

## SCALE AWS INTEGRATION ACROSS AWS ORGANIZATIONS



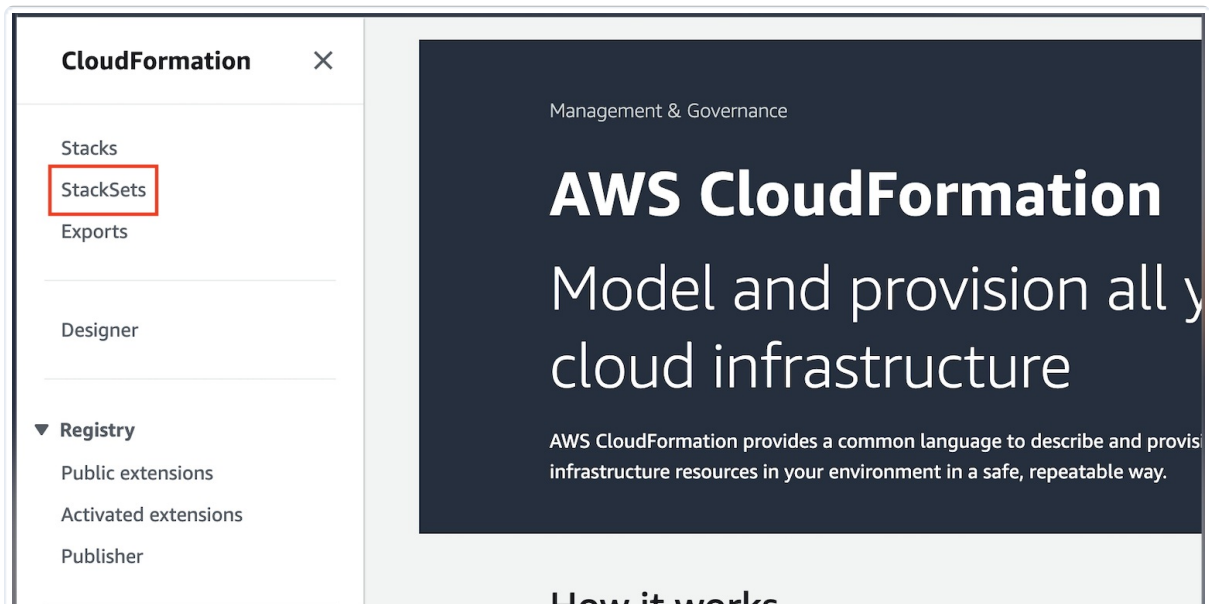
The following information is not intended to apply to all variations of customer environments. There can be several factors that may prohibit you from achieving the intended results. As such, this document should be treated as general guidance. These instructions were written for an out-of-box AWS organization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

There are two steps in this process:

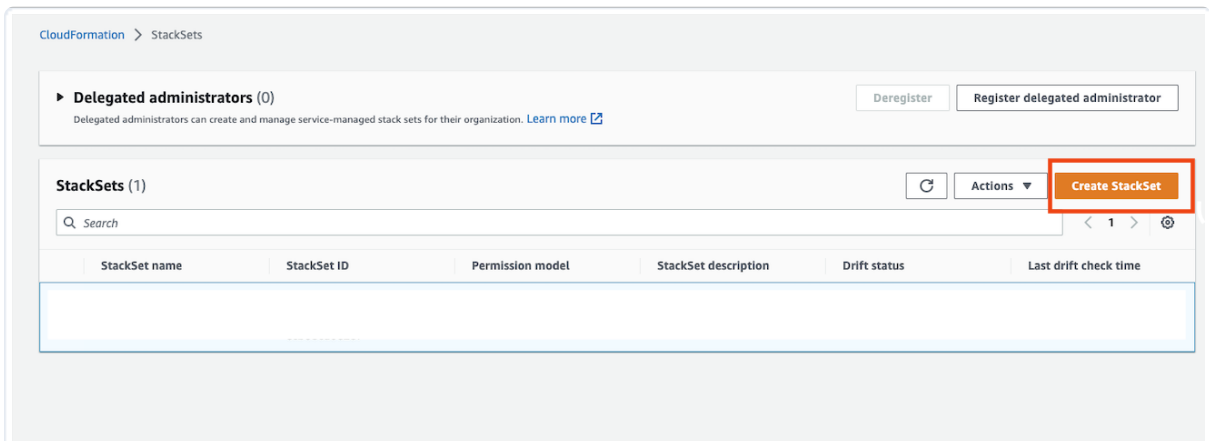
1. **Create the Stack Set**
2. **Gather the Role ARNs**

### 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**.



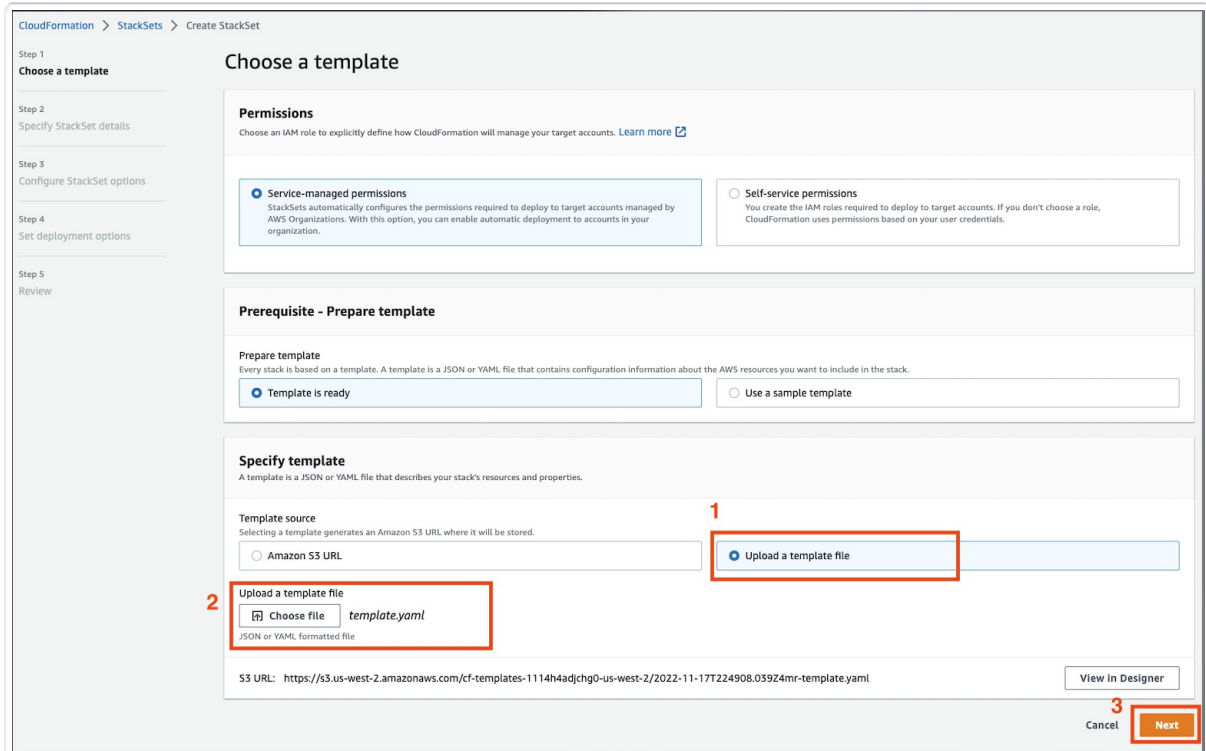
4. Under the **Specify template**, select **Upload a template file**, upload this

## 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`.



CloudFormation > StackSets > Create StackSet

Step 1  
Choose a template

Step 2  
Specify StackSet details

Step 3  
Configure StackSet options

Step 4  
Set deployment options

Step 5  
Review

### Choose a template

**Permissions**  
Choose an IAM role to explicitly define how CloudFormation will manage your target accounts. [Learn more](#)

**Service-managed permissions**  
StackSets automatically configures the permissions required to deploy to target accounts managed by AWS Organizations. With this option, you can enable automatic deployment to accounts in your organization.

**Self-service permissions**  
You create the IAM roles required to deploy to target accounts. If you don't choose a role, CloudFormation uses permissions based on your user credentials.

**Prerequisite - Prepare template**

**Prepare template**  
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

**Template is ready**  Use a sample template

**Specify template**  
A template is a JSON or YAML file that describes your stack's resources and properties.

**Template source**  
Selecting a template generates an Amazon S3 URL where it will be stored.

Amazon S3 URL  **Upload a template file**

**Upload a template file**

`template.yaml`  
JSON or YAML, formatted file

S3 URL: `https://s3.us-west-2.amazonaws.com/cf-templates-1114h4adjhg0-us-west-2/2022-11-17T224908.03924mr-template.yaml`

5. Populate the following fields and click **Next**.

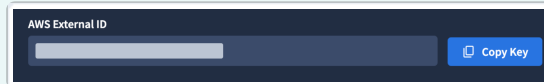
- StackSet name:** This should be a memorable value such as `Mandiant-ASM-Integration-StackSet`.
- StackSet description**
- External ID**



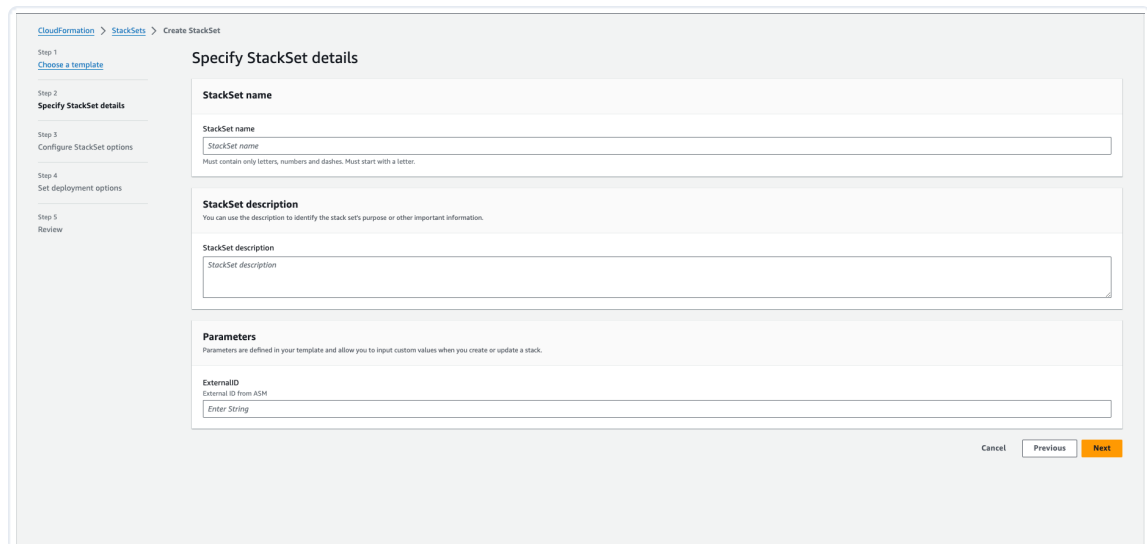
Requiring an External ID is an AWS best practice when a third party (MA-ASM, in this case) assumes the role.

### 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



CloudFormation > StackSets > Create StackSet

Step 1  
Choose a template

Step 2  
**Specify StackSet details**

Step 3  
Configure StackSet options

Step 4  
Set deployment options

Step 5  
Review

### Specify StackSet details

**StackSet name**

StackSet name

StackSet name

Must contain only letters, numbers and dashes. Must start with a letter.

**StackSet description**

You can use the description to identify the stack set's purpose or other important information.

StackSet description

StackSet description

**Parameters**

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

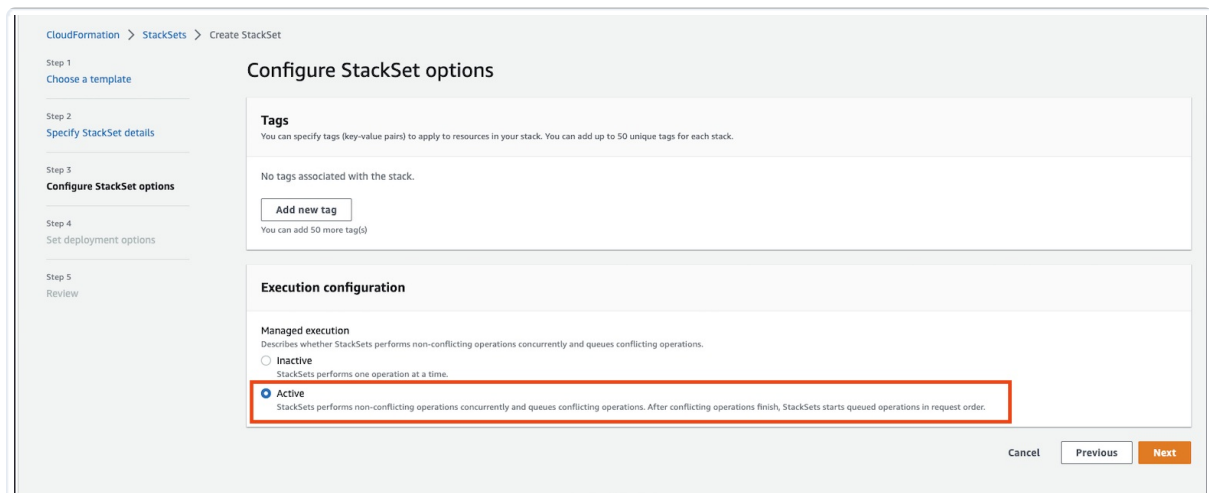
**ExternalID**

External ID from ASM

Enter String

Cancel Previous Next

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



CloudFormation > StackSets > Create StackSet

Step 1  
Choose a template

Step 2  
Specify StackSet details

Step 3  
**Configure StackSet options**

Step 4  
Set deployment options

Step 5  
Review

### Configure StackSet options

**Tags**

You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack.

No tags associated with the stack.

Add new tag

You can add 50 more tag(s)

**Execution configuration**

**Managed execution**

Describes whether StackSets performs non-conflicting operations concurrently and queues conflicting operations.

Inactive  
StackSets performs one operation at a time.

**Active**  
StackSets performs non-conflicting operations concurrently and queues conflicting operations. After conflicting operations finish, StackSets starts queued operations in request order.

Cancel Previous Next

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.

CloudFormation > StackSets > Create StackSet

Step 1  
[Choose a template](#)

Step 2  
[Specify StackSet details](#)

Step 3  
[Configure StackSet options](#)

Step 4  
**Set deployment options**

Step 5  
[Review](#)

### Set deployment options

**Add stacks to stack set**

Deploy new stacks  Import stacks to stack set

**Deployment targets**

StackSets deploys stack instances to all accounts in the target organization or organizational units (OUs). If you add a parent OU as a target, StackSets also adds any child OUs as targets. [Learn more](#)

Deploy to organization  Deploy to organizational units (OUs)

**Auto-deployment options**

**Automatic deployment**  
With automatic deployment enabled, if an account is added to an OU, StackSets automatically deploys additional stack instances to this account. If an account is removed from an OU, StackSets automatically deletes stack instances in this account.

Enabled  Disabled

**Account removal behavior**  
When an account is removed from a target OU, should stack instances in the account be deleted or retained?

Delete stacks  Retain stacks

**Specify regions**

Choose the regions in which you want to deploy stacks. Stacks are deployed in these regions in the order that you specify. Note that during stack set operations, administrator and target accounts exchange metadata regarding the accounts themselves, as well as the stack set and stack set instances involved. [Learn more](#)

Africa (Cape Town)	^	v	Remove
Asia Pacific (Hong Kong)	^	v	Remove
Asia Pacific (Tokyo)	^	v	Remove
Asia Pacific (Seoul)	^	v	Remove

### Deployment options

**Maximum concurrent accounts - optional**  
Number of accounts per region to which you can deploy stacks at one time. The higher the number, the faster the operation

Number

**Failure tolerance - optional**  
Number of account, per region, for which stacks can fail before CloudFormation stops the operation in that region. If the operation is stopped in one region, it does not continue in other regions. The lower the number the safer the operation.

Number

**Region Concurrency**  
Choose to deploy StackSets into regions sequentially or in parallel.

Sequential  
Deploy StackSets operations into one region at a time, specified by the region deployment order.

Parallel  
Deploy StackSets operations into all specified regions in parallel.

8. Review and click **Submit**.

CloudFormation > StackSets > Create StackSet

Step 1: Choose a template Edit

Step 2: Specify StackSet details Edit

Step 3: Configure StackSet options Edit

Step 4: Set deployment options

Step 5: Review

### Review

**StackSet overview**

Template URL: `https://s3-us-east-1.amazonaws.com/[redacted]/cloudformation-template.yaml`

StackSet Description: StackSet to create the Mandiant ASM Integration across all accounts in the Organization

**Permissions**

Permission management: SERVICE\_MANAGED

**Step 2: Specify StackSet details**

**Parameters (1)**

Search:

Key	Value
ExternalID	*****

**Step 3: Configure StackSet options**

**Tags**

**Execution configuration**

Managed execution: Active

**Step 4: Set deployment options** Edit

**Deployment configuration**

Automatic deployment: Enabled | Retain stacks on account removal: Delete stacks

Deployment targets: r-vrtm

**Regions**

Search:

Region: us-east-1

**Deployment options**

Maximum concurrent accounts: 1 | Failure tolerance: 0

Region Concurrency: PARALLEL

**Capabilities**

**The following resource(s) require capabilities: [AWS::IAM::Policy, AWS::IAM::Role]**

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. [Learn more](#)

I acknowledge that AWS CloudFormation might create IAM resources with custom names.

Cancel Previous 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::111111111111:role/Mandiant-ASM-Access  
arn:aws:iam::222222222222:role/Mandiant-ASM-Access  
arn:aws:iam::333333333333: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.