AWS Integration Options

AWS (including IAM Identity Center-AWS SSO) can be integrated with Authomize so that Authomize can pull information about identities, groups and assets that are known on your AWS account.

AWS can be integrated with Authomize on specific accounts or an organizational account. The procedure is a bit different in each case, so they are described separately:

Legacy method

- Generate a user for Authomize with an access key.
- Create a role in each user account.
- Your user can use the roles to gain access to your accounts

Assumed Role-based Integration

CloudFormation for individual accounts

- Create a role for each account.
- Allow an Authomize users to access the roles.

CloudFormation for an organizational account

- Create a role and assign it to all your accounts.
- Allow an Authomize user to access the role.

Notes:

- Authomize generates a role on AWS that Authomize can use.
- Authomize randomly generates a unique ExternalID for each customer (as recommended by AWS).
- The AWS role requires a unique ExternalID (supplied by Authomize) to make the connection more secure.

Before you begin

To integrate AWS with Authomize, you need the following privileges:

- the ability to create new roles on AWS
- access to a management account (only if you want to set up an organizational account, or set up an SSO).
- AWS CloudFormation privileges

With the legacy method, you need to create a user with “programmatic" credentials and one role per account that the user can assume.

What Do We Do with Those Credentials?

We list resources, policies and CloudTrail logs. We don't make too many calls there, and it shouldn't cost anything or cost very little (the number of objects is small). To be exact, those are the actions we perform at low numbers repeatedly. The list might grow a bit as we expand our AWS coverage, but the cost should remain low.

We read CloudTrail logs (only management ones, not data events). Those do cost, but it should be quite low.

API calls we make:

- list groups
- list local policies
- list roles
- list users
- list AWS policies
- list AWS users access keysEc2 service resources
- EC2 network