Collecting AWS Inventory and Configuration Data to Snowflake

This tutorial teaches you how to set up your AWS accounts for inventory and configuration data gathering to Snowflake. Once the configuration steps are completed, your SnowAlert container will be able to collect extensive audit data to Snowflake for analysis.

Guidance

- We recommend running the SnowAlert container in an AWS account dedicated to your security or audit team. Having such an account is helpful in restricting who can assume security audit permissions.
- For a general reference on AWS cross-account role assumption, see Tutorial: Delegate Access Across AWS Accounts Using IAM Roles.

Step 1: Create a security auditor role

Follow the process below to create a new role in the AWS account where SnowAlert is running. The new role will be assumed by SnowAlert Connectors Runner in order to enumerate the accounts in the organization and then to assume the local audit roles in each of those accounts. The process for creating the role is:

1. Sign in to the AWS Management Console as an administrator of the security account (e.g. 111111111111) where SnowAlert is running.
2. In the navigation bar, choose **Support**, and then **Support Center**. The 12-digit account number (ID) appears in the Support Center title bar, copy it for use in the trust policy as detailed below.
3. Open the IAM console Roles page at https://console.aws.amazon.com/iam/home#/roles
4. Click the button to create a new IAM role.
5. Select **AWS Service**, then, if SnowAlert is running in ECS Fargate, select **Elastic Container Service** and **Elastic Container Service Task**, and if SnowAlert is running on an EC2 instance, select **EC2**.
6. Select the AWS managed policy **`SecurityAudit`** to attach to the new role.
7. Enter **`security-auditor`** as the role name.
8. Click **Create role**.
9. Edit this newly created role to allow SnowAlert to assume it from within your security account by specifying the security account ID in the following policy document:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "ecs-tasks.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111111111111:root"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

For a detailed walkthrough on role creation, see Now Create and Manage AWS IAM Roles More Easily with the Updated IAM Console.

Step 2: Create a local audit roles

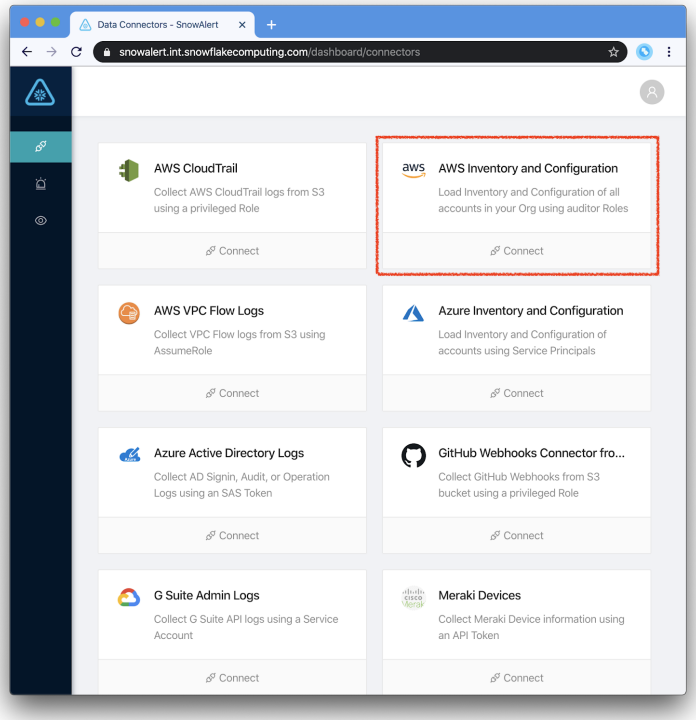
Follow the process below to create a new role in the master account of your AWS Organization, as well as all of the other AWS account in the organization. In the master account, this role will be used to get a full listing of your AWS accounts, and to audit inventory and configurations of all of the accounts. The process to create local auditor roles is:

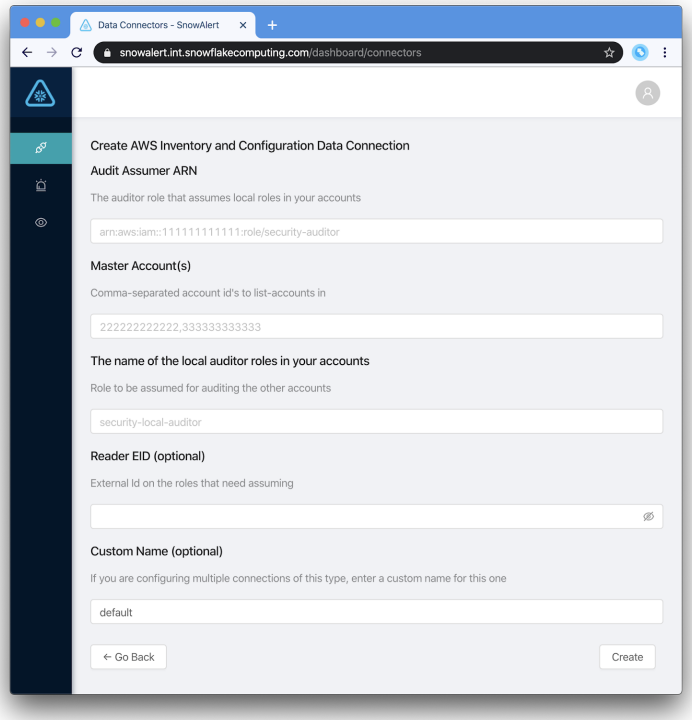
1. Sign in to the AWS Management Console as an administrator of the master account where your AWS Organization was created.
2. Open the IAM console at https://console.aws.amazon.com/iam/.
3. Click the button to create a new IAM role.
4. Select **AWS Service**, then, if SnowAlert is running in ECS Fargate, select **Elastic Container Service** and **Elastic Container Service Task**, and if SnowAlert is running on an EC2 instance, select **EC2**.
5. Select the AWS managed policy **`SecurityAudit`** to attach to the new role.
6. Enter **`security-local-auditor`** as the role name.
7. Click **Create role**.
8. Edit the Trust Policy of the newly created role to allow SnowAlert to assume it from within your security account by specifying the security account ID in the following policy document:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111111111111:role/security-auditor"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

For more information on AWS Organizations and the master account that owns them, see Managing Access Permissions for Your AWS Organization.

3. Create a AWS Inventory and Configuration Connection





SnowAlert comes with a Data Connector for streaming AWS inventory and configuration data to Snowflake. This data supports analytics such as CIS compliance validation.

In SnowAlert v1.9.2, specify the following values in the “AWS Collect” data connector:

- Audit Assumer ARN
  - In this tutorial, the security account ID was 111111111111.
  - For example: **`arn:aws:iam::111111111111:role/security-auditor`**
- The Account ID's of the Master accounts to be scanned
  - In this tutorial, the account ID where the Organization resides is 222222222222
  - The connector AssumeRole in each of these, run list-accounts, and use the results if it gets a list, or the account alone if it gets an error, to AssumeRole and gather Inventory and Configuration Data
  - For example: `222222222222`
- The reader role in Org’s accounts
  - Use the name of the local auditor roles that were created in each account.
  - Note that no ARN needs to be specified because the account IDs are taken from the list of accounts performed within the master account.
  - For example: **`security-local-auditor`**
- Reader EID
  - Leave blank unless you used an EID in your Trust Policies (advanced).

Press the **Create** button and verify that data is landing in the new AWS Collect tables using:

```
SHOW TABLES LIKE 'aws_collect_%' IN SCHEMA data;
```

You have completed configuring your AWS environment for centralized auditing using the SnowAlert “AWS Inventory and Configuration” Data Connector.