



AWSマルチアカウント 構成ガイド

Okta Inc.
301 Brannan Street,
San Francisco, CA 94107 USA

info@okta.com
1- 888-722-7871

目次

[概要](#)

[仕組み](#)

[AWSのアカウントとロールへのユーザーアクセス](#)

[ユーザーやグループによるアカウントとロールへのアクセスの管理](#)

[設計の概略](#)

[SAML用にAWSを設定する](#)

[AD / LDAPでグループの管理レイヤーを作成する](#)

[グループベースのロール割り当て用にOktaでAWSアプリを構成する](#)

[設定手順](#)

[ステップ1: SAML SSO用にAWSのアカウントとロールをセットアップする](#)

[ステップ2: AD / LDAPでAWSロールグループを作成する](#)

[ステップ3: ユーザーをAWSのアカウントとロールにマッピングするためにAD / LDAP管理グループを構成する](#)

[ステップ4: AWSロールグループと管理グループをOktaにインポートする](#)

[ステップ5: Oktaでグループベースのロールマッピングを有効にする](#)

[ステップ6: OktaですべてのAWS管理グループをAWSアプリに割り当てる](#)

概要

AWSの顧客が多数のAWSアカウントを所有することがますます一般的になり、開発用、テスト用、本番環境用などというような使い分けがなされています。実際、このようなあらゆるユースケースを管理するために、100個以上のAWSアカウントを所有することもよくあります。

Oktaはこれに応じて、無数のAWSのアカウントとロールにシングルサインオンでアクセスできる、安全でスケーラブルな機能の提供を開始しました。また、このモデルでは各ユーザーグループに必要なAWSロールへのアクセス権のみが付与されるため、詳細なエンタイトルメント管理を実現できます。

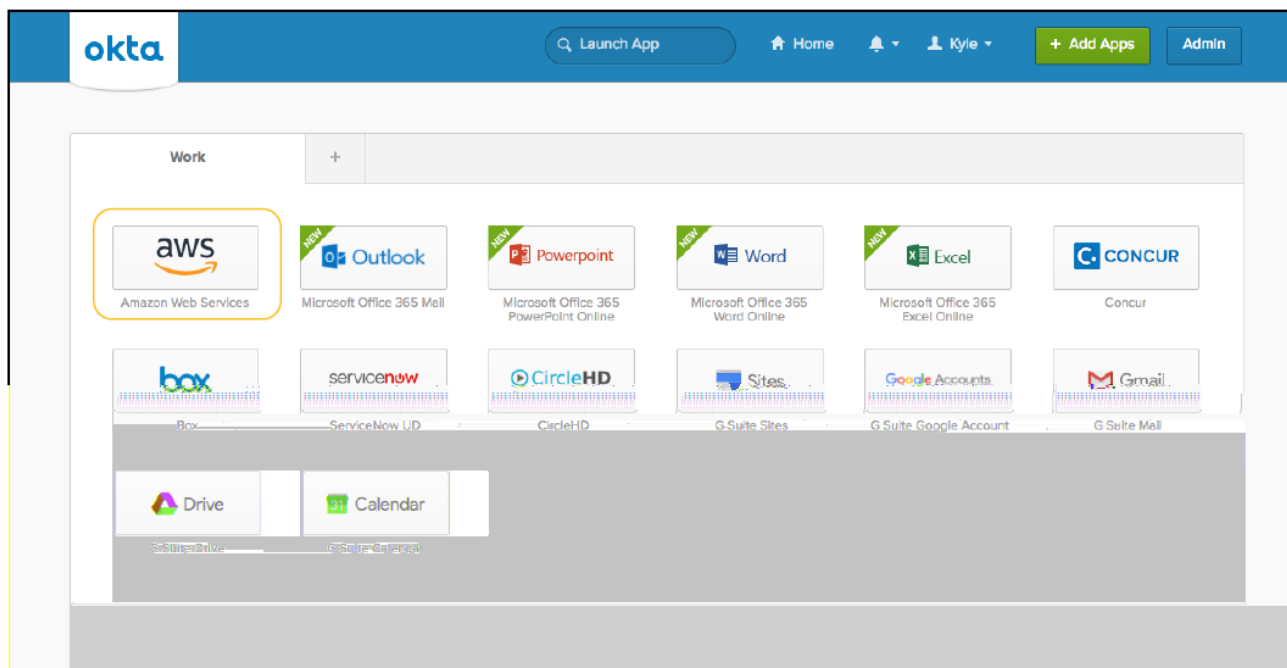
これは早期アクセス機能です。有効にする場合は、Oktaサポートにお問い合わせください。

このガイドでは、OktaのAWSマルチアカウントソリューションの仕組みと、この新しい機能を開始するためのセットアップ手順について説明します。

仕組み

1 AWSのアカウントとロールへのユーザーアクセス

特定の個人やユーザーにAWSアクセスを付与すると、各ユーザーはOktaエンドユーザーダッシュボードにログインするだけで開始できるようになります。ユーザーがアプリに割り当てられると、そのユーザーはOktaエンドユーザーダッシュボードから**AWS**のチクレットを選択できるようになります。



AWSアプリを選択すると、AWSのアカウントとロールのピッカーページが表示されます。このページには、特定のユーザーにアクセスが許可されているすべてのアカウントのすべてのロールが表示されます。ここに表示されるものは、そのユーザーに付与されたエンタイトルメントに応じて変わります。たとえば、DevOps管理者には、ティア1のサポートエージェントよりも昇格された権限を必要とするロールやアカウントが表示される場合があります。

Select a role:

▼ Account: PROD (96629466...)

☐ EC2_FullAccess
 ☐ EC2_ReadOnly

▼ Account: TEST (86593466...)

☐ EC2_FullAccess
 ☐ EC2_ReadOnly

Sign In

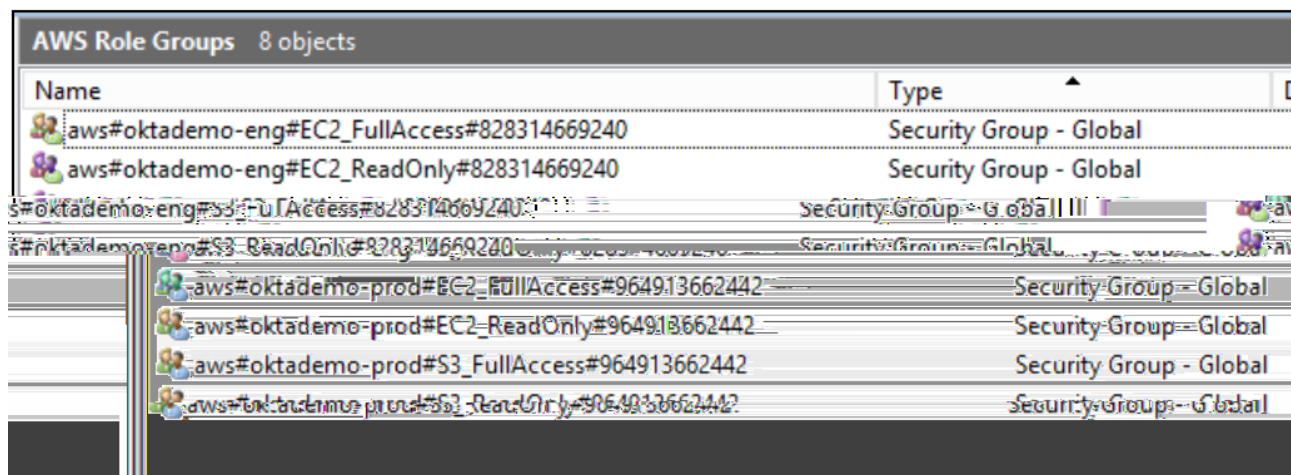
また、そのユーザーが所属する具体的なグループに基づいて、そのユーザーが許可されているロールとアカウントのリストを、OktaからAWSに暗示的にリアルタイムで渡すことができます。特定のAWSアカウントとロールへのアクセスが許可されたADグループやLDAPグループにユーザーを割り当てるだけですむため、管理者による管理が非常に簡単になります。管理者エクスペリエンスの詳細については、以下で説明します。

1 ユーザーやグループによるアカウントとロールへのアクセスの管理

このソリューションの初回リリースでは、この機能の管理は主にADとLDAPでサポートされます。管理者は、次からAD / LDAPグループの2種類の論理セットを操作します：

1 AWSロール固有のグループ

アクセスを提供する特定のアカウントとロールの組み合わせごとに、ADまたはLDAP内にグループが存在する必要があります。これらのグループは、AWSロール固有のグループと呼ばれます。このグループの名前も、特定の構文に従う必要があります（詳細は、この項目の[セットアップ手順](#)に記載されています）。



Name	Type
aws#oktademo-eng#EC2_FullAccess#828314669240	Security Group - Global
aws#oktademo-eng#EC2_ReadOnly#828314669240	Security Group - Global
aws#oktademo-eng#S3_FullAccess#828314669240	Security Group - Global
aws#oktademo-eng#S3_ReadOnly#828314669240	Security Group - Global
aws#oktademo-prod#EC2_FullAccess#964913662442	Security Group - Global
aws#oktademo-prod#EC2_ReadOnly#964913662442	Security Group - Global
aws#oktademo-prod#S3_FullAccess#964913662442	Security Group - Global
aws#oktademo-prod#S3_ReadOnly#964913662442	Security Group - Global

ロール固有のグループのメンバーであるユーザーには、基本的には単一のエンタイトルメント（特定の1つのAWSアカウントの特定の1つのロールへのアクセス権）が付与されます。このグループはスクリプトで作成するか、AWSからリストとしてエクスポートするか、手動で作成できます。

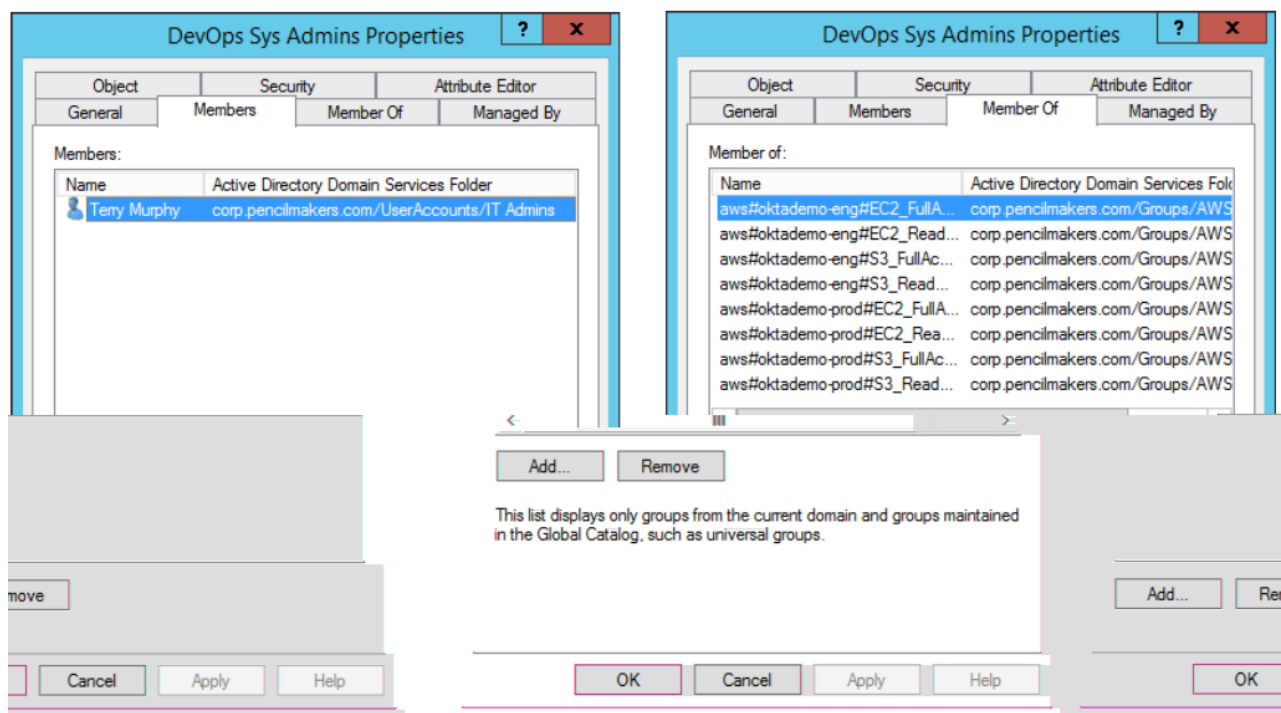
2 管理グループ

各ユーザーを特定のAWSロールグループに割り当ててユーザーアクセスを管理することは、効率的ではありません。管理をシンプルにするために、異なるAWSエンタイトルメントのセットを要求する組織内の異なるユーザーセットごとに、複数のグループを作成することをお勧めします。

このグループは、異なる部門固有のグループの形でAD/LDAP階層にすでに存在している場合がありますが、必要に応じてAWS専用で作成することもできます。

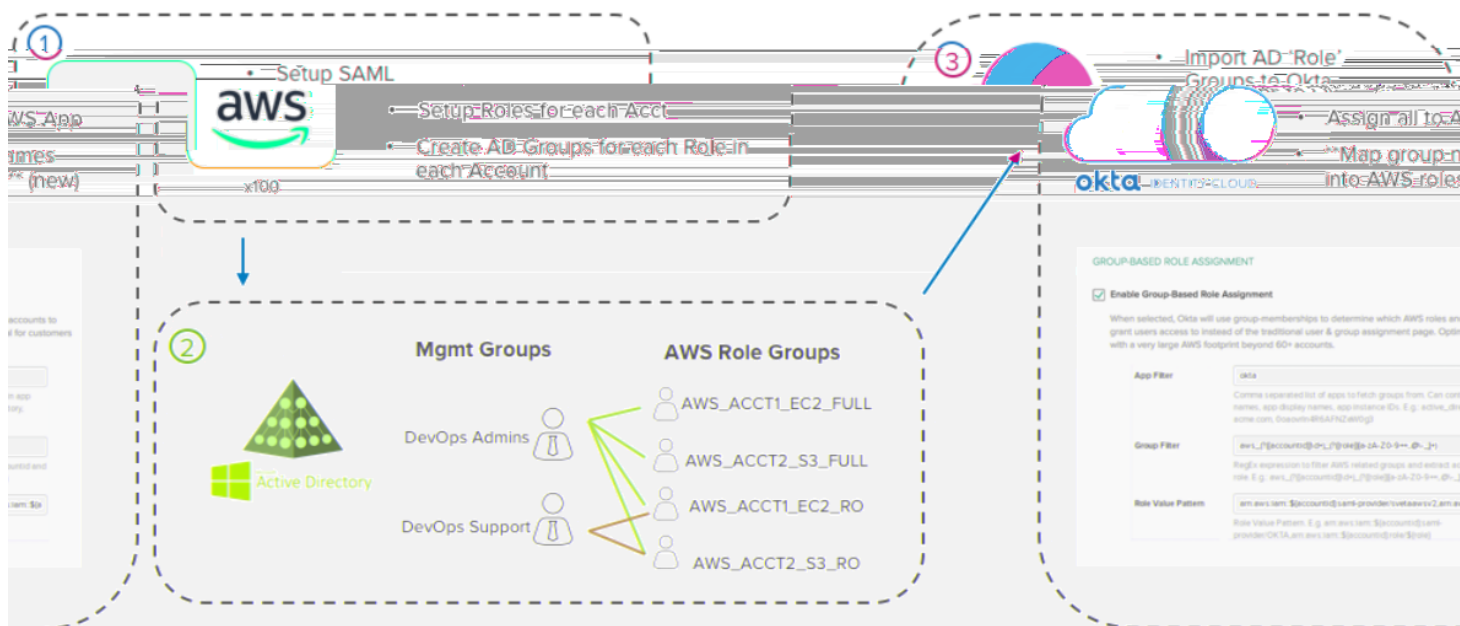
AWS Mgmt Groups 4 objects	
Name	Type
 DevOps Sys Admins	Security Group - Global
 DevOps Tier 1	Security Group - Global
 EC2 Admins	Security Group - Global
 S3 Admins	Security Group - Global

この管理グループは、(グループのMembersとして)ユーザーを割り当て、(Members Ofとして)AWSロールグループを介して特定のエンタイトルメントにユーザーをマッピングする管理レイヤーになります。



Active DirectoryまたはLDAPでこのグループを作成したら、すべての管理操作はこの管理グループで行う必要があります。このグループでのユーザーの追加/削除を行うことで登録されたAWSのアカウントとロールへのアクセス権の付与を行い、Member OfグループプロパティでAWSロールグループの追加や削除を行うことで特定のエンタイトルメントのアップデートを行います。

設計の概略



2 SAML用にAWSを設定する

まず、各AWSアカウントをSAMLアクセス用に構成する必要があります。これを行うには、信頼できるIDPとしてOktaをAWSアカウントに追加してから、新しいIDPを介したアクセスを許可する各ロールの信頼関係を作成します。これは、単一のAWSアカウントにSAML SSOを提供する場合と同じ手順ですが、すべてのアカウントで実行する必要があります。先進的な組織の場合、Cloud FormationやAWS APIスクリプトでこのプロセスを自動化し、各アカウントでSAMLを簡単に設定できます。

2 AD / LDAPでグループの管理レイヤーを作成する

SAMLを構成したら、ユーザーがOktaを介してアクセスできるようにするごとに、AD / LDAPでAWSロールグループを作成する必要があります。これは、AWSとAD/LDAPとの間のスクリプトで行うことも、CSVをADにエクスポートしてから、AD側でそのCSVに対してスクリプトを実行して行うことも、手動で行うこともできます。

次に、管理グループを、アクセスを許可するAWSロールグループのメンバーとして割り当てることにより、これらのAWSロール固有のグループと他のAD / LDAPグループの間にリンクを作成できます。完了したら、ユーザーを管理グループに割り当てて、管理グループがメンバーになっているすべてのAWSのロールとアカウントへのアクセスを許可します。

2 グループベースのロール割り当て用にOktaでAWSアプリを構成する

最後にOktaで、AD/LDAP管理グループとロールグループの両方を、OktaのADエージェントかLDAPエージェントを介してインポートします。次に、管理グループをステップ1でセットアップしたAWSアプリケーションに割り当てます（これにより、適切なユーザーがAWSアプリに割り当てられます）。最後に、グループベースのロール割り当てをセットアップして、各AWSロールグループをの名前をAWSが使用できる形式に変換し、ロールのピッカーページに適切なロールが表示されるようにします。

設定手順

この手順では、この機能で[想定されるエクスペリエンス](#)と、この機能の[設計の概略](#)について理解していることを想定しています。不明な場合は、上記のセクションをご覧ください。

ステップ1: SAML SSO用にAWSのアカウントとロールをセットアップする

まず、OktaですべてのAWSアカウントをSAMLアクセス用にセットアップします。

Oktaで新しいAWSアプリを作成し、[Single Sign-On (シングルサインオン)] タブで[SAML]を選択して開始します。

- 2 製品内ガイドを開いて、ガイドの「Oktaを[単一のAWSインスタンス](#)に接続する」の箇所に記載されたステップ1とステップ2を実行します:
 - a. [\(単一のインスタンス\)ステップ1: OktaをAWSアカウントのIDプロバイダーとして構成する](#)
 - b. [\(単一のインスタンス\)ステップ2: Okta IDプロバイダーをAWSロールの信頼できるソースとして追加する](#)

これを、ユーザーにアクセスを許可するすべてのAWSのアカウントとロールごとに行い、すべてのアカウントが同じ正確なSAMLメタデータでセットアップされ、同じ正確な名前で命名されるようにします。異なるSAMLプロバイダー名やメタデータドキュメントを持つアカウントにはアクセスできなくなります。

ステップ2: AD / LDAPでAWSロールグループを作成する

すべてのAWSアカウントをSAML用に構成したら、ユーザーがアクセスする各アカウントの各AWSロールごとにグループをADで作成する必要があります。これは、いくつかの異なる方法で行えます:

- オプション1: AWSとAD / LDAP間のスクリプトで、各アカウントの各ロールごとにADグループを作成するこのオプションを使用すると自動化の可能性が最も高くなりますが、スクリプトを構成するために、AWS管理チームとAD / LDAP管理チームとの間で調整が必要になります。今後、セットアップを簡単にするためのサンプルスクリプトを提供する予定ですが、このソリューションの初回リリースでは、そのようなスクリプトは提供されません。
- オプション2: AWSからCSVでエクスポートする
AWSとAD / LDAPとの間のスクリプトによる方法が不可能な場合には、各AWSアカウントのロール名のリストをCSVファイルにエクスポートして、AD / LDAP管理者チームに提供するという軽量アプロー

チを利用できます。ここからAWSロールグループの作成を管理できますが、依存関係を設定したり、AWSアカウント自体と直接統合したりする必要はありません。

- オプション3: 手動で作成する

AWSロールグループはAD / LDAPでいつでも手動で作成できます。これは最も単純な方法ですが、各アカウントの各ロール用にAD / LDAPでグループを作成するには、維持管理と十分な設定時間が必要になります。

AWSロール固有のグループをディレクトリでどのように作成するかにかかわらず、次の手順を行うことを推奨します:

- 1 ディレクトリのどこかに新しいOUを作成して、すべてのAWSロール固有のグループを分離できるようにします。必須ではありませんが、管理者によるグループ管理をシンプルにするためにこれを行うことを推奨します。OUの名前は、「AWSロールグループ」、「AWSエンタイトルメント」などにします。
- 2 標準の構文を使用して、ロールごとにADセキュリティグループを作成します。わかりやすくするために、Oktaは次の構文の使用を推奨しています。

aws#<account alias>#<role name>#<account #>

例: **aws#northamerica-production#Tier1_Support#828416469395**

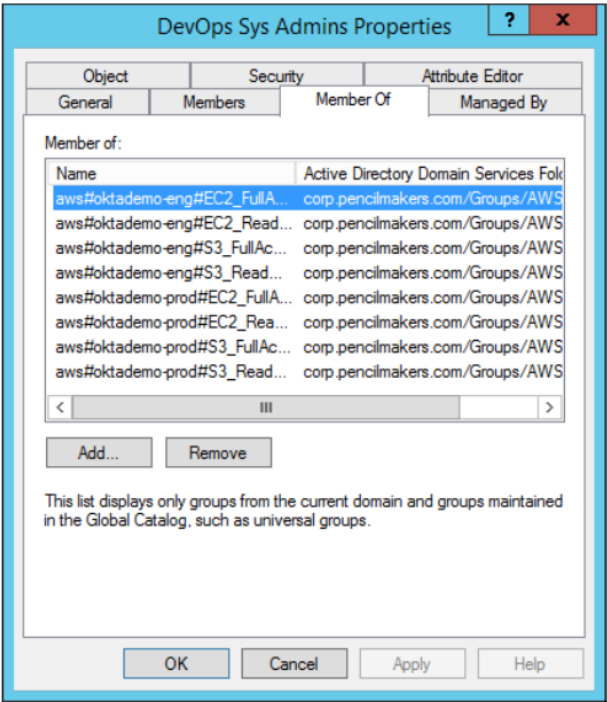
独自のグループ構文を使用する場合は、アカウントのエイリアス、ロール名、アカウント番号を、それぞれの間に識別可能な区切り文字を加えて含めてください。また、後の手順でカスタムの正規表現式を作成できる必要があるため、これを行う場合は高度な項目に慣れている必要があります。

ステップ3: ユーザーをAWSのアカウントとロールにマッピングするためにAD / LDAP管理グループを構成する

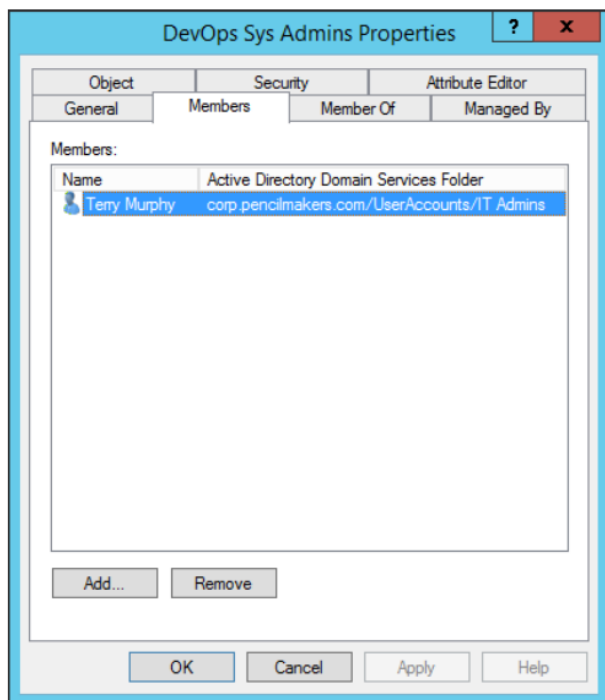
次に、別のAD / LDAPグループのセットを作成または使用して、ユーザーのセットと、ユーザーがアクセスする特定のAWSのアカウントとロールとのリンクを確立します。

- 1 さまざまなユーザーがアクセスするAWSエンタイトルメントの管理に使用するグループがADにまだない場合は、以下を行います:
 - a. 「AWS管理グループ」用の別のOUをディレクトリに作成します。AWS管理グループをディレクトリ内の好きな場所に配置することもできますが、管理を容易にするために別のOUを使用することを推奨します。
 - b. 異なるAWSのロールとアカウントのセットを必要とするユーザーの集団ごとにグループを作成します。「ティア1 AWSサポート」「データベース管理者」「AWSスーパー管理者」など、作成したグループに好きな名前を付けます。

使用する管理グループを用意したら、それぞれのグループを、そのグループがアクセスするすべてのAWSロールグループのメンバーにします。これにより、管理グループと、グループユーザーがアクセスする必要があるすべてのAWSアカウントのエンタイトルメントの間にリンクが確立されます。このページから、AWSエンタイトルメントの追加、削除、変更、監査を管理グループごとに行えます。



- 3 次に、ユーザーをグループのメンバーにすることで、ユーザーをグループに直接割り当てます。各グループのユーザーメンバーシップの追加、削除、変更、監査も、このページから行えます。














この管理グループは、さまざまなAWSエンタイトルメントのセットへのユーザーアクセスの管理と監査を行うための中央コントロールポイントになります。

ステップ4: AWSロールグループと管理グループをOktaにインポートする

次に、AWSロールグループと管理グループの両方をOktaにインポートして、ステップ1で構成したAWSアプリで使用するために構成する必要があります。

グループのインポートは、通常Okta ADエージェントかLDAPエージェントを介して実行されます。Okta AD / LDAP エージェントのインストール手順は、製品内で[**Directory**(ディレクトリ)]>[**Directory Integrations**(ディレクトリ統合)]に移動して確認できます。

完了後、Okta管理コンソールの[**Groups**(グループ)]ページに、AWSロールグループと管理グループの両方が表示されるはずです。

All Rules				
Add Group		Search...		
Source	Name	People	Apps	Directories
	aws#oktademo-eng#EC2_FullAccess#828314669240 corp.pencilmakers.com/Groups/AWS Role Groups/aws\#oktademo-eng\#EC2_FullAccess\#828314669240	2	0	0
	aws#oktademo-eng#EC2_ReadOnly#828314669240 corp.pencilmakers.com/Groups/AWS Role Groups/aws\#oktademo-eng\#EC2_ReadOnly\#828314669240	2	0	0
	aws#oktademo-eng#S3_FullAccess#828314669240 corp.pencilmakers.com/Groups/AWS Role Groups/aws\#oktademo-eng\#S3_FullAccess\#828314669240	1	0	0
	aws#oktademo-eng#S3_ReadOnly#828314669240 corp.pencilmakers.com/Groups/AWS Role Groups/aws\#oktademo-eng\#S3_ReadOnly\#828314669240	1	0	0
	aws#oktademo-prod#EC2_FullAccess#964913662442 corp.pencilmakers.com/Groups/AWS Role Groups/aws\#oktademo-prod\#EC2_FullAccess\#964913662442	2	0	0
	aws#oktademo-prod#EC2_ReadOnly#964913662442 corp.pencilmakers.com/Groups/AWS Role Groups/aws\#oktademo-prod\#EC2_ReadOnly\#964913662442	2	0	0
	aws#oktademo-prod#S3_FullAccess#964913662442 corp.pencilmakers.com/Groups/AWS Role Groups/aws\#oktademo-prod\#S3_FullAccess\#964913662442	1	0	0
	aws#oktademo-prod#S3_ReadOnly#964913662442 corp.pencilmakers.com/Groups/AWS Role Groups/aws\#oktademo-prod\#S3_ReadOnly\#964913662442	1	0	0
	DevOps Sys Admins corp.pencilmakers.com/Groups/AWS Mgmt Groups/DevOps Sys Admins	1	1	0
	DevOps Tier 1 corp.pencilmakers.com/Groups/AWS Mgmt Groups/DevOps Tier 1	0	1	0
	EC2 Admins corp.pencilmakers.com/Groups/AWS Mgmt Groups/EC2 Admins	1	1	0

ステップ5: Oktaでグループベースのロールマッピングを有効にする

グループをOktaにインポートした後、ステップ1でセットアップしたAWSアプリケーションを構成して、AWSロールグループのメンバーシップをAWSが構文として解釈可能なエンタイトルメントに変換します。

1. ステップ1でセットアップしたAWSアプリケーションに移動します。
2. [Single Sign On (シングルサインオン)] タブに移動して、ページ右上の [Edit (編集)] を選択します。
3. **App Filter**、**Group Filter**、**Role Value Pattern** のフィールドを見つけます - これらのフィールドは、Oktaがこの機能でAWSロールグループをエンタイトルメントにどのようにマッピングするかを制御します。このフィールドを次のように構成します:

App Filter	<input type="text" value="active_directory"/> Comma separated list of apps to fetch groups from. Can contain app names, app display names, app instance IDs. E.g.: active_directory, acme.com, 0oaovrn4R6AFNZeW0g3
Group Filter	<input type="text" value="^aws\#\S+\#(?:{role})[\\w\-\+)]\#(?:{accountid})\d+\$"/> RegEx expression to filter AWS related groups and extract accountid and role. E.g.: aws_{accountid}\d+_{role}[a-zA-Z0-9+.,@_-]+)
Role Value Pattern	<input type="text" value="arn:aws:iam::\${accountid}:saml-provider/ReInvent.Oktapreview,arn:a"/> Role Value Pattern. E.g. arn:aws:iam::\${accountid}:saml-provider/OKTA,arn:aws:iam::\${accountid}:role/\${role}

- **App Filter** - アプリフィルターは、Oktaが特定のアプリやディレクトリへのAWSエンタイトルメントマッピングで使用するグループのリストを絞り込みます。これはセキュリティ上の目的で導入されるもので、不正な管理者が特定のAWSのアカウントやロールに意図的に不正アクセスするために、特定の構文に従ってグループを作成する問題を回避できます。Active Directoryでグループを作成している場合には、**active_directory**を入力できます。
- **Group Filter** - グループフィルターフィールドは正規表現式を使用して、特定の構文に従う選択したアプリフィルターのグループのみを検査します。上で表示されているデフォルトの推奨AWSロールグループ構文を使用する場合は、次の正規表現文字列を使用します:

```
^aws\#\S+\#(?:{role})[\\w\-\+)]\#(?:{accountid})\d+$
```

-この正規表現式は論理的には、AWSで始まり、次に#、次にテキスト文字列、次に#、次にAWSロール、次に#、次にAWSアカウントIDがあるグループを検索することに相当します。

デフォルトの推奨AWSロールグループ構文を使用しない場合、AWSロールグループを適切に

フィルタリングし、**{{role}}**および**{{accountid}}**という2つの異なる正規表現グループ内でAWSロール名とAWSアカウントIDを取得する正規表現式を作成する必要があります。

- **Role Value Pattern** - このフィールドは、AWSロールグループの構文内で取得されたAWSのロールとアカウントIDを取得し、Okta SAMLアサーションで必要となる適切な構文に変換することで、ユーザーがサインイン時にアカウントとロールを確認できるようにします。

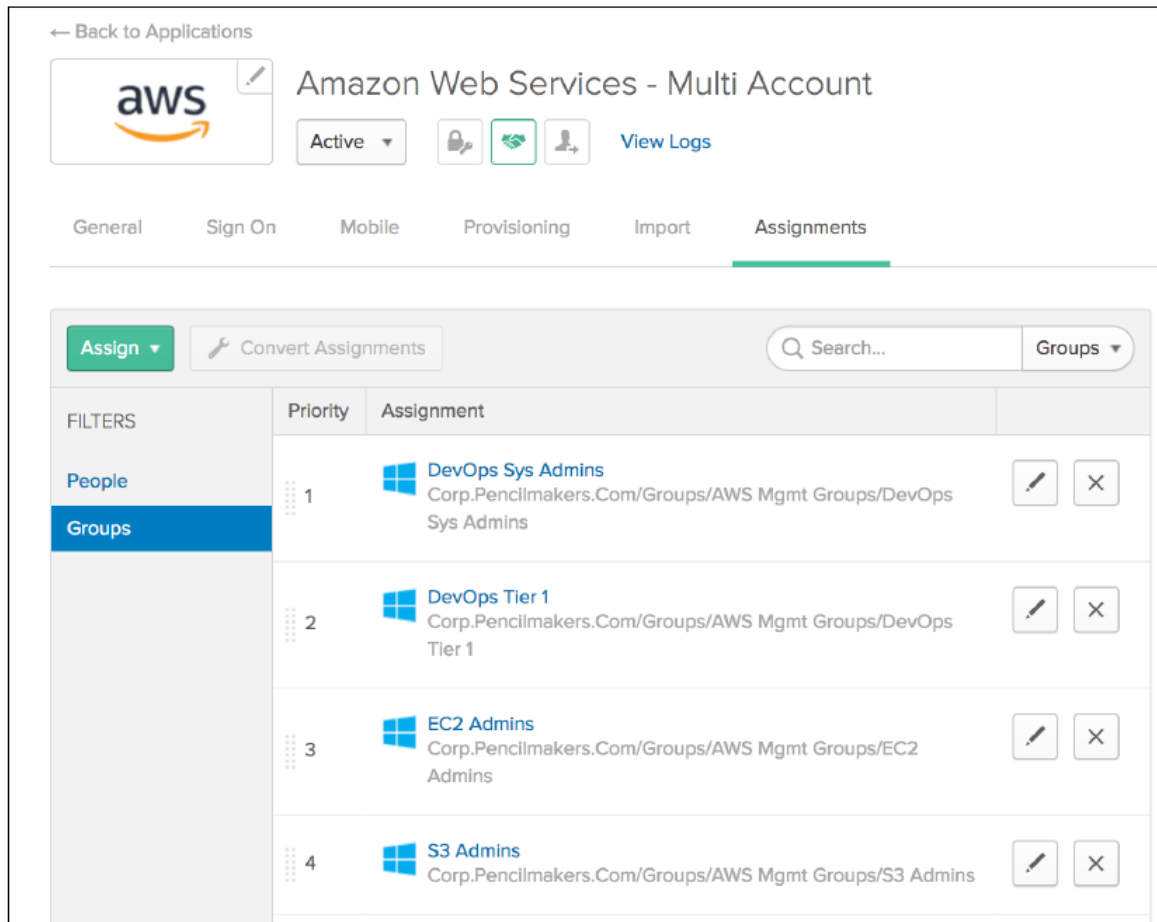
このフィールドは、常に次の特定の構文に従う必要があります：

arn:aws:iam::\${accountid}:saml-provider/<<SAML Provider Name>>,arn:aws:iam::\${accountid}:role/\${role}


<<SAML Provider Name>>を、ステップ1ですべてのAWSアカウントでセットアップしたSAMLプロバイダーの名前に置き換えます。それ以外の文字列は変更せず、コピー&ペーストのみ行います。




ステップ6: OktaですべてのAWS管理グループをAWSアプリに割り当てる

AWSロールグループをエンタイトルメントにマッピングするようにAWSアプリを適切に構成できたので、最後にOktaですべてのAWS管理グループをアプリケーションに割り当てます。これにより、適切なすべてのユーザーがAWSアプリに自動的に割り当てられます。また、ステップ5で完了した手順のおかげで、アクセスする必要のある適切なエンタイトルメントのみがユーザーに表示されるようになります。
















← Back to Applications

 Amazon Web Services - Multi Account

Active    View Logs

General Sign On Mobile Provisioning Import **Assignments**

Assign  Convert Assignments Groups

FILTERS	Priority	Assignment	
People			
Groups			
	1	 DevOps Sys Admins Corp.Pencilmakers.Com/Groups/AWS Mgmt Groups/DevOps Sys Admins	 
	2	 DevOps Tier 1 Corp.Pencilmakers.Com/Groups/AWS Mgmt Groups/DevOps Tier 1	 
	3	 EC2 Admins Corp.Pencilmakers.Com/Groups/AWS Mgmt Groups/EC2 Admins	 
	4	 S3 Admins Corp.Pencilmakers.Com/Groups/AWS Mgmt Groups/S3 Admins	 

これで、セットアップが完了しました！ユーザーがOktaエンドユーザーダッシュボードからAWSアプリにアクセスできること、シームレスにサインインできることを確認します。