
```

このコマンドには次のパラメータが含まれます。

- `instance-arn` - オペレーションが実行される IAM アイデンティティセンターインスタンスの Amazon リソースネーム (ARN)。
- `resource-arn` — リストアップされるタグを含むリソースの ARN。
- `tags` – タグのキー/値ペア。

一度に複数のタグを割り当てるには、カンマ区切りリストで指定します。

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

タグの表示

アクセス権限セットに割り当てたタグを表示するには、以下のコマンドを使用します。

Example **list-tags-for-resource** アクセス権限セットのコマンド

コマンドの sso セット内の list-tags-for-resource 使用して、アクセス権限セットにタグを割り当てます。

```
$ aws sso-admin list-tags-for-resource --resource-arn sso-resource-arn
```

タグの削除

アクセス権限セットからタグを削除するには、以下のコマンドを使用します。

Example **untag-resource** アクセス権限セットのコマンド

sso セットのコマンドの中で untag-resource を使って、アクセス権限セットからタグを削除します。

```
$ aws sso-admin untag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tag-keys Stage CostCenter Owner
```

--tag-keys パラメータには、1 つ以上のタグキーを指定します。タグ値は含めないでください。

権限セット作成時のタグの適用

アクセス権限セットにタグを作成するには、以下のコマンドを使用します。

Example **create-permission-set** コマンドとタグ

create-permission-set コマンドを使用してアクセス権限セットを作成するときは、--tags パラメータと共にタグを指定できます。

```
$ aws sso-admin create-permission-set \
> --instance-arn sso-instance-arn \
> --name permission=set-name \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

IAM Identity Center API を使用してタグを管理する

次の API アクションを使用して、IAM アイデンティティセンターの許可セットまたはインスタンスのタグを割り当て、表示、削除します。

- TagResource
- ListTagsForResource
- UntagResource
- CreatePermissionSet
- CreateInstance

AWS CLI と IAM Identity Center の統合

AWS コマンドラインインターフェイス (CLI) バージョン 2 と IAM Identity Center の統合により、サインインプロセスが簡略化します。デベロッパーは、IAM Identity Center へのサインインに通常使用している Active Directory や IAM Identity Center の認証情報を用いて AWS CLI に直接サインインし、割り当てられたアカウントやロールにアクセスすることができます。例えば、管理者が IAM Identity Center を設定して認証に Active Directory を使用すると、デベロッパーは Active Directory の認証情報を使って AWS CLI に直接サインインすることができます。

AWS CLI と IAM Identity Center の統合により、以下のようなメリットがあります。

- 企業は、Directory Service を使って IAM Identity Center を Active Directory に接続することで、IAM Identity Center や Active Directory からの認証情報を使ってデベロッパーがサインインできるようになります。
- デベロッパーは CLI からサインインすることで、より迅速なアクセスが可能になります。
- デベロッパーは、自分がアクセス権を割り当てたアカウントやロールを一覧表示して切り替えることができます。
- デベロッパーは、CLI 構成で名前付きロールプロファイルを自動的に生成し、保存し、CLI で参照することで、目的のアカウントやロールでコマンドを実行することができます。
- CLI は短期間の認証情報を自動的に管理するため、開発者は中断することなく安全に CLI を開始して使用し、長時間実行するスクリプトを実行することができます。

AWS CLI と IAM Identity Center の統合方法

AWS CLI と IAM アイデンティティセンターの統合を使用するには、AWS Command Line Interface バージョン 2 をダウンロードし、インストールし、設定します。AWS CLI をダウンロードして IAM Identity Center と統合する方法の詳細な手順については、「AWS Command Line Interface ユーザーガイド」の「IAM Identity Center を使用するためのAWS CLI の設定」を参照してください。

AWS マネジメントコンソールプライベートアクセスに関する注意事項

組織が AWS マネジメントコンソールプライベートアクセス機能を使用している場合は、ユーザーが IAM アイデンティティセンターにサインインする方法を検討する必要があります。

VPC エンドポイントポリシーは、管理コンソールへのサインインを制限します。これにより、ユーザーはアクセス権限のない AWS アカウント にサインインすることはできなくなります。詳細については、「AWS マネジメントコンソール Getting Started Guide」の「AWS マネジメントコンソール Private Access」を参照してください。

VPC エンドポイントが IAM アイデンティティセンターへのサインインをブロックする

VPC エンドポイントを使用すると IAM アイデンティティセンターへのサインインが拒否されることに注意してください。これは、ユーザーがすでに VPC エンドポイントを通じて管理コンソールにログインしている場合に起こります。ユーザーが IAM アイデンティティセンターに引き続きサインインできるようにするには、VPC エンドポイントではなく、パブリックエンドポイントを使用して AWS にサインインする必要があります。

IAM アイデンティティセンターのクォータと制限

次の表では、IAM Identity Center 内のクォータについて説明します。クォータの増額リクエストは、管理者アカウントまたは委任管理者アカウントから行う必要があります。クォータの増加をリクエストするには、「クォータ増加のリクエスト」を参照してください。

> **Note**
>
> 50,000 人を超えるユーザー、10,000 以上のグループ、500 を超えるアクセス許可セット、または 3,000 を超えるアプリケーションがある場合は、AWS CLI と API を使用して IAM Identity Center を一元管理することをお勧めします。CLI の詳細については、 を参照してくださいAWS CLI と IAM Identity Center の統合 API の詳細については、「Welcome to the IAM Identity Center API Reference」参照してください。

アプリケーションクォータ

リソース	デフォルトのクォータ	引き上げ可能
サービスプロバイダーの SAML 証明書のファイルサイズ (PEM 形式)	2 KB	なし
SAML アサーション制限	50,000 文字	なし
IAM アイデンティティセンターにアップロードされる IdP 証明書のファイルサイズ制限	UTF-8 で 2500 文字	なし
アプリケーションごとのアクセススコープ	25	なし

AWS アカウント のクォータ

リソース	デフォルトのクォータ	引き上げ可能
IAM Identity Center で許可される許可セット数	3500	はい
AWS アカウント あたりに許可されるアクセス権限セット数	500	はい
アクセス権限セットあたりのインラインポリシーの数	1	いいえ
権限セットごとの AWS 管理ポリシーとカスタマー管理ポリシーの数	25[1]	いいえ
アクセス権限セットあたりのインラインポリシーの最大サイズ	32,768 バイト 権限セットごとのインラインポリシー内の空白以外の文字の最大サイズは 10,240 バイトです。	いいえ
一度に更新できる AWS アカウント 内の IAM ロール (権限セット) の数	1	いいえ

[1]AWS Identity and Access Management (IAM) では、ロールごとに 10 個の管理ポリシーの割り当てが設定されます。このクォータを利用するには、権限セットをデプロイしたい AWS アカウント ごとに、Service Quotas コンソールで IAM クォータ「IAM ロールに追加された管理ポリシー」の増加をリクエストします。

> **Note**
>
> 権限セットを使用して AWS アカウントを管理する は IAM ロールとして AWS アカウント でプロビジョニングされるか、AWS アカウント で既存の IAM ロールを使用するため、IAM

クォータに従います。IAM ロールに関する IAM クォータの詳細については、「IAM と STS クォータ」を参照してください。

Active Directory のクォータ

リソース	デフォルトのクォータ	引き上げ可能
一度に実現できる接続ディレクトリの数	1	いいえ

IAM Identity Center Identity Store クォータ

リソース	デフォルトのクォータ	引き上げ可能
IAM Identity Center でサポートされるユーザーの数	200000	はい
IAM Identity Center でサポートされるグループの数	100000	はい

IAM Identity Center のスロットル制限

リソース	デフォルトのクォータ
IAM Identity Center API	「IAM Identity Center API」のコレクティブスロットルは、毎秒 20 トランザクション (TPS) までに制限されています。読み取り API の場合、サポートケースを開いて上限の引き上げをリクエストできます。CreateAccountAssignment 書き込み API は、未処理の非同期呼び出しが 15 件に制限されています。この制限を増やすことはできません。

リソース	デフォルトのクォータ
Identity Store API	「Identity Store API」のスロットルは、API ごとに毎秒 20 トランザクション (TPS) までに制限されています。この制限は、Identity Store インスタンスごとに適用されます。サポートケースを開いて、制限の引き上げをリクエストできます。
SCIM API	SCIM API には API ごとにスロットリングの制限があり、書き込み API は 1 秒あたり 25 トランザクション (TPS)、読み取り API は 40 TPS です。これらの制限は、Identity Store インスタンスごとに適用されます。サポートケースを開いて、制限の引き上げをリクエストできます。 `CreateGroup` や `PatchGroup` を呼び出す際の各メンバーシップオペレーションは、トランザクションとしてカウントされ、Identity Store ごとに別個のメンバーシップオペレーションスロットリング制限の対象となります。

IAM Identity Center インスタンスが複数の AWS リージョン で有効になっている場合、スロットリング制限は有効になっている各リージョンに等しく適用されます。例えば、有効な各リージョンの Identity Store API には 20 TPS のスロットリング制限があります。追加リージョンで使用できる API オペレーションの詳細については、対応する表を参照してください。

OIDC サービスリクエストのクォータ

リソース	デフォルト値 (1 秒あたりのリクエスト)	引き上げ可能
パブリック OAuth クライアントを登録するリモートアドレスからのリクエストレート	20	はい

リソース	デフォルト値 (1 秒あたりのリクエスト)	引き上げ可能
適用先: RegisterClient		
OIDC サービスに登録されたパブリッククライアントからのリクエストレート 適用先: CreateToken、StartDeviceAuthorization	80	はい
同じ IAM アイデンティティセンターインスタンスに登録されているすべてのパブリッククライアントからのリクエストレート 適用先: CreateToken	250	はい
トークン交換付与および更新トークン付与を使用して IAM Identity Center インスタンスに登録された IAM Identity Center アプリケーションからのリクエストレート 適用先: CreateTokenWithIAM	80	はい
同じ IAM アイデンティティセンターインスタンスに登録されているすべての IAM アイデンティティセンターアプリケーションによる、JWT ベアラー認可方式でのトークン生成レート 適用先: CreateTokenWithIAM	10	AWS Support へのお問い合わせ

IAM Identity Center インスタンスが複数の AWS リージョン で有効になっている場合、上記のリクエストレートは有効な各リージョンに等しく適用されます。例えば、リモートアドレスからパブリック OAuth クライアントを登録するために許可されたリクエストレートが 1 秒あたり 20 リクエストの場合、このスループットは有効な各リージョンで使用できます。追加リージョンで使用できる API オペレーションの詳細については、対応する表を参照してください。

追加のクォータ

リソース	デフォルトのクォータ	引き上げ可能
設定できる AWS アカウントまたはアプリケーションの総数 * **	7000	はい
IAM アイデンティティセンターのアカウントごとの合計インスタンス数	1	いいえ
信頼できるトークン発行者の総数	10	いいえ
AWS アカウント ごとにアクセス許可セットまたはアプリケーションに割り当てることができるグループの総数	100	いいえ
1 つの IAM Identity Center インスタンスで有効になっている AWS リージョン の総数	6	はい

* このクォータは、AWS アカウント とアプリケーションに個別に適用されます。最大 7,000 個のアカウントと最大 7,000 個のアプリケーションを設定できます。

** `ProvisionPermissionSet` API オペレーションは、オプション `ALL_PROVISIONED_ACCOUNTS` を使用してアクセス許可セットを最大 3500 AWS アカウント にプロビジョニングできます。アクセス許可セットを 3500 を超える AWS アカウント にプロビジョニングする必要がある場合は、`AWS_ACCOUNT` オプションで `ProvisionPermissionSet` API オペレー

ションを使用できます。これにより、アクセス許可セットが 1 つの AWS アカウント にプロビジョニングされます。ProvisionPermissionSet に対して最大 3 つの同時呼び出しを行うことができます。

IAM Identity Center の問題のトラブルシューティング

以下は、IAM Identity Center コンソールを設定または使用するときに発生する可能性のある問題のトラブルシューティングに役立ちます。

IAM アイデンティティセンターのアカウントインスタンスの作成に関する問題

IAM アイデンティティセンターのアカウントインスタンスを作成する場合、いくつかの制限が適用される場合があります。IAM アイデンティティセンターコンソールからアカウントインスタンスを作成できない場合や、サポートされている AWS マネージドアプリケーションを設定した経験がない場合は、以下のユースケースを確認してください。

- アカウントインスタンスを作成しようとしている他の AWS リージョン を AWS アカウント で確認します。IAM アイデンティティセンターのインスタンスは AWS アカウント につき 1 つに制限されています。アプリケーションを有効にするには、IAM アイデンティティセンターのインスタンスがある AWS リージョン に切り替えるか、IAM アイデンティティセンターのインスタンスがないアカウントに切り替えます。
- 2023 年 9 月 14 日より前に IAM アイデンティティセンターを有効にしている組織は、管理者がアカウントインスタンスの作成にオプトインする必要がある場合があります。管理者と協力して、管理アカウントの IAM アイデンティティセンターコンソールからアカウントインスタンスを作成できるようにします。
- 管理者が IAM アイデンティティセンターのアカウントインスタンスの作成を制限するサービスコントロールポリシーを作成した可能性があります。管理者と協力してアカウントを許可リストに追加します。

IAM アイデンティティセンターと連携するように事前設定されているクラウドアプリケーションのリストを表示しようとすると、エラーが表示されます。

以下のエラーは、`sso:ListApplications` は許可するが、他の IAM アイデンティティセンター API は許可しないポリシーがある場合に発生します。ポリシーを更新してこのエラーを解決します。

`ListApplications` アクセス許可は複数の API を承認します。

- ListApplications API。
- IAM アイデンティティセンターコンソールで使用される ListApplicationProviders API に似た内部 API。

重複を解決するために、内部 API も ListApplicationProviders アクションの使用を許可するようになりました。パブリック ListApplications API を許可し、内部 API を拒否するには、ポリシーに ListApplicationProviders アクションを拒否するステートメントを含める必要があります。

```
      "Statement": [
    {
         "Effect": "Deny",
         "Action": "sso:ListApplicationProviders",
         "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "sso:ListApplications",
        "Resource": "<instanceArn>" // (or "*" for all instances)
    }
]
```

内部 API を許可して ListApplications を拒否するには、ポリシーで ListApplicationProviders のみ許可する必要があります。ListApplications API は明示的に許可されない場合は拒否されます。

```
      "Statement": [
    {
         "Effect": "Allow",
         "Action": "sso:ListApplicationProviders",
         "Resource": "*"
    }
]
```

ポリシーが更新されたら、サポート に連絡して、この予防措置を削除してもらいます。

IAM Identity Center によって作成された SAML アサーションの内容に関する問題

IAM Identity Center は、AWS アクセスポータルから AWS アカウント や SAML アプリケーションにアクセスする際に、IAM Identity Center で作成および送信された SAML アサーション (アサーション内の属性を含む) のウェブベースのデバッグエクスペリエンスを提供します。IAM Identity Center が生成する SAML アサーションの詳細を確認するには、以下の手順を行います。

1. AWS アクセスポータルにサインインします。
2. ポータルにサインインしている状態で、Shift キーを押しながらアプリケーションタイルを選択し、Shift キーを離します。
3. [You are now in administrator mode] (現在、管理者モードです) ページの情報を調べます。この情報を保存しておきたい場合は、[Copy XML] をクリックして、その内容を別の場所に貼り付けます。
4. [Send to <application>] (<アプリケーション>に送信する) をクリックして続けます。このオプションは、アサーションをサービスプロバイダに送信します。

> **Note**
>
> ブラウザの設定やオペレーティングシステムによっては、この手順をサポートしていない場合があります。この手順は、Firefox、Chrome、Edge ブラウザを使用して Windows 10 で評価されています。

特定のユーザーが、外部の SCIM プロバイダーからの IAM Identity Center に同期できません

お使いの ID プロバイダー (IdP) が SCIM 同期を使用して IAM アイデンティティセンターにユーザーをプロビジョニングするように構成されている場合、ユーザープロビジョニングプロセス中に同期エラーが発生する可能性があります。この場合、お使いの IdP のユーザー設定が IAM あの要件と互換性がない可能性があります。その場合、IAM アイデンティティセンター SCIM API は問題の根本原因に関するエラーメッセージを返します。これらのエラーメッセージは、お使いの IdP のログまたは UI で確認できます。また、プロビジョニングの失敗に関する詳細情報は AWS CloudTrail ログでも確認できます。

IAM アイデンティティセンターSCIM 実装の詳細 (ユーザーオブジェクトに必須の、あるいはオプションの、もしくは禁止されているパラメータや操作の仕様など) は、「SCIM Developer Guide」の「IAM Identity Center SCIM Implementation Developer Guide」に記載されています。

このエラーが発生する一般的な理由は以下のとおりです。

1. IdP のユーザーオブジェクトに、名 (given)、姓 (family)、もしくは表示名がありません。

   「エラーメッセージ: 2 つの検証エラーが検出されました。*'name.givenName'* の値が制約を満たせませんでした。メンバーは正規表現パターン [\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r]+ を満たす必要があります。 *'name.givenName'* の値が制約を満たせませんでした。メンバーの長さは 1 以上である必要があります」

   - 解決策: ユーザーオブジェクト向けに、名 (given)、姓 (family)、表示名を追加します。さらに、IdP のユーザーオブジェクトに対する SCIM プロビジョニングマッピングが、これらの属性すべてに対して空ではない値を送信するように構成されていることを確認してください。

2. 1 つの属性に対して複数の値がユーザーに送信されています (「マルチバリュー属性」とも知られれています)。例えば、ユーザーが IdP で職場と自宅の両方の電話番号を指定していたり、複数の E メールや実際の住所を指定していたりする場合、IdP はその属性の複数またはすべての値を同期するように設定されています。

   エラーメッセージ: 「List attribute *emails* exceeds allowed limit of 1」

   - ソリューションオプション:

     i. IdP のユーザーオブジェクトに対する SCIM プロビジョニングマッピングを更新して、特定の属性に対して単一の値のみを送信するようにします。例えば、各ユーザーの職場の電話番号のみを送信するマッピングを設定します。

     ii. IdP でユーザーオブジェクトから追加属性を安全に削除できる場合は、追加値を削除して、ユーザーのその属性に設定された値を 1 つまたは完全に無くすことができます。

     iii. その属性が AWS でのアクションに必要ない場合は、IdP でのユーザーオブジェクトの SCIM プロビジョニングマッピングからその属性のマッピングを削除します。

3. お客様の IdP は、複数の属性に基づいてターゲット (ここでは IAM Identity Center) のユーザーをマッチさせようとします。ユーザー名は、特定の IAM Identity Center インスタンス内で一意であることが保証されているため、マッチングに使用する属性として `username` 指定するだけです。

- 解決策: IdP の SCIM 構成が、IAM Identity Center でのユーザーとのマッチングに単一の属性のみを使用していることを確認します。例えば、IAM Identity Center へのプロビジョニングのために、IdP の `username` または `userPrincipalName` を SCIM の `userName` 属性にマッピングすることは、ほとんどの実装で十分に要件を満たします。

外部 ID プロバイダーを使用してユーザーまたはグループをプロビジョニングする際の重複ユーザーまたはグループのエラー

外部 ID プロバイダー (IdP) でユーザーまたはグループをプロビジョニングする際に IAM アイデンティティセンターの同期の問題が発生する場合は、外部 IdP ユーザーまたはグループが一意の属性値を持っていないことが原因である可能性があります。外部 IdP に次のようなエラーメッセージが表示されます。

「Refused to create a new, duplicate resource」

この問題は、次のようなシナリオで発生する可能性があります。

- シナリオ 1
  - IAM アイデンティティセンターにおいて一意でなければならない属性に、外部 IdP でカスタマイズされた一意でない属性が使用されています。既存の IAM アイデンティティセンターのユーザーまたはグループは、お使いの IdP と同期できません。
- シナリオ 2
  - IAM アイデンティティセンターで一意でなければならない属性について、重複する属性値を持つユーザーを作成しようとしました。
    - 例えば、次のような属性を持つ IAM アイデンティティセンターユーザーを作成したか、またはそのような既存のユーザーが存在します。
      - ユーザー名: Jane Doe
      - プライマリ E メールアドレス: `jane_doe@example.com`
    - ここで、外部 IdP に次の属性を持つ別のユーザーを作成しようとしたとします。
      - ユーザー名: Richard Doe
      - プライマリ E メールアドレス： `jane_doe@example.com`
        - 外部 IdP は、IAM アイデンティティでもこのユーザーを同期および作成しようと試みます。ただし、2 つのユーザーのプライマリメールアドレスの値が重複しており、プライマリメールアドレスは一意でなければならないため、このアクションは失敗します。

外部 IdP ユーザーが IAM アイデンティティセンターと正常に同期するには、ユーザー名、プライマリ E メールアドレス、そして外部 ID がそれぞれ一意である必要があります。同様に、外部 IdP グループを IAM アイデンティティセンターに正常に同期するには、グループ名が一意である必要があります。

問題を解決するには、ID ソースの属性が一意であることを確認してください。

ユーザー名が UPN 形式の場合、ユーザーはサインインできません

サインインページでユーザー名を入力する際のフォーマットによっては、ユーザーが AWS アクセスポータルにサインインできない場合があります。通常、ユーザーは、プレーンなユーザー名、ダウンレベルのログオン名 (DOMAIN\UserName)、UPN のログオン名 (`UserName@Corp.Example.com`) のいずれかを使ってユーザーポータルにサインインできます。ただし、IAM Identity Center が MFA を有効にした接続ディレクトリを使用しており、検証モードが Context-aware または Always-on のいずれかに設定されている場合は例外です。このシナリオでは、ユーザーは下位レベルのログオン名 (DOMAIN\UserName) でサインインする必要があります。詳細については、「アイデンティティセンターディレクトリユーザーの MFA」を参照してください。アクティブディレクトリへのサインインに使用されるユーザー名の形式についての一般的な情報は、Microsoft のドキュメントサイトの「User Name Formats」(ユーザー名形式) を参照してください。

IAM ロールを変更すると、「Cannot perform the operation on the protected role」(保護されたロールでオペレーションを実行できません) というエラーが発生する

アカウントの IAM ロールを確認すると、「AWSReservedSSO_」で始まるロール名だと気づくと思います。これらは、IAM Identity Center サービスがアカウントに作成したロールであり、アカウントにアクセス権限セットを割り当てたものです。IAM コンソール内からこれらのロールを変更しようとすると、次のエラーが発生します。

```
'Cannot perform the operation on the protected role 'AWSReservedSSO_RoleName_Here' -
 this role is only modifiable by AWS'
```

これらのロールは、AWS Organizations の管理アカウントにある IAM Identity Center 管理コンソールからのみ変更可能です。変更後は、割り当てられている AWS アカウントに変更を反映させることができます。

ディレクトリユーザーが、パスワードをリセットできません

ディレクトリユーザーが AWS アクセスポータルへのサインイン時に [パスワードを忘れましたか？] オプションを使用してパスワードをリセットした場合、新しいパスワードは IAM Identity Center で ID を管理する際のパスワード要件 に記載されているデフォルトのパスワードポリシーに準拠している必要があります。

ユーザーがポリシーに準拠したパスワードを入力した後にエラー `We couldn't update your password` が発生した場合、AWS CloudTrail に障害が記録されているかどうかを確認します。これは、CloudTrail の Event History (イベントの履歴) コンソールで以下のフィルターを使って検索できます。

```
"UpdatePassword"
```

メッセージに次のように記載されている場合は、サポートに連絡する必要があります。

```
"errorCode": "InternalFailure",
      "errorMessage": "An unknown error occurred“
```

この問題の別の原因として、ユーザー名の値が命名規則に反していることが考えられます。命名規則は、「surname.givenName」などの特定のパターンに従う必要があります。しかし、ユーザー名の中には非常に長いものや特殊な文字を含むものがあり、API コールの中で文字が抜けてしまい、エラーになってしまうことがあります。同じ方法でテストユーザーとパスワードのリセットを試みて、これが当てはまるかどうかを確認することもできます。

問題が解決しない場合は、AWS サポートセンターまでお問い合わせください。

ユーザーはアクセス権限セットを参照しているが、割り当てられたアカウントやアプリケーションにアクセスできません

この問題は、クロスドメイン ID 管理 (SCIM) システムを外部の ID プロバイダーで使用している場合に発生します。具体的には、ユーザーまたはユーザーが所属していたグループが削除された後、ID プロバイダーで同じユーザー名 (ユーザーの場合) または名前 (グループの場合) を使用して再作成された場合、IAM Identity Center では新しいユーザーまたはグループに新しい一意の内部識別子が作成されます。しかし、IAM Identity Center は権限データベースに古い識別子への参照を保持しているため、ユーザーやグループの名前は UI に表示されますが、アクセスは失敗します。これは、UI が参照するときのベースとなるユーザーまたはグループ ID がもはや存在しないためです。

この場合、AWS アカウント のアクセス権を回復するには、古いユーザーやグループのアクセス権を元々割り当てられていた AWS アカウント から削除して、そのユーザーやグループにアクセス権を再び割り当てます。これにより、新しいユーザーまたはグループの正しい識別子でアクセス権限セットが更新されます。同様に、アプリケーションのアクセス権を回復するには、そのアプリケーションの割り当てユーザーリストからそのユーザーまたはグループのアクセス権を削除し、その後、そのユーザーまたはグループを再び追加します。

また、AWS CloudTrail が障害を記録しているかどうかを確認するには、CloudTrail のログで、問題のユーザーやグループの名前を参照している SCIM 同期イベントを検索します。

アプリケーションカタログからアプリケーションを正しく設定できない

IAM アイデンティティセンターのアプリケーションカタログからアプリケーションを追加した場合は、各サービスプロバイダーが独自の詳細なドキュメントを提供していることに注意してください。この情報は、IAM アイデンティティセンターコンソール上でアプリケーションの [設定] タブから確認できます。

問題が、サービスプロバイダーのアプリケーションと IAM Identity Center の間の信頼関係の設定に関係している場合は、必ず手順書でトラブルシューティングのステップを確認してください。

ユーザーが外部の ID プロバイダーを使用してサインインしようとすると、「予期しないエラーが発生しました」というエラーが発生します

このエラーは複数の理由で発生する可能性がありますが、よくあるのは、SAML リクエストで送信したユーザー情報と IAM Identity Center でのユーザー情報との間にミスマッチがあることが挙げられます。

IAM Identity Center のユーザーが、外部の IdP を ID ソースとして使用しているときに正常にサインインするためには、以下の条件を満たす必要があります。

- SAML nameID 形式 (アイデンティティプロバイダーで設定) は「E メール」でなければなりません。
- nameID の値は、適切に (RFC2822) でフォーマットされた文字列である必要があります (user@domain.com)

- nameID の値は、IAM Identity Center の既存ユーザーのユーザー名と完全に一致する必要があります (IAM Identity Center のメールアドレスが一致するかどうかは問題ではありません - インバウンドマッチはユーザー名に基づいて行われます)。
- SAML 2.0 フェデレーションの IAM Identity Center　実装では、ID プロバイダーと IAM Identity Center　間の SAML レスポンスで 1 つのアサーションのみがサポートされます。暗号化された SAML アサーションはサポートされていません。
- 以下の記述は、IAM Identity Center アカウントで アクセスコントロールの属性 が有効になっている場合に適用されます。
  - SAML リクエストでマッピングされる属性の数は、50 以下でなければなりません。
  - SAML リクエストに複数の値を持つ属性を含めることはできません。
  - SAML リクエストには、同じ名前の複数の属性を含めることはできません。
  - 属性の値として、構造化された XML を含んではいけません。
  - Name の形式は、汎用的な形式ではなく、SAML で指定された形式でなければなりません。

> **Note**
>
> IAM Identity Center は、SAML フェデレーションを介した新しいユーザーやグループの「ジャストインタイム」での作成はできません。つまり、IAM Identity Center にサインインするためには、手動または自動プロビジョニングによって、ユーザーが IAM Identity Center であらかじめ作成されている必要があります。

このエラーは、ID プロバイダーで構成されたアサーションコンシューマサービス (ACS) のエンドポイントが、IAM Identity Center インスタンスで提供された ACS の URL と一致しない場合にも発生します。この 2 つの値が正確に一致するようにしてください。

さらに AWS CloudTrail にアクセスして、イベント名 ExternalIdPDirectoryLogin でフィルタリングすることで、外部 ID プロバイダーのサインインの失敗をトラブルシューティングすることもできます。

エラー「アクセスコントロールのための属性の有効化に失敗しました」

このエラーは、ABAC を有効にしているユーザーが、アクセスコントロールの属性 を有効にするために必要な `iam:UpdateAssumeRolePolicy` 権限を持っていない場合に発生することがあります。

MFA にデバイスを登録しようとすると、「Browser not supported」(サポートされていないブラウザ) というメッセージが表示されます。

WebAuthn は現在、Google Chrome、Mozilla Firefox、Microsoft Edge、Apple Safari の各ウェブブラウザ、および Windows 10 と Android プラットフォームに対応しています。WebAuthn のサポートには、macOS と iOS のブラウザでのプラットフォーム認証のサポートなど、さまざまなコンポーネントがあります。サポートされていないブラウザやプラットフォームで WebAuthn デバイスを登録しようとすると、サポートされていない特定のオプションがグレーアウトで表示されたり、サポートされているメソッドがサポートされていないというエラー表示になったりします。このような場合のブラウザ/プラットフォームのサポートについては、「FIDO2: Web Authentication (WebAuthn)」(FIDO2: ウェブ認証 (WebAuthn)) を参照してください。IAM Identity Center の WebAuthn の詳細については、「FIDO2 認証機能」を参照してください。

アクティブディレクトリの「ドメインユーザー」グループが IAM Identity Center に正しく同期しない

アクティブディレクトリのドメインユーザーグループは、AD ユーザーオブジェクトのデフォルトの「プライマリグループ」です。アクティブディレクトリのプライマリグループとそのメンバシップは、IAM Identity Center では読み取れません。IAM Identity Center リソースまたはアプリケーションへのアクセスを割り当てる際には、グループメンバーシップが IAM Identity Center ID ストアに適切に反映されるように、ドメインユーザーグループ (またはプライマリグループとして割り当てられた他のグループ) 以外のグループを使用してください。

無効な MFA 認証情報エラー

このエラーは、SCIM プロトコルを使用してアカウントが IAM Identity Center に完全にプロビジョニングされる前に、ユーザーが外部 ID プロバイダー (Okta または Microsoft Entra ID など) のアカウ

ントを使用して IAM Identity Center にサインインしようとすると発生する可能性があります。ユーザーアカウントが IAM Identity Center にプロビジョニングされると、この問題は解決します。アカウントが IAM Identity Center にプロビジョニングされていることを確認します。されていない場合は、外部 ID プロバイダーのプロビジョニングログを確認します。

認証アプリケーションを使って登録やサインインをしようとすると、「予期しないエラーが発生しました」というメッセージが表示されます

コードベースの認証アプリケーションと組み合わせて IAM Identity Center で使用されるような、タイムベースドワンタイムパスワード (TOTP) システムは、クライアントとサーバー間の時間の同期に依存しています。認証システムのアプリケーションをインストールしているデバイスが信頼できるタイムソースに正しく同期されていることを確認するか、またはデバイスの時間を、NIST (https://www.time.gov/) やその他のローカル/地域など、信頼できるソースと一致するように手動で設定してください。

IAM アイデンティティセンターへのサインインを試行すると、「ご迷惑をおかけしています」と表示されます

このエラーは、IAM アイデンティティセンターのインスタンス、または IAM アイデンティティセンターが ID ソースとして使用している外部 ID プロバイダー (IdP) の設定に問題があることを示しています。この場合、以下を確認することをお勧めします。

- サインインに使用するデバイスの日付と時刻の設定を確認してください。日付と時刻は自動設定にすることをお勧めします。自動設定が利用できない場合には、日付と時刻を既知の Network Time Protocol (NTP) サーバーに同期するとよいでしょう。
- IAM アイデンティティセンターにアップロードされた IdP 証明書が、お使いの IdP から提供される証明書と同じであることを確認してください。IAM アイデンティティセンターコンソールで証明書を確認するには、[設定] に移動します。[ID ソース] タブで [アクション] > [認証の管理] を選択します。IdP と IAM アイデンティティセンターの証明書が一致しない場合は、新しい証明書を IAM アイデンティティセンターにインポートします。
- ID プロバイダーのメタデータファイルの NameID 形式が以下に従っていることを確認します。
  - `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
- AWS Directory Service の AD Connector を ID プロバイダーとして使用している場合は、サービスアカウントの認証情報が正常で、かつ失効していないことを確認してください。詳細については、

「Update your AD Connector service account credentials in AWS Directory Service」を参照してください。

ユーザーが IAM Identity Center からのメールを受信できません

IAM Identity Center サービスで送信されるすべてのメールは、アドレス no-reply@signin.aws または no-reply@login.awsapps.com のいずれかから送信されます。これらの送信者メールアドレスからのメールを受け入れ、ジャンクやスパムとして処理しないようにお使いのメールシステムを設定する必要があります。

エラー: 管理アカウントにプロビジョニングされたアクセス権限セットを削除/変更/削除/割り当てることはできません

このメッセージは、委任された管理 機能が有効になっており、試行された操作は AWS Organizations で管理アカウント権限を持つユーザーのみが正常に実行できるものであることを示しています。この問題を解決するには、これらの権限を持つユーザーとしてサインインし、タスクをもう一度実行してみるか、適切な権限を持つユーザーにこのタスクを割り当ててください。詳細については、「メンバーアカウントを作成する」を参照してください。

エラー: セッショントークンが見つからない、または無効です

このエラーは、Web ブラウザ、AWS Toolkit、または AWS CLI などのクライアントが、サーバー側で取り消されたか、または無効になったセッションを使用しようとした時に発生します。この問題を修正するには、該当するクライアントアプリケーションまたは Web サイトに戻り、プロンプトが表示されたら再度ログインするなどの対応を試してください。ただしそのためには、例えば IDE 内の AWS Toolkitからの接続試行など、実施待ちのリクエストをキャンセルしなければならないことがあります。

信頼できるドメインのグループメンバーが IAM Identity Center と同期しない

セキュリティグループが IAM Identity Center と正常に同期されたものの、信頼できるオンプレミスドメインのメンバーが IAM Identity Center に表示されない場合、その原因としては、グループが AWS Managed Microsoft AD に存在し、信頼できるドメインのユーザーを表す外部セキュリティプリンシパル (FSP) が含まれていることが考えられます。

次の手順を使用して、トラブルシューティングを試します。

- 信頼できるドメインから直接グループを同期する: クロスドメインメンバーが含まれている AWS Managed Microsoft AD からグループを同期するのではなく、信頼できるオンプレミスドメインから直接グループを作成して同期します。IAM Identity Center がソースドメイン内の実際のユーザーオブジェクトにアクセスできるため、このアプローチは正常に機能します。
- サービスアカウントのアクセス許可を確認する: IAM Identity Center サービスアカウントに、信頼できるドメインのユーザーオブジェクトに対して必要なアクセス許可 (ReadProperties および ListContents) が付与されていることを確認します。

AWS IAM アイデンティティセンター でのカスタマーマネージドキーのトラブルシューティング

このトピックでは、AWS IAM アイデンティティセンター の使用時に発生する可能性がある一般的なカスタマーマネージドキー関連のエラーと、それらを解決するためのトラブルシューティング手順について説明します。

アクセス拒否: KMS 復号アクセス許可の問題

エラー:「ユーザー xxxxxxx は、この暗号文に関連付けられたリソースに対して kms:Decrypt を実行する権限がありません。これは、アイデンティティベースのポリシーで kms:Decrypt アクションが許可されていないためです。」

ユーザーまたは IAM プリンシパルに、IAM ポリシーまたは KMS キーポリシーに必要な `kms:Decrypt` アクセス許可がありません。

のトラブルシューティング:AWS CloudTrail

1. CloudTrail で `kms.amazonaws.com` イベントを検索する
2. イベント名 `Decrypt` を検索する
3. `errorCode` フィールドと `errorMessage`フィールドを確認する
4. どのプリンシパルがオペレーションを試みたか `userIdentity` を確認する

この問題を解決するには、IAM ポリシーと KMS キーポリシーでユーザーまたは IAM プリンシパル `kms:Decrypt` にアクセス許可を付与します。詳細については、「AWS IAM アイデンティティセンター でのカスタマーマネージド KMS キーの実装」を参照してください。

IAM Identity Center でカスタマーマネージドキーを有効にした AWS マネージドアプリケーションのログインに失敗する

アイデンティティセンターユーザーが AWS マネージドアプリケーションにログインできず、IAM Identity Center インスタンスでカスタマーマネージドキーが有効になっている場合は、KMS キーポリシーにより、カスタマーマネージドキーを使用するためのアクセス許可が AWS マネージドアプリケーションに付与されていることを確認します。詳細については、「ベースライン KMS キーポリシー」を参照してください。

IAM Identity Center でカスタマーマネージドキーを有効にした AWS マネージドアプリケーションのインストールおよび/またはユーザー割り当てが失敗する

エラー:「ユーザー xxxxxxx は、この暗号文に関連付けられたリソースに対して kms:Decrypt を実行する権限がありません。これは、アイデンティティベースのポリシーで kms:Decrypt アクションが許可されていないためです。」

ユーザーまたは IAM プリンシパルに、IAM ポリシーまたは KMS キーポリシーに必要な `kms:Decrypt` アクセス許可がありません。

CloudTrail を使用したトラブルシューティング:

1. イベント名 `Decrypt` を検索する
2. `errorCode` フィールドと `errorMessage`フィールドを確認する
3. どのプリンシパルがオペレーションを試みたか `userIdentity` を確認する

この問題を解決するには、IAM ポリシーと KMS キーポリシーでユーザーまたは IAM プリンシパル `kms:Decrypt` にアクセス許可を付与します。詳細については、「AWS IAM アイデンティティセンター でのカスタマーマネージド KMS キーの実装」を参照してください。

KMS アクセス許可の問題: AWS IAM アイデンティティセンター でカスタマーマネージドキーを設定する

ユーザーまたは IAM プリンシパルには、カスタマーマネージドキーを有効にするときに 1 つ以上の必要な KMS アクセス許可 (`kms:Decrypt`、`kms:Encrypt`、`kms:GenerateDataKey`、`kms:DescribeKey`) がありません。

CloudTrail を使用したトラブルシューティング:

1. Decrypt、Encrypt、GenerateDataKey または DescribeKey イベントを検索する
2. errorCode フィールドと errorMessageフィールドを確認する
3. どのプリンシパルがオペレーションを試みたか userIdentity を確認する

この問題を解決するには、ID ベースのポリシーまたは KMS キーポリシーで、必要なすべての KMS アクセス許可をユーザーまたは IAM プリンシパルに付与します。詳細については、「AWS IAM アイデンティティセンター でのカスタマーマネージド KMS キーの実装」を参照してください。

IAM Identity Center でカスタマーマネージドキーを有効にした場合に、AWS アクセスポータルのログインに失敗する

エラー:「ERROR Code: 0001 - IdentityCenter サービスへのアクセスがブロックされています。詳細な手順については、IdentityCenter 管理者にお問い合わせください。」

ユーザーが AWS アクセスポータルにログインできず、IAM Identity Center インスタンスでカスタマーマネージドキーが有効になっている場合は、KMS キーポリシーが Identity Center と ID ストアに必要なアクセス許可を付与していることを確認します。詳細については、「ベースライン KMS キーポリシー」を参照してください。

AWS IAM アイデンティティセンター でのマルチリージョンセットアップをトラブルシューティングする

このトピックでは、AWS IAM アイデンティティセンター の使用時に発生する可能性がある一般的なマルチリージョンセットアップ関連のエラーと、それらを解決するためのトラブルシューティング手順について説明します。

IAM Identity Center インスタンスのレプリケート先にしたいリージョンが、IAM Identity Center コンソールで使用できない

まず、IAM Identity Center インスタンスのレプリケート先となるリージョンに、カスタマーマネージドキーのレプリカキーを作成する必要があります。レプリカキーが作成されると、レプリケーションに使用できるリージョンのリストに目的のリージョンが表示されます。詳細については、「the section called “ステップ 1: レプリカキーを作成する”」を参照してください。

追加リージョンで AWS マネージドアプリケーションのサインインに失敗する

IAM Identity Center でリージョンを追加した後で、IAM Identity Center ユーザーが追加リージョンで AWS マネージドアプリケーションにサインインできない場合は、the section called “手順 3 (外部 ID プロバイダーのみ): 外部 IdP 設定を更新する” の説明に従って、外部 ID プロバイダーで追加リージョンのアサーションコンシューマーサービス (ACS) URL が設定されていることを確認します。また、ユーザーがそのリージョンに接続できることを確認します。

IAM Identity Center のマルチリージョンインスタンスを有効にする際の問題

IAM Identity Center を有効にするときに、マルチリージョンインスタンスを選択した場合、セットアッププロセスがカスタマーマネージドキーを作成して追加リージョンにレプリケートし、インスタンスを有効にして、追加リージョンを追加します。これらの手順のいずれかが失敗した場合、次のいずれかのエラーが表示されることがあります。

キーの作成に失敗する

アカウントでカスタマーマネージドキーを作成できませんでした。インスタンスが有効になっていませんでした。

これがアクセス許可エラーの場合は、ロールに `kms:CreateKey` および `kms:TagResource` のアクセス許可があることを確認し、[有効] を選択して再試行します。

キーのレプリケーションに失敗する

アカウントでカスタマーマネージドキーが作成されたものの、追加リージョンにレプリカキーを作成できませんでした。インスタンスが有効になっていませんでした。

これがアクセス許可エラーの場合は、ロールに `kms:ReplicateKey` のアクセス許可があることを確認します。

[有効] を選択して再試行します。同じキーが使用されます。

後で戻る場合は、タグ `CreatedBy: IAM Identity Center` でフィルタリングして、AWS KMS コンソールでキーを見つけます。キー ID をコピーし、[カスタムインスタンス] を選択して、そのキーを選択します。

新しく開始するには、AWS KMS コンソールでキーを削除し、マルチリージョンインスタンスを選択して新しいキーを作成します。

インスタンスの作成に失敗する

カスタマーマネージドキーが作成され、追加リージョンにレプリケートされたものの、インスタンスを有効にできませんでした。

これがアクセス許可エラーの場合は、ロールに IAM Identity Center インスタンスを作成するために必要なアクセス許可があることを確認します。

[有効] を選択して再試行します。同じキーが使用されます。

後で戻る場合は、タグ `CreatedBy: IAM Identity Center` でフィルタリングして、AWS KMS コンソールでキーを見つけます。キー ID をコピーし、[カスタムインスタンス] を選択して、そのキーを選択します。

新しく開始するには、AWS KMS コンソールでキーとそのレプリカを削除し、マルチリージョンインスタンスを選択して新しいインスタンスを作成します。

> **Note**
>
> これらのエラーは、カスタムインスタンスを使用しているときに、インスタンスの作成またはリージョンのレプリケーションが失敗した場合にも発生する可能性があります。独自のカスタマーマネージドキーを指定した場合、キーの作成とレプリケーションの手順は適用されません。

ドキュメント履歴

次の表は、AWS IAM アイデンティティセンター ドキュメントへの重要な追加項目をまとめたものです。また、お客様からいただいたフィードバックに対応するために、ドキュメントを頻繁に更新しています。

- ドキュメントの主要な最終更新日: 2025 年 10 月 21 日

変更	説明	日付
ワンクリックでマルチリージョンインスタンスを作成する	サポート対象のリージョンで新しい組織インスタンスを有効にする場合、シングルリージョン、マルチリージョン、カスタムのいずれかのインスタンス設定を選択できます。マルチリージョンオプションを選択すると、カスタマーマネージド KMS キーを自動的に作成し、インスタンスを追加リージョンにレプリケートすることで、ワンクリックでマルチリージョンレジリエンスを有効にできます。	2026 年 8 月 6 日
新しいインスタンスではマルチアカウントのアクセス許可がオプションに	組織インスタンスを作成するときに、マルチアカウントのアクセス許可を有効にするかどうかを選択できるようになりました。デフォルトでは、マルチアカウントのアクセス許可が有効になっています。マルチアカウントのアクセス許可は、後でインスタンス設定から有効にすることも、UpdateInstance API を使	2026 年 8 月 4 日

	用して有効にすることもできます。	
Identity Center ディレクトリへマルチリージョンのサポートを拡張	マルチリージョンのサポートは、外部 ID プロバイダーに加えて、ID ソースとして Identity Center ディレクトリでも機能するようになりました。	2026 年 7 月 28 日
AWS アカウントとアプリケーションに別個のクォータ	AWS IAM アイデンティティセンター では、AWS アカウントとアプリケーションに別個のクォータが適用されるようになりました。以前は、これらのリソースは 1 つの結合クォータを共有していました。それぞれの新しいデフォルトのクォータは 7,000 です。	2026 年 6 月 22 日
カスタマーマネージドアプリケーションで AWS アカウントアクセスを有効にする	カスタマーマネージドアプリケーションに信頼できるトークン発行者を持たせて `sso:account:access` スコープを有効にすることで、エンドユーザーに代わってプログラムで AWS アカウント認証情報にアクセスできるようになりました。	2026 年 6 月 19 日

グループメンバーシップの変更に関する認証セッションタイミングを更新	新しいセッションの作成時にアクセス許可とアプリケーションアクセスの変更がすぐに有効になるように、グループメンバーシップセッション動作テーブルを更新しました。	2026 年 5 月 28 日
ベースライン KMS キーポリシーを簡素化	ベースライン KMS キーポリシーステートメントを 1 つのポリシーにまとめて簡素化しました。これにより、保管中の暗号化のためのカスタマーマネージド KMS キーを効率よく設定できます。	2026 年 4 月 30 日
マルチリージョンサポート	追加リージョンへのレプリケーション、追加リージョンでの AWS アカウント アクセスおよび AWS マネージドアプリケーションの使用など、マルチリージョンのサポートを追加しました。	2026 年 2 月 2 日
AWS 管理ポリシーの更新	プロビジョニングテナントの ARN を変更するように、`AWSIdentityCenterExternalManagementPolicy` AWS マネージドポリシーを更新しました。	2025 年 12 月 5 日
新しい AWS マネージドポリシートピック	`AWSIdentityCenterExternalManagementPolicy` AWS マネージドポリシーの詳細を追加しました。	2025 年 11 月 21 日

監査と調整のガイダンスの自動プロビジョニング	ID ストア API と AWS CLI コマンドを使用して SCIM 自動プロビジョニングされたユーザー、グループ、グループメンバーシップを監査および調整するためのガイダンスを追加しました。	2025 年 10 月 17 日
OIDC サービスリクエストのクォータ	OAuth クライアント登録、トークン作成、その他の OIDC オペレーションのレート制限を含む OIDC サービスリクエストクォータを追加しました。	2025 年 10 月 13 日
AWS 管理ポリシーの更新	IAM アイデンティティセンターは、 マネージドポリシー `AWSSSOMasterAccountAdministrator` 、`AWSSSOMemberAccountAdministrator` 、`AWSSSOReadOnly` 、`AWSSSODirectoryAdministrator` 、`AWSSSODirectoryReadOnly` を更新し暗号化にカスタマーマネージドキーを使用する IAM アイデンティティセンターインスタンスに必要な AWS KMS アクセス許可を追加しました。	2025 年 9 月 17 日
保管時の暗号化用カスタマーマネージドキー	保管中のワークフォース ID データを暗号化するためのカスタマーマネージド KMS キーのサポートが追加されました。	2025 年 9 月 17 日

トークン作成を許可するリソースベースのポリシーの例	承認されたクライアントアプリケーションのトークン作成を許可するリソースベースのポリシーの例を追加しました。	2025 年 9 月 16 日
ユーザーバックグラウンドセッションのサポート	ユーザーバックグラウンドセッションのコンテンツを追加しました。	2025 年 8 月 11 日
ID 拡張コンソールセッション	ID 拡張コンソールセッション (以前は ID 認識セッションと呼ばれていました) の用語を更新しました。	2025 年 5 月 12 日
開始方法の再編成	わかりやすさとユーザーエクスペリエンスを向上させるため、開始方法のコンテンツを再編成しました。	2025 年 5 月 6 日
IAM アイデンティティセンター AD 同期の廃止	IAM アイデンティティセンター AD 同期を使用して Active Directory ユーザーをプロビジョニングすることはできなくなりました。代わりに、IAM アイデンティティセンターで設定可能な AD 同期を使用できます。	2025 年 4 月 17 日
認証済みセッションのコンテンツを更新しました	ユーザーセッションが削除されたときの IAM アイデンティティセンターセッション期間を更新します。	2025 年 4 月 2 日
AWS 管理ポリシーの更新	`AWSSSOServiceRolePolicy` AWS管理ポリシーの権限が更新されました。	2025 年 2 月 11 日

IAM アイデンティティセンターの有効化ワークフローの改善	IAM アイデンティティセンターの組織インスタンスとアカウントインスタンスを有効にするためのワークフローを更新しました。	2025 年 2 月 11 日
IAM アイデンティティセンターの有効化の更新	IAM アイデンティティセンターの組織インスタンスとアカウントインスタンスを有効にするための内容と手順を更新しました。	2024 年 10 月 10 日
AWS 管理ポリシーの更新	AWSIAMIdentityCenterAllowListForIdentityContext AWS管理ポリシーの権限が更新されました。	2024 年 10 月 2 日
AWS 管理ポリシーの更新	AWSSSOMasterAccountAdministrator AWS管理ポリシーの権限が更新されました。	2024 年 9 月 26 日
AWS 管理ポリシーの更新	AWSIAMIdentityCenterAllowListForIdentityContext AWS管理ポリシーの権限が更新されました。	2024 年 9 月 4 日
「IAM アイデンティティセンターとは?」の更新 \? [topic]	IAM アイデンティティセンターのメリットと機能を説明するコンテンツを更新しました。	2024 年 8 月 19 日

AWS 管理ポリシーの更新	AWSIAMIdentityCenterAllowListForIdentityContext AWS管理ポリシーの権限が更新されました。	2024 年 7 月 12 日
AWS 管理ポリシーの更新	AWSIAMIdentityCenterAllowListForIdentityContext AWS管理ポリシーの権限が更新されました。	2024 年 6 月 27 日
AWS 管理ポリシーの更新	AWSIAMIdentityCenterAllowListForIdentityContext AWS管理ポリシーの権限が更新されました。	2024 年 5 月 17 日
AWS 管理ポリシーの更新	AWSIAMIdentityCenterAllowListForIdentityContext AWS管理ポリシーの権限が更新されました。	2024 年 4 月 30 日
AWS 管理ポリシーの更新	AWSSSOMasterAccountAdministrator AWS管理ポリシーの権限が更新されました。	2024 年 4 月 26 日
AWS 管理ポリシーの更新	AWSSSOMemberAccountAdministrator AWS管理ポリシーの権限が更新されました。	2024 年 4 月 26 日
AWS 管理ポリシーの更新	AWSSSOReadOnly AWS管理ポリシーの権限が更新されました。	2024 年 4 月 26 日

AWS 管理ポリシーの更新	AWSIAMIdentityCenterAllowListForIdentityContext AWS管理ポリシーの権限が更新されました。	2024 年 4 月 26 日
AWS 管理ポリシーの更新	AWSIAMIdentityCenterAllowListForIdentityContext AWS管理ポリシーの権限が更新されました。	2024 年 4 月 24 日
AWS 管理ポリシーの更新	AWSIAMIdentityCenterAllowListForIdentityContext AWS管理ポリシーの権限が更新されました。	2024 年 4 月 19 日
AWS 管理ポリシーの更新	AWSIAMIdentityCenterAllowListForIdentityContext AWS管理ポリシーの権限が更新されました。	2024 年 4 月 11 日
AWS 管理ポリシーの更新	AWSIAMIdentityCenterAllowListForIdentityContext AWS管理ポリシーの権限が更新されました。	2023 年 11 月 26 日
新しい AWS マネージドポリシートピック	AWSIAMIdentityCenterAllowListForIdentityContext AWS マネージドポリシーの詳細を追加しました。	2023 年 11 月 15 日

IAM Identity Center の使用を開始するためのガイダンスの強化	IAM Identity Center の使用開始と管理ユーザーの作成に関する新しいコンテンツを追加しました。	2022 年 9 月 23 日
Identity Center API リファレンスのユーザーとグループが更新されました	この更新には、Identity Center API リファレンスガイドの新しい「API の作成、更新、削除」への参照が含まれます。	2022 年 8 月 31 日
AWS シングルサインオン (AWS SSO) は AWS IAM Identity Center に名称が変更されました。	AWS について説明します。AWS IAM アイデンティティセンターIAM アイデンティティセンターは、AWS Identity and Access Management (IAM) の機能を拡張し、ワークフォースユーザーのアカウントとアプリケーションへのアクセスを一元管理するのに役立ちます。IAM Identity Center の機能には、アプリケーション割り当て、マルチアカウント権限、AWSアクセスポータルなどがあります。	2022 年 7 月 26 日
権限セットにおける権限境界と顧客管理ポリシーをサポート	AWS管理ポリシーと顧客管理AWS Identity and Access Management (IAM) ポリシーを権限セットとともに使用するためのコンテンツを追加しました。	2022 年 7 月 14 日
手動で有効化されたAWSリージョンをサポート	手動で有効化されたリージョンで IAM Identity Center を使用するコンテンツが追加されました。	2022 年 6 月 15 日

AWS 管理ポリシーの更新	AWSSSOServiceRolePolicy AWS管理ポリシーの権限が更新されました。	2022 年 5 月 11 日
委任された管理者のサポートを追加	委任管理機能のコンテンツが追加されました。	2022 年 5 月 11 日
AWS 管理ポリシーの更新	AWSSSOMasterAccountAdministrator 、AWSSSOMemberAccountAdministrator 、および AWSSSOReadOnly AWS マネージドポリシーの権限を更新しました。	2022 年 4 月 28 日
設定可能な AD 同期をサポート	設定可能な AD 同期機能のコンテンツが追加されました。	2022 年 4 月 14 日
新しい AWS マネージドポリシートピック	AWSSSOMasterAccountAdministrator AWS マネージドポリシーの詳細を追加しました。	2021 年 8 月 4 日
クォータの更新	クォータテーブルを調整しました。	2020 年 12 月 21 日
新しいポリシーの例	新しいカスタマーマネージドポリシーの例を追加し、必要な権限のセクションを更新しました。	2020 年 12 月 21 日
属性ベースのアクセス制御 (ABAC) のサポート	ABAC 機能のコンテンツを追加しました。	2020 年 11 月 24 日
MFA 強制登録のサポート	サインイン時に MFA デバイスの登録をリクエストするための更新です。	2020 年 11 月 23 日

WebAuthn のサポート	新しい WebAuthn 機能のコンテンツが追加されました。	2020 年 11 月 20 日
Ping ID のサポート	サポートされている外部 ID プロバイダーとして Ping Identity 製品と統合するためのコンテンツを追加しました。	2020 年 10 月 26 日
OneLogin のサポート	サポートされている外部 ID プロバイダーとして OneLogin と統合するためのコンテンツを追加しました。	2020 年 7 月 31 日
のサポートOkta	サポートされている外部 ID プロバイダーとして Okta と統合するためのコンテンツを追加しました。	2020 年 5 月 28 日
外部 ID プロバイダーのサポート	ディレクトリから ID ソースへの参照を変更し、外部の ID プロバイダーをサポートするコンテンツを追加しました。	2019 年 11 月 26 日
新しい MFA 設定	2 段階認証のトピックを削除し、代わりに新しい MFA のトピックを追加しました。	2019 年 10 月 24 日
段階認証を追加するための新しい設定	ユーザーの 2 段階認証を有効にする方法について、コンテンツを追加しました。	2019 年 1 月 16 日
AWS アカウントでのセッションの有効期間のサポート	AWS アカウントのセッションの有効期間を設定する方法に関するコンテンツを追加しました。	2018 年 10 月 30 日

Identity Center ディレクトリを使用する新しいオプション	Identity Center ディレクトリを選択するか、既存の AD ディレクトリに接続するためのコンテンツを追加しました。	2018 年 10 月 17 日
アプリケーションでのリレーステートとセッションの有効期間のサポート	アプリケーションのリレー状態とセッションの有効期間に関するコンテンツを追加しました。	2018 年 10 月 10 日
新しいアプリケーションの追加サポート	4me, BambooHR, Bonusly, Citrix ShareFile, ClickTime, Convo, Deputy, Deskpro, Dome9, DruvaInSync, Egnyte, Engagedly, Expensify, Freshdesk, IdeaScale, Igloo, Jitbit, Kudos, LiquidFiles, Lucidchart, PurelyHR, Samanage, ScreenSteps, Sli.do, SmartSheet, Syncplicity, TalentLMS, Trello, UserVoice, Zoho, OpsGenie, DigiCert, WeekDone, ProdPad, と UserEcho をアプリケーションカタログに追加しました。	2018 年 8 月 3 日
管理アカウントへのマルチアカウントアクセスのサポート	管理アカウントでユーザーにマルチアカウントアクセスを委任する方法に関するコンテンツを追加しました。	2018 年 7 月 9 日
新しいアプリケーションのサポート	DocuSign, Keeper Security, と SugarCRM をアプリケーションカタログに追加しました。	2018 年 3 月 16 日

CLI アクセスの一時認証情報の取得	AWS CLI コマンドを実行するための一時認証情報を取得する方法に関する情報を追加しました。	2018 年 2 月 22 日
新規ガイド	これは IAM Identity Center ユーザーガイドの最初のリリースです。	2017 年 12 月 7 日

AWS 用語集

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