SCALE AWS INTEGRATION ACROSS AWS ORGANIZATIONS

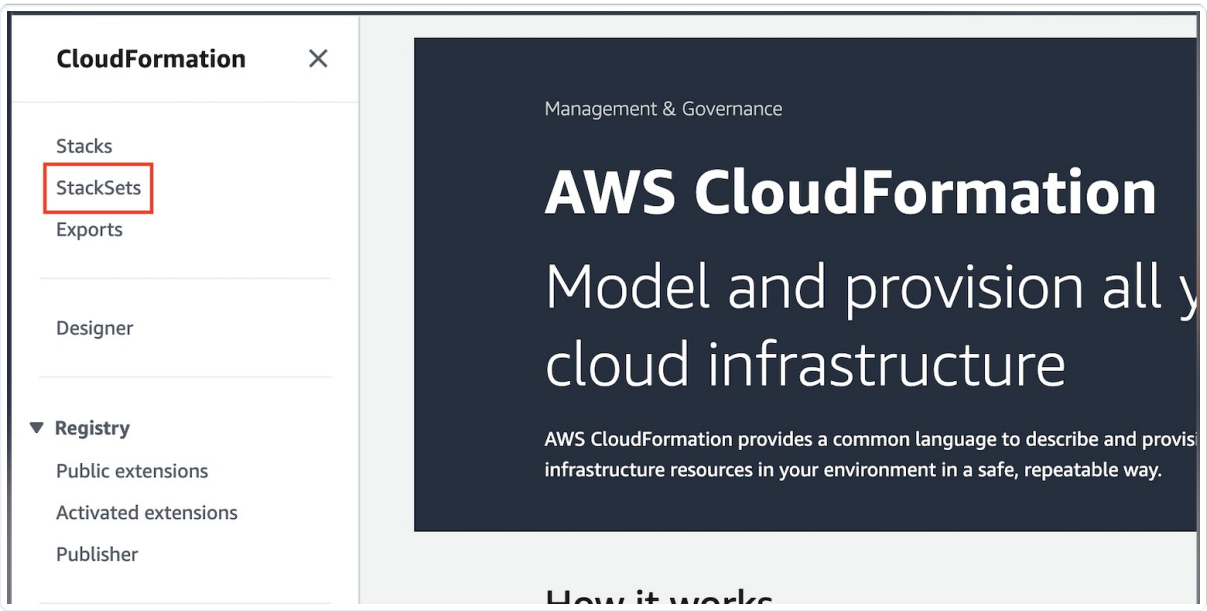
> The following information is not intended to apply to all variations of customer environments. There can be several factors that may prohibit you from achieving the intended results. As such, this document should be treated as general guidance. These instructions were written for an out-of-box AWS organization containing a single organization unit. If your organization differs, please adapt the instructions to fit your requirements.

There are two steps in this process:

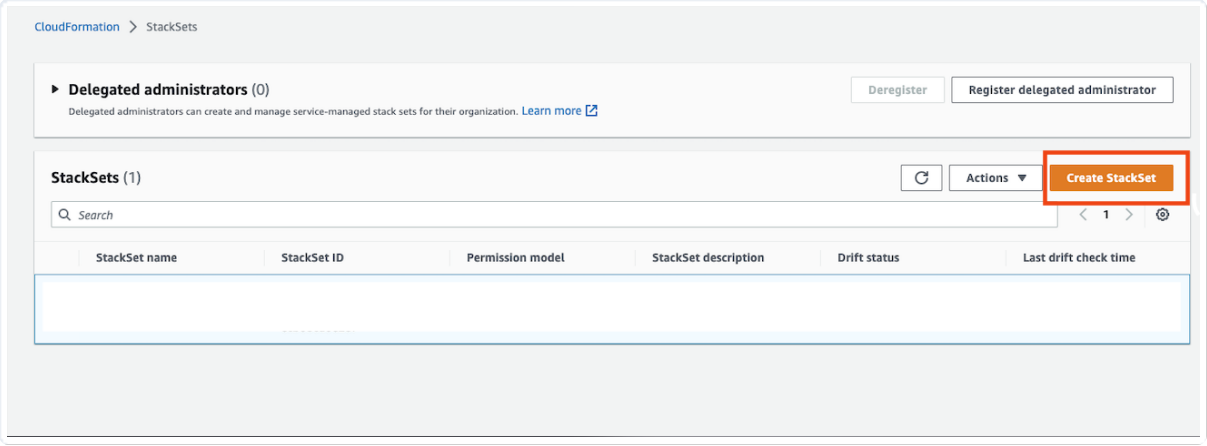
1. **Create the Stack Set**
2. **Gather the Role ARNs**

Create the Stack Set

1. Sign in to the AWS Management Console as the root user.
2. Navigate to the **CloudFormation** service and select **StackSets**.



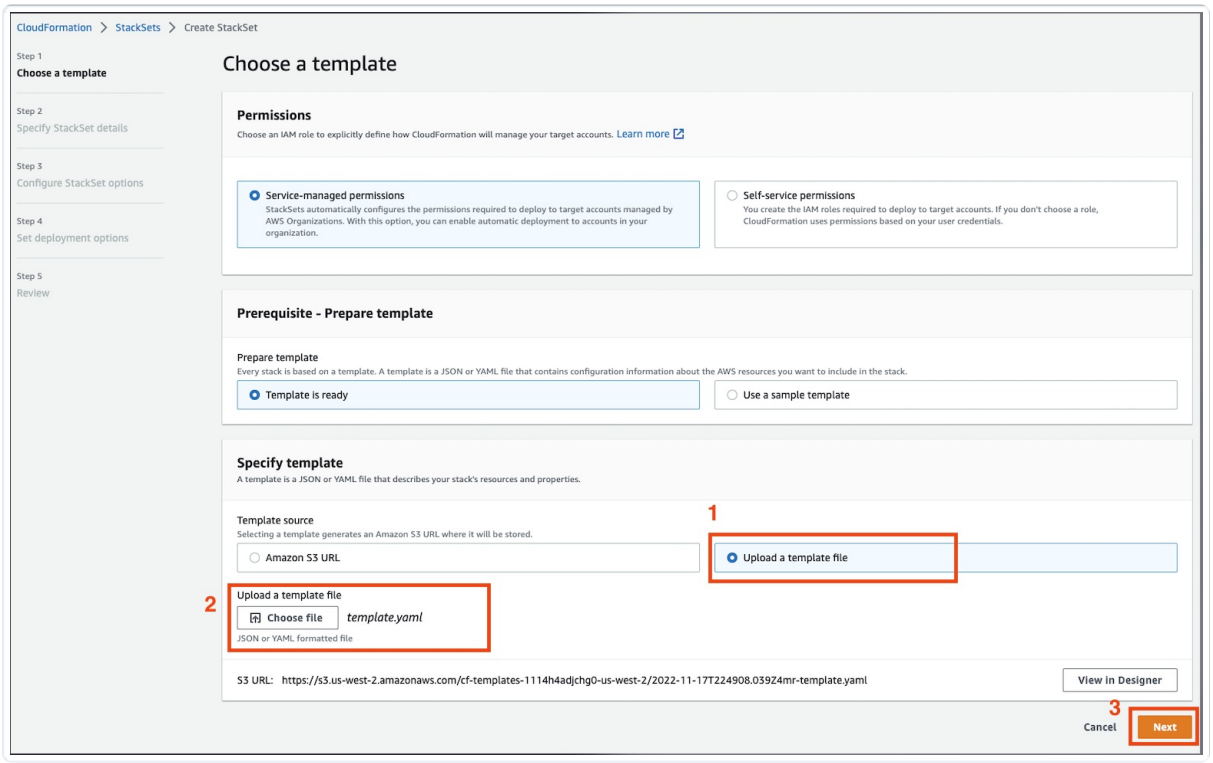
3. Click **Create StackSet**.



4. Under the **Specify template**, select **Upload a template file**, upload this

CloudFormation template file (https://dyzz9obi78pm5.cloudfront.net/app/image/id/66c8986f7d85fddd810af7c2/n/cloudformation-template.yaml), and click **Next**.

> Ensure you are using the version of this template file that allows the `masm-access-policy` policy access to `ec2:DescribeInstances`, `route53:ListHostedZones`, `route53:ListResourceRecordSets`, `s3:ListAllMyBuckets`, and `rds:DescribeDBInstances`.



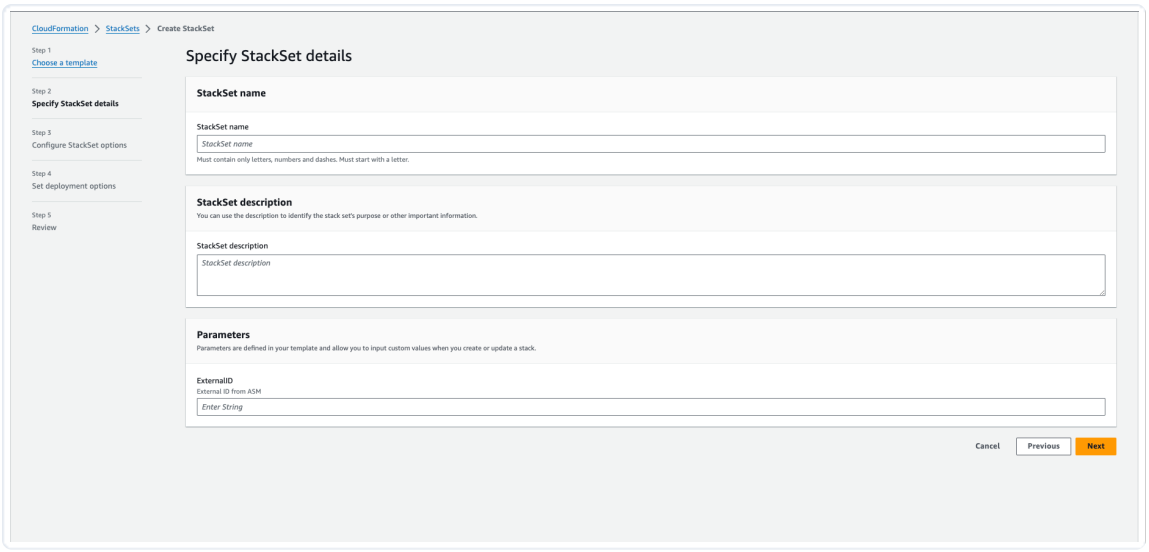
5. Populate the following fields and click **Next**.
   a. **StackSet name**: This should be a memorable value such as *Mandiant-ASM-Integration-StackSet*.
   b. **StackSet description**
   c. **External ID**

> Requiring an External ID is an AWS best practice when a third party (MA-ASM, in this case) assumes the role.

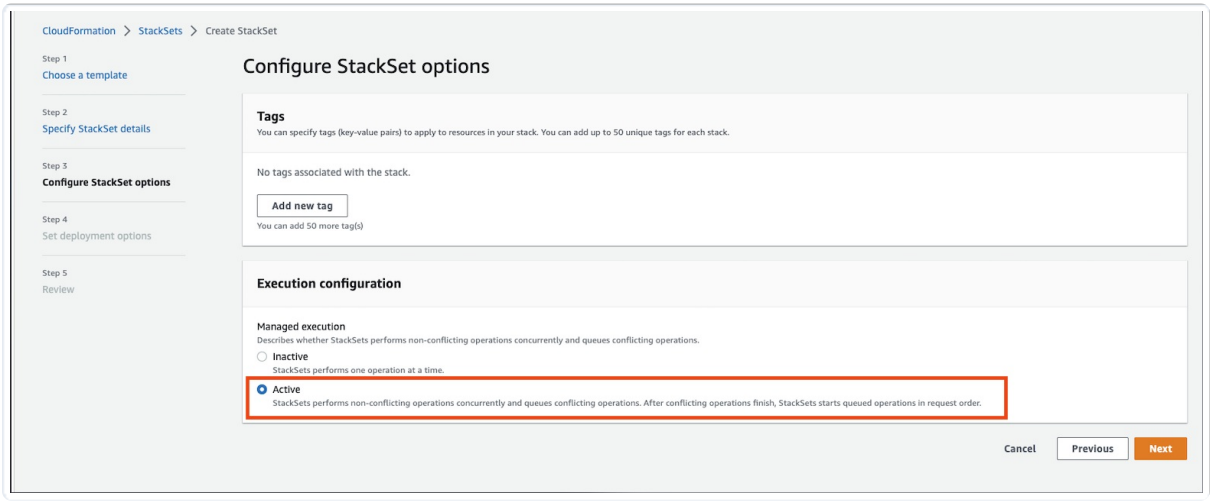
External ID per MA-ASM

- There is one External ID per MA-ASM project.
- To access the **AWS External ID** from MA-ASM:
  1. From the **Projects and Settings** menu in MA-ASM, select the appropriate Project then click Account Settings.
  2. Click **Integrations**.
  3. Click **Add New** for **AWS (Roles)**.
  4. Click **Copy Key**.

AWS External ID in MA-ASM with **Copy Key** option



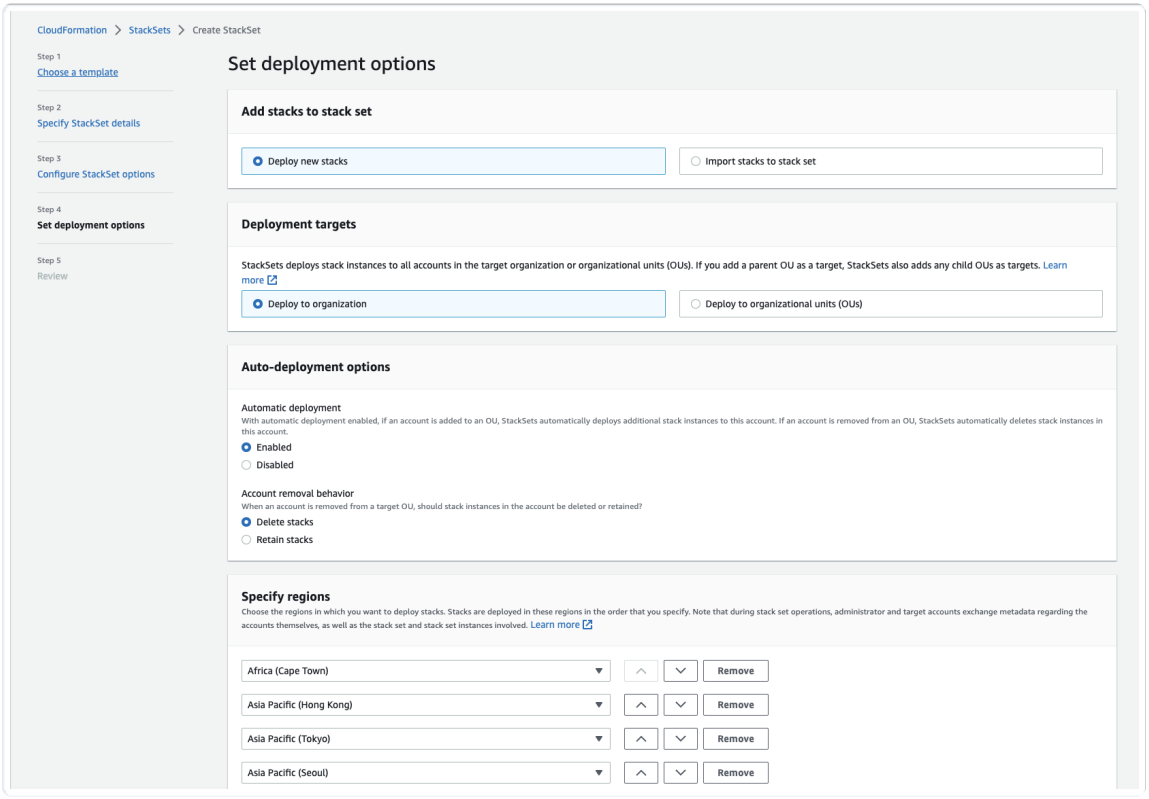
6. Under **Execution configuration**, select **Active**.

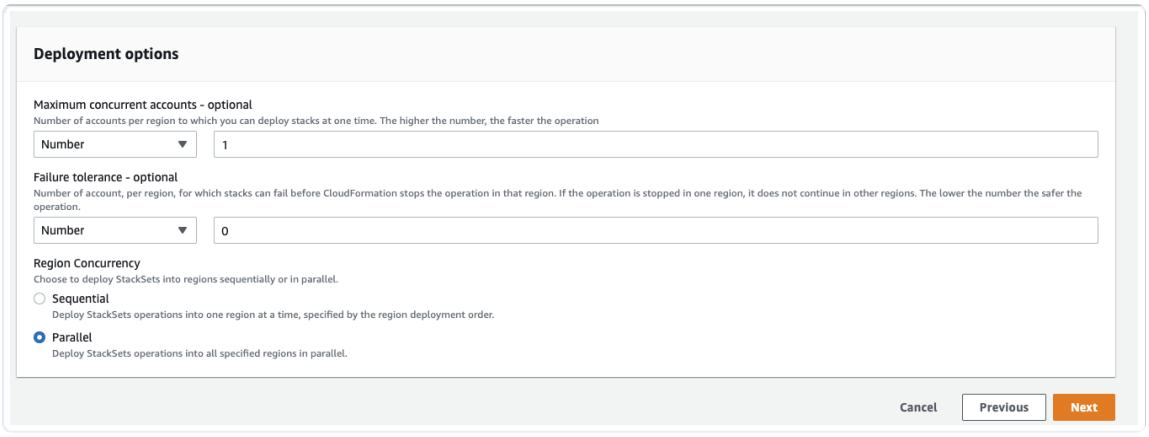


7. Define **Set deployment options** and click **Next**.
   a. **Deployment targets**:

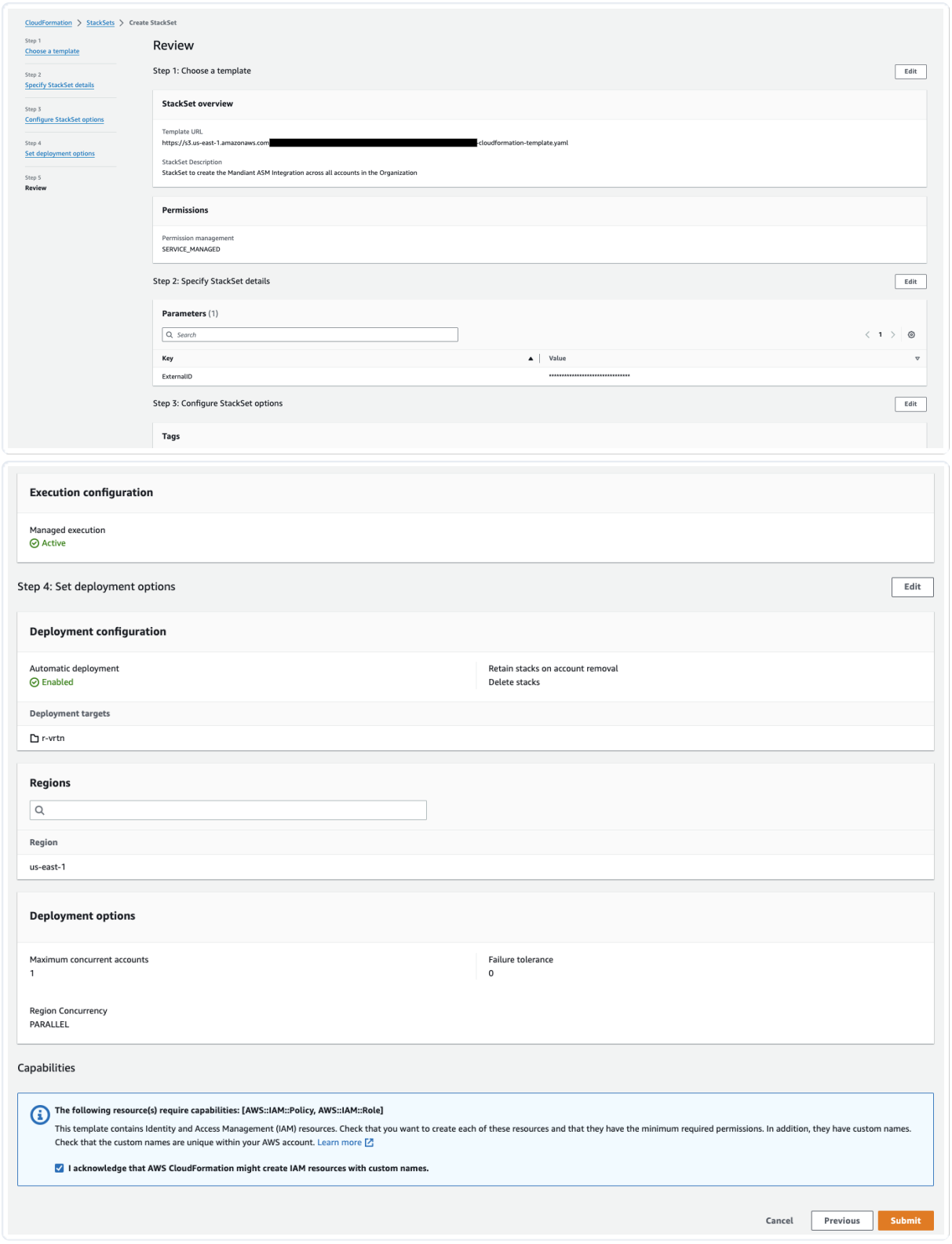
i. **Deploy to organization** (default): Deploys the stack to all accounts in the organization.
ii. **Deploy to organizational units (OUs)**: Deploys the stack to specific organizational units.

b. **Specify regions**: As IAM is Global, you can select any single region of your choice.
c. **Deployment options**: The default options are shown here, but can be modified to suit the needs of your organization.





8. Review and click **Submit**.



Gather the Role ARNs

The MA-ASM **AWS Integration (https://docs.mandiant.com/home/asm-aws-integration)** requires you to input the **Role ARN** associated with the **Mandiant-ASM-Access Role** belonging to each child account the StackSet was deployed to.

This list is easy to produce as the name of the role are the same across all accounts and AWS' Role ARNs follow a specific format.

Using the parent account in the AWS CLI, run the following command to obtain the Role ARNs associated with the AWS accounts belonging to your organization:

```
aws cloudformation list-stack-instances --stack-set-name change-stackset-name | jq -r '.Summaries[] | select(.StackInstanceStatus.DetailedStatus == "SUCCEEDED") | .Account | "arn:aws:iam::\(.):role/Mandiant-ASM-Access"'
```

- *change-stackset-name* is a variable and should be replaced with the StackSet name provided in step 4a.
- The `jq` utility parses the resulting JSON and forms the **Role ARN**.
- If the *Role Name* was changed from what is listed in the **CloudFormation template file**, be sure to update the preceding command to include the correct *Role Name*.

Sample Result (where each line is an individual **Role ARN**):

```
arn:aws:iam::11111111111:role/Mandiant-ASM-Access
arn:aws:iam::22222222222:role/Mandiant-ASM-Access
arn:aws:iam::33333333333:role/Mandiant-ASM-Access
```

Create a new **AWS Integration** **(https://docs.mandiant.com/home/asm-aws-integration)** for every **Role ARN** listed. If there are too many, it's highly suggested to script this process. The **API Docs** **(https://docs.mandiant.com/home/asm-api#tag/Integrations)** can help provide more insight.