**ISS Technologies**

**Document Name: Wazuh Cluster Setup on VMs**

**Version No: 1.0**

**Created by: Ram Moahan**

**Reviewed & Approved by: Sasidhar.**

**Version Control:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Version** | **Description of change** | **Prepared by** | **Reviewed and Approved by** |
| **10/03/2025** | **1.0** | **Original – created** | **Ram Mohan** | **Sasidhar B** |

**Prerequisites**

1. **Create or Use an Existing S3 Bucket**

* Create a new S3 bucket or use an existing one to store AWS CloudTrail logs.
* Note the bucket name for later reference in Wazuh configuration.

2. **Create a CloudTrail Trail**

* Go to **AWS Console** → **Search for CloudTrail** or navigate to **Management & Governance > CloudTrail**.
* Click **Create trail**.
* Assign a **Trail Name** and select the S3 bucket created earlier.
* Ensure that **Log file SSE-KMS encryption** is configured if required.
* AWS CloudTrail logs will follow this structure:

3. IAM Policy for S3 Access

Create an IAM policy for read-only access:

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "VisualEditor0",

"Effect": "Allow",

"Action": [

"s3:GetObject",

"s3:ListBucket"

],

"Resource": [

"arn:aws:s3:::<WAZUH\_AWS\_BUCKET>/\*",

"arn:aws:s3:::<WAZUH\_AWS\_BUCKET>"

]

}

]

}

 Replace <WAZUH\_AWS\_BUCKET> with the actual bucket name.

 Attach the policy to an IAM user or user

Then create a AWS IAM role with attach the policy which is previously created

Then copy the ARN and update the policy is

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "VisualEditor0",

"Effect": "Allow",

"Action": [

"s3:GetObject",

"s3:ListBucket",

"s3:GetBucketPolicy",

"sts:AssumeRole"

],

"Resource": [

"arn:aws:s3:::s3-bucktforcloudtrail/\*",

"arn:aws:s3:::s3-bucktforcloudtrail",

"arn:aws:iam::423623872287:role/wazuh-cloudtrail-01-role-210325"

]

}

]

}

Then create a AWS IAM user attach this policy and copy the ARN of the user and update the trustrelationship policy of the role

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Principal": {

"Service": "s3.amazonaws.com",

"AWS": "arn:aws:iam::423623872287:user/cloudtrail-user-group-210325"

},

"Action": "sts:AssumeRole"

}

]

}

Then update the wazuh config file for cloudtrail logs.

<wodle name="aws-s3">

<disabled>no</disabled>

<interval>10m</interval>

<run\_on\_start>yes</run\_on\_start>

<skip\_on\_error>yes</skip\_on\_error>

<bucket type="cloudtrail">

<name><WAZUH\_AWS\_BUCKET></name>

<aws\_profile>default</aws\_profile>

</bucket>

</wodle>

Then restart the wazuh-manager

Systemctl restart wazuh-manager