**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** |

[AWS CloudWatch Logs](https://aws.amazon.com/cloudwatch/" \t "_blank) is a service that allows the users to centralize the logs from all their systems, applications, and AWS services in a single place. To understand how Cloudwatch Logs works it is important to learn about the following concepts:

* **Log events**: CloudWatch saves the logs generated by the application or resource being monitored as log events. A log event is a record with two properties: the timestamp when the event occurred and the raw log message.
* **Log streams**: Log events are stored in log streams. A log stream represents a sequence of events coming from the application instance or resource being monitored. All log events in a log stream share the same source.
* **Log groups**: Log streams are grouped using log groups. A log group defines a group of log streams that share retention, monitoring, and access control settings.

# **Prerequisites**

### **AWS Setup**

1. AWS IAM Role
2. AWS IAM user
3. Wazuh server

1.Create an IAM Role [cw-ec2-wazuh-ram-2202-role](https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/details/cw-ec2-wazuh-ram-2202-role)

* + CloudWatchFullAccess (CloudWatchFullAccess)
  + AmazonSSMManagedInstanceCore

We need to add this policy to ec2 instance directly to collect the logs

2.create IAM role(cw-wazuh-ram-role1) with the policies

* [CloudWatchEventsInvocationAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Fservice-role%2FCloudWatchEventsInvocationAccess)
* [CloudWatchEventsBuiltInTargetExecutionAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Fservice-role%2FCloudWatchEventsBuiltInTargetExecutionAccess)
* cw-ram-policy-1

then trust relationship policy the role is updated with user ARN

*{*

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

*"Statement": [*

*{*

*"Sid": "",*

*"Effect": "Allow",*

*"Principal": {*

*"Service": "events.amazonaws.com",*

*"AWS": "arn:aws:iam::352837684612:user/ISS\_Ramu"*

*},*

*"Action": "sts:AssumeRole"*

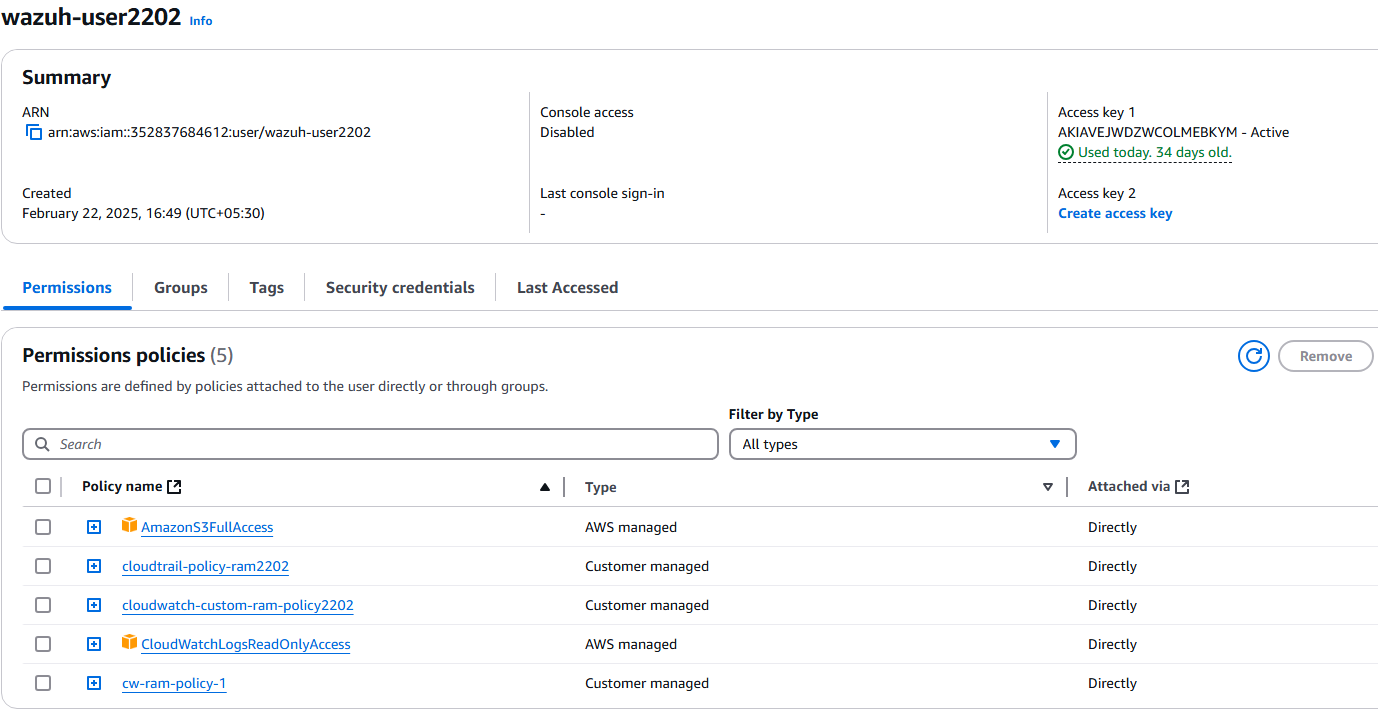
*}*

*]*

*}*

**IAM user with attach the policies**

* AmazonS3Fullaccess
* CloudWatchReadOnlyAcces
* CloudWatch custom policy
* cw-ram-policy-1



1.Cloudwatch custom-ram-policy2202

*{*

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

*"Statement": [*

*{*

*"Effect": "Allow",*

*"Action": [*

*"logs:GetLogEvents",*

*"logs:DescribeLogGroups",*

*"logs:DescribeLogStreams"*

*],*

*"Resource": "arn:aws:logs:us-east-1:423623872287:log-group:/my/app/logs:\*"*

*}*

*]*

*}*

2. cw-ram-policy-1

*{*

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

*"Statement": [*

*{*

*"Sid": "VisualEditor0",*

*"Effect": "Allow",*

*"Action": [*

*"logs:DescribeLogStreams",*

*"sts:AssumeRole"*

*],*

*"Resource": [*

*"arn:aws:logs:us-east-1:352837684612:log-group:/my/app/logs:\*",*

*"arn:aws:iam::352837684612:role/cw-wazuh-ram-role1"*

*]*

*},*

*{*

*"Sid": "VisualEditor1",*

*"Effect": "Allow",*

*"Action": [*

*"logs:GetLogEvents",*

*"sts:AssumeRole"*

*],*

*"Resource": [*

*"arn:aws:logs:us-east-1:352837684612:log-group:/my/app/logs:log-stream:i-0ef3d3ad36cb0ab53",*

*"arn:aws:iam::352837684612:role/cw-wazuh-ram-role1"*

*]*

*}*

*]*

*}*

**AWS cloudwatch agent installation:**

*wget https://s3.amazonaws.com/amazoncloudwatch-agent/ubuntu/amd64/latest/amazon-cloudwatch-agent.deb*

*sudo dpkg -i amazon-cloudwatch-agent.deb*

*sudo systemctl enable amazon-cloudwatch-agent*

*sudo systemctl start amazon-cloudwatch-agent*

**Configure CloudWatch Agent:**

*vim /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json*

*{*

*"agent": {*

*"region": "us-east-1"*

*},*

*"metrics": {*

*"metrics\_collected": {*

*"mem": {*

*"measurement": ["mem\_used\_percent"]*

*},*

*"swap": {*

*"measurement": ["swap\_used\_percent"]*

*}*

*}*

*},*

*"logs": {*

*"logs\_collected": {*

*"files": {*

*"collect\_list": [*

*{*

*"file\_path": "/var/log/syslog",*

*"log\_group\_name": "/my/app/logs",*

*"log\_stream\_name": "{instance\_id}"*

*}*

*]*

*}*

*}*

*}*

*}*

**Validate & Apply the Configuration**

*sudo amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -c file:/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json -s*

*sudo systemctl restart amazon-cloudwatch-agent*

**Verify Logs in CloudWatch**

*aws logs describe-log-streams --log-group-name "/my/app/logs" --region us-east-1*

*sudo tail -f /opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log*

**we need to update the config file of wazuh**

vim /var/ossec/etc/ossec.conf

*<wodle name="aws-s3">*

*<disabled>no</disabled>*

*<interval>5m</interval>*

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

*<service type="cloudwatchlogs">*

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

*<aws\_log\_groups>/my/app/logs</aws\_log\_groups>*

*<regions>us-east-1</regions>*

*</service>*

*</wodle>*

**Restart Wazuh Manager:**

Systemctl restart wazuh-manager

## **Validate Wazuh-AWS Integration**

cat /var/ossec/logs/ossec.log | grep aws

cd /var/ossec/logs

ls -lrt

cat ossec.log

**Wazuh server configuration for Wazuh integration with CloudWatch**

*vim /var/ossec/etc/internal-options.conf*

Change “wazuh-modules.debug=2”

We need to replace 0 to 2

*Systemctl restart wazuh-manager*

*Tail -f cat /var/ossec/logs/archives/archives.json | grep “ip-172-133-142-99”*

*Tail -f cat /var/ossec/logs/alerts/alerts.log*

*vim /var/ossec/etc/ossec.conf*

*<logall>yes</logall>*

*systemctl restart wazuh-manager*

Then we can get the dashboard visualization outputs.

