**bucketAV - antivirus for Amazon S3**

Contents

[bucketAV - antivirus for Amazon S3 2](#_Toc115351831)

[Scope: 2](#_Toc115351832)

[Problem statement that we are trying to solve: 2](#_Toc115351833)

[Introduction: 2](#_Toc115351834)

[Key benefits 3](#_Toc115351835)

[Subscribe to the product in AWS marketplace: 3](#_Toc115351836)

[Configuring S3 buckets: 10](#_Toc115351837)

[Scan buckets at regular intervals: 14](#_Toc115351838)

[Reporting and visibility: 14](#_Toc115351839)

Document Name: bucketAV - antivirus for Amazon S3

Owner: Pooja Sawat

# Scope:

bucketAV Scans files immediately after upload or on-demand and Tag, delete, or quarantine infected files automatically. Your data never leaves your AWS account.

# Problem statement that we are trying to solve:

How to Subscribe to the bucketAV product in AWS Marketplace and how to configure S3 AWS bucket

# Introduction:

It scans S3 buckets for viruses, worms and trojans. bucketAV detects Malware in real time or on demand. our data never leaves the AWS account.

## Key benefits

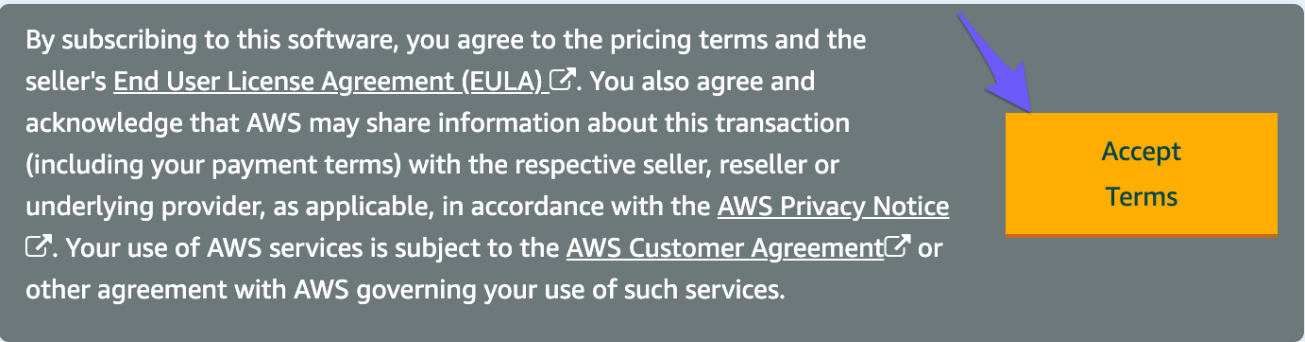
* data protection: scan your data with virtual machine running in your account no need to transfer data to an external service
* simple: get started within 15 minutes with the help of our setup guide and auto installer based on a cloudformation
* up-to-date Marwar database: the signatures are updated continuously to protect you against threats . The database contains more than 1 million viruses, worms and trojans.
* scalable: scan as many files as needed for bucketAV sales automatically. that's ensuring cost efficiency even for spiky workload
* fast: uploaded files are scanned within a second to detect Malware as quickly as possible
* automated mitigation: bucketAV quarantines, deletes, tags, and notifies about infected files configure the automated actions as needed.

# Subscribe to the product in AWS marketplace:

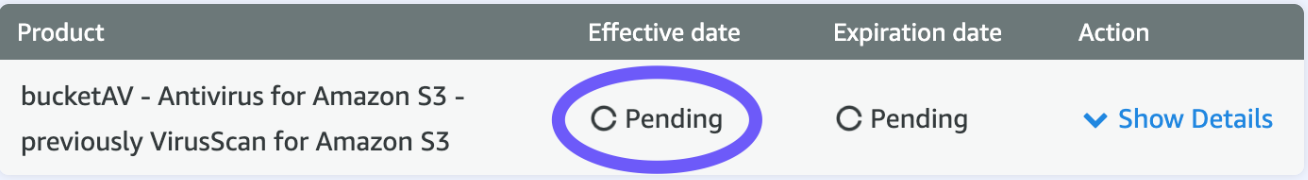
* Go to the AWS Marketplace . Click on Continue to Subscribe.



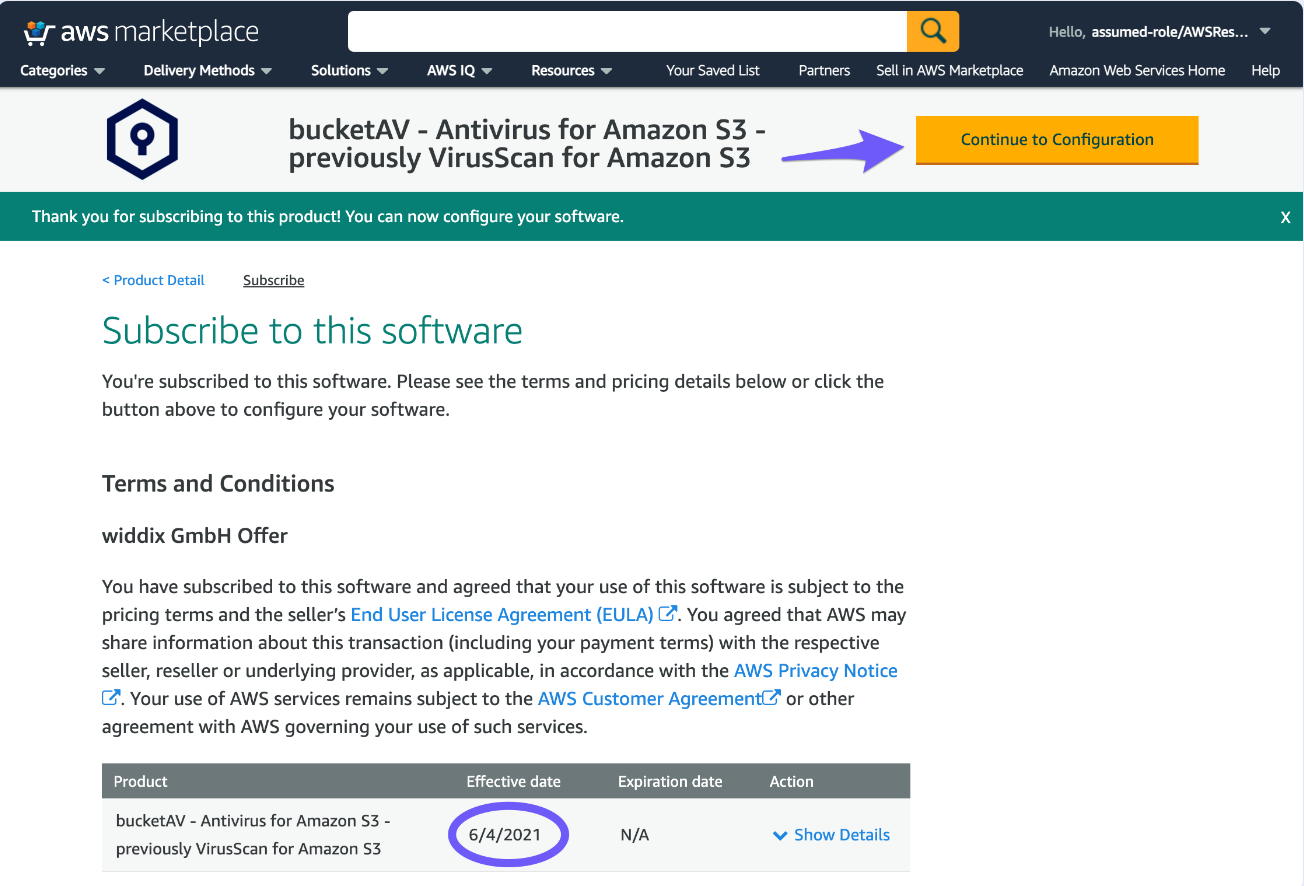
* Click on Accept Terms.



* The subscription is now Pending.



* Wait until the subscription is active and click on Continue to Configuration.

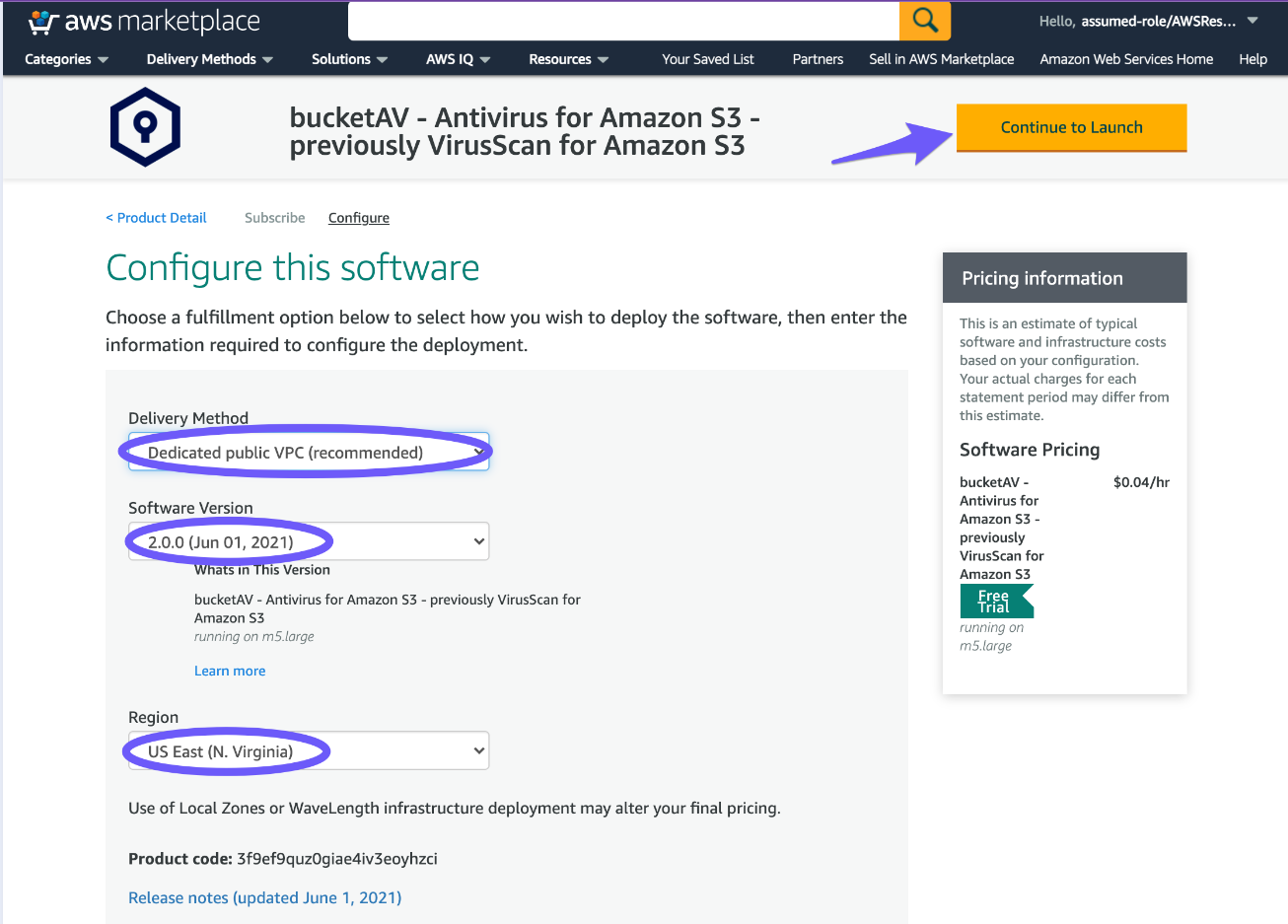


* We provide three delivery methods:

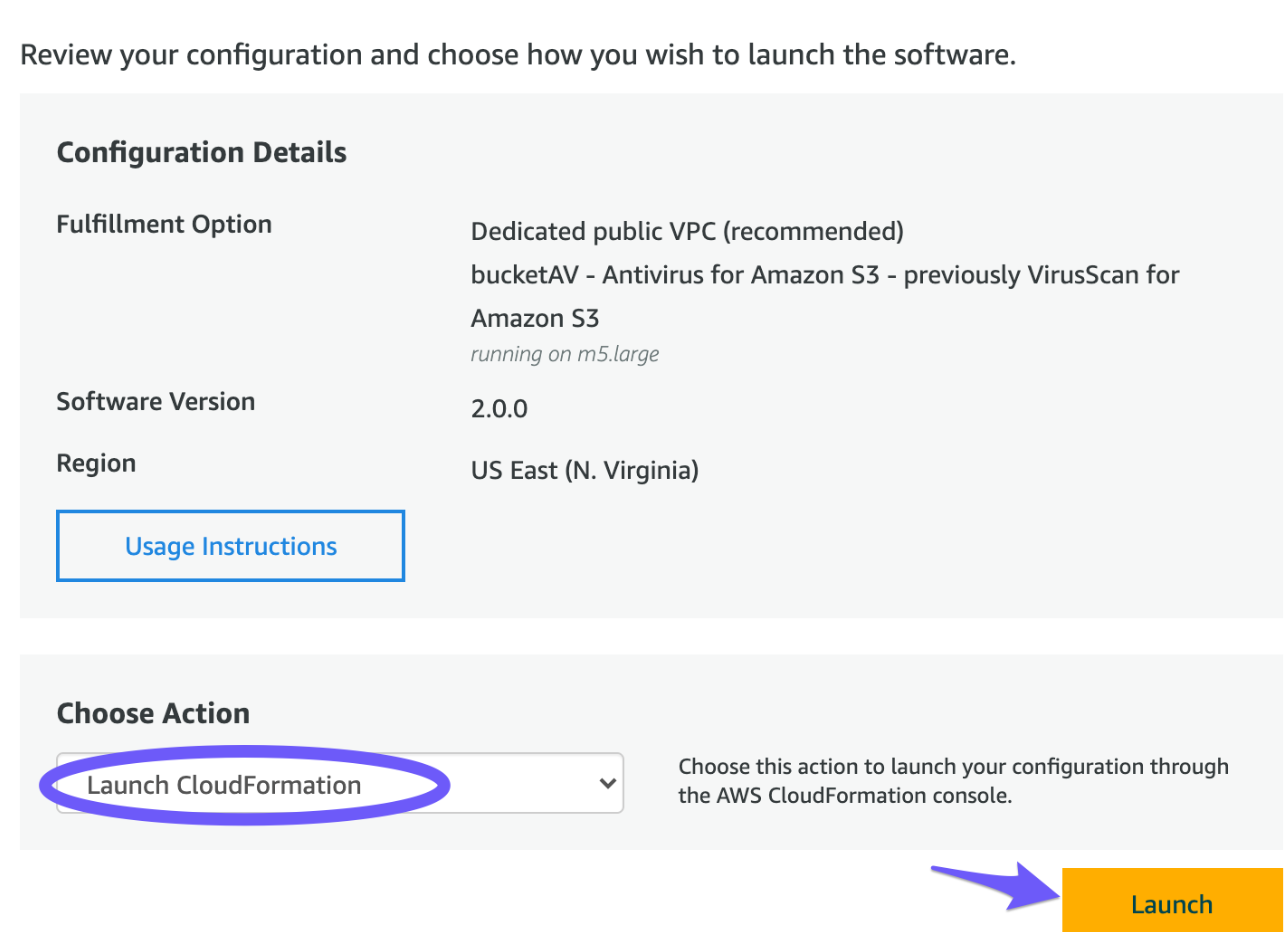
1. Dedicated public VPC (recommended): This is the most cost-efficient option where the network setup is included.
2. Dedicated private VPC: The EC2 instances run in private subnets (additional traffic charges apply). We recommend this option only if your internal security guidelines require it.
3. Existing VPC: Deploy bucketAV into an existing VPC . Ensure that required outbound ports and AWS services are reachable.

The Region you select must match with the region of your S3 buckets. If you use S3 buckets in multiple regions, repeat the setup for each region.

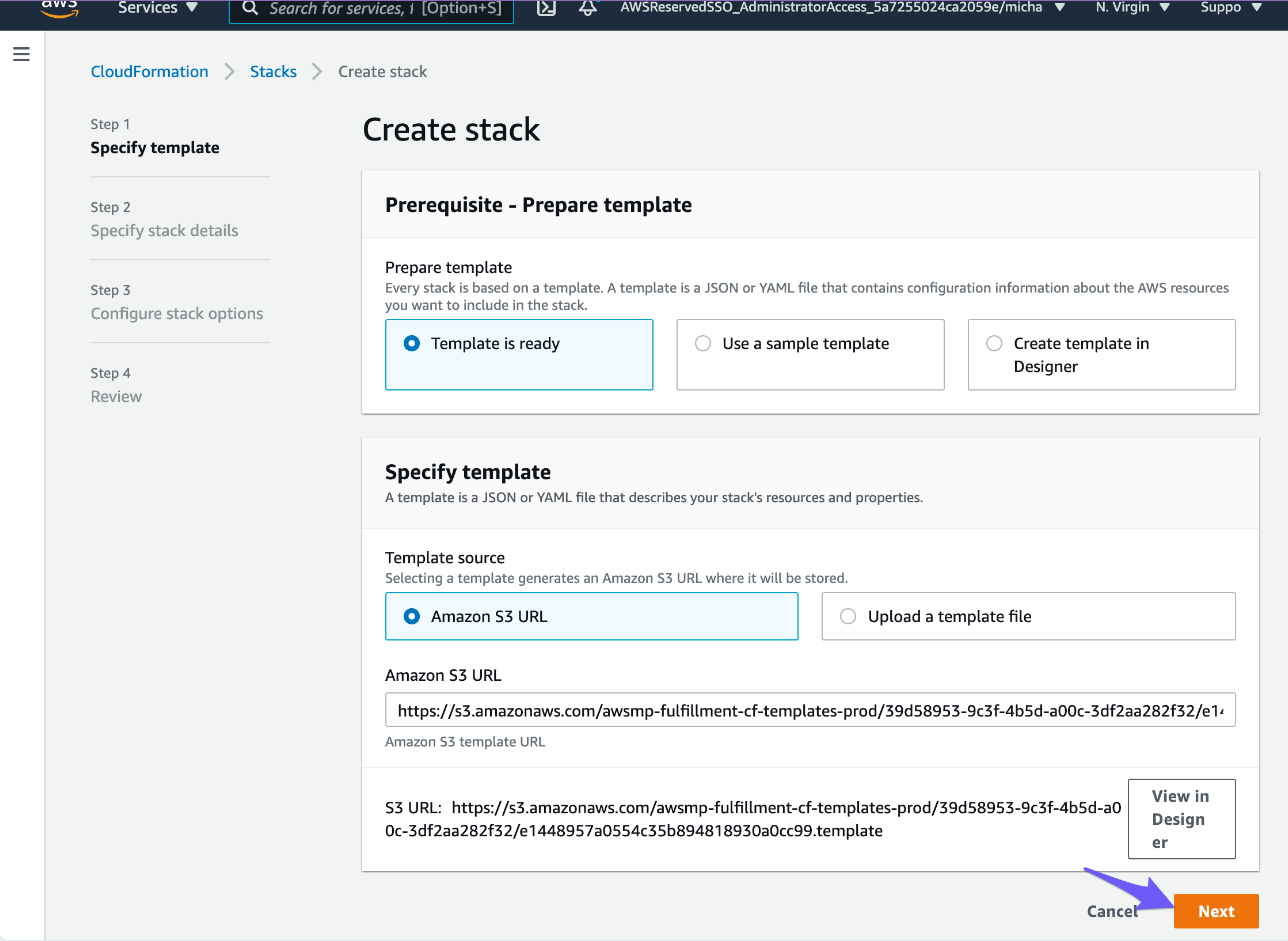
* Click on Continue to Launch.



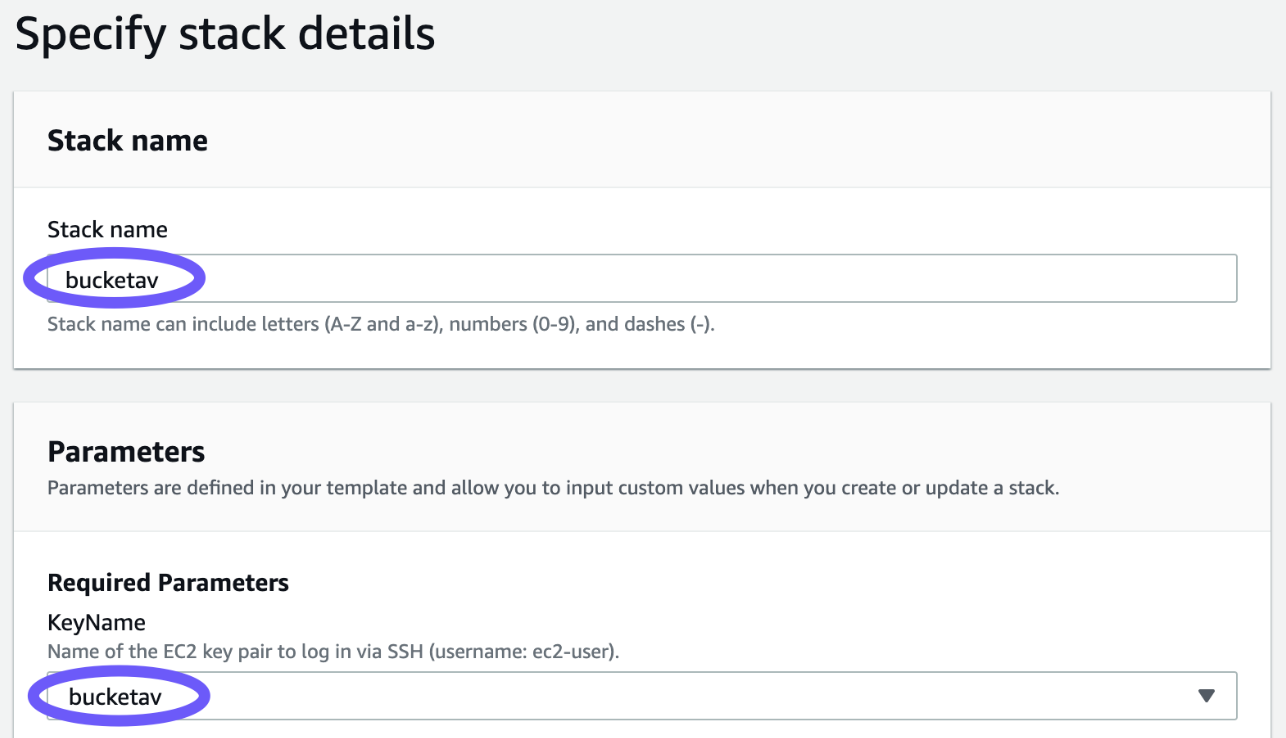
* Choose the Action Launch CloudFormation and click on Launch.



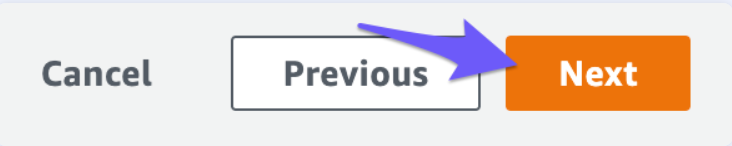
* You are redirected to CloudFormation. bucketAV is managed and configured via CloudFormation. Click on Next.



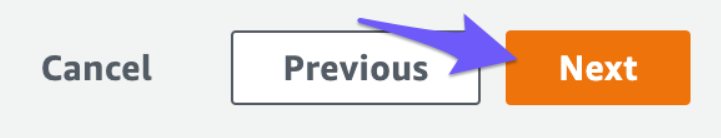
* Set a stack name(eg.: bucketav)
* Under Required Parameters, set the KeyName to an EC2 key pair.
* Review the rest of the parameter and go with the defaults (recommended)



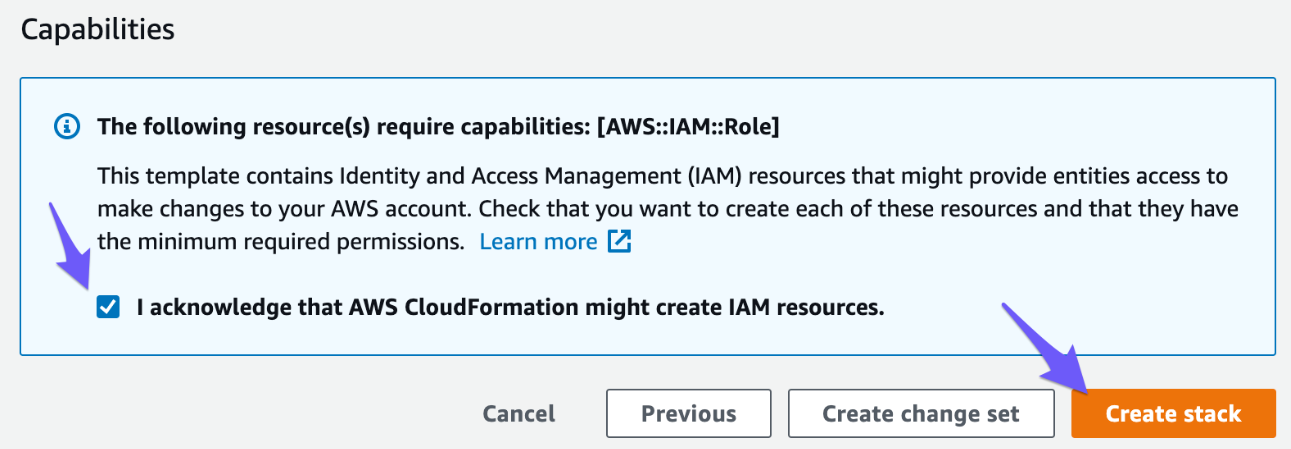
* Scroll to the bottom of the page and click on Next.



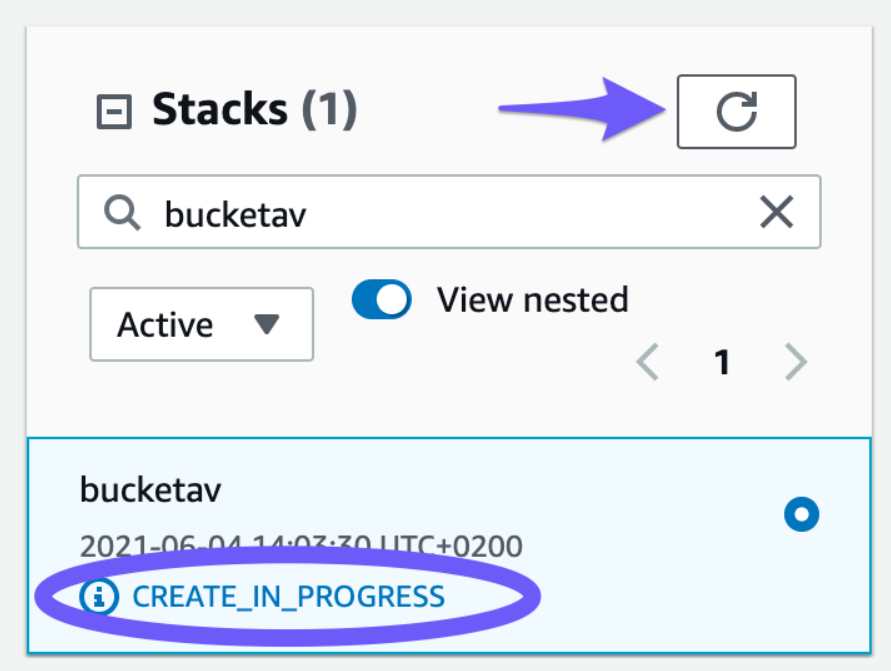
* Scroll to the bottom of the page and click on Next.



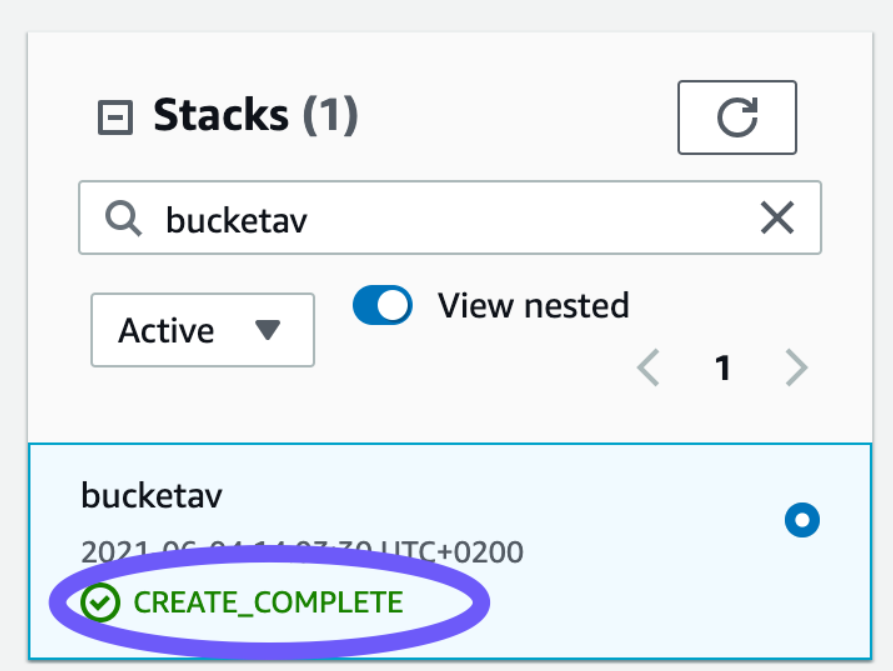
* Scroll to the bottom of the page, enable I acknowledge that AWS CloudFormation might create IAM resources, and click on Create.



* The stack status is CREATE\_IN\_PROGRESS. Reload the table from time to time and …



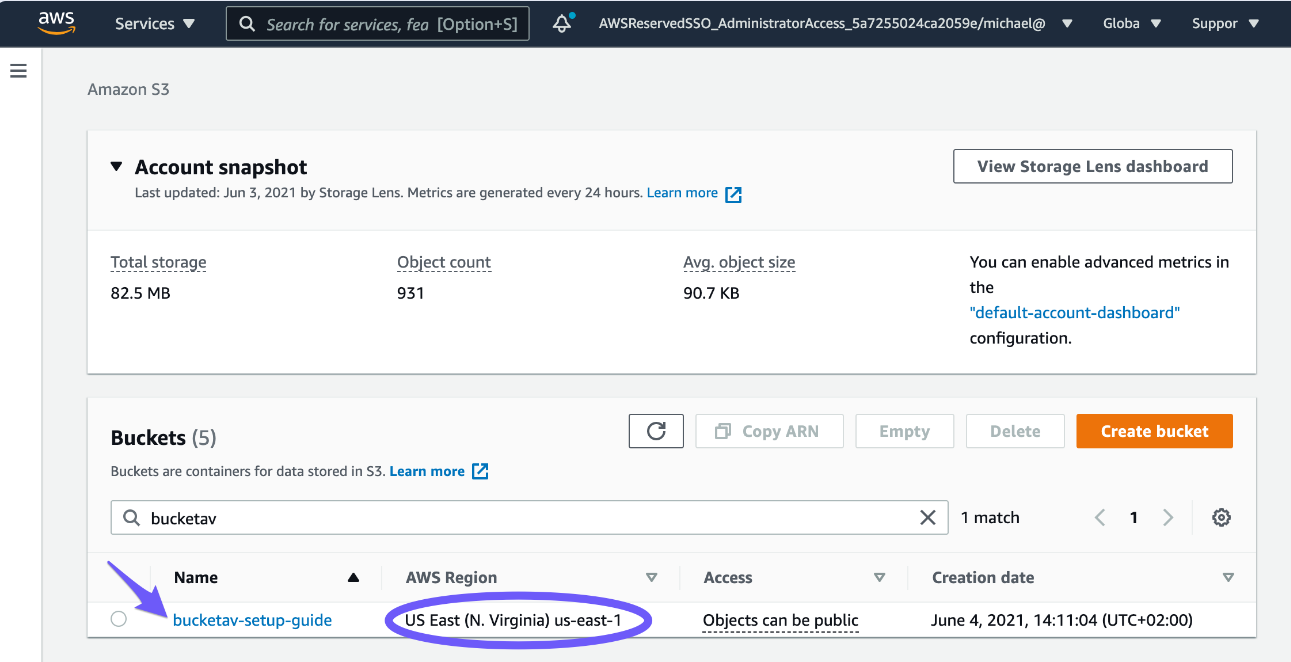
* … wait until the CloudFormation stack status switches to CREATE\_COMPLETE.



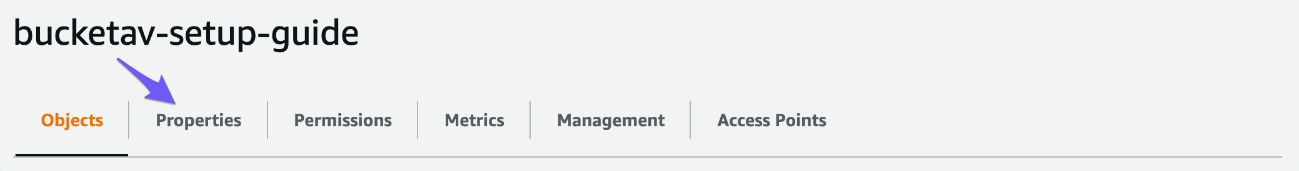
bucketAV is now up and running. Continue to connect your S3 buckets.

# Configuring S3 buckets:

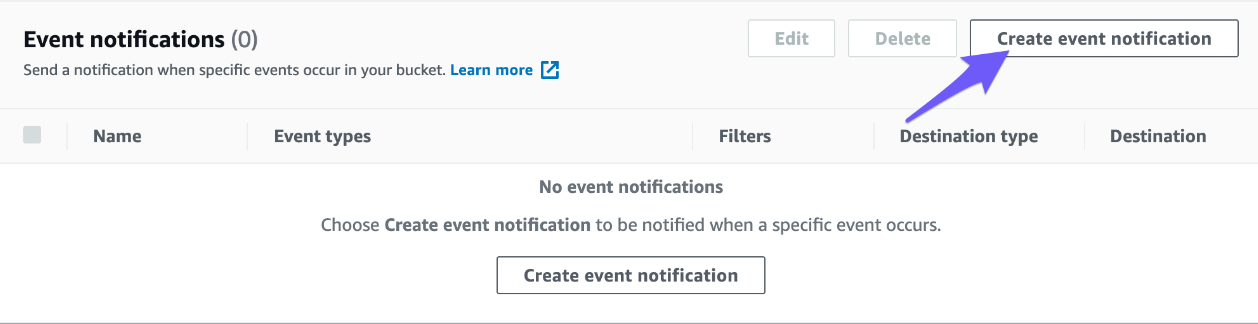
* In the AWS S3 Management console , click on the bucket you want to connect to bucketAV. Make sure the bucket’s region matches the bucketAV region.



* Click on the Properties tab.



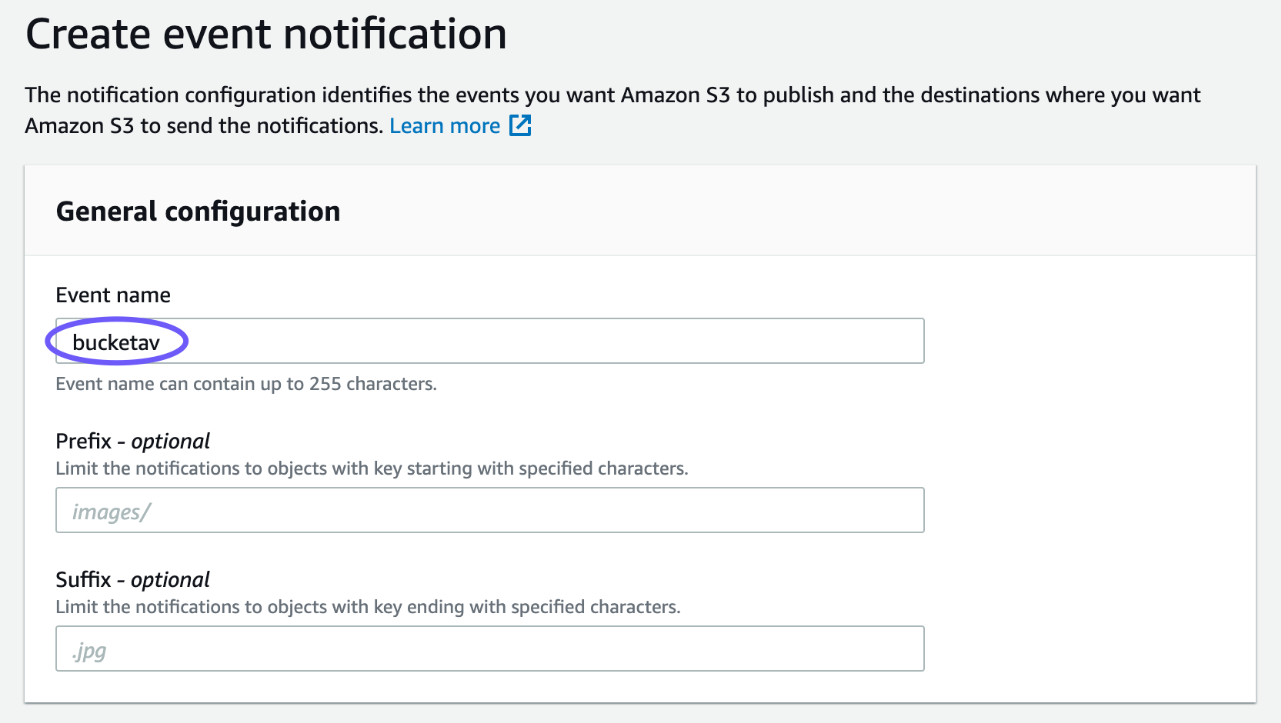
* Scroll down to the Event notifications box click on Create event notification.

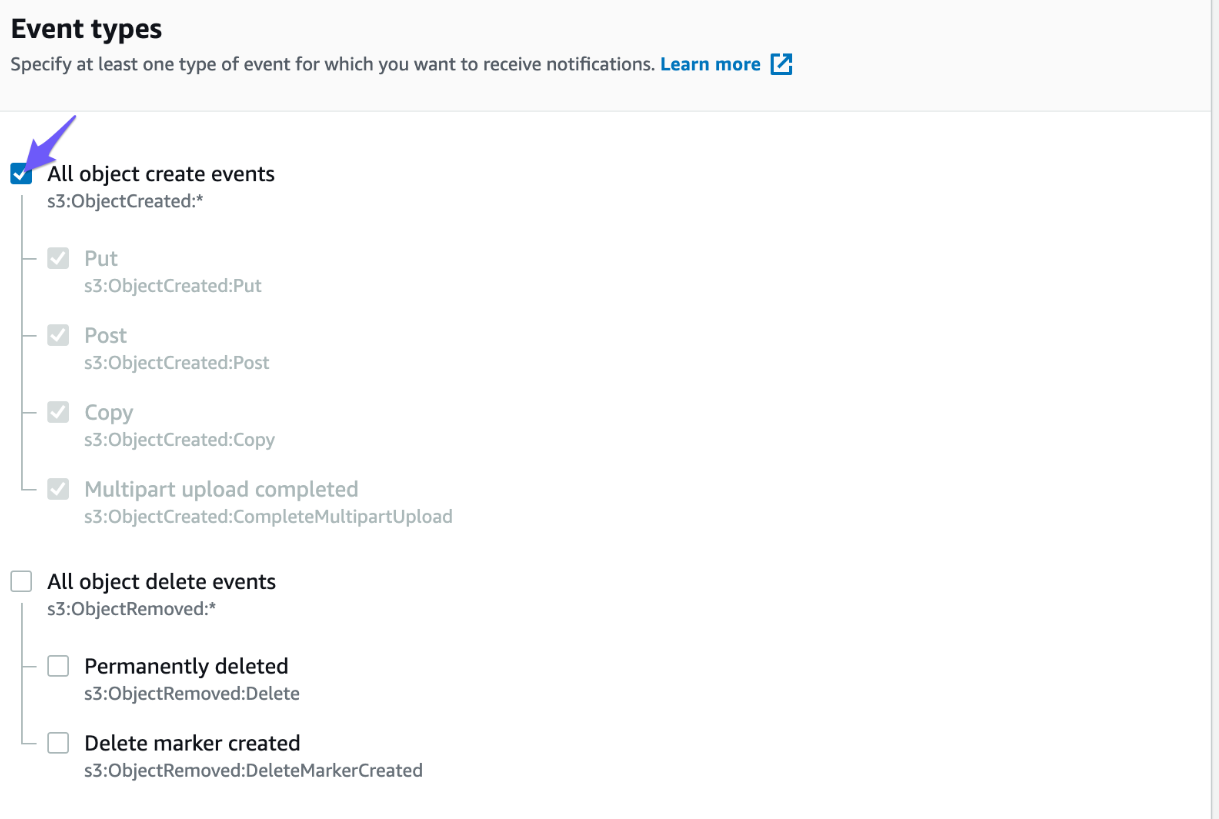


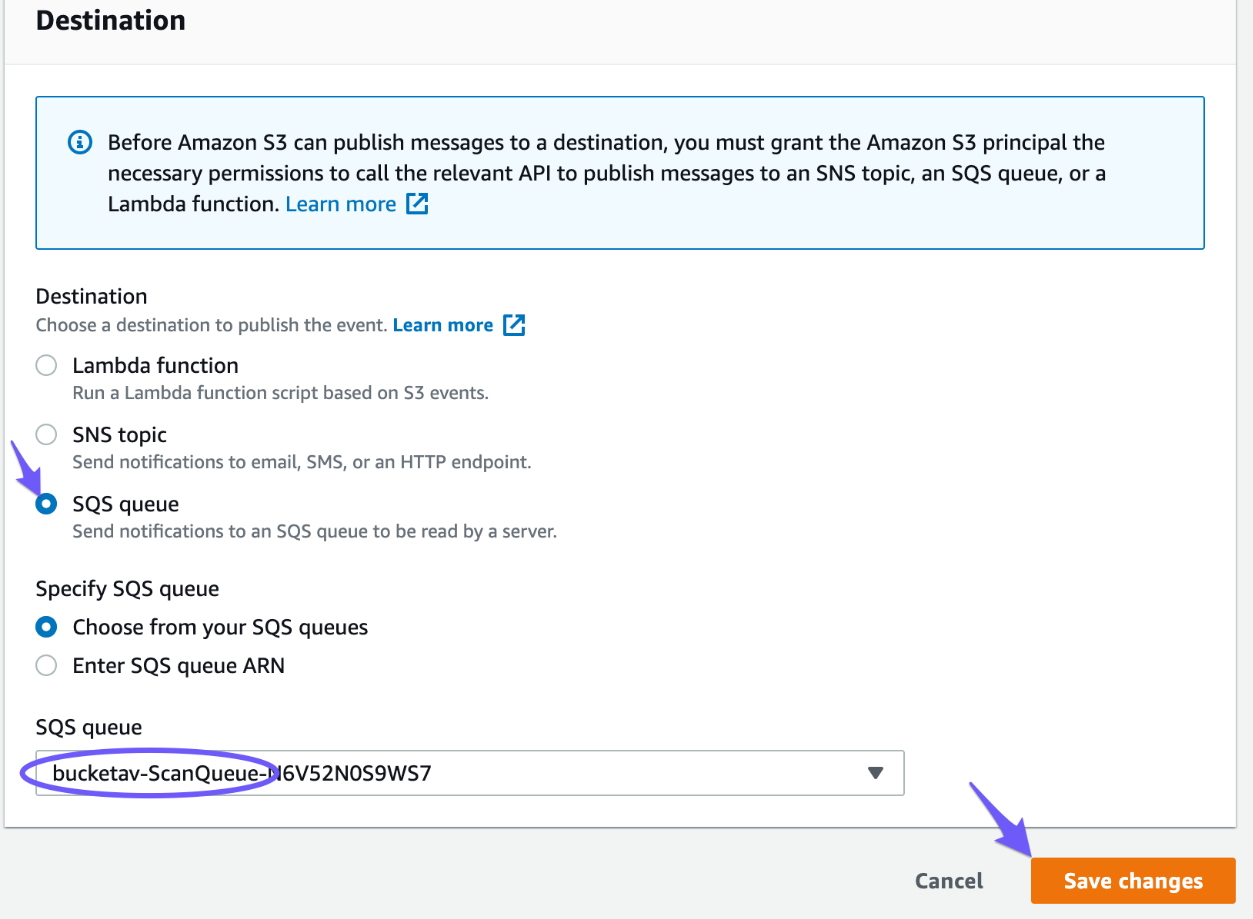
* Set the event name (eg.: bucketav)
* select the all object create events event type
* select the destination sqs queue and choose the sqs queue with scanqueue in the name

don't select the queue with DeadLetter queue in the name!

* click on save changes



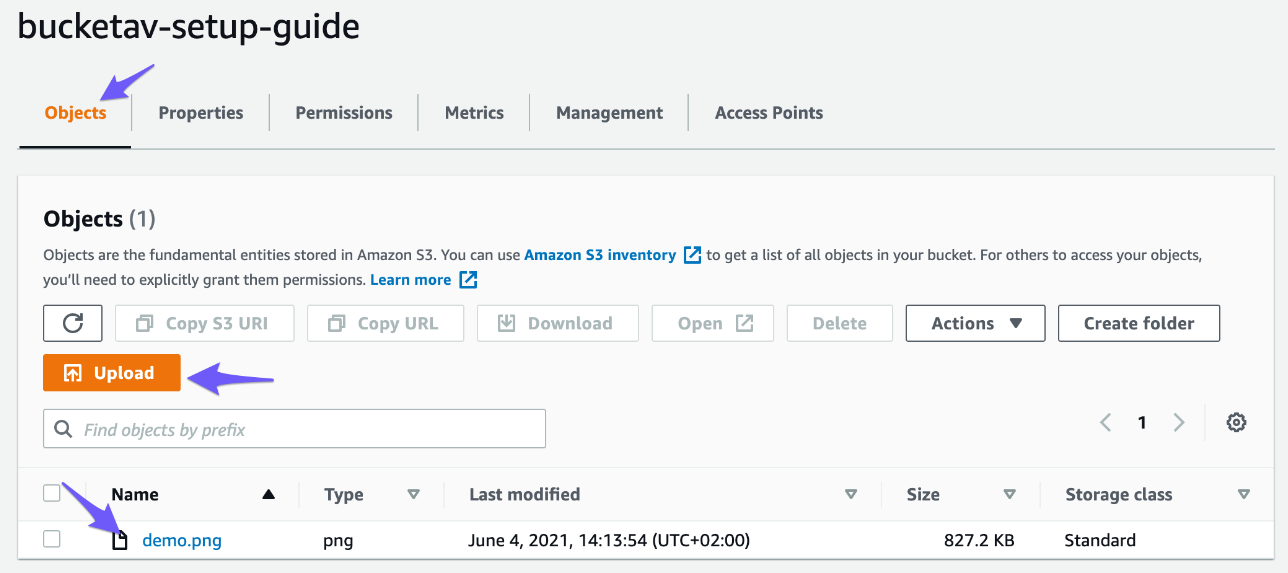




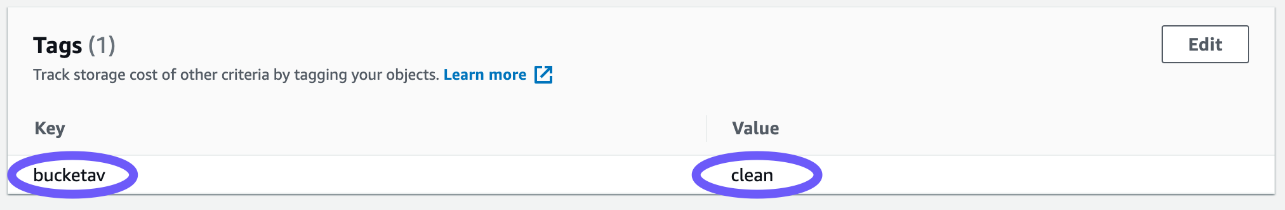
That’s it. From now on, each file that gets uploaded to your S3 bucket is scanned for trojans, viruses, and malware automatically. Repeat the steps for each bucket that needs protection!

Follow these steps to test your configuration

1. Upload a file to take the configuration
2. Click on the uploaded file



1. Scroll down to the Tags box. Within a few seconds, the bucketav tag is added with the scan result



1. Continue to configure scheduled bucket scans.

# Scan buckets at regular intervals:

If we want to scan all files in a bucket on schedule, install a **Scan bucket at regular intervals add-on.** continue to configure reporting and open the dashboard.

# Reporting and visibility:

To receive a daily /weekly/ monthly email report you have to install our Reporting Add-on