**Wazuh-aws cloudwatch integration**

apt update -y

sudo apt update && sudo apt upgrade -y

apt install vim curl -y

**#awscli installation:**

sudo apt update  
sudo apt install unzip curl -y  
curl "[https://awscli.amazonaws.com/awscli-exe-linux-x86\_64.zip"](https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip%22) -o "awscliv2.zip"  
unzip awscliv2.zip  
sudo ./aws/install  
aws --version

aws configure

#**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

**we need to create role with CloudWatch full access and that role is assigned to ec2 instance it will create the log streams.**

Policies required to add to the role is

**CloudWatchful access**

**AmazonSSMManagedInstanceCore**

**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

right now onwords logs will be stored in cloudwatchlog group

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

**policies required to user cloud watch loggroup.**

**Policy-01**

{

"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:\*"

}

]

}

**Policy-2**

{

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

"Statement": [

{

"Sid": "VisualEditor0",

"Effect": "Allow",

"Action": [

"logs:DescribeLogStreams",

"sts:AssumeRole"

],

"Resource": [

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

"arn:aws:iam::423623872287:role/cloud-watch-role-07"

]

},

{

"Sid": "VisualEditor1",

"Effect": "Allow",

"Action": [

"logs:GetLogEvents",

"sts:AssumeRole"

],

"Resource": [

"arn:aws:logs:us-east-1:423623872287:log-group:/my/app/logs:log-stream:log-events",

"arn:aws:iam::423623872287:role/cloud-watch-role-07"

]

}

]

}

**Policy-03**

[AdministratorAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAdministratorAccess)(optional)

**Role created for wazuh and aws integration:**

Here we need to create role with usecase aws cloudwatch ,if you select aws cloudwatch then the following rules are added defaultly

a.[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),

b.[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)

**we need to add the wazuh policy is**

d**.**custom wazuh policy

{

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

"Statement": [

{

"Sid": "VisualEditor0",

"Effect": "Allow",

"Action": [

"logs:DescribeLogStreams",

"sts:AssumeRole"

],

"Resource": [

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

"arn:aws:iam::423623872287:role/cloud-watch-role-07"

]

},

{

"Sid": "VisualEditor1",

"Effect": "Allow",

"Action": [

"logs:GetLogEvents",

"sts:AssumeRole"

],

"Resource": [

"arn:aws:logs:us-east-1:423623872287:log-group:/my/app/logs:log-stream:log-events",

"arn:aws:iam::423623872287:role/cloud-watch-role-07"

]

}

]

}

**And we need to edit the trust relationship policy of the same role is**

{

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

"Statement": [

{

"Sid": "",

"Effect": "Allow",

"Principal": {

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

"AWS": "arn:aws:iam::423623872287:user/cloud-watch-user-07"

},

"Action": "sts:AssumeRole"

}

]

}

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>

**Configuration of wazuh and aws integration.**

1./var/ossec/etc/internal-options.conf

Change “wazuh-modules.debug=2”

We need to replace 0 to 2

Systemctl restart wazuh-manager

1.cat /var/ossec/logs/0ssec.log | grep aws

2.cd /var/ossec/logs

3.ls -lrt

4.cat ossec.log

It gives the cloud watch log events

5.vim /var/ossec/etc/ossec.conf

Change the log format json to plain

6. Systemctl restart wazuh-manager

7.cat /var/ossec/logs/ossec.conf |grep aws

8. cat /var/ossec/logs/ossec.conf |grep cloudwatch

9.>/var/ossec/logs/ossec.log

10. Systemctl restart wazuh-manager

11.>/var/ossec/logs/ossec.log

12.cat ossec.log | grep aws-s3

The above command will display the logs along with one following command

/wodle/aws/aws-s3 –service cloudwatch logs –aws-profile default --regions us-east-1 –aws -log-groups /my/app/logs –debug 2

13./var ossec/wodle/aws/aws-s3 --service

It will display the log events

14.Cat /var/ossec/logs/archives/archives.json | grep cloudwatch

15. /var ossec/wodle/aws/aws-s3 –service

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

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

18. Tail -f -n 500 cat /var/ossec/logs/archives/archives.json | grep “ip-172-133-142-99”|grep “aws”

It will display the logs copy the line and write and run the following command

19. Tail -f -n 500 cat /var/ossec/logs/archives/archives.json | grep “ip-172-133-142-99”|grep wazuh-manager.service

tail -f /var/ossec/logs/archives/archives.log

**if nothing will display here from above two commands, we need to do the following steps**

Check Other Logs for Errors

Since archives.log is empty, check if logs are being recorded elsewhere:

Wazuh Alerts Log

tail -f /var/ossec/logs/alerts/alerts.json

tail -f /var/ossec/logs/ossec.log ------------🡪 Wazuh Main Log

**Check if archiving logs is enabled in Wazuh’s config file:**

cat /var/ossec/etc/ossec.conf | grep logall

<logall>yes</logall>

nano /var/ossec/etc/ossec.conf

systemctl restart wazuh-manager

20 . Tail -f -n 1000 cat /var/ossec/logs/archives/archives.json | grep “ip-172-133-142-99”|grep wazuh-manager.service

**Write the decoders:**

21 vim /var/ossec/etc/decoders/local\_decor.xml(no need to edit here)

20th command will gives the the logs ,from that logs we need to create decoder.copy the content from there and enter it after the command is

“DEBUG:the message is ……. Consumed 33.184s cpu time

22./var/ossec/bin/wazuh-logtest

It gives the decoders information

2 vim /var/ossec/etc/decoders/local\_decoder.xml

“<decoder name="custom\_test">

<prematch>wazuh-manager.service: </prematch>

</decoder>

<decoder name="custom\_test-child">

<parent>custom\_test</parent>

<regex>Consumed (\.+)s CPU time</regex>

<order>cpuconsumed</order>

</decoder>”

Some code of decoder will present in this filr copy the format of that and enter it in the next line and some little bit changes depends on the logs getting from the above command, after that here we write the child decoder.

23./var/ossec/bin/wazuh-logtest

Again you can write the “DEBUG message from logs ” you can write the rules

24. vim /var/ossec/etc/rules/local\_rules.xml

</group>

<group name="amazon">

<rule id="100234" level="3">

<decoded\_as>custom\_test</decoded\_as>

<description>custom rule for CPU </description>

</rule>

</group>

If you want see the syntax of rules you can get them from google.

25 /var/ossec/bin/wazuh-logtest

Enter the one log in single line

26 systemctl restart wazuh-manager

27 . Tail -f -n 1000 cat /var/ossec/logs/archives/archives.json | grep “ip-172-133-142-99”|grep wazuh-manager.service

After that goto wazuh dash board aws module, if it won’t come you can change the rulegroups name

28.vim /var/ossec/etc/rules/local.rules.xml

Group name changed to amazon

30 systemctl restart wazuh-manager