AWS のクレデンシャルと権限

Cloud Manager

Ben Cammett, Aksel Davis
April 08, 2021

目次

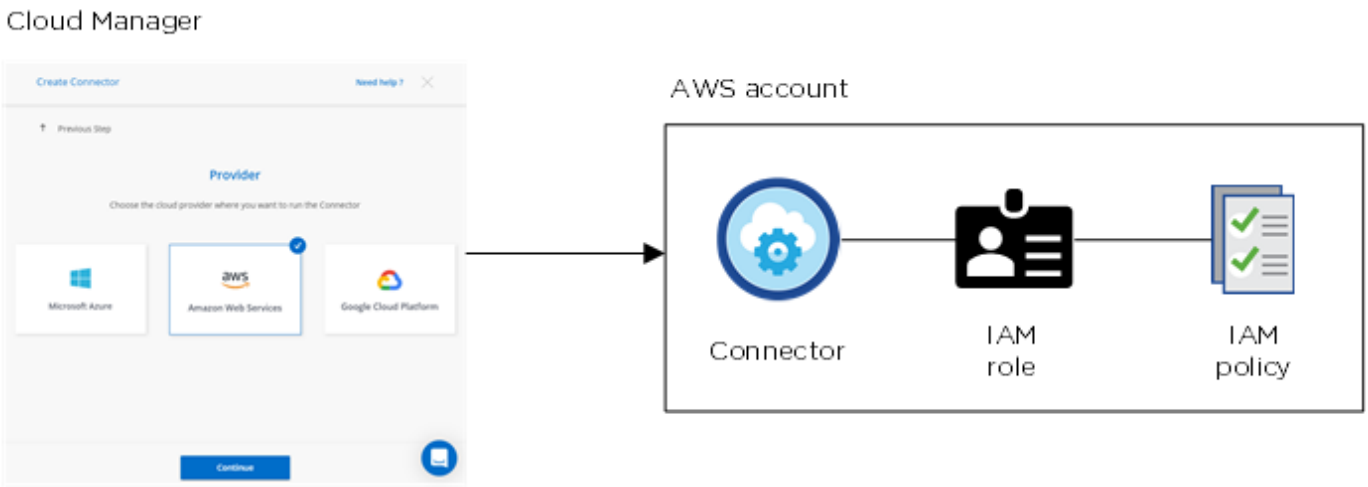
AWS のクレデンシャルと権限

Cloud Manager では、 Cloud Volumes ONTAP の導入時に使用する AWS クレデンシャルを選択できます。すべての Cloud Volumes ONTAP システムは、初期の AWS クレデンシャルを使用して導入することも、クレデンシャルを追加することもできます。

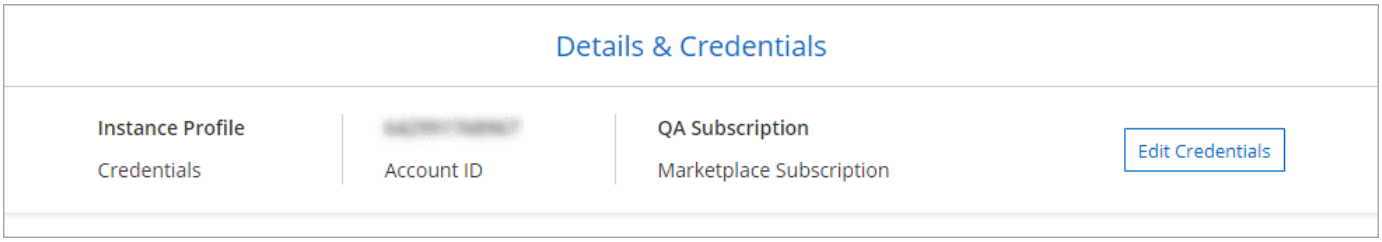
AWS の初期クレデンシャル

Cloud Manager からコネクタを導入するときは、権限を持つ AWS アカウントを使用して Connector インスタンスを起動する必要があります。必要な権限は、に表示されます "AWS 用のコネクタ導入ポリシー"。

Cloud Manager が AWS でコネクタインスタンスを起動すると、インスタンス用の IAM ロールとインスタンスプロファイルが作成されます。また、 Cloud Manager にその AWS アカウント内のリソースやプロセスを管理する権限を付与するポリシーも適用されます。 "Cloud Manager での権限の使用方法を確認します。"。

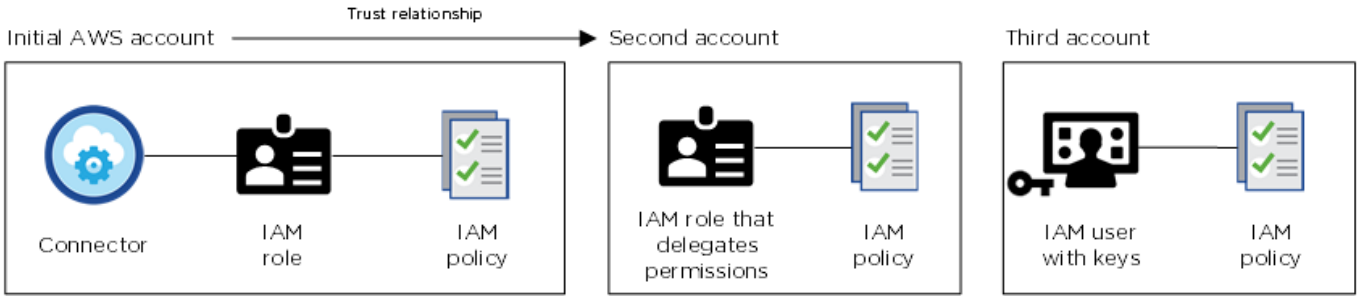


Cloud Volumes ONTAP の新しい作業環境を作成すると、 Cloud Manager で選択される AWS クレデンシャルにはデフォルトで次のものがあります。



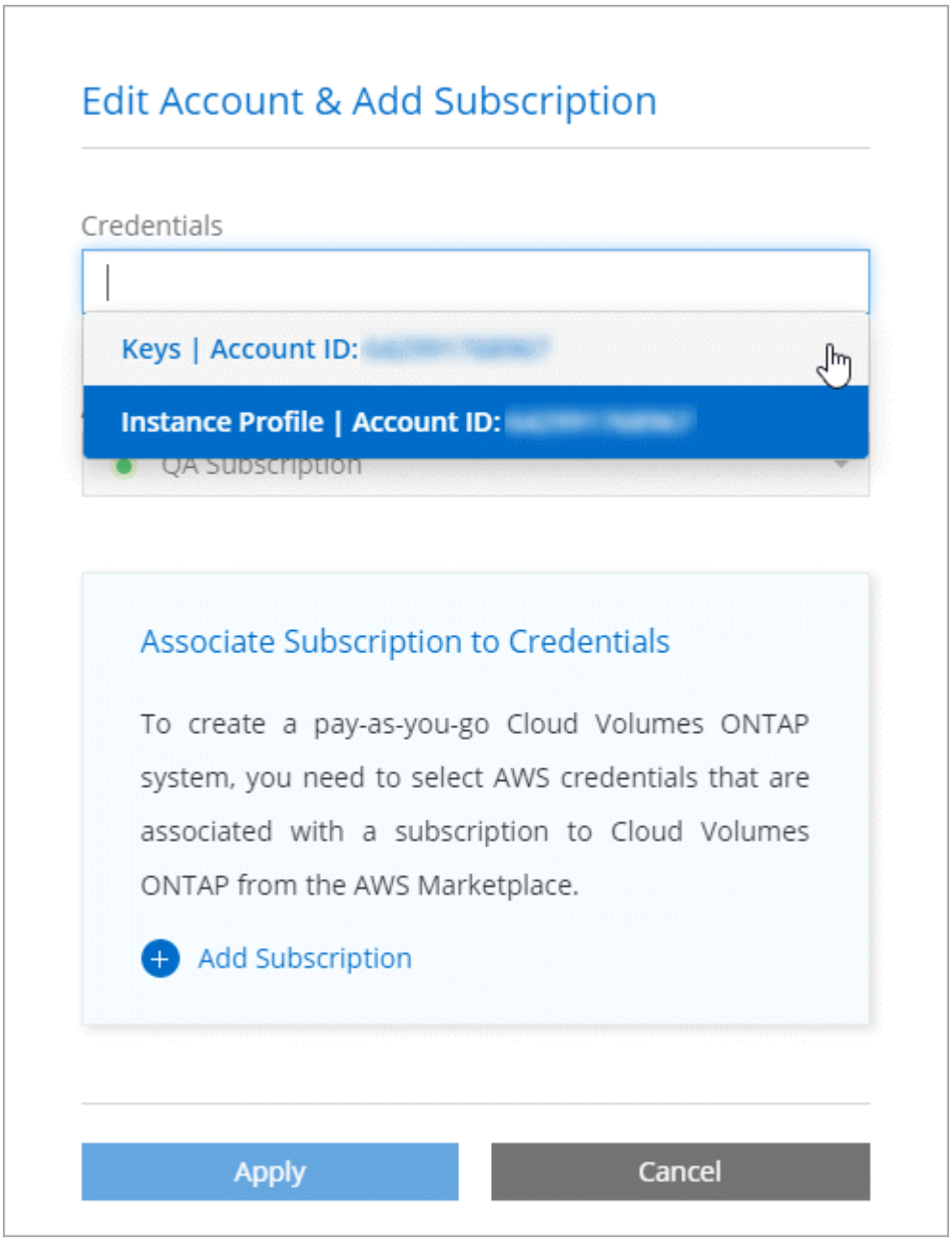
追加の AWS クレデンシャル

別々の AWS アカウントで Cloud Volumes ONTAP を起動する場合は、どちらかを実行します "IAM ユーザまたは ARN に AWS キーを指定します 信頼できるアカウントのロール"。次の図は、 2 つの追加アカウントを示しています。 1 つは、信頼されたアカウントの IAM ロールを介してアクセス許可を提供し、もう 1 つは IAM ユーザの AWS キーを使用してアクセス許可を提供します。



そのあとで "Cloud Manager にアカウントのクレデンシャルを追加します" IAM ロールの Amazon リソース名（ ARN ）、または IAM ユーザの AWS キーを指定します。

クレデンシャルを追加したら、新しい作業環境を作成するときにクレデンシャルに切り替えることができます。



ページで [アカウントの切り替え] をクリックした後に、クラウドプロバイダアカウントを選択する方法を示すスクリーンショット。"]

市場への導入とオンプレミスの導入についてはどうでしょうか。

上記の各セクションでは、 Cloud Manager のコネクタで推奨される導入方法について説明します。から AWS に Connector を導入することもできます "AWS Marketplace" また、次のことも可能です "コネクタをオンプレミスにインストールします"。

Marketplace を使用する場合も、アクセス許可は同じ方法で提供されます。IAM ロールを手動で作成して設定し、追加のアカウントに権限を付与するだけで済みます。

オンプレミス環境では、 Cloud Manager システム用の IAM ロールを設定することはできませんが、追加の AWS アカウントの場合と同様に権限を付与することはできます。

AWS クレデンシャルを安全にローテーションするにはどうすればよいですか。

前述したように、 Cloud Manager では、いくつかの方法で AWS クレデンシャルを提供できます。信頼されたアカウントで IAM ロールを割り当てるか、 AWS アクセスキーを指定することで、コネクタインスタンスに関連付けられた IAM ロールを指定できます。

最初の 2 つのオプションでは、 Cloud Manager は AWS Security Token Service を使用して、継続的にローテーションする一時的なクレデンシャルを取得します。このプロセスはベストプラクティスであり、自動的に実行され、セキュリティが確保されています。

Cloud Manager に AWS アクセスキーを指定する場合は、 Cloud Manager でキーを一定の間隔で更新して、キーをローテーションする必要があります。これは完全に手動で行います。