**ISS Technologies**

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

**Version No: 1.0**

**Created by: Ram Moahan**

**Reviewed & Approved by: Sasidhar.**

**Version Control:**

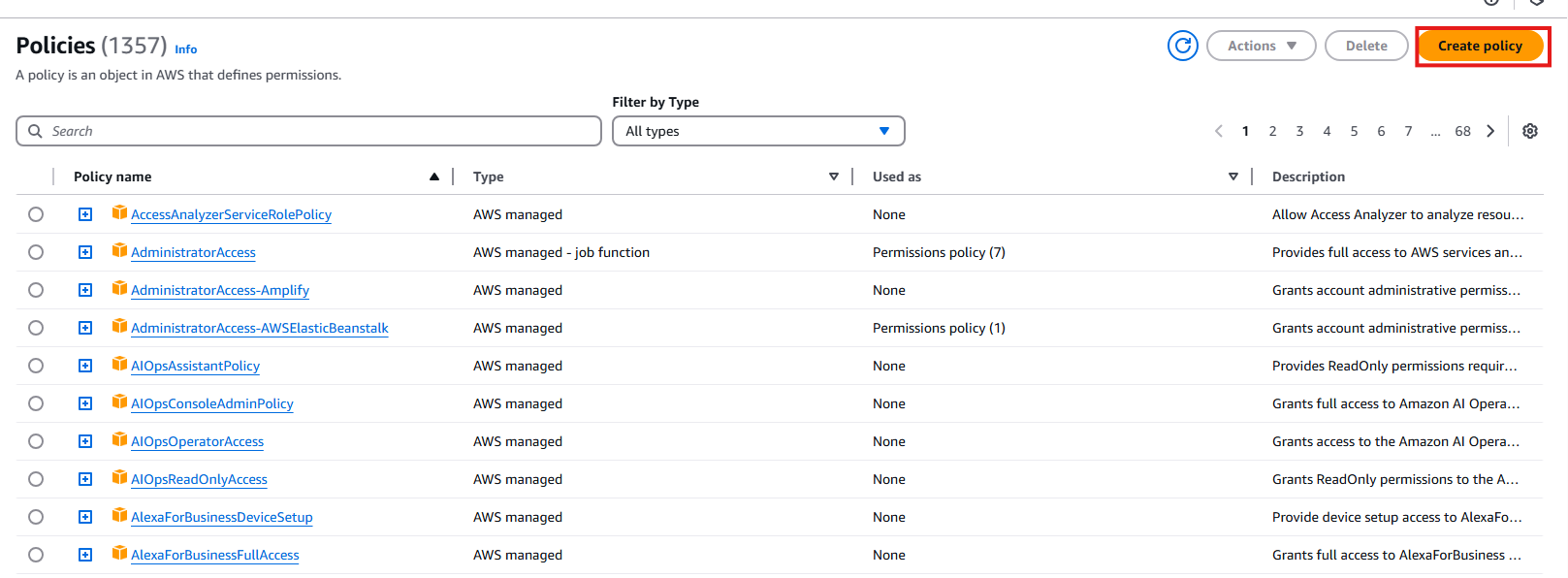
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Version** | **Description of change** | **Prepared by** | **Reviewed and Approved by** |
| **25/03/2025** | **1.0** | **Original – created** | **Ram Mohan** | **Sasidhar B** |

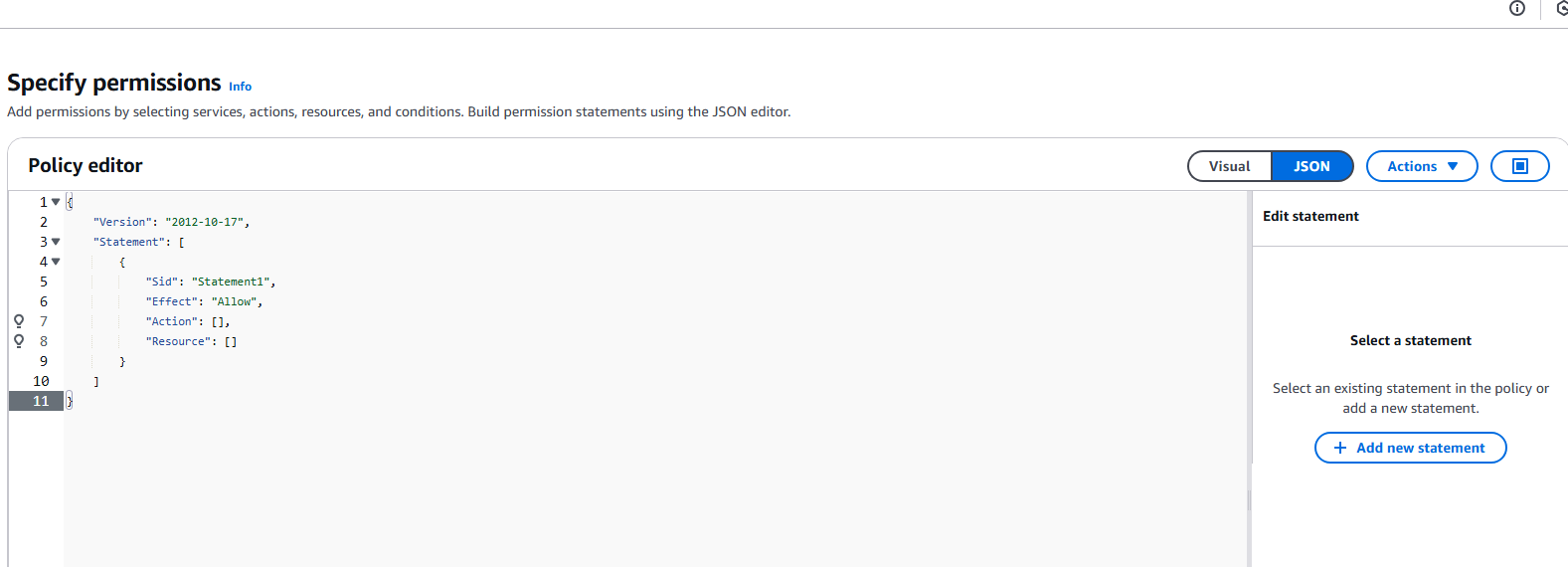
**Prerequisites**

### **AWS Configuration Prerequisites**

1. **S3 Bucket Creation & Configuration:**
   * Create an S3 bucket or use an existing one.
   * Copy the Amazon Resource Name (ARN) of the bucket.
2. **Enable VPC Flow Logs:**
   * Go to AWS Console → **Services** → **EC2**.
   * Navigate to **Network & Security** → **Network Interfaces**.
   * Select a network interface and click **Create flow log**.
   * Configure it to send logs to the S3 bucket using its ARN.

3**.IAM Policy Configuration**:



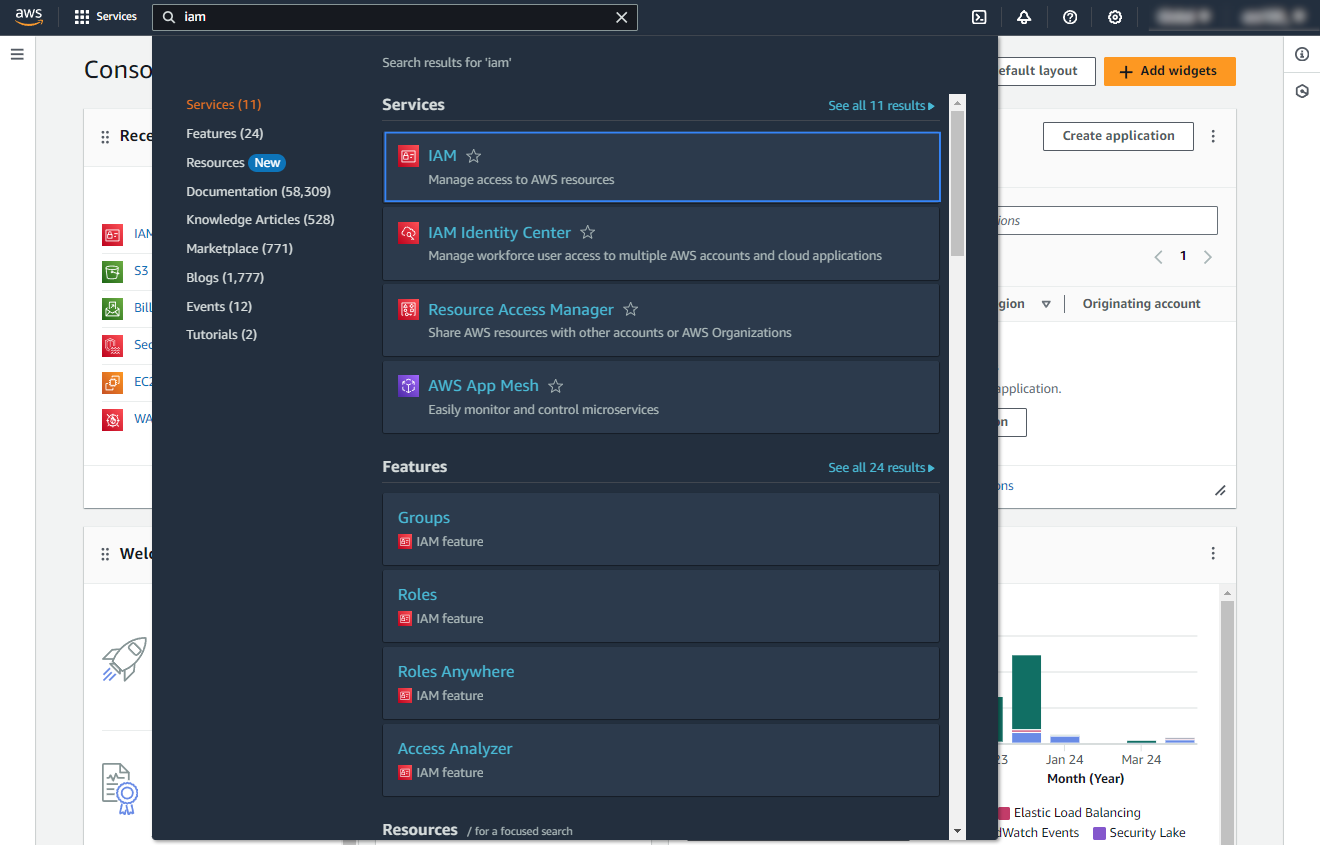


## Creating an AWS policy

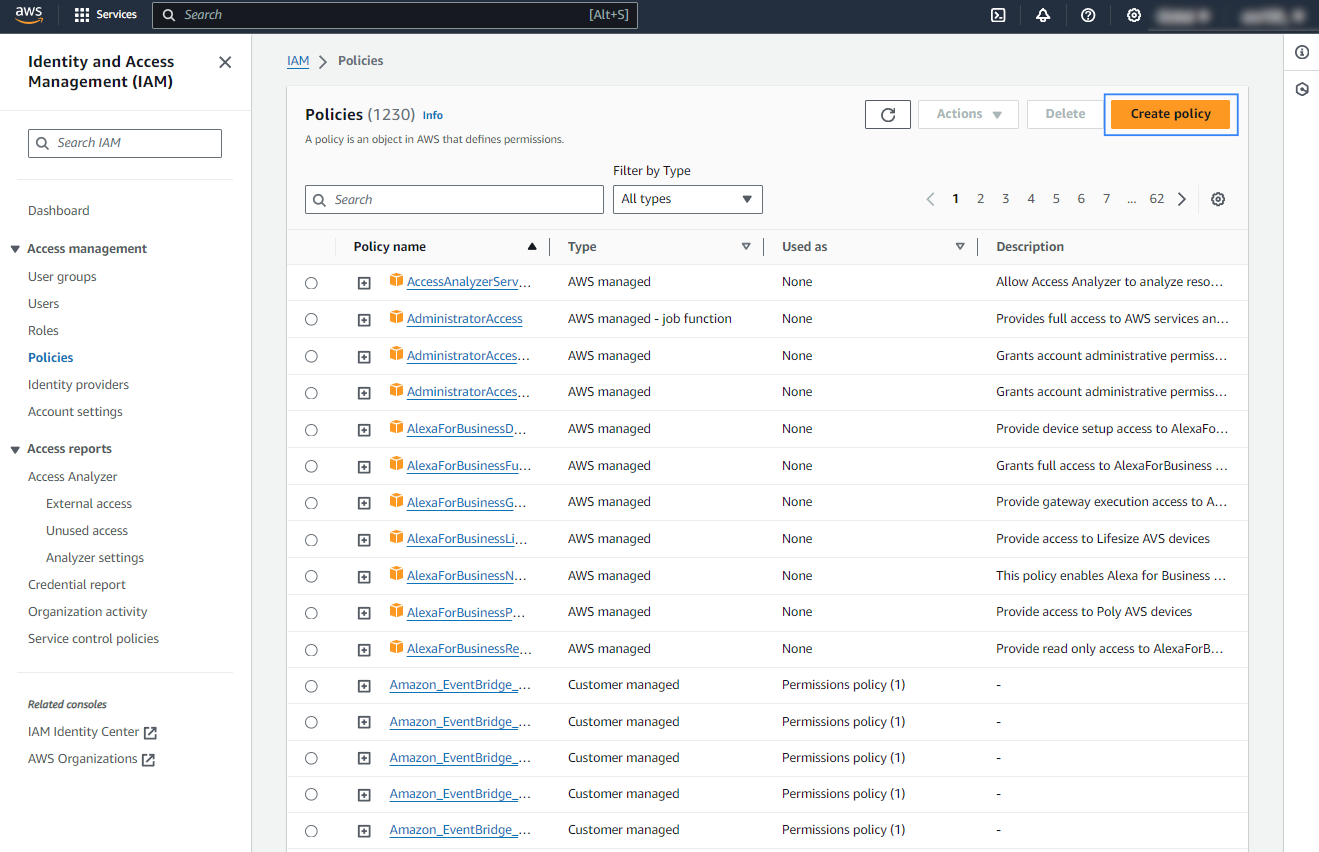
Depending on the AWS service that will be monitored, the AWS IAM user will need different sets of permissions. The permissions required for each AWS service are explained on each page of the [supported services](https://documentation.wazuh.com/current/cloud-security/amazon/services/supported-services/index.html) section.

Follow the steps below on your AWS console to create an AWS policy that collects logs from an S3 bucket.

1. On the AWS console, search for IAM and click **IAM** from the results



2.Click **Policies** > **Create policy**.



Switch to **JSON** view, remove the default statement, and paste the following configuration. Replace <WAZUH\_AWS\_BUCKET> with the name of the previously created [S3 bucket](https://documentation.wazuh.com/current/cloud-security/amazon/services/prerequisites/S3-bucket.html). In this example, the policy allows the IAM user to return and retrieve an object from the specified S3 bucket.

{

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

"Statement": [

{

"Sid": "GetS3Logs",

"Effect": "Allow",

"Action": [

"s3:GetObject",

"s3:ListBucket"

],

"Resource": [

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

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

]

}

]

}

Then replace the WAZUH\_AWS\_BUCKET with actual bucket which is created inside the aws account.

Create AWS IAM Role and attach this policy to the role.and take the ARN of the role.

And edit the policy which is previously created update with ARN and sts,then it become

{

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

"Statement": [

{

"Sid": "GetS3Logs",

"Effect": "Allow",

"Action": [

"s3:GetObject",

"s3:ListBucket",

"sts:AssumeRole"

],

"Resource": [

"arn:aws:s3:::s3bucket-250325/\*",

"arn:aws:s3:::s3bucket-250325",

"arn:aws:iam::352837684612:role/250325-role"

]

},

{

"Sid": "VisualEditor0",

"Effect": "Allow",

"Action": "ec2:DescribeFlowLogs",

"Resource": "\*"

}

]

}

Now create one user and attach the policy to user and copy the ARN of the user

For collecting the VPC logs wazuh require the policy is

{

"Sid": "VisualEditor0",

"Effect": "Allow",

"Action": "ec2:DescribeFlowLogs",

"Resource": "\*"

}

It should be attached to the policy which is created previously.

Now we need to update the the policy and edit the role and go to trustrelationship policy of the role and update it with user ARN

{

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

"Statement": [

{

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::352837684612:user/user2503",

"Service": "s3.amazonaws.com"

},

"Action": "sts:AssumeRole"

}

]

}

Now we need to update the config file of the wazuh

<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="vpcflow">

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

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

</bucket>

</wodle>

Then we need to restart the wazuh server

Systemctl restart wazuh-manager