

CLOUDWATCH AGENT INSTALLATIONS STEPS

STEPS

- 1.create the instances
- 2.install cloudwatch agent
- 3.configure cloud watch agent
- 4.create the iam role

INSTALL CWA IN SERVER

FOR UBUNTU GO TO THIS LINK:

<https://docs.bitnami.com/aws/faq/administration/install-use-cloudwatch/>

FOR CENTOS GO TOLINK

<https://marbot.io/blog/monitoring-ec2-disk-usage.html>

INSTALL CWA AGENT:

```
# sudo -i
```

```
# sudo apt-get update
```

```
# sudo wget https://s3.amazonaws.com/amazoncloudwatch-agent/debian/  
amd64/latest/amazon-cloudwatch-agent.deb
```

```
# sudo dpkg -i -E ./amazon-cloudwatch-agent.deb
```

```
# sudo apt-get update && sudo apt-get install collect
```

NEXT WE CONFIGURE THE CWA

```
# sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-  
config-wizard
```

when you entered the command the cloudwatch agent config screen will appear cofig as we need

THEN START THE CWA

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

THEN CHECK THE STATUS OF CWA

```
# sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl
```

-m ec2 -a status

```
~$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cl
udwatch-agent-ctl -m ec2 -a status
{
  "status": "running",
  "starttime": "2019-07-23T08:00:48+00:00",
  "version": "1.223987.0"
}
```

THEN CREATED THE I AM ROLE

go to i am console and created the role

Create role 1 2 3 4

Select type of trusted entity

AWS service
EC2, Lambda and others

Another AWS account
Belonging to you or 3rd party

Web identity
Cognito or any OpenID provider

SAML 2.0 federation
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

API Gateway	Comprehend	ElastiCache	Lambda	SMS
AWS Backup	Config	Elastic Beanstalk	Lex	SNS
AWS Support	Connect	Elastic Container Service	License Manager	SWF
Amplify	DMS	Elastic Transcoder	Machine Learning	SageMaker

and search and select the policy for the cloud watch agent

Create role

1 2 3 4

▼ Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy

Filter policies Showing 17 results

	Policy name ▼	Used as	Description
<input type="checkbox"/>	▶ AmazonAPIGatewayPushToCloudWatchLogs	None	Allows API Gateway to push logs to u...
<input type="checkbox"/>	▶ AmazonDMSCloudWatchLogsRole	None	Provides access to upload DMS repli...
<input type="checkbox"/>	▶ AWSAppSyncPushToCloudWatchLogs	None	Allows AppSync to push logs to user'...
<input type="checkbox"/>	▶ AWSOpsWorksCloudWatchLogs	None	Enables OpsWorks instances with the...
<input type="checkbox"/>	▶ CloudWatchActionsEC2Access	None	Provides read-only access to CloudW...
<input type="checkbox"/>	▶ CloudWatchAgentAdminPolicy	None	Full permissions required to use Ama...
<input checked="" type="checkbox"/>	▶ CloudWatchAgentServerPolicy	Permissions policy (1)	Permissions required to use Amazon...
<input type="checkbox"/>	▶ CloudwatchApplicationInsightsServiceLinked...	None	Cloudwatch Application Insights Serv...

▶ Set permissions boundary

then give the name to role as you wanted and create the role

ATTACH THE ROLE TO EC2 INSTANCES

Go to the ec2 console and selected the the instance which u are installed the cloud watch agent

then go the action button select the security and select the iam role you are created and reboot the instances