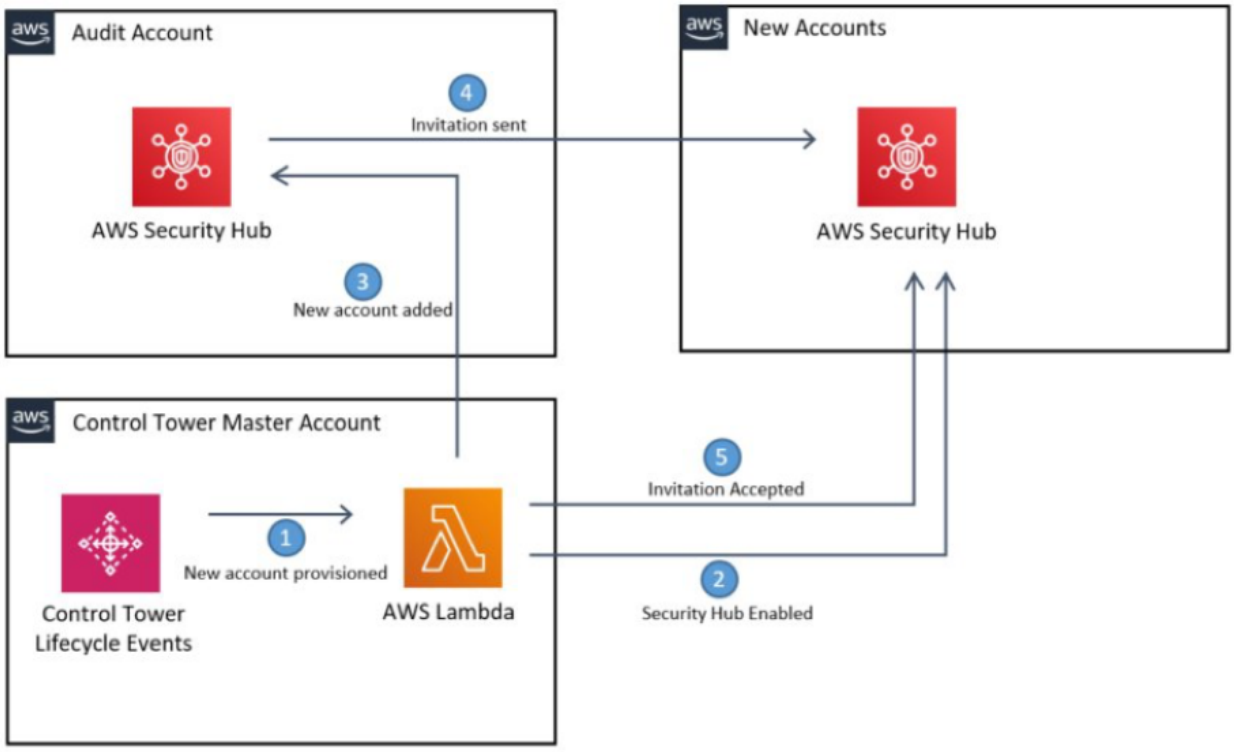
Synctree Flosports | SecurityHub

In SecurityHub, installing this customization will enable Security Hub in all Control Tower managed accounts, with the Audit account as the default Security Hub Master.

This is done by deploying a SecurityHub enabler lambda function in the master account. It runs periodically and checks each Control Tower managed account/region to ensure they have been invited into the master SecurityHub account and that SecurityHub is enabled. Control Tower Lifecycle events also trigger it to ensure minimal delay between new accounts being created and Security Hub being enabled in them.

- For more easy understanding, refer below Diagram:



Let's Start it practically (step-by-step):

Step 1: Upload the src/securityhub_enabler.zip file to an S3 bucket, note the bucket name for adding in cloud-formation stack and also copy the URL of this bucket.

Step 2: We do some changes in `ReservedConcurrentExecution` of our YAML file set as Default instend of 10 .

```
SecurityHubEnablerLambda:
  Type: "AWS::Lambda::Function"
  DependsOn:
    - SecurityHubEnablerRole
  Properties:
    Handler: "securityhub_enabler.lambda_handler"
    Role: !Sub "arn:aws:iam::${AWS::AccountId}:role/${SecurityHubEnablerRole}"
    Code:
      S3Bucket: !Ref S3SourceBucket
      S3Key: !Ref S3SourceKey
    Runtime: "python3.8"
    MemorySize: 256
    Timeout: 900
    # ReservedConcurrentExecutions: 10
    Environment:
```

Step 3: Gather other information for deployment parameters:

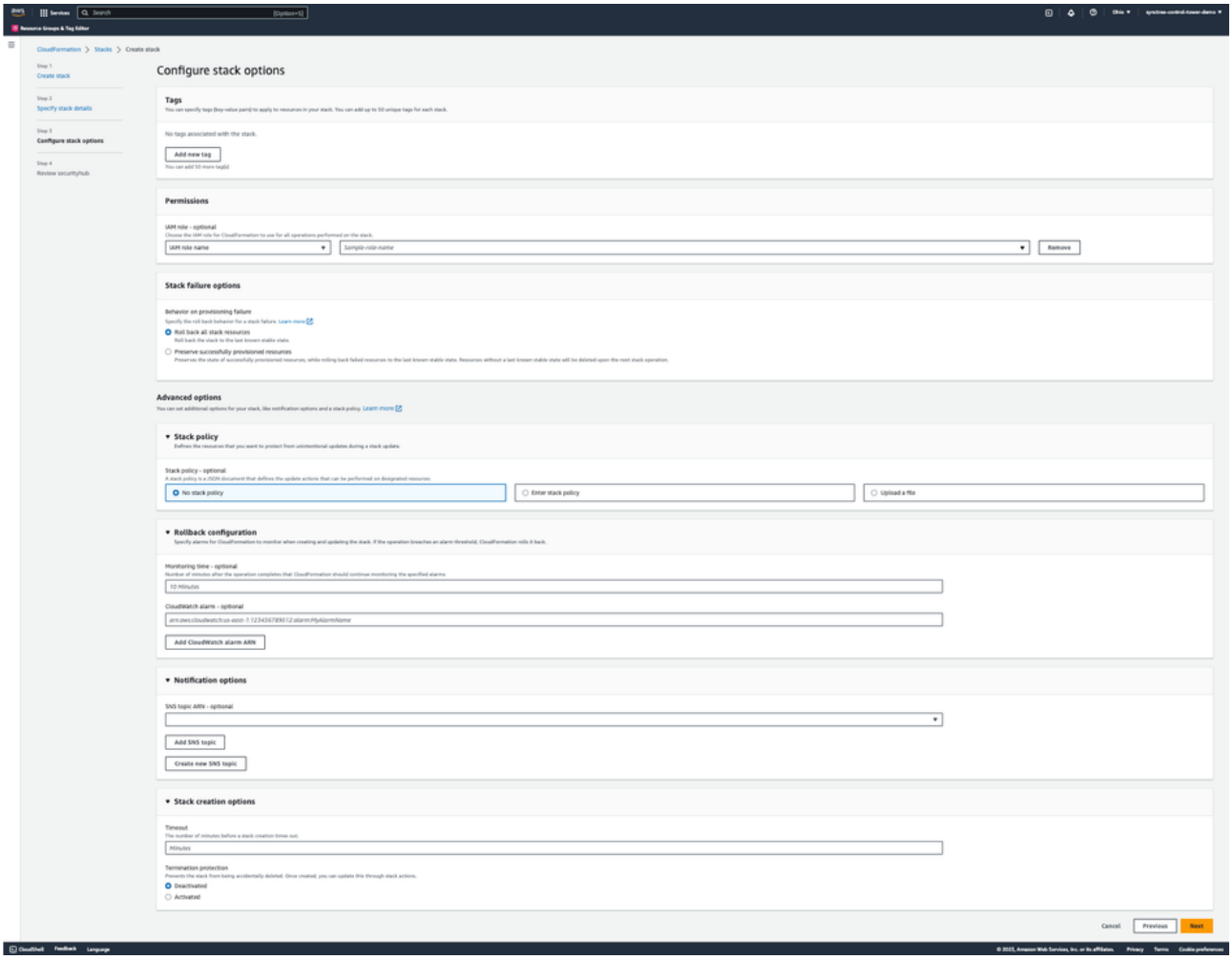
- Take Organization ID of Audit account
- Take SecurityAccountId

Step 4: Start to create Cloud-Formation stack and adding parameters in this one by one

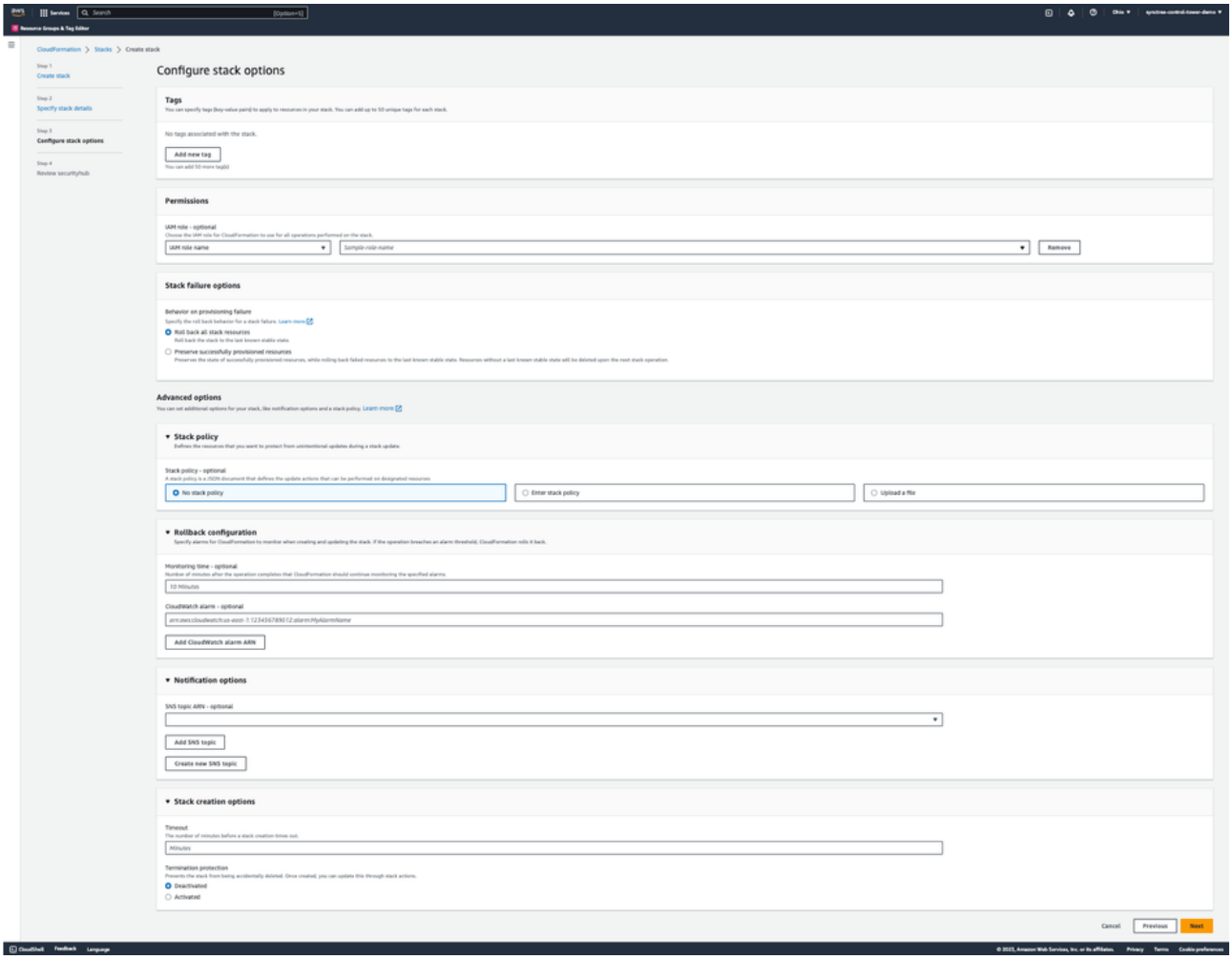
In cloud-formation stack add following details as below;

- In this we added stack name- `securityhub`
- AWSStandard & CISStandard are enable `YES`
- ComplianceFrequency bydefault set to 7
- Excluded Accounts- All accounts Id's that you want to exclude (e.g. ['111111111111', '222222222222',])
- OUfilter-All
- OrganizationId- Organisation Id
- Region filter- add `Control-Tower`
- Role-to-Assume-AWS- `Control-Tower-Execution`
- S3-Source-Bucket- Add your Source Bucket name
- S3-Source-Key- Add path of source code of lambda file
- Finally add SecurityAccountId

Also, check next stage as follows and click **Next**



Finally, Review All parameter Details:



Now, please check your SecurityHub on console is working properly….✅

Reference Link:

Repository: aws-samples/aws-control-tower-securityhub-enabler