Westcon AWS
Secure Storage Starter Kit
Deployment Guide

Westcon | powered by aws

Secure Storage – CloudFormation Deployment Guide

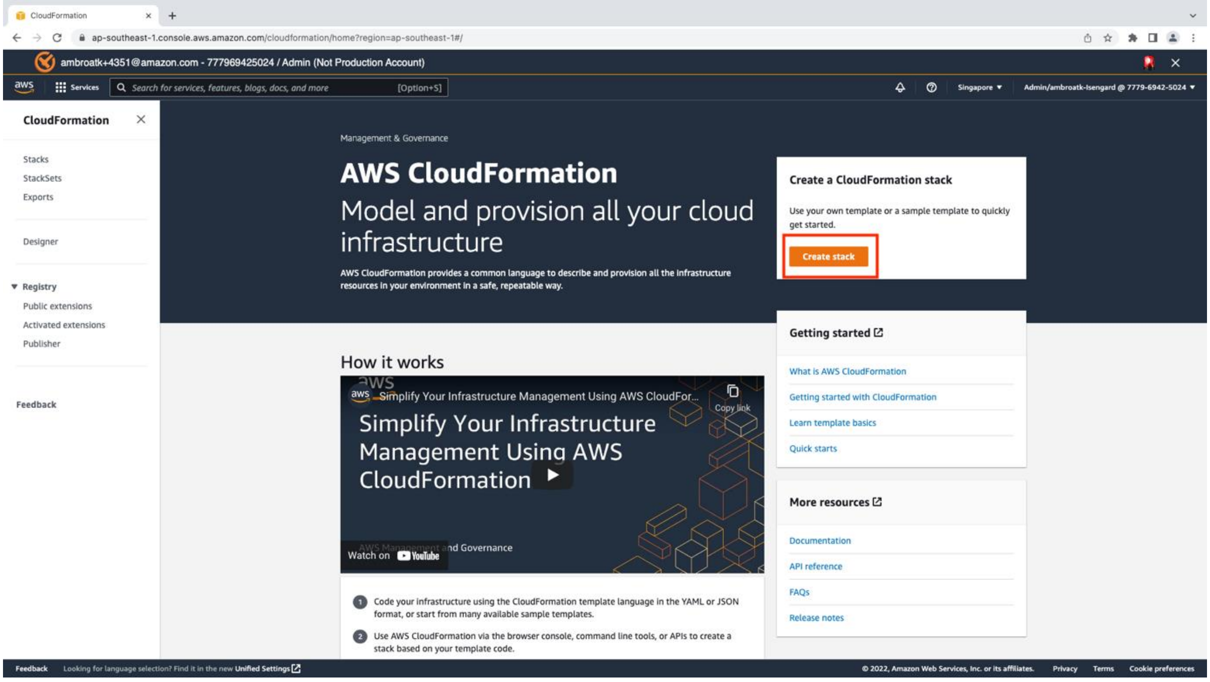
This guide is for the deployment of the **Secure Storage Bundle** using CloudFormation.

Pre-requisites

1. An existing Trend Micro Cloud One Account

Deploying Template Using CloudFormation

1. On the AWS console, navigate to the CloudFormation service. Click “Create stack”.



CloudFormation
ap-southeast-1.console.aws.amazon.com/cloudformation/home?region=ap-southeast-1#/
ambroatk+4351@amazon.com - 777969425024 / Admin (Not Production Account)
aws
Services
Search for services, features, blogs, docs, and more
[Option+S]
Singapore ▾
Admin/ambroatk-Isengard @ 7779-6942-5024 ▾
CloudFormation
Stacks
StackSets
Exports
Designer
▾ Registry
Public extensions
Activated extensions
Publisher
Feedback
Management & Governance
AWS CloudFormation
Model and provision all your cloud infrastructure
Create a CloudFormation stack
Create stack
Getting started
What is AWS CloudFormation
Getting started with CloudFormation
Learn template basics
Quick starts
More resources
Documentation
API reference
FAQs
Release notes
How it works
Simplify Your Infrastructure Management Using AWS CloudFor...
Copy link
Simplify Your Infrastructure Management Using AWS CloudFormation
AWS Management and Governance
Watch on YouTube
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

AWS CloudFormation provides a common language to describe and provision all the infrastructure resources in your environment in a safe, repeatable way.

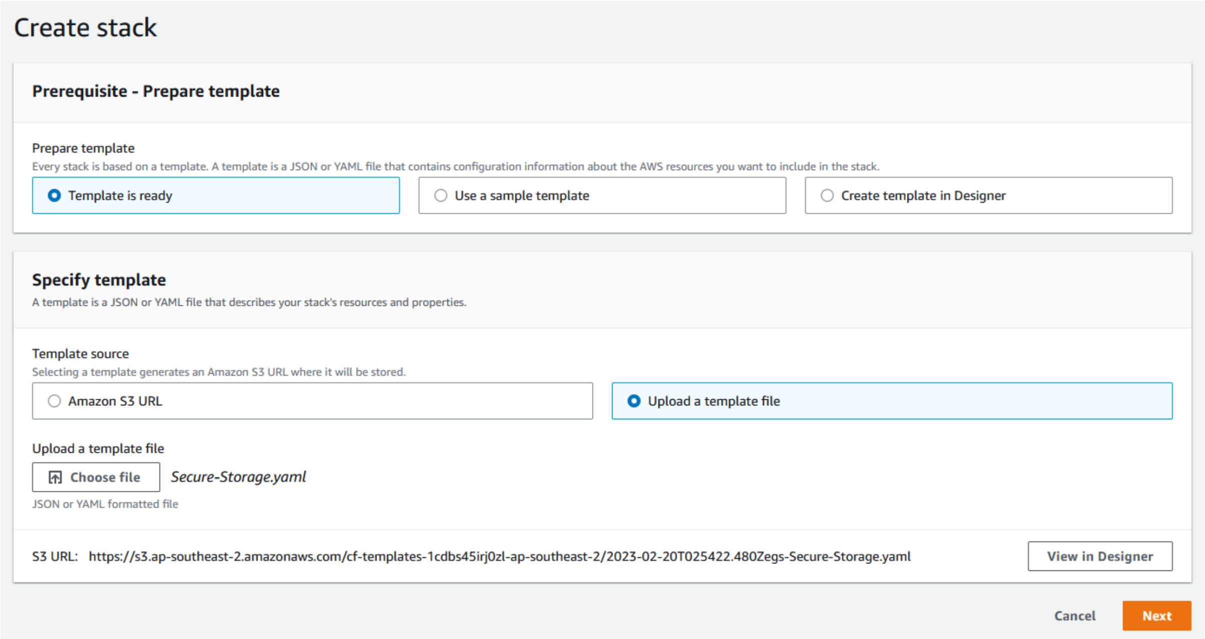
Use your own template or a sample template to quickly get started.

1 Code your infrastructure using the CloudFormation template language in the YAML or JSON format, or start from many available sample templates.

2 Use AWS CloudFormation via the browser console, command line tools, or APIs to create a stack based on your template code.

2. Select “Upload a template file”

3. Click on “Choose File”, then select the “Secure-Storage.yaml” file. Click “Next”.



Create stack

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 ○ Create template in Designer

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

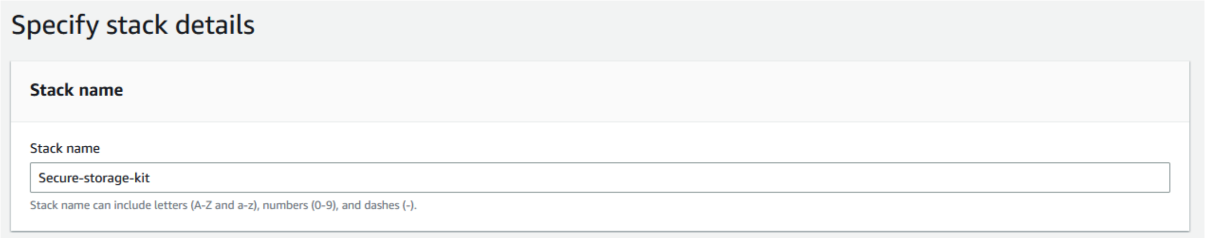
Upload a template file

Choose file *Secure-Storage.yaml*

JSON or YAML formatted file

S3 URL: https://s3.ap-southeast-2.amazonaws.com/cf-templates-1cdbs45irj0zl-ap-southeast-2/2023-02-20T025422.480Zegs-Secure-Storage.yaml

4. Enter a name for the stack.



Specify stack details

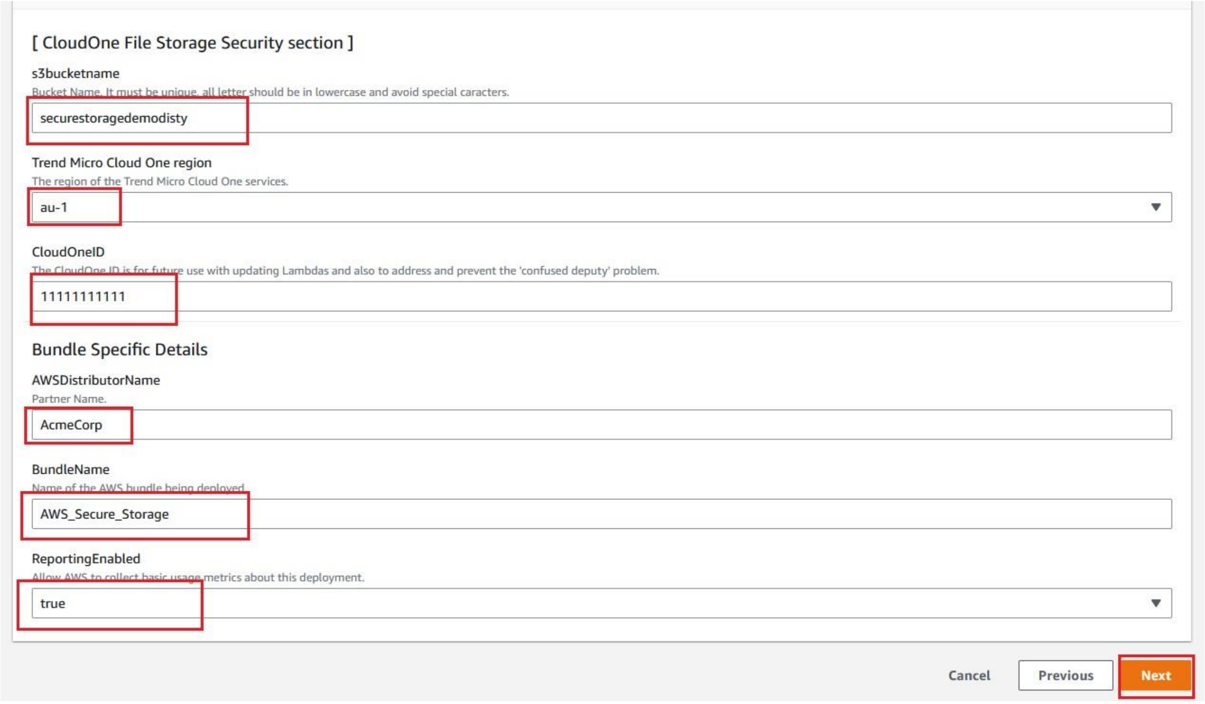
Stack name

Stack name

Secure-storage-kit

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

5. Enter the name of the bucket that you one to create along with the Trend Micro Cloud One region that you want to use. You will need a Cloud One ID to link your Bucket with your Cloud One Account.
6. Under Bundle Specific details enter the distributor name, the bundle name (you can leave the default), and specify if you want to send this details to AWS.



[CloudOne File Storage Security section]

s3bucketname

Bucket Name. It must be unique, all letter should be in lowercase and avoid special caracters.

securestoragedemodisty

Trend Micro Cloud One region

The region of the Trend Micro Cloud One services.

au-1 ▼

CloudOneID

The CloudOne ID is for future use with updating Lambdas and also to address and prevent the 'confused deputy' problem.

11111111111

Bundle Specific Details

AWSDistributorName

Partner Name.

AcmeCorp

BundleName

Name of the AWS bundle being deployed.

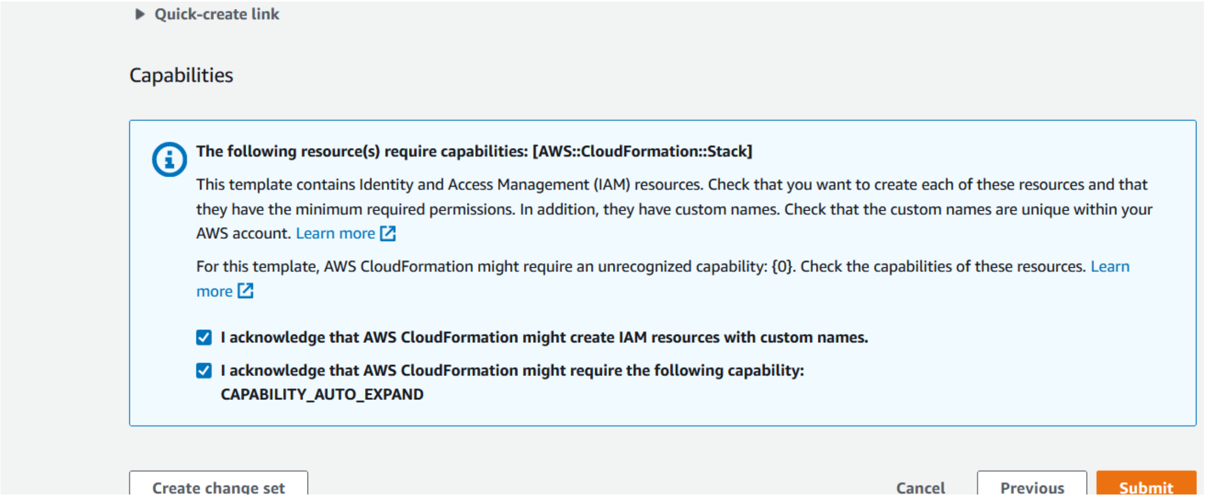
AWS_Secure_Storage

ReportingEnabled

Allow AWS to collect basic usage metrics about this deployment.

true ▼

7. Click “Next”.
8. In the “Configuration Stack Option” click “Next”.
9. In the “Review Page” make sure that you allow the template to create custom IAM resources and then click “Submit”.



Capabilities

The following resource(s) require capabilities: [AWS::CloudFormation::Stack]

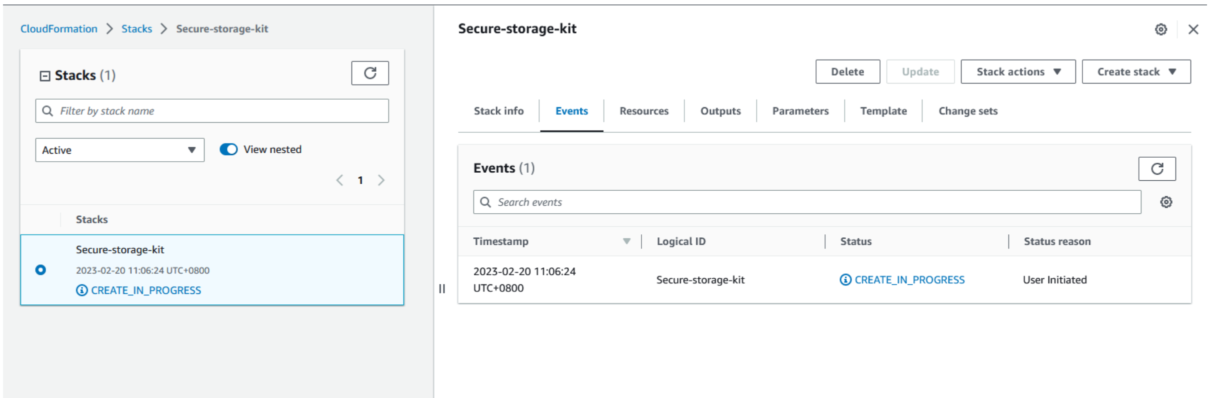
This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. Learn more

For this template, AWS CloudFormation might require an unrecognized capability: {0}. Check the capabilities of these resources. Learn more

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

☑ **I acknowledge that AWS CloudFormation might require the following capability: CAPABILITY_AUTO_EXPAND**

10. Once submitted you will see the template being deployed.



Secure-storage-kit

Stacks

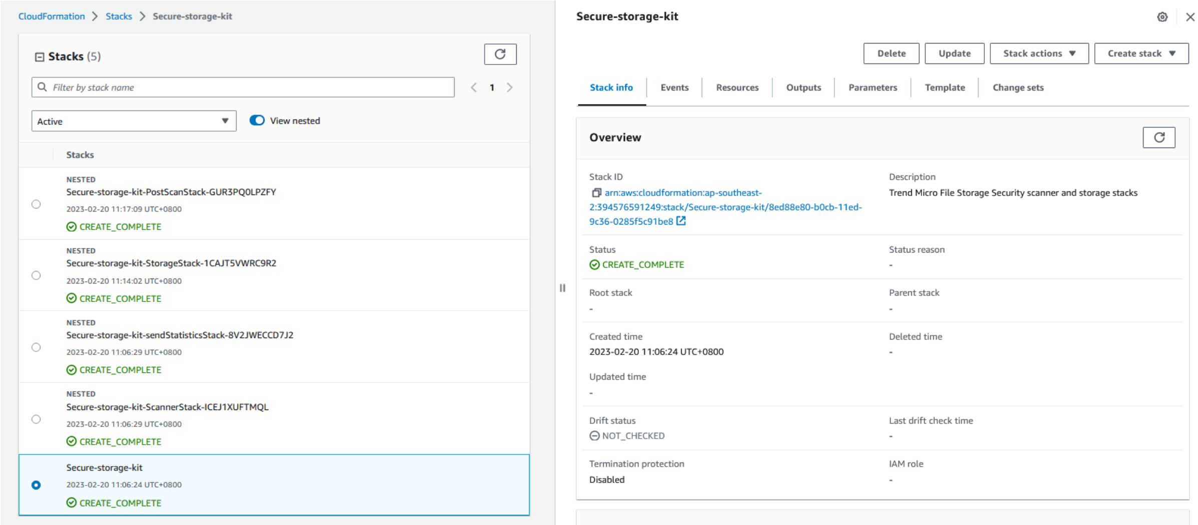
● Secure-storage-kit
2023-02-20 11:06:24 UTC+0800
CREATE_IN_PROGRESS

Secure-storage-kit

Events (1)

Timestamp	Logical ID	Status	Status reason
2023-02-20 11:06:24 UTC+0800	Secure-storage-kit	CREATE_IN_PROGRESS	User Initiated

11. Wait for all the resources to be created. Press the refresh button on the top right until the stack creation is complete.



Stacks

○ NESTED
Secure-storage-kit-PostScanStack-GUR3PQOLPZFY
2023-02-20 11:17:09 UTC+0800
CREATE_COMPLETE

○ NESTED
Secure-storage-kit-StorageStack-1CAJT5VWRC9R2
2023-02-20 11:14:02 UTC+0800
CREATE_COMPLETE

○ NESTED
Secure-storage-kit-sendStatisticsStack-8V2JWECCD7J2
2023-02-20 11:06:29 UTC+0800
CREATE_COMPLETE

○ NESTED
Secure-storage-kit-ScannerStack-ICEJ1XUFTMQL
2023-02-20 11:06:29 UTC+0800
CREATE_COMPLETE

● Secure-storage-kit
2023-02-20 11:06:24 UTC+0800
CREATE_COMPLETE

Secure-storage-kit

Overview

Stack ID
arn:aws:cloudformation:ap-southeast-2:394576591249:stack/Secure-storage-kit/8ed88e80-b0cb-11ed-9c36-0285f5c91be8

Description
Trend Micro File Storage Security scanner and storage stacks

Status
CREATE_COMPLETE

Status reason
-

Root stack
-

Parent stack
-

Created time
2023-02-20 11:06:24 UTC+0800

Deleted time
-

Updated time
-

Drift status
NOT_CHECKED

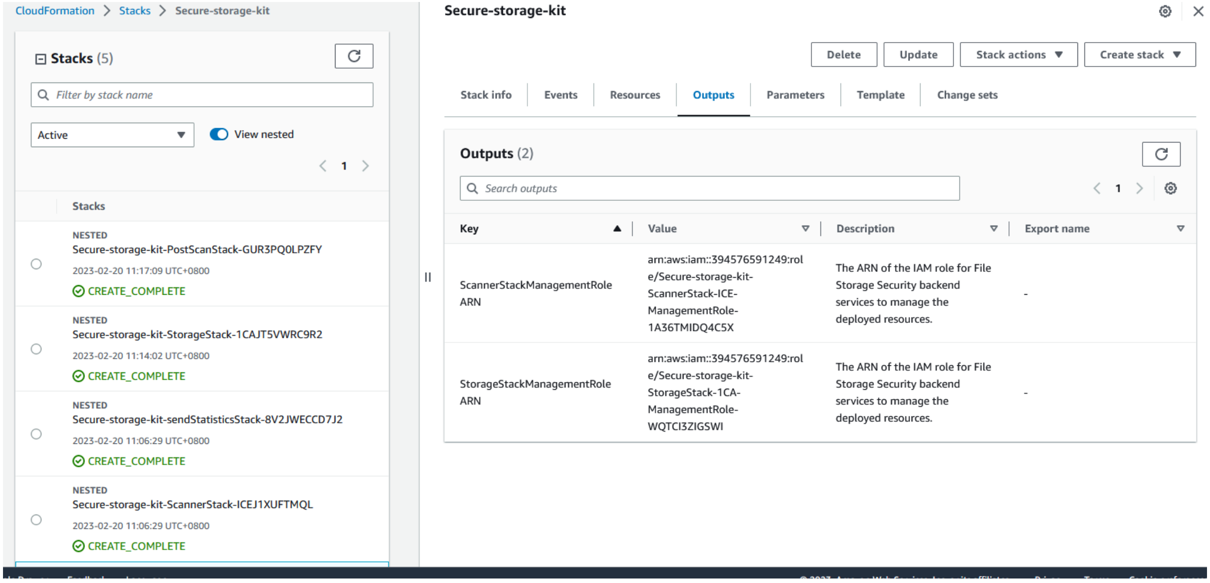
Last drift check time
-

Termination protection
Disabled

IAM role
-

12. The created stack should look like this. All the resources have now been created and deployed.

13. Click on the “Outputs” tab to retrieve the Public IP of the Bastion Host



CloudFormation > Stacks > Secure-storage-kit

Stacks (5)

Filter by stack name

Active ▼ View nested

Stacks

NESTED
Secure-storage-kit-PostScanStack-GUR3PQOLPZFY
2023-02-20 11:17:09 UTC+0800
CREATE_COMPLETE

NESTED
Secure-storage-kit-StorageStack-1CAJT5VWRC9R2
2023-02-20 11:14:02 UTC+0800
CREATE_COMPLETE

NESTED
Secure-storage-kit-sendStatisticsStack-8V2JWECCD7J2
2023-02-20 11:06:29 UTC+0800
CREATE_COMPLETE

NESTED
Secure-storage-kit-ScannerStack-ICEJ1XUFTMQL
2023-02-20 11:06:29 UTC+0800
CREATE_COMPLETE

Secure-storage-kit

Outputs (2)

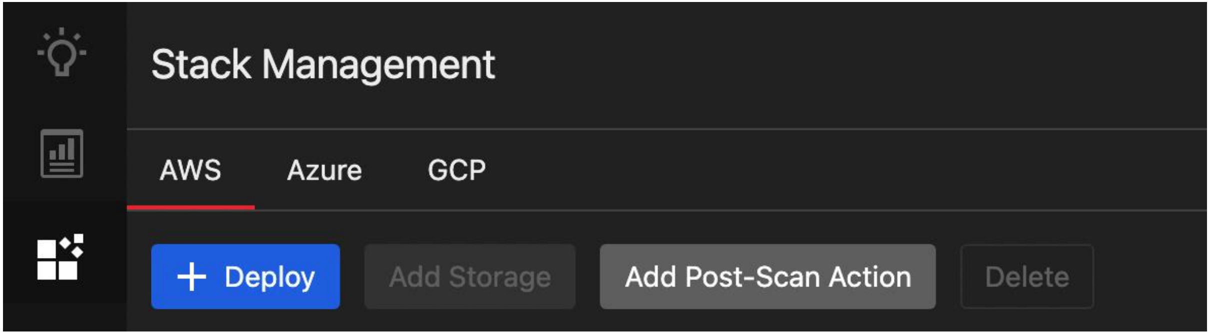
Search outputs

Key	Value	Description	Export name
ScannerStackManagementRole ARN	arn:aws:iam::394576591249:role/Secure-storage-kit-ScannerStack-ICE-ManagementRole-1A36TMIDQ4C5X	The ARN of the IAM role for File Storage Security backend services to manage the deployed resources.	-
StorageStackManagementRole ARN	arn:aws:iam::394576591249:role/Secure-storage-kit-StorageStack-1CA-ManagementRole-WQTCI3ZIGSWI	The ARN of the IAM role for File Storage Security backend services to manage the deployed resources.	-

14. Use this ARN to link the S3 bucket to your One Cloud Account

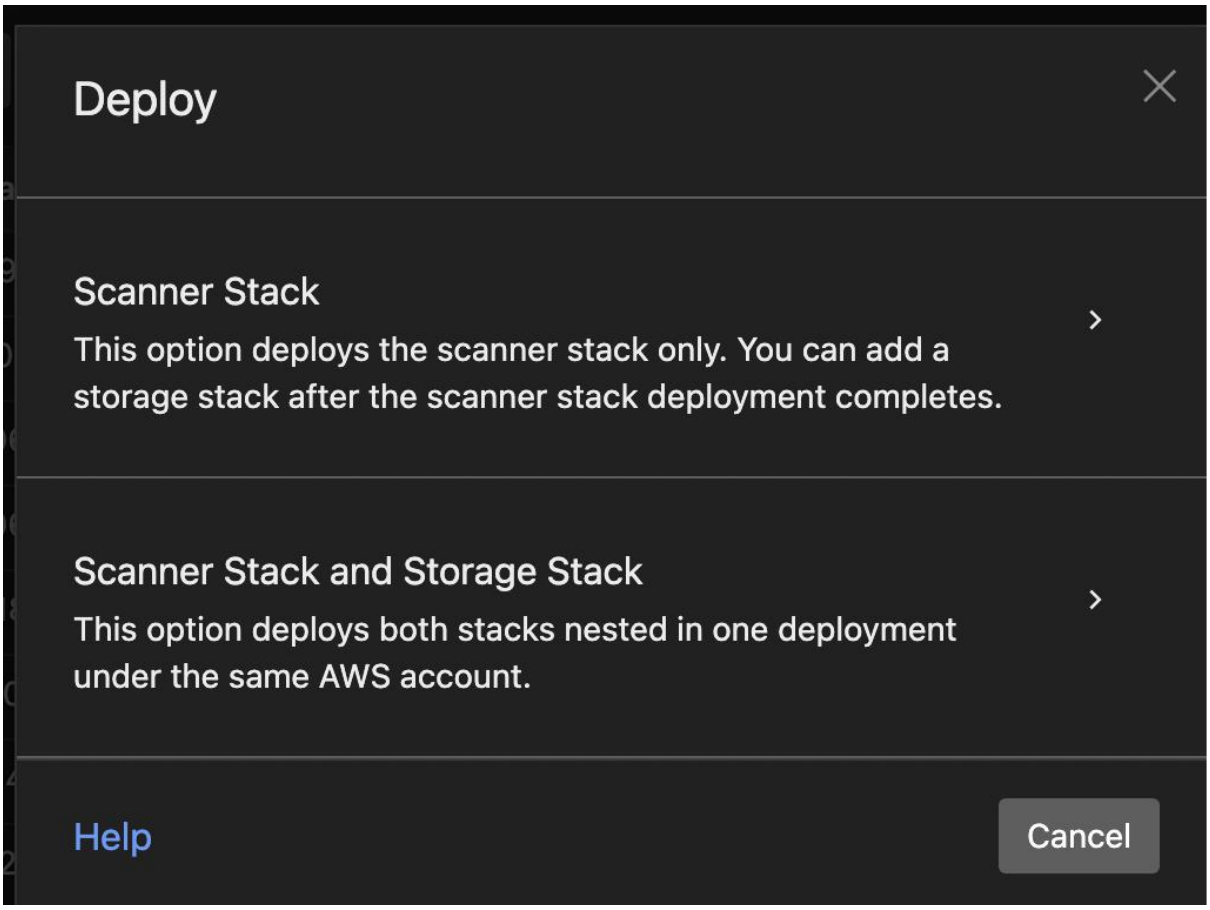
Register FSS In CLOUDONE

1. Go to https://cloudone.trendmicro.com/filestorage/deployment
2. Click on Deploy



Stack Management

3. Select Scanner Stack and Storage Stack



Deploy

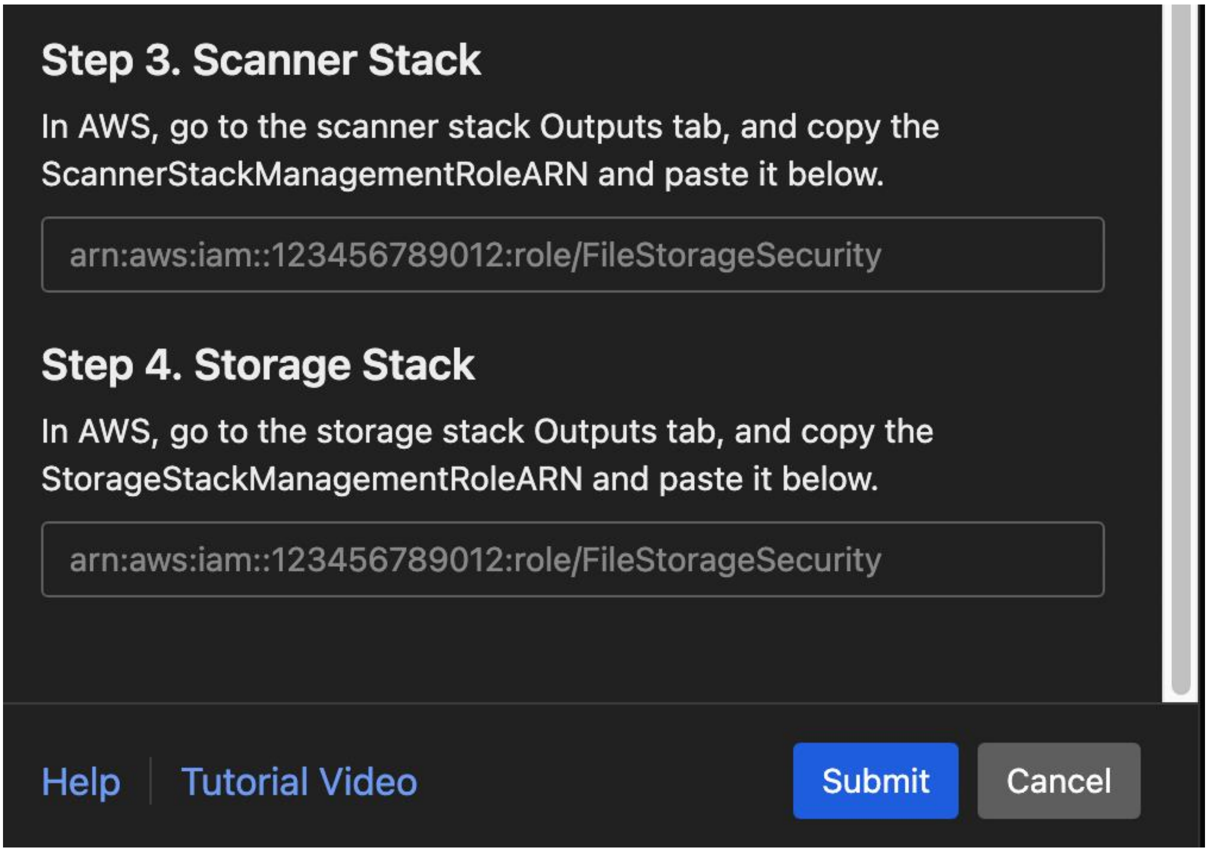
Scanner Stack

This option deploys the scanner stack only. You can add a storage stack after the scanner stack deployment completes.

Scanner Stack and Storage Stack

This option deploys both stacks nested in one deployment under the same AWS account.

4.



Step 3. Scanner Stack

In AWS, go to the scanner stack Outputs tab, and copy the ScannerStackManagementRoleARN and paste it below.

arn:aws:iam::123456789012:role/FileStorageSecurity

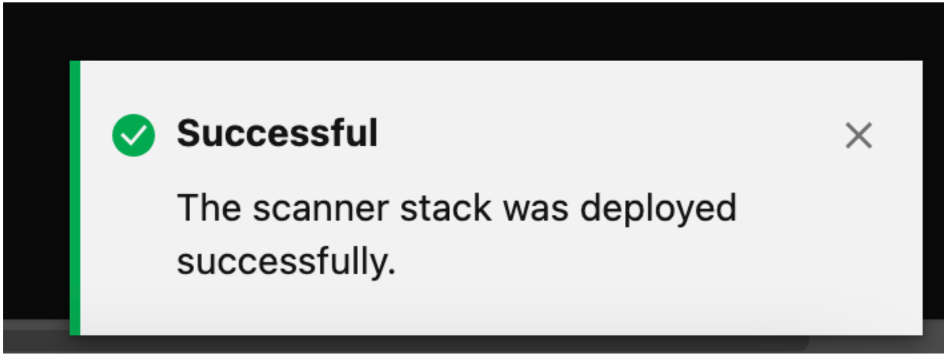
Step 4. Storage Stack

In AWS, go to the storage stack Outputs tab, and copy the StorageStackManagementRoleARN and paste it below.

arn:aws:iam::123456789012:role/FileStorageSecurity

a. Fill up Scanner Stack ARN: retrieved from Section Setup FSS via CloudFormation output result
key: ScannerStackManagementRoleARN
b. Fill up Storage Stack ARN: retrieved from Section Setup FSS via CloudFormation output result
key: StorageStackManagementRoleARN

5. Once fill up, click on Submit and wait until it show as



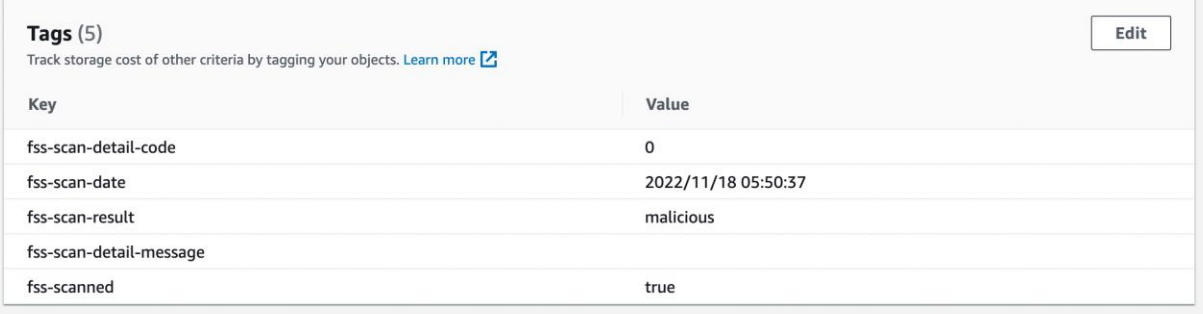
Successful

The scanner stack was deployed successfully.

Testing your deployment

1. Test upload file to the application S3 bucket and FSS will start do the scanning

2. Result will be shown as AWS tag under S3 bucket



Tags (5)

Track storage cost of other criteria by tagging your objects. Learn more

Key	Value
fss-scan-detail-code	0
fss-scan-date	2022/11/18 05:50:37
fss-scan-result	malicious
fss-scan-detail-message	
fss-scanned	true

3. If it is malicious file, it will be moved to quarantine S3 bucket predefined in the CloudFormation template.

Have a question?

Contact us

NZ Cloud Sales: +64 9 477 7211
cloudsales.nz@westcon.com

AU Cloud Sales: +61 2 8412 1212
cloudsales.au@westcon.com

SG Cloud Sales: +65 6424 0570
cloudsales.sg@westcon.com

ID Cloud Sales: +62 21 8062 1470
cloudsales.id@westcon.com