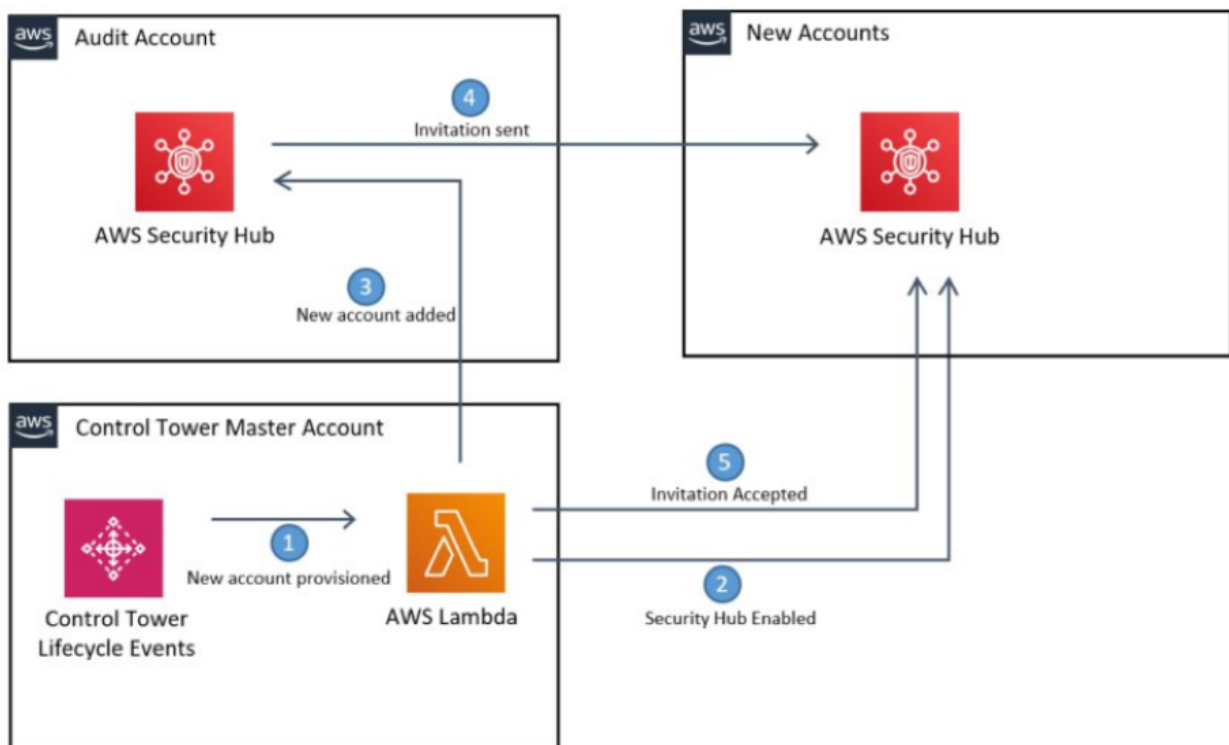


## Syntree Flosports | SecurityHub

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 instead 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:
      Variables:
```

### 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;

**Parameters**

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

---

**AWSStandard**

(Should Security Hub enable the AWS Foundational Security Best Practices v1.0.0 security standard?)

---

**CISStandard**

(Should Security Hub enable the CIS AWS Foundations Benchmark v1.2.0 security standard?)

---

**ComplianceFrequency**

(Frequency to check between 1 and 30. Default is 15 to check organizational compliance)

---

**ExcludedAccounts**

(Included Accounts list. This list should contain Management Account, Log Archive and Audit accounts at the minimum)

]

---

**OUIFilter**

(Should Security Hub be enabled for all accounts, or only accounts Control Tower Managed Stack)

---

**OrganizationalUnitId**

(AWS Organizations ID for the Control Tower. This is used to restrict permissions to least privilege.)

---

**PCIStandard**

(Should Security Hub enable the PCI DSS v3.2.1 Security Standard?)

---

**RegionFilter**

(Should Security Hub be enabled for all Security Hub supported regions, or only Control Tower supported regions)

---

**RoleToAssume**

(IAM role to be assumed in child accounts to enable SecurityHub. The default is ARN:ControlTowerExecution for a Control Tower environment.)

---

**S3SourceBucket**

(S3 bucket containing SecurityHubInitiated Lambda deployment package)

---

**S3SourceKey**

(S3 object key for SecurityHubInitiated Lambda deployment package)

---

**SecurityAccountID**

(Which account will be the SecurityHub Admin account? Enter the AWS account ID. This is generally the AWS Control Tower Audit account)

- 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**

Stacks

Resource Groups & Tag Editor

CloudFormation > Stacks > Create stack

Step 1: Create stack

Step 2: Specify stack details

Step 3: Configure stack options

Step 4: Review security policy

Configure stack options

Tags

You can specify tags that you want to apply to resources in your stack. You can add up to 10 unique tags for each stack.

No tags associated with the stack.

Add new tag

You can add 10 more tags

Permissions

IAM role - optional

Choose the IAM role for CloudFormation to use for all operations performed on the stack.

IAM role name

template-role-12345

Remove

Stack failure options

Behavior on provisioning failure

Specify the roll-back behavior for a stack failure. [Learn more](#)

☒ Roll back all stack resources

Roll back the stack to the last known stable state.

☐ Preserve successfully provisioned resources

Preserve the state of successfully provisioned resources, while rolling back failed resources to the last known stable state. Resources without a last known stable state will be deleted upon the next stack operation.

Advanced options

You can set additional options for your stack, like notification options and a stack policy. [Learn more](#)

Stack policy

Define the resources that you want to protect from unintentional updates during a stack update.

Stack policy - optional

A stack policy is a JSON document that defines the update actions that can be performed on designated resources.

☒ No stack policy

☐ Enter stack policy

☐ Upload a file

Rollback configuration

Specify alarms for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back.

Monitoring time - optional

Number of minutes after the operation completes that CloudFormation should continue monitoring the specified alarms.

10 Minutes

CloudWatch alarm - optional

arn:aws:cloudwatch:us-east-1:123456789012:alarm:HqAlarmName

Add CloudWatch alarm ARN

Notification options

SNS topic ARN - optional

Add SNS topic

Create new SNS topic

Stack creation options

Timeout

The number of minutes before a stack creation times out.

Minutes

Termination protection

Prevents the stack from being accidentally deleted. Once created, you can update this through stack actions.

☒ Disabled

☐ Protected

Cancel

Previous

Next

CloudShell

Feedback

Language

© 2021, Amazon Web Services, Inc. or its affiliates. Privacy

Terms

Contact us

Finally, Review All parameter Details:

CloudFormation > Stacks > Create stack

Step 1: Create stack

Step 2: Specify stack details

Step 3: **Configure stack options**

Step 4: Review securityhub

### Configure stack options

**Tags**  
You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 10 unique tags for each stack.

No tags associated with the stack.

[Add new tag](#)  
You can add 10 more tags.

**Permissions**  
IAM role - optional  
Choose the IAM role for CloudFormation to use for all operations performed on the stack.

[Remove](#)

**Stack failure options**  
Behavior on provisioning failure  
Specify the roll-back behavior for a stack failure. [Learn more](#)

☒ Roll back all stack resources  
Roll back the stack to the last known stable state.

☐ Preserve successfully provisioned resources  
Preserve the state of successfully provisioned resources, while rolling back failed resources to the last known stable state. Resources without a last known stable state will be deleted upon the next stack operation.

**Advanced options**  
You can set additional options for your stack, like notification options and a stack policy. [Learn more](#)

**Stack policy**  
Define the resources that you want to protect from unintentional updates during a stack update.

Stack policy - optional  
A stack policy is a JSON document that defines the update actions that can be performed on designated resources.

☒ No stack policy ☐ Enter stack policy ☐ Upload a file

**Rollback configuration**  
Specify alarms for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back.

Monitoring time - optional  
Number of minutes after the operation completes that CloudFormation should continue monitoring the specified alarms.

CloudWatch alarm - optional

[Add CloudWatch alarm ARN](#)

**Notification options**  
SNS topic ARN - optional

[Add SNS topic](#)  
[Create new SNS topic](#)

**Stack creation options**  
Timeout  
The number of minutes before a stack creation times out.

Termination protection  
Prevents the stack from being accidentally deleted. Once created, you can update this through stack actions.

☒ Disabled ☐ Activated

[Cancel](#) [Previous](#) [Next](#)

CloudWatch Feedback Language

© 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Contact us

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

Reference Link:

Repository: [aws-samples/aws-control-tower-securityhub-enabler](#)