
Antivirus for Amazon S3

This template creates a malware scanner cluster for S3 buckets. Connect as many S3 buckets as you like.

bucketAV - Antivirus for Amazon S3 with additional features is available at AWS Marketplace.

Features

- Uses ClamAV to scan newly added files on S3 buckets
- Updates ClamAV database every 3 hours automatically
- Scales EC2 instance workers to distribute the workload
- Publishes a message to SNS in case of a finding
- Can optionally delete compromised files automatically
- Logs to CloudWatch Logs

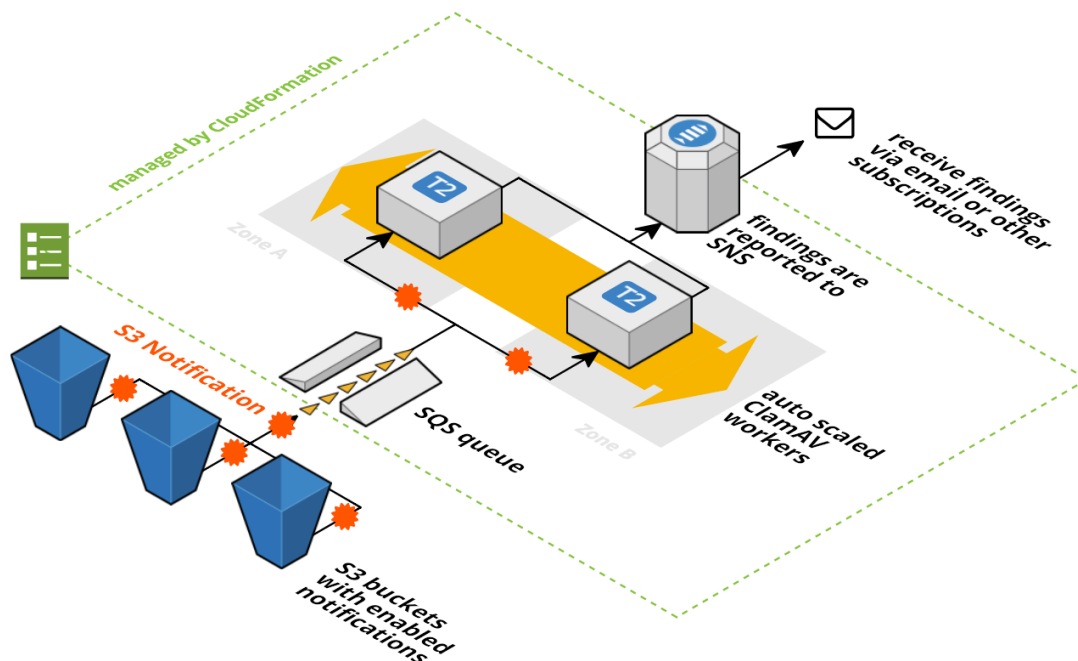
Additional Commercial Features by bucketAV

- Reporting capabilities
- Dashboard
- Scan buckets at regular intervals / initial bucket scan
- Quarantine infected files
- Enhanced security features (e.g., IMDSv2)
- Regular Security updates
- Multi-Account support
- AWS Integrations:
 - CloudWatch Integration (Metrics and Dashboard)
 - Security Hub Integration
 - SSM OpsCenter Integration
- S3 -> SNS fan-out support
- Support

bucketAV - Antivirus for Amazon S3 with additional features is available at AWS Marketplace.

How does it work

A picture is worth a thousand words:



1. A SQS queue is used to decouple scan jobs from the ClamAV workers. Each S3 bucket can fire events to that SQS queue in case of new objects. This feature of S3 is called S3 Event Notifications.
2. The SQS queue is consumed by a fleet of EC2 instances running in an Auto Scaling Group. If the number of outstanding scan jobs reaches a threshold a new ClamAV worker is automatically added. If the queue is mostly empty workers are removed.
3. The ClamAV workers run a simple ruby script that executes the clamscan command. In the background the virus db is updated every three hours.
4. If `clamscan` finds a virus the file is directly deleted (you can configure that) and a SNS notification is published.

Installation

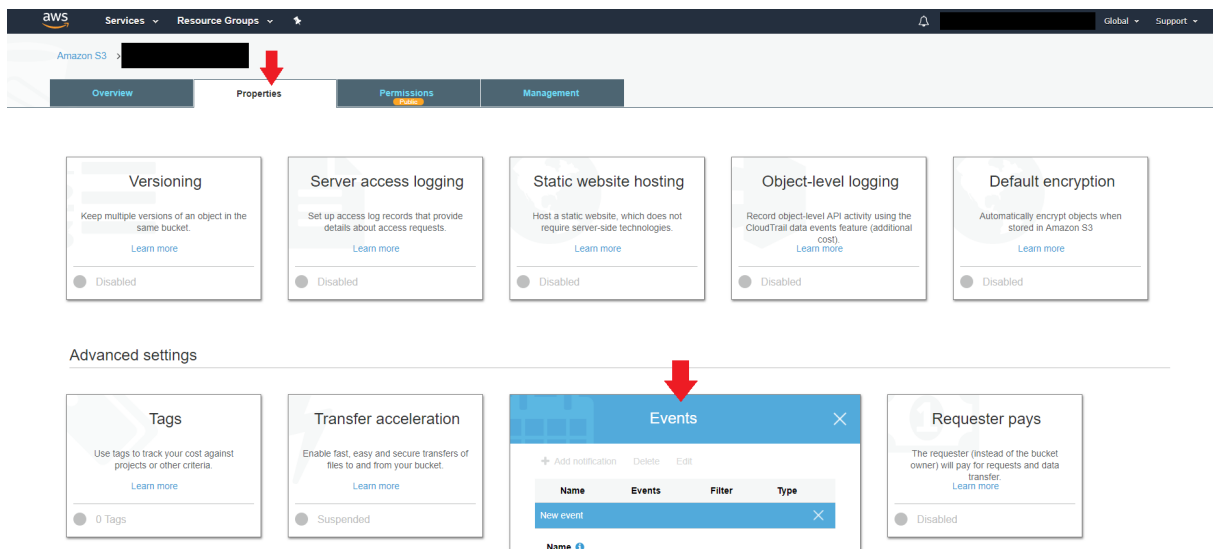
Create the CloudFormation Stack

1. This templates depends on one of our `vpc-aws.yaml` templates. Launch Stack
2. Launch Stack
3. Click **Next** to proceed with the next step of the wizard.
4. Specify a name and all parameters for the stack.
5. Click **Next** to proceed with the next step of the wizard.

6. Click **Next** to skip the **Options** step of the wizard.
7. Check the **I acknowledge that this template might cause AWS CloudFormation to create IAM resources.** checkbox.
8. Click **Create** to start the creation of the stack.
9. Wait until the stack reaches the state **CREATE_COMPLETE**

Configure the buckets

Configure the buckets you want to connect to as shown in the next figure:



Events

[+ Add notification](#) [Delete](#) [Edit](#)

Name	Events	Filter	Type
New event			

Name ⓘ

s3-virusscan

Events ⓘ

☐ PUT

☐ POST

☐ COPY

☐ Multipart upload completed

☒ All object create events

☐ Object in RRS lost

☐ Permanently deleted

☐ Delete marker created

☐ All object delete events

☐ Restore from Glacier initiated

☐ Restore from Glacier completed

Prefix ⓘ

e.g. images/

Suffix ⓘ

e.g. .jpg

Send to ⓘ

SQS Queue

SQS

s3-virusscan-ScanQueue-KLPKIG3U7K46

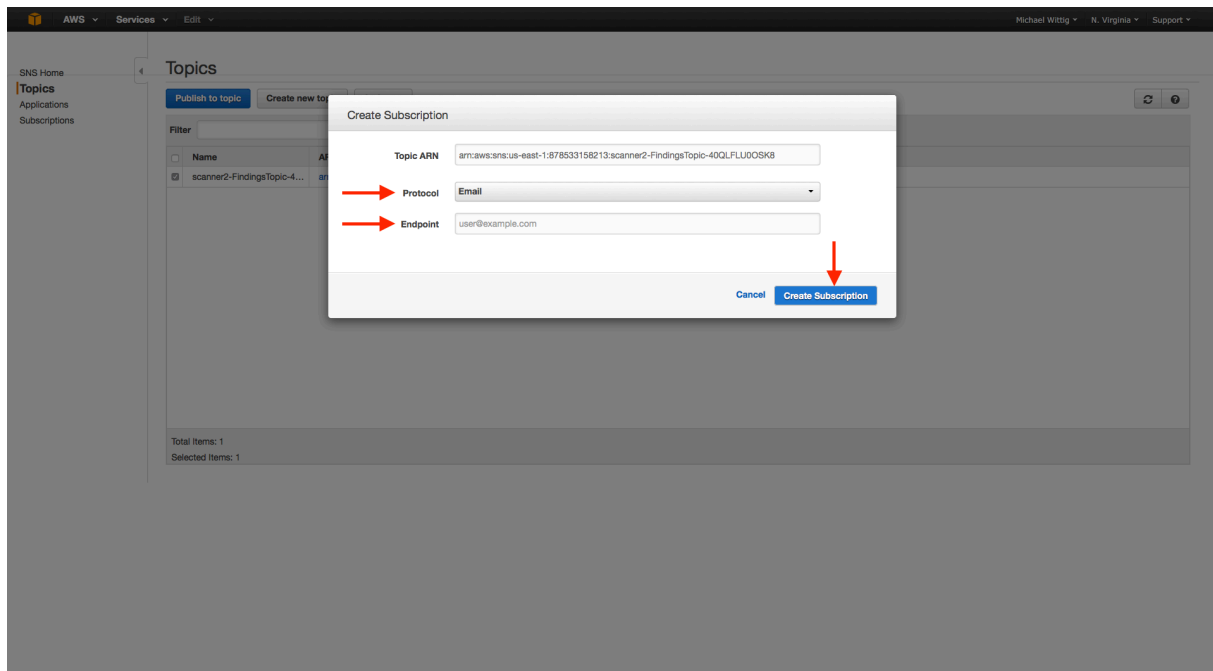
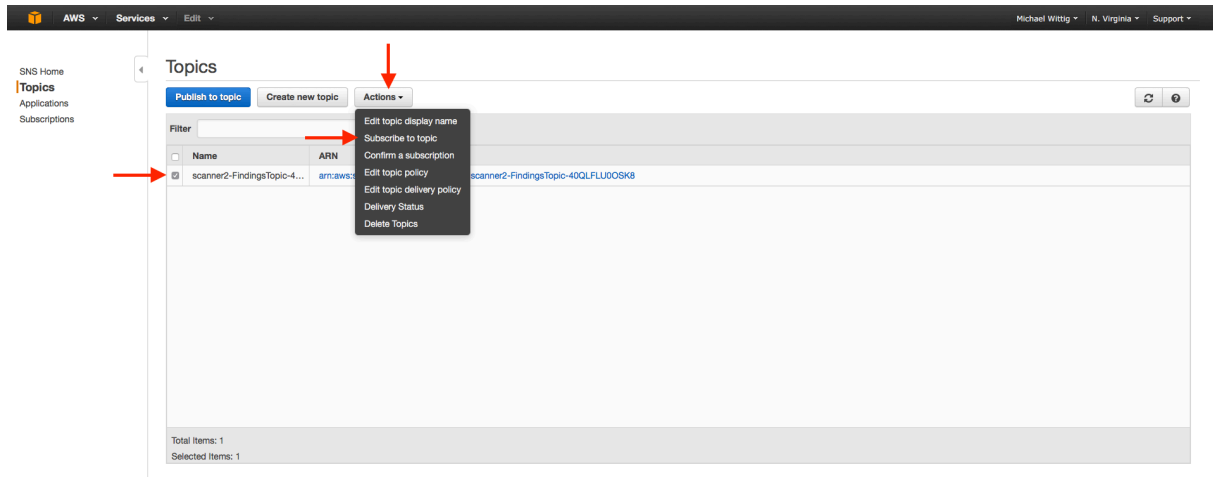
Cancel

Save

Make sure you select the -ScanQueue- NOT the -ScanQueueDLQ-!

Configure E-Mail subscription

If you like to receive emails if a virus was found you must subscribe to the SNS topic as shown in the next two figures:



You will receive a confirmation email.

bucketAV - Antivirus for Amazon S3 with additional features is available at AWS Marketplace.

Troubleshooting

1. Go to CloudWatch Logs in the AWS Management Console
2. Click on the log group of the s3-virusscan
3. Click on the blue **Search Log Group** button
4. Search for "s3-virusscan["

Known issues / limitations

- It was reported that the solution does not run on a t2.micro or smaller. Use at least a t2.small instance.
- An initial scan may also be useful but is not performed at the moment. This could be implemented with a Lambda function that pushes every key to SQS.