Synctree Flosports | AWS Macie

What is Amazon Macie?

Amazon Macie is a data security service that discovers sensitive data by using machine learning and pattern matching, provides visibility into data security risks, and enables automated protection against those risks.

To help you manage the security posture of your organization's Amazon Simple Storage Service (Amazon S3) data estate, Macie provides you with an inventory of your S3 buckets, and automatically evaluates and monitors the buckets for security and access control. If Macie detects a potential issue with the security or privacy of your data, such as a bucket that becomes publicly accessible, Macie generates a finding for you to review and remediate as necessary.

Macie also automates discovery and reporting of sensitive data to provide you with a better understanding of the data that your organization stores in Amazon S3. To detect sensitive data, you can use built-in criteria and techniques that Macie provides, custom criteria that you define, or a combination of the two. If Macie detects sensitive data in an S3 object, Macie generates a finding to notify you of the sensitive data that Macie found.

In addition to findings, Macie provides statistics and other data that offer insight into the security posture of your Amazon S3 data, and where sensitive data might reside in your data estate. The statistics and data can guide your decisions to perform deeper investigations of specific S3 buckets and objects. You can review and analyze findings, statistics, and other data by using the Amazon Macie console or the Amazon Macie API. You can also leverage Macie integration with Amazon EventBridge and AWS Security Hub to monitor, process, and remediate findings by using other services, applications, and systems.

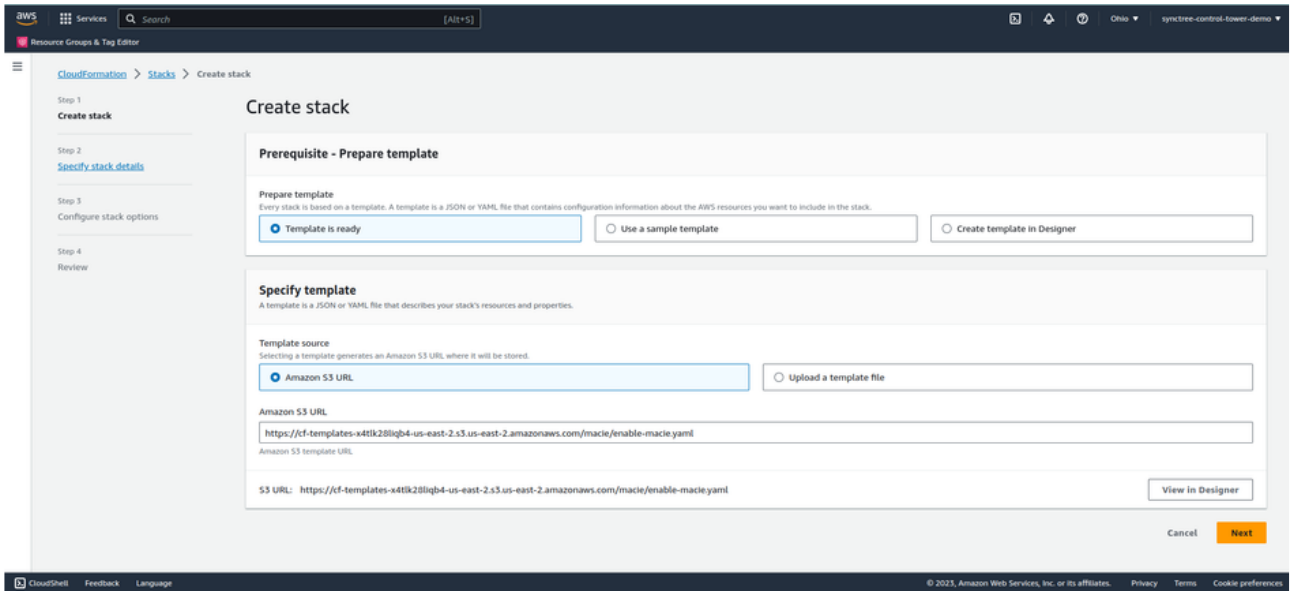
Important Features of Amazon Macie:

- Automate the discovery of sensitive data
- Discover a variety of sensitive data types
- Evaluate and monitor data for security and access control
- Review and analyze findings
- Monitor and process findings with other services and systems
- Centrally manage multiple Macie accounts
- Develop and manage resources programmatically

Start Creating Stack of CloudFormation:

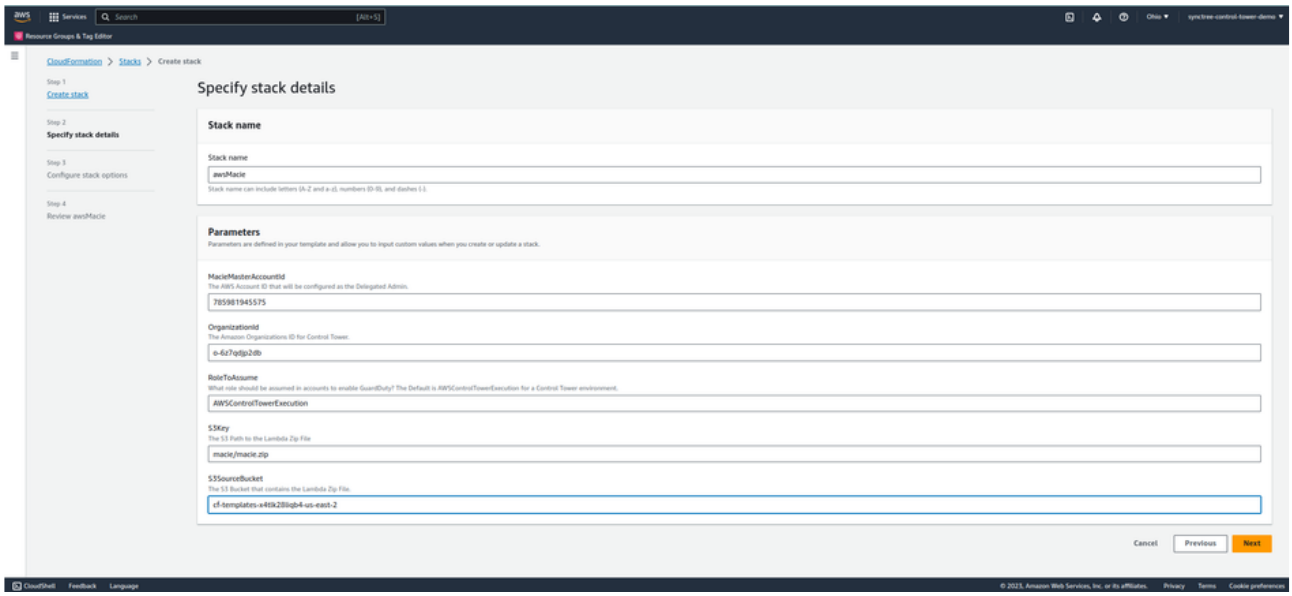
Step: 1

- Added Object URL of your S3 source Bucket in below



Step: 2

- Add parameters of CloudFormation Stack

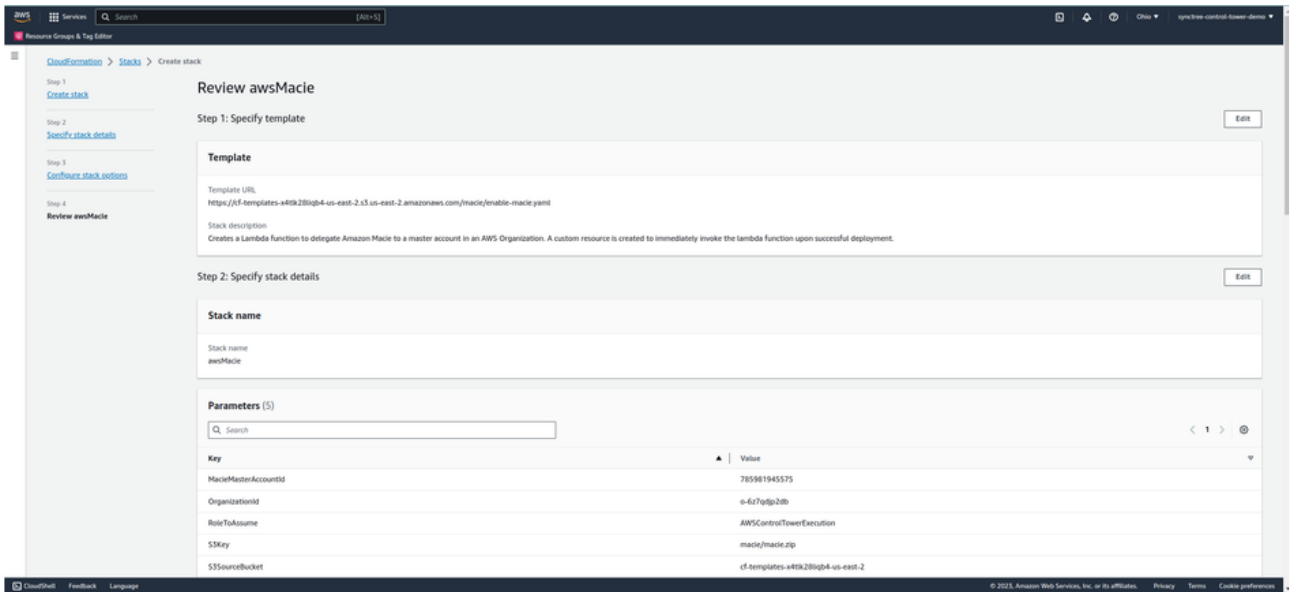


`S3 key -` Add lambda zip file of Macie

`MacieMasterAccount-` Add Audit account ID here

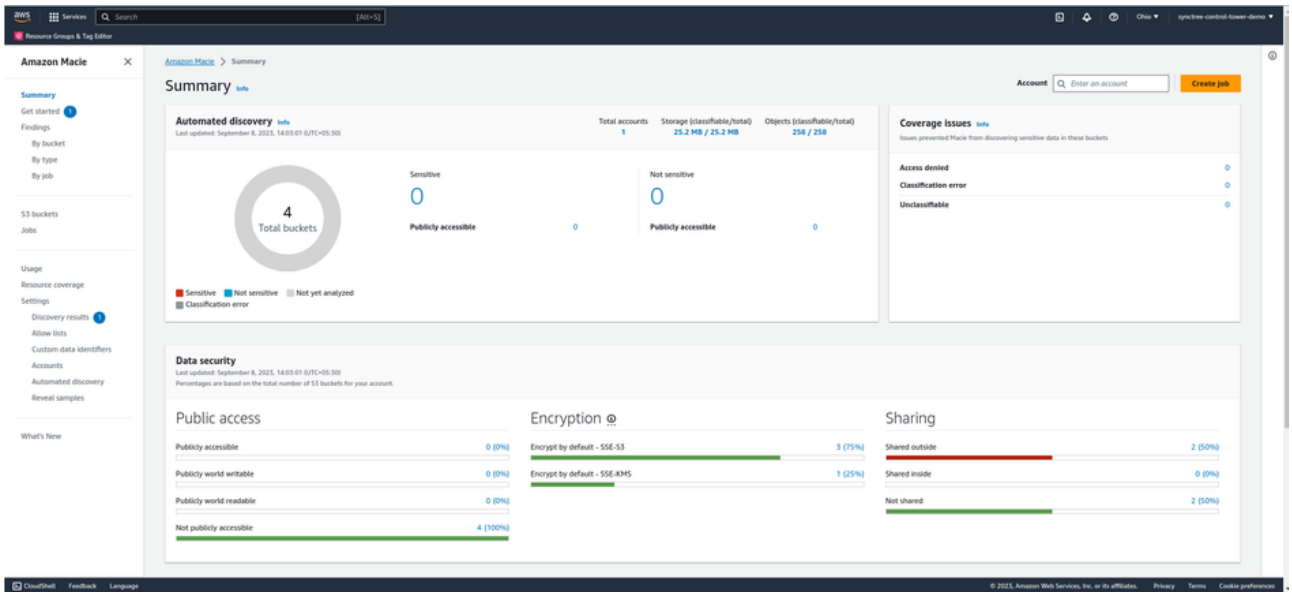
Step: 3

- Once reviewed parameters of the stack and acknowledged enable after that click on submit.



Step4:

- Go on AWS Macie dashboard and check it's working & showing your all S3 Bucket's.



Reference Link:

Repository: CfCT-Amazon-Macie