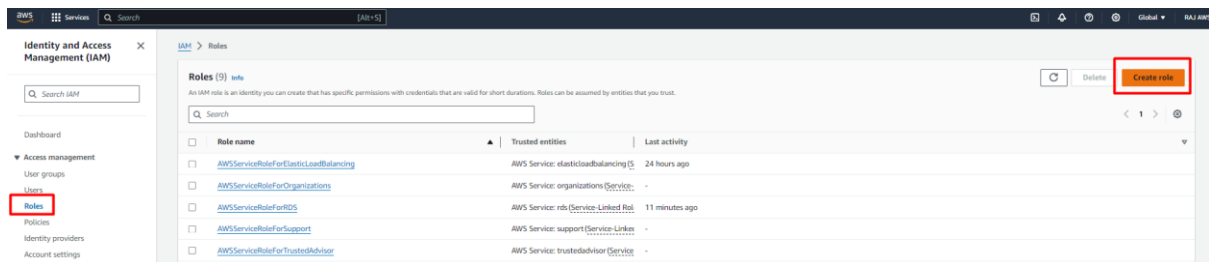


Install CloudWatch agent in Widows EC2 Instance - enable Memory and Storage metrics.

STEP 1: Create a IAM role

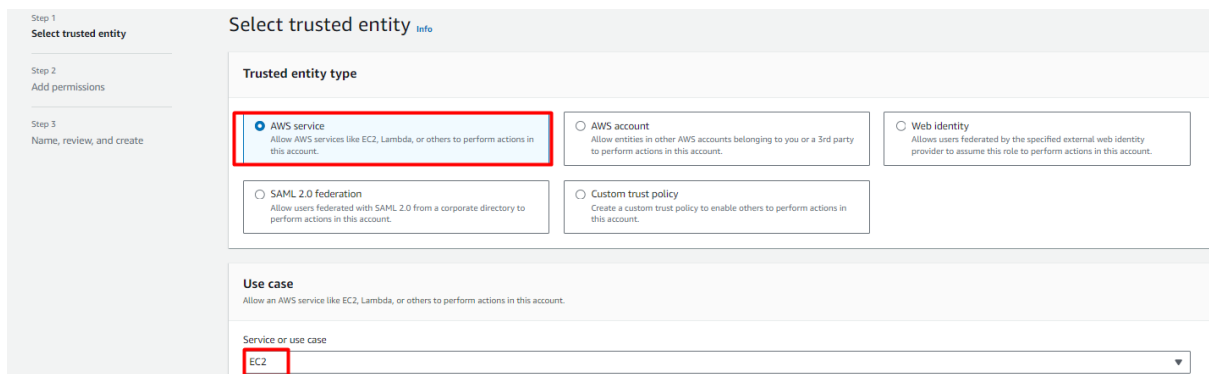
- Go to IAM
- On the Left Side of the screen search for Roles
- Then Click on Create Role



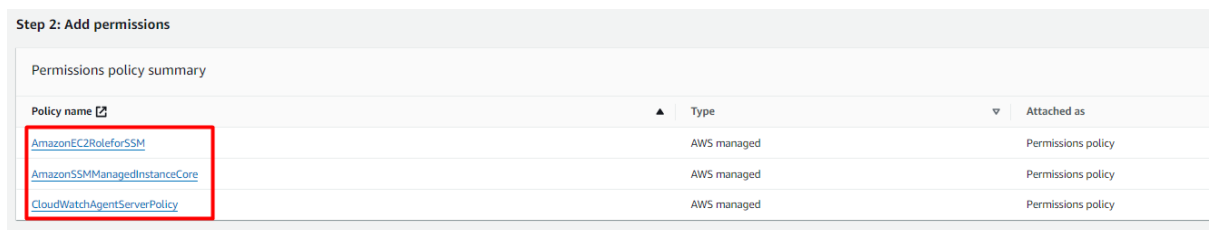
As we want to use this role inside the This Account

We will choose AWS service

Now we want this Role Applicable for EC2 Instance So we will Choose EC2



- Then Click on next
- Now Attach policy (permission) :
 - “ AmazonEC2RoleforSSM
 - AmazonSSMMManagedInstanceCore
 - CloudWatchAgentServerPolicy “



- Then Click on Next
- Enter Name of the Role and Create this Role

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

ROLE-FOR-CLOUDWATCH

Maximum 64 characters. Use alphanumeric and '+=, @-_' characters.

- Hence, we have Created a IAM Role.

STEP 2: Now create a Windows Server

- Choose AMI as Windows Server
- In security Group Choose RDP at Anywhere
- Create a Key Pair (It is used for the password to Decrypt)
- Then Scroll Down to Advance Details
- There Select IAM instance Profile
- There Choose your Create Role

Instances (2) Info									
<input type="text" value="Find instance by attribute or tag"/>				All states ▾		Refresh Connect Instance state ▾ Actions ▾ Launch instances ▾			
<input type="checkbox"/>	Name ↗	Instance ID	Instance state ▾	Instance type ▾	Status check	Alarm status	Availability Zone ▾	Public IPv4 DNS	Public IPv4 ...
<input type="checkbox"/>	LINUX METRIX	i-0e000e3615c212318	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1a	ec2-52-66-207-255.ap-...	52.66.207.255
<input type="checkbox"/>	WINDOWS SERVER	i-059b963025e38c1f8	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1a	ec2-3-110-131-116.ap-...	3.110.131.116

Select an instance

- Hence and create the Windows Sever

STEP 3: Connect the RDP

- Select the windows Server and Click on Connect
- Go to RDP Client and Use Username ,IP address and Password to login inside the RDP
- Firstly Decrypt the password by using Key Pair (.pem file)
- And Login in inside the Windows Server



- Hence we are inside the Windows Server

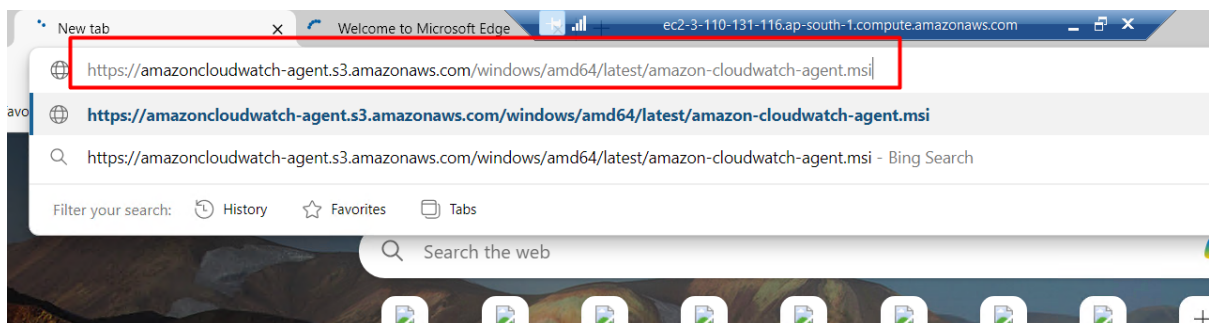
STEP 4: Now install CloudWatch Agent

- Open browser in RDP
- And Search for this link

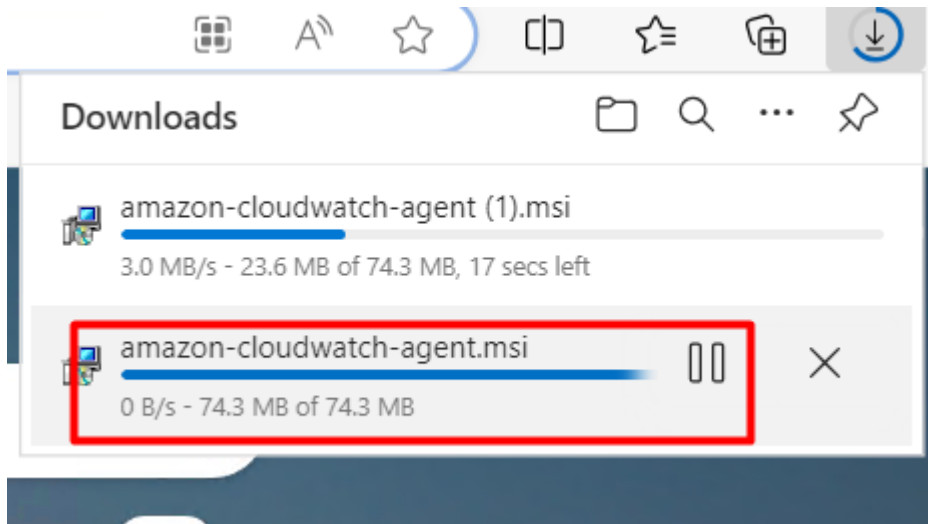
“

<https://amazoncloudwatch-agent.s3.amazonaws.com/windows/amd64/latest/amazon-cloudwatch-agent.msi>

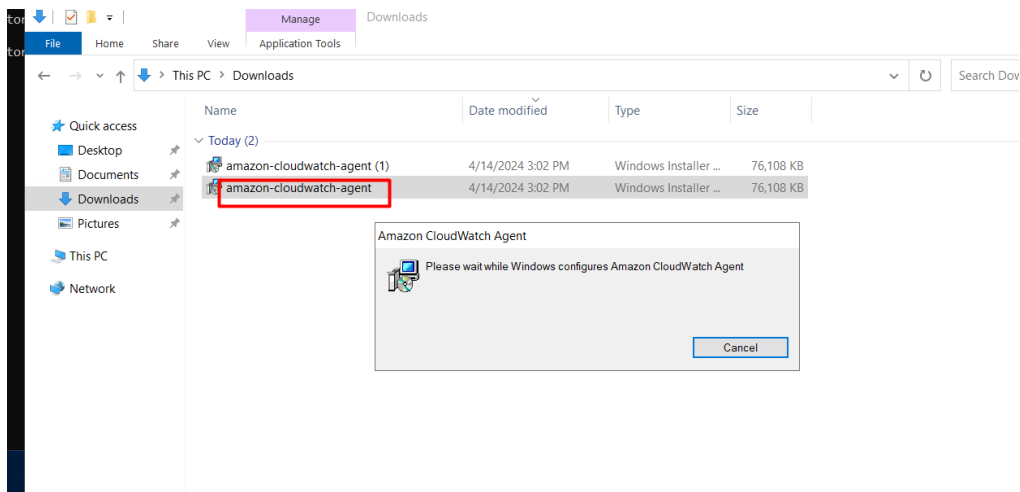
”



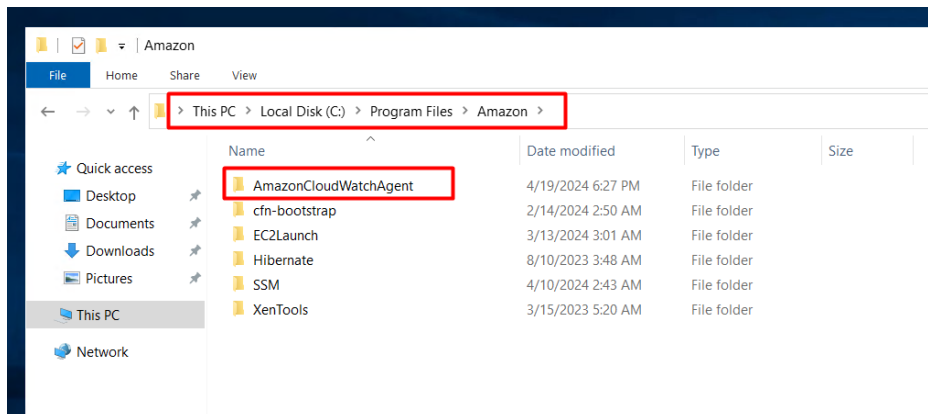
- Hence, we can see download has been started in the Brower ,



- Now go to Download and Open the link,
- Now go to download of Window server
- And double click on the Cloudwatch agent
- Wait for the Installion

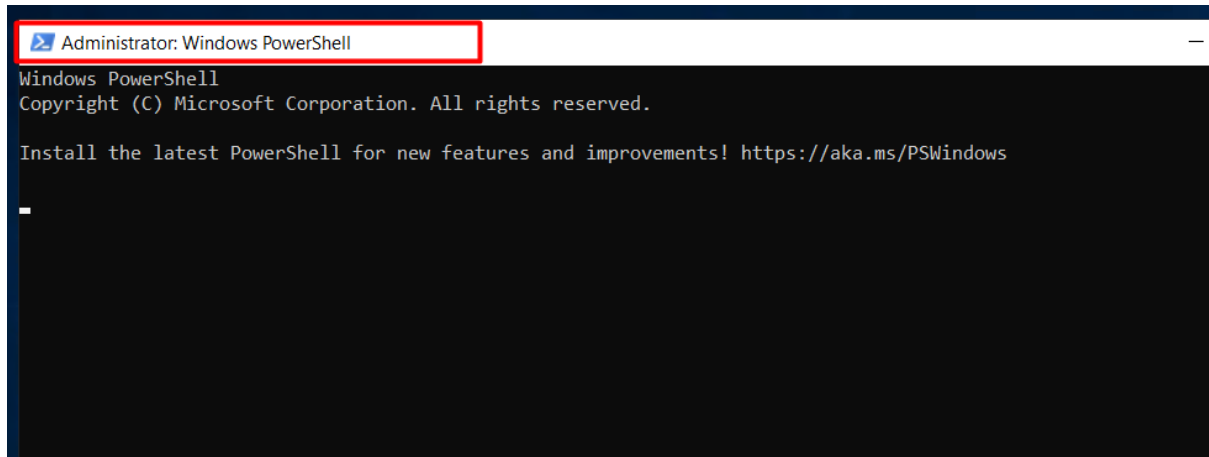


- Hence we can see the CloudWatch agent has been install in the windows server :
- Path : C > Program Files > Amazon > AmazonCloudWatchAgent



STEP 5: Run CloudWatch Agent wizard

- **Open PowerShell**



- Use the given command to configure metric in agent

Command Use :

cd 'C:/Program Files/Amazon/AmazonCloudwatchAgent' //we will configurw
wizard file in this location

.\amazon-cloudwatch-agent-config-wizard.exe //this command will
execute the wizard file

```
=====
= Welcome to the Amazon CloudWatch Agent Configuration Manager =
=
= CloudWatch Agent allows you to collect metrics and logs from =
= your host and send them to CloudWatch. Additional CloudWatch =
= charges may apply. =
=====
On which OS are you planning to use the agent?
1. linux
2. windows
3. darwin
default choice: [2]:
2
Trying to fetch the default region based on ec2 metadata...
1! imds retry client will retry 1 timesAre you using EC2 or On-Premises hosts?
1. EC2
2. On-Premises
default choice: [1]:

Do you want to turn on StatsD daemon?
1. yes
2. no
default choice: [1]:

Which port do you want StatsD daemon to listen to?
default choice: [8125]:

What is the collect interval for StatsD daemon?
1. 10s
2. 30s
3. 60s
default choice: [1]:

What is the aggregation interval for metrics collected by StatsD daemon?
1. Do not aggregate
2. 10s
3. 30s
4. 60s
default choice: [4]:

Do you have any existing CloudWatch Log Agent configuration file to import for migration?
1. yes
2. no
default choice: [2]:

Do you want to monitor any host metrics? e.g. CPU, memory, etc.
1. yes
2. no
default choice: [1]:
```

```
Do you want to monitor cpu metrics per core?
1. yes
2. no
default choice: [1]:

Do you want to add ec2 dimensions (ImageId, InstanceId, InstanceType, AutoScalingGroupName) into all of yo
1. yes
2. no
default choice: [1]:

Do you want to aggregate ec2 dimensions (InstanceId)?
1. yes
2. no
default choice: [1]:

Would you like to collect your metrics at high resolution (sub-minute resolution)? This enables sub-minute
1. 1s
2. 10s
3. 30s
4. 60s
default choice: [4]:
```

```

Which default metrics config do you want?
1. Basic
2. Standard
3. Advanced
4. None
default choice: [1]:
1
Current config as follows:
{
  "metrics": {
    "aggregation_dimensions": [
      [
        "InstanceId"
      ]
    ],
    "append_dimensions": {
      "AutoScalingGroupName": "${aws:AutoScalingGroupName}",
      "ImageId": "${aws:ImageId}",
      "InstanceId": "${aws:InstanceId}",
      "InstanceType": "${aws:InstanceType}"
    },
    "metrics_collected": {
      "LogicalDisk": {
        "measurement": [
          "% Free Space"
        ],
        "metrics_collection_interval": 60,
        "resources": [
          "*"
        ]
      },
      "Memory": {
        "measurement": [
          "% Committed Bytes In Use"
        ],
        "metrics_collection_interval": 60
      },
      "statsd": {
        "metrics_aggregation_interval": 60,
        "metrics_collection_interval": 10,
        "service_address": ":8125"
      }
    }
  }
}
Are you satisfied with the above config? Note: it can be manually customized after the wizard completes to add additional items.
1. yes
2. no
default choice: [1]:
1

```

```

Are you satisfied with the above config? Note: it can be manually customized af
1. yes
2. no
default choice: [1]:
1
Do you want to monitor any customized log files?
1. yes
2. no
default choice: [1]:
1
Log file path:
/var/logs/security
Log group name:
default choice: [security]
Log group class:
1. STANDARD
2. INFREQUENT_ACCESS
default choice: [1]:
1
Log stream name:
default choice: [{instance_id}]
Log Group Retention in days
1. -1
2. 1
3. 3
4. 5
5. 7
6. 14
7. 30
8. 60
9. 90
10. 120
11. 150
12. 180
13. 365
14. 400
15. 545
16. 731
17. 1096
18. 1827
19. 2192
20. 2557
21. 2922
22. 3288
23. 3653
default choice: [1]:
1

```

- During the Log group name : /var/logs/systemwindows

```

Do you want to specify any additional log files to monitor?
1. yes
2. no ←
default choice: [1]:
2
Do you want to monitor any Windows event log?
1. yes ←
2. no
default choice: [1]:

Windows event log name:
default choice: [System] ←

Do you want to monitor VERBOSE level events for Windows event log System ?
1. yes ←
2. no
default choice: [1]:

Do you want to monitor INFORMATION level events for Windows event log System ?
1. yes ←
2. no
default choice: [1]:

Do you want to monitor WARNING level events for Windows event log System ?
1. yes ←
2. no
default choice: [1]:

Do you want to monitor ERROR level events for Windows event log System ?
1. yes ←
2. no
default choice: [1]:

Do you want to monitor CRITICAL level events for Windows event log System ?
1. yes ←
2. no
default choice: [1]:

Log group name:
default choice: [System]
/var/logs/systemwindows ←
Log stream name:
default choice: [{instance_id}] ←

Which log group class would you like to have for this log group?
1. STANDARD ←
2. INFREQUENT_ACCESS
default choice: [1]:

```

- Then enter no and exit

```

Please check the above content of the config.
The config file is also located at config.json.
Edit it manually if needed.
Do you want to store the config in the SSM parameter store?
1. yes
2. no ←
default choice: [1]:
2
Please press Enter to exit...
Program exits now.
PS C:\Program Files\Amazon\AmazonCloudWatchAgent>

```

- Hence we have Done the configuration As we can also see the config file is been created

> This PC > Local Disk (C:) > Program Files > Amazon > AmazonCloudWatchAgent

Name	Date modified	Type	Size
amazon-cloudwatch-agent	3/21/2024 9:03 PM	Application	112,664 KB
amazon-cloudwatch-agent-config-wizard	3/21/2024 9:03 PM	Application	13,843 KB
amazon-cloudwatch-agent-ctl	3/21/2024 9:03 PM	Windows PowerSh...	17 KB
amazon-cloudwatch-agent-schema.json	3/21/2024 9:03 PM	JSON File	41 KB
config.json	4/19/2024 6:43 PM	JSON File	2 KB
config-downloader	3/21/2024 9:03 PM	Application	37,527 KB
config-translator	3/21/2024 9:03 PM	Application	107,910 KB
CWAGENT_VERSION	3/21/2024 9:03 PM	File	1 KB
LICENSE	3/21/2024 9:03 PM	File	2 KB
NOTICE	3/21/2024 9:03 PM	File	1 KB
permission	3/21/2024 9:03 PM	Windows PowerSh...	1 KB
RELEASE_NOTES	3/21/2024 9:03 PM	File	27 KB
start-amazon-cloudwatch-agent	3/21/2024 9:03 PM	Application	1,927 KB
THIRD-PARTY-LICENSES	3/21/2024 9:03 PM	File	167 KB

STEP 6 : Now start the agent

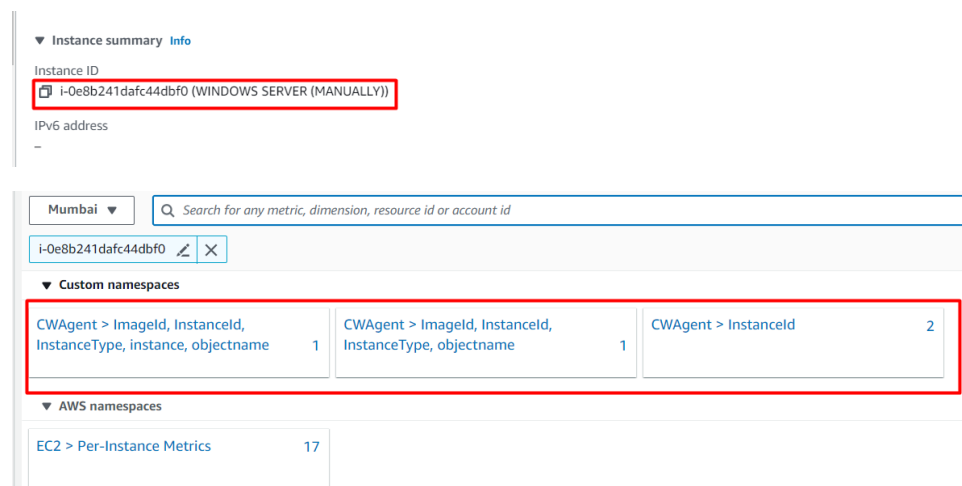
Command Use :

```
# & "C:\Program Files\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1" -a fetch-config -m ec2 -s -c file:config.json
```

```
PS C:\Program Files\Amazon\AmazonCloudWatchAgent> & "C:\Program Files\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1" -a fetch-config -m ec2 -s -c file:config.json
***** processing amazon-cloudwatch-agent *****
I! Trying to detect region from ec2
D! [EC2] Found active network interface
I! imds retry client will retry 1 timesSuccessfully fetched the config and saved in C:\ProgramData\Amazon\AmazonCloudWatchAgent\Configs\file_config.json.tmp
Start configuration validation...
2024/04/19 18:46:35 Reading json config file path: C:\ProgramData\Amazon\AmazonCloudWatchAgent\Configs\file_config.json.tmp ...
2024/04/19 18:46:35 I! Valid json input schema.
I! Trying to detect region from ec2
D! [EC2] Found active network interface
I! imds retry client will retry 1 times2024/04/19 18:46:36 D! ec2tagger processor required because append_dimensions is set
2024/04/19 18:46:36 D! pipeline hostDeltaMetrics has no receivers
2024/04/19 18:46:36 Configuration validation first phase succeeded
Configuration validation second phase succeeded
Configuration validation succeeded
amazonCloudWatchAgent has been stopped
amazonCloudWatchAgent has been started
PS C:\Program Files\Amazon\AmazonCloudWatchAgent>
```

STEP 7: OUTPUT

- Open CloudWatch
- There go to All Metric
- And in the search Bar enter the Instance ID
- Hence we have Metrics of CPU,Disk,Memory.



- Hence we can see the Log in Log group which we have created early in the configuration process

Log groups (5)							
By default, we only load up to 10000 log groups.							
Filter log groups or try prefix search				Exact match			
<input type="checkbox"/>	Log group	Log class	Anomaly d...	Data prot...	Sensitive ...	Retention	Metric filt...
<input type="checkbox"/>	/aws/lambda/StartEC2Instance	Standard	Configure	-	-	Never expire	-
<input type="checkbox"/>	/aws/lambda/StopEC2Instances	Standard	Configure	-	-	Never expire	-
<input type="checkbox"/>	/var/logs/systemwindows	Standard	Configure	-	-	1 day	-
<input type="checkbox"/>	Security	Standard	Configure	-	-	Never expire	-
<input type="checkbox"/>	demo	Standard	Configure	-	-	Never expire	-

Command Use :

<https://amazoncloudwatch-agent.s3.amazonaws.com/windows/amd64/latest/amazon-cloudwatch-agent.msi>

download the Link

```
# cd 'C:\Program Files\Amazon\AmazonCloudWatchAgent'
```

```
# .\amazon-cloudwatch-agent-config-wizard.exe
```

```
# & "C:\Program Files\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1" -a fetch-config -m ec2 -s -c file:config.json
```

Reference Link :

<https://youtu.be/vAnIhIwE5hY?si=rvCFVecsvqjdw8FO>

<https://youtu.be/U7X3ehGZYwQ?si=VYPZDmznatw8dMds>