AWS Services Integration

1.S3 bucket creation

1. Go to Services > Storage > S3
2. Click on Create bucket.
3. Give it a name, then click on the *Create button.*

2.Create IAM User

2.1. Create IAM Policy

1. First create a policy with limited permission to access AWS s3 bucket.
2. Create new policy and add this code to the JSON tab.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::aws-wazuhs3bucket ",
        "arn:aws:s3:::aws-wazuhs3bucket /*"
      ]
    }
  ]
}
```

Note : Under the resources section, you have to replace with your own s3 bucket name we previously created.

2.2. Create user

1. Define a name and select AWS credential type as access-key.
2. And the attach the policy which we created previously.

2.3 Wazuh side Requirements

1. Access key
2. Secret key
3. Region

   Ex: ap-south-1

Note: This is for build the authentication between aws and the Wazuh server

2.AWS S3 Log Integration

1. Go to Services > Storage > S3
2. Look for the S3 bucket you want to monitor and click on its name.
3. Create folder for store s3 logs
4. Then go back to the bucket section and select s3 bucket again.
5. Then find the **Server access logging**, click edit.
6. Enable **Server access logging**, and click on the Browse S3 button to look for the bucket in which you want S3 Server Access logs to be stored.

Note It is possible to store the S3 Server Access logs in the same bucket to be monitored. It is also possible to specify a custom path inside the bucket to store the logs in it.

2.2.Wazuh side Requirements

- S3 bucket name.
- Path of the s3 logs.(including folder created in previous steps)

3.AWS CloudTrail

1. Create New Trail
2. Define a trail name
3. Then select previously created s3 bucket.
4. Create new kms key
5. Then keep default settings and click *next***.**
6. By default its only selected management events, we can recommend to choose other two options as well.
   - Insight Events – measure unusual activity against a seven day baseline.

- Data Events - Data events provide visibility into the resource operations performed on or within a resource. These are also known as data plane operations. Data events are often high-volume activities.

7. After selecting those you can create trail.

4.AWS Virtual Private Cloud.

1. Go to Network & Security > Network Interfaces on the left menu. Select a network interface and select Create a flow log on the Actions menu.
2. Select second option called s3 bucket in destination.
3. Enter the ARN of the previously created bucket.
4. You should partition your logs per hour to reduce your query costs and get faster responses if you have large volume of logs and typically run queries targeted to a specific hour timeframe.
5. Then create vpc flow logs.

5.AWS GuardDuty

1. Go to Services > Analytics > Kinesis.
2. Click Get started
3. Click on Create delivery stream button.
4. Select Source as Direct PUT and Destination as Amazon S3.
5. You can define a Delivery stream name or else you can keep default settings.
6. Keep default settings in Transform and Convert records.
7. Select Amazon S3 as the destination, then select the previously created S3 bucket and add a prefix where logs will be stored.

   S3 bucket prefix – firehose/

8. Then Click **Create delivery stream.**
9. Go to Services > Management Tools > CloudWatch:
10. Click “**Go to the Amazon EventBridge”** button
11. Create a rule
12. Define a rule name, Event bus – default, rule type – rule with an event pattern.
13. In buld event pattern keep the default settings in place.
14. Scroll down and include Event source as **AWS services,** AWS service as GuardDuty, Event type – All Events.
15. Then Select a target as **Firehose delivery stream, and then select the stream you created.**
16. Then click next and create.
17. Finally go to the Guard Duty and enable it.

5.1 Wazuh side Requirements

- S3 bucket prefix name