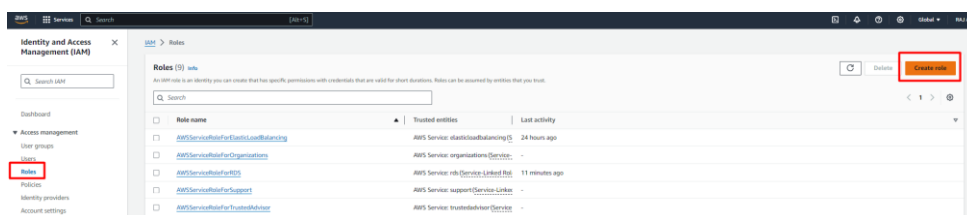


Install CloudWatch agent in Widows EC2 Instance - enable Memory and Storage metrics.

(Using System Manager)

STEP 1: Create a IAM role

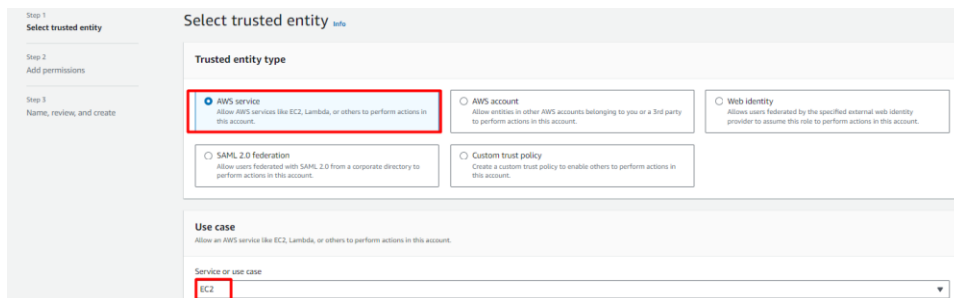
- Go to IAM
- On the Left Side of the screen search for Roles
- Then Click on Create Role



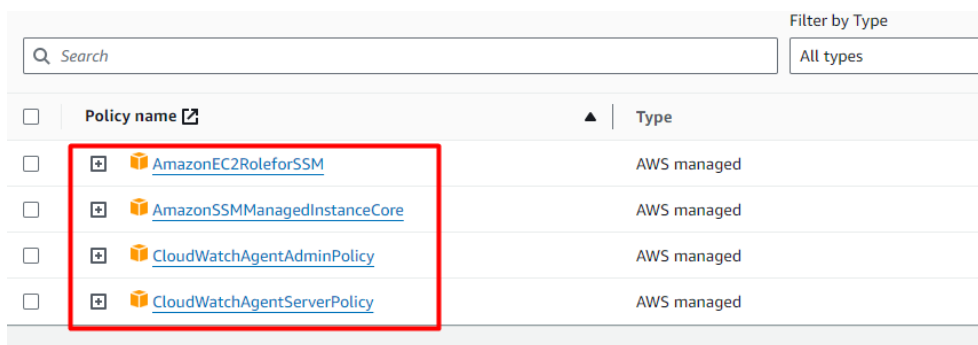
As we want to use this role inside the This Account

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
 - AmazonSSMManagedInstanceCore
 - CloudWatchAgentServerPolicy
 - CloudWatchAgentAdminPolicy “



- 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

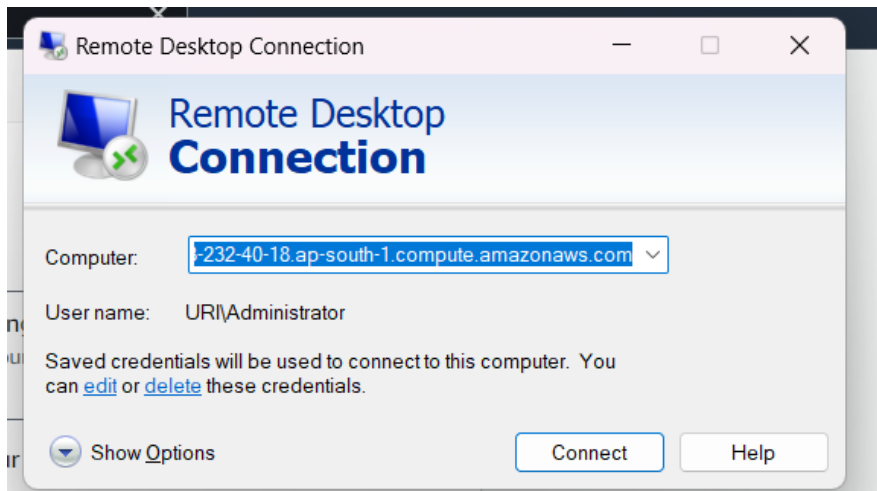
- Choose AMI as Windows Server
- In security Group Choose RDP at Anywhere
- Create a Key Pair (It is used for the password to Decrypt)
- Then Scroll Down to Advance Details
- There Select IAM instance Profile
- There Choose your Create Role

Instances (1) Info					
<input type="text" value="Find Instance by attribute or tag"/> All states ▼					
Name = WINDOWS SERVER (SYSTEM MANAGER) X Clear filters					
<input type="checkbox"/>	Name ✎	Instance ID	Instance state	Instance type	S
<input type="checkbox"/>	WINDOWS SERVER (SYSTEM MANAGER)	i-036a8b1d078d0190f	Running 🔍 🔍	t2.micro	🔍

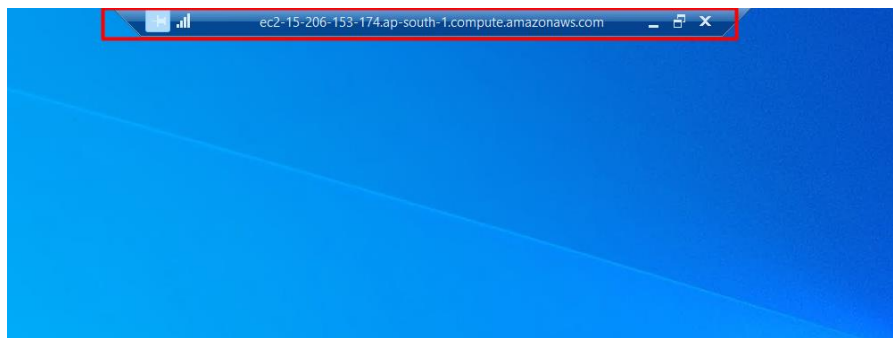
- Hence we have create the Windows Sever

STEP 3: Connect to RDP

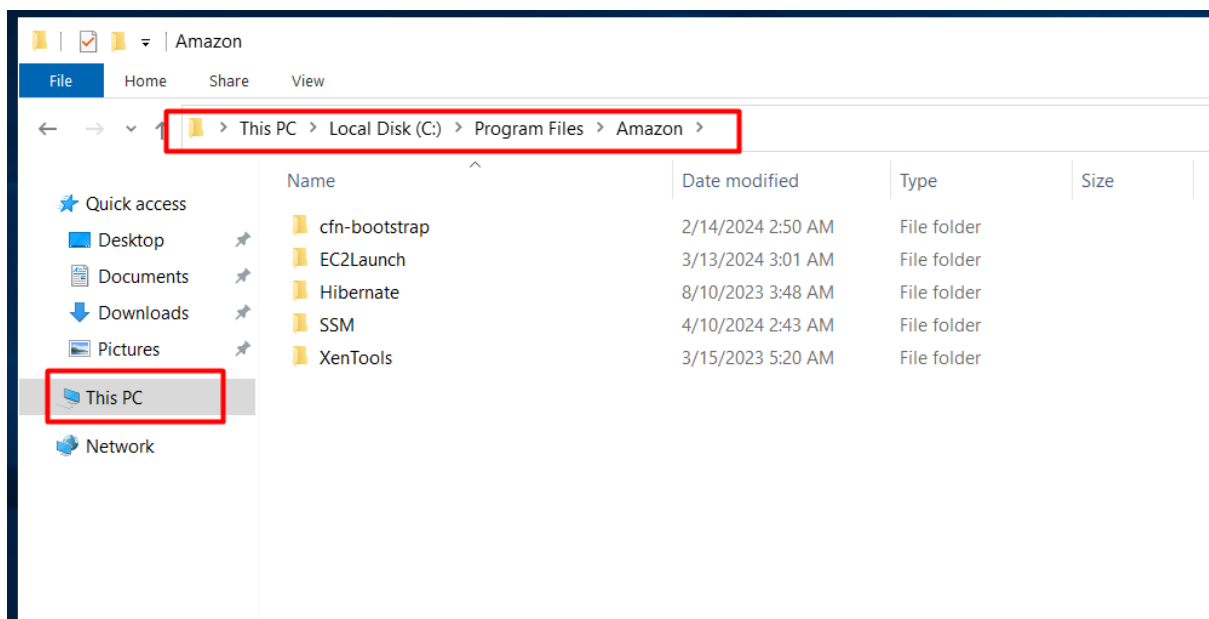
Connect Inside RDP using credentials



- Hence, we are inside the Window server,



- Now go to My PC
- **Path : C:>Program Files>Amazon**



- So here we can see the CloudWatch agent is not install,

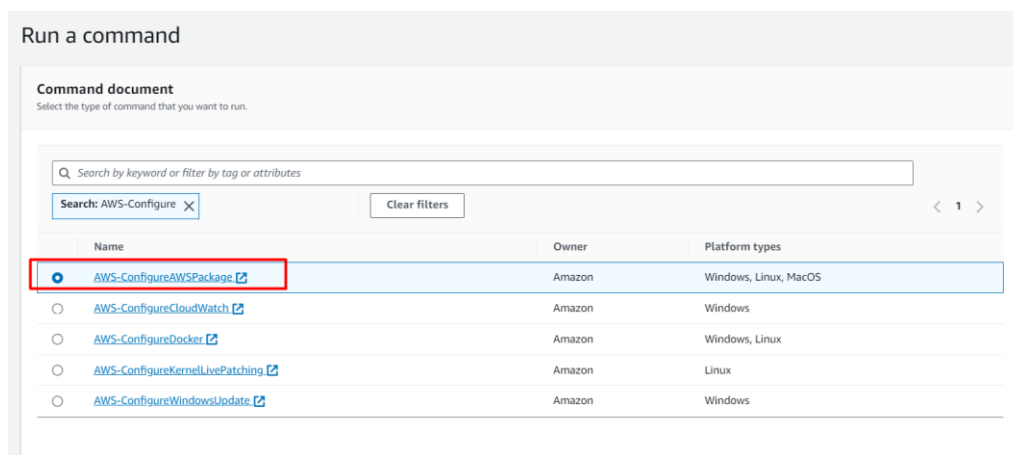
STEP 4: Install CloudWatch Agent using SSM (Systems Manager)

- Go to System Manager
- There search for Run command
- Click on it



- Search for this in search bar:

“AWS-ConfigureAWSPackage”



- Select the Package and Scroll down
- Then Choose Document version : Latest version
- And In Name enter : AmazonCloudWatchAgent
- Version : Latest

Document version
Choose the document version you want to run.

Latest version at runtime

Command parameters

Action
(Required) Specify whether to install or uninstall the package.

Install

Installation Type
(Optional) Specify the type of installation. Uninstall and reinstall: The application is taken offline until the reinstallation process completes. In-place update: The application is available while new or updated files are added to the installation.

Uninstall and reinstall

Installation Type
(Optional) Specify the type of installation. Uninstall and reinstall: The application is taken offline until the reinstallation process completes. In-place update: The application is available while new or updated files are added to the installation.

Uninstall and reinstall

Name
(Required) The package to install/uninstall.

AmazonCloudWatchAgent

Version
(Optional) The version of the package to install or uninstall. If you don't specify a version, the system installs the latest published version by default. The system will only attempt to uninstall the version that is currently installed. If no version is specified, the system returns an error.

latest

Additional Arguments
(Optional) The additional parameters to provide to your install, uninstall, or update scripts.

- Scroll Down to target selection,
- Choose Instance Manually
- Select the instance which we need to configure,

Target selection

Target selection
Choose a method for selecting targets.

☐ Specify instance tags
Specify one or more tag key-value pairs to select instances that share those tags.

☒ **Choose instances manually**
Manually select the instances you want to register as targets.

☐ Choose a resource group
Choose a resource group that includes the resources you want to target.

i-036a8b1d078d0190f X

Instances

Q < 1 >

	Name	Instance ID	Instance state	Availability zone	Ping status	Last ping time
<input type="checkbox"/>	WINDOWS SERVER (MANUALLY)	i-0e8b241dafc44dbf0	running	ap-south-1a	Online	4/20/2024 at 01:40:00 GMT+0530 (India Standard Tim
<input checked="" type="checkbox"/>	WINDOWS SERVER (SYSTEM MANAGER)	i-036a8b1d078d0190f	running	ap-south-1a	Online	4/20/2024 at 01:41:31 GMT+0530 (India Standard Tim

- And **RUN** the package.

Cancel **Run**

- Wait for few minutes to gets it done

AWS Systems Manager > Run Command > Command ID: 1169257c-4bb0-4e01-ba4d-d108e8bd6cbd

Command ID: 1169257c-4bb0-4e01-ba4d-d108e8bd6cbd Refresh Cancel command Rerun Copy to new

Command status

Overall status	Detailed status	# targets	# completed	# error	# delivery timed out
Success	Success	1	1	0	0

Targets and outputs View output

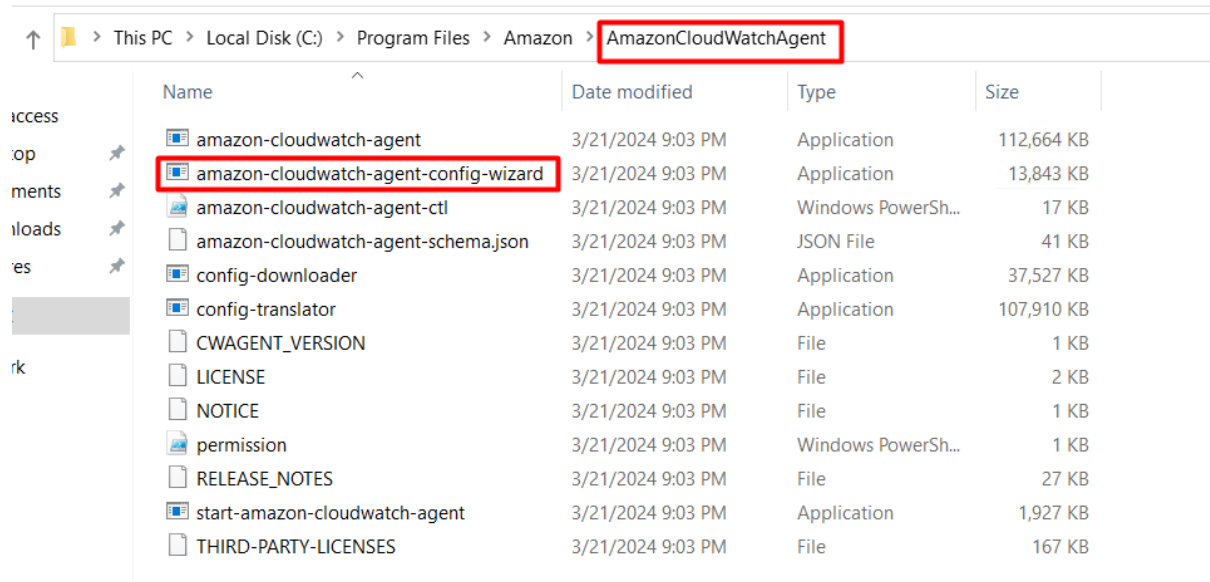
Q Search command invocations < 1 >

	Instance ID	Instance name	Status	Detailed Status	Start time	Finish time
<input type="radio"/>	i-036a8b1d078d0190f	EC2AMAZ-SKTF4RM.WORKGROUP	Success	Success	Fri, 19 Apr 2024 20:17:37 GMT	Fri, 19 Apr 2024 20:18:07 GMT

- Hence,we can see the package has been created successfully.

STEP 6: Run Cloudwatch Agent Wizard

- Open RDP
- Hence we can see the CloudWatch agent is install now we need to Configure the wizard File



↑ > This PC > Local Disk (C:) > Program Files > Amazon > AmazonCloudWatchAgent					
	Name	Date modified	Type	Size	
ccess	amazon-cloudwatch-agent	3/21/2024 9:03 PM	Application	112,664 KB	
op	amazon-cloudwatch-agent-config-wizard	3/21/2024 9:03 PM	Application	13,843 KB	
ments	amazon-cloudwatch-agent-ctl	3/21/2024 9:03 PM	Windows PowerSh...	17 KB	
loads	amazon-cloudwatch-agent-schema.json	3/21/2024 9:03 PM	JSON File	41 KB	
es	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	
rk	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	

- Open PowerShell

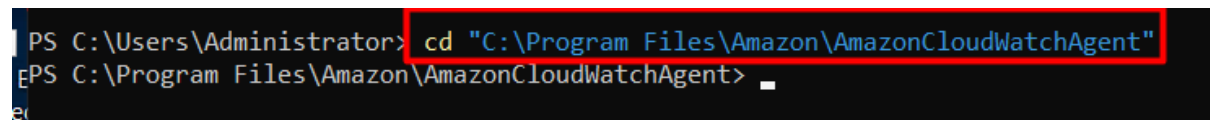
Command used :

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

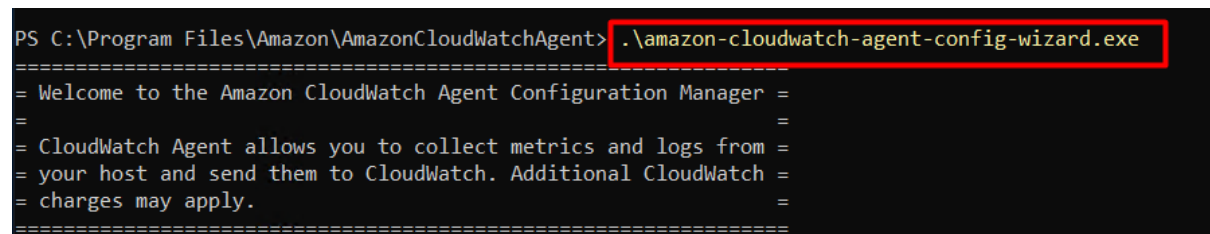
//change the directory to the location where the CloudWatch agent is installed

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

// this command will use to execute the wizard file



```
PS C:\Users\Administrator> cd "C:\Program Files\Amazon\AmazonCloudWatchAgent"
PS C:\Program Files\Amazon\AmazonCloudWatchAgent>
```



```
PS C:\Program Files\Amazon\AmazonCloudWatchAgent> .\amazon-cloudwatch-agent-config-wizard.exe
=====
= 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.
=====
```

```
=====
= 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...
! imds retry client will retry 1 timesAre you using EC2 or On-Premises hosts?
1. EC2
2. On-Premises
default choice: [1]:
1
Do you want to turn on StatsD daemon?
1. yes
2. no
default choice: [1]:
1
Which port do you want StatsD daemon to listen to?
default choice: [8125]
8125
What is the collect interval for StatsD daemon?
1. 10s
2. 30s
3. 60s
default choice: [1]:
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]:
4
Do you have any existing CloudWatch Log Agent configuration file to import for migration?
1. yes
2. no
default choice: [2]:
2
```

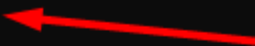
```
Do you want to monitor any host metrics? e.g. CPU, memory, etc.
1. yes
2. no
default choice: [1]:
1
Do you want to monitor cpu metrics per core?
1. yes
2. no
default choice: [1]:
1
Do you want to add ec2 dimensions (ImageId, InstanceId, InstanceType, AutoScalingGroupName) in
1. yes
2. no
default choice: [1]:
1
Do you want to aggregate ec2 dimensions (InstanceId)?
1. yes
2. no
default choice: [1]:
1
Would you like to collect your metrics at high resolution (sub-minute resolution)? This enable
1. 1s
2. 10s
3. 30s
4. 60s
default choice: [4]:
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
1. yes
2. no
default choice: [1]:
1
```

```
Are you satisfied with the above config? Note: it can be manually customized
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:
/demo/logs/windowslogs
Log group name:
default choice: [windowslogs]

Log group class:
1. STANDARD
2. INFREQUENT_ACCESS
default choice: [1]:
1
Log stream name:
default choice: [{instance_id}]
```


Do you want to monitor any customized log files?

1. yes 

2. no

default choice: [1]:


Log file path:

/var/logs/windowslogs

Log group name:

default choice: [windowslogs]


Log group class:

1. STANDARD 

2. INFREQUENT_ACCESS

default choice: [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]:

2

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/windows-logs
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]:

In which format do you want to store windows event to CloudWatch Logs?
1. XML: XML format in Windows Event Viewer
2. Plain Text: Legacy CloudWatch Windows Agent (SSM Plugin) Format
default choice: [1]:

```

- Enter the Log group name where you want to send the log of this server

```

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]:

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

Do you want the CloudWatch agent to also retrieve X-ray traces?
1. yes
2. no
default choice: [1]:

```

- Choose by default
- Wait at config file is also Located at “config.json” :
- The config file will be get stored in SSM parameters and if we want to run any other instance with the same configuration, we can use this easy and perform it easily

```

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]:

What parameter store name do you want to use to store your config? (Use 'AmazonCloudWatch-' prefix if you use our
default choice: [AmazonCloudWatch-windows]

Trying to fetch the default region based on ec2 metadata...
I! imds retry client will retry 1 timesWhich region do you want to store the config in the parameter store?
default choice: [ap-south-1]

Which AWS credential should be used to send json config to parameter store?
1. ASIATCKAS3TMUUCFGOKI(From SDK)
2. Other
default choice: [1]:

Please make sure the creds you used have the right permissions configured for SSM access.
Which AWS credential should be used to send json config to parameter store?
1. ASIATCKAS3TMUUCFGOKI(From SDK)
2. Other
default choice: [1]:

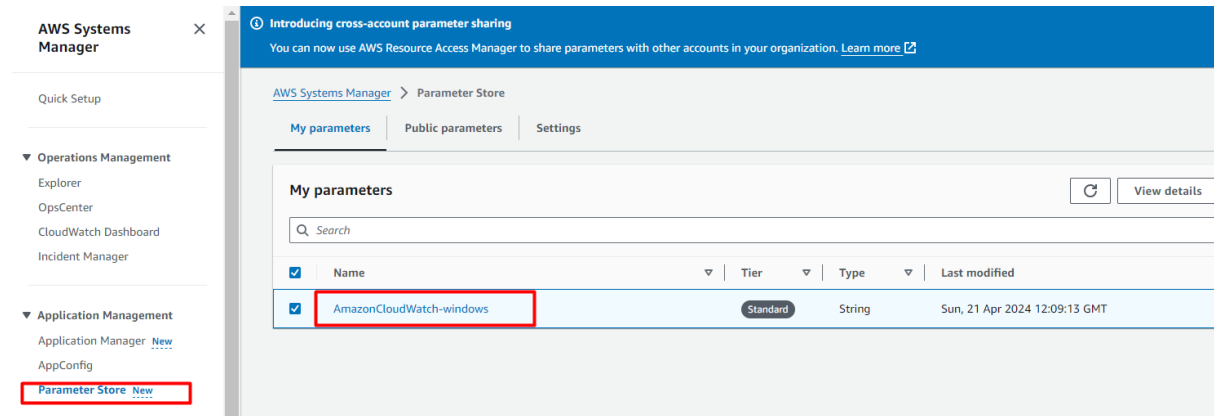
Please make sure the creds you used have the right permissions configured for SSM access.
Error in putting config to parameter store AmazonCloudWatch-windows: AccessDeniedException: User: arn:aws:sts::211
PutParameter on resource: arn:aws:ssm:ap-south-1:211125722329:parameter/AmazonCloudWatch-windows because no identi
status_code: 400, request id: 623d925d-8adf-49a2-a77b-67f3c87c25c2
Please press Enter to exit...
Program exits now.

```

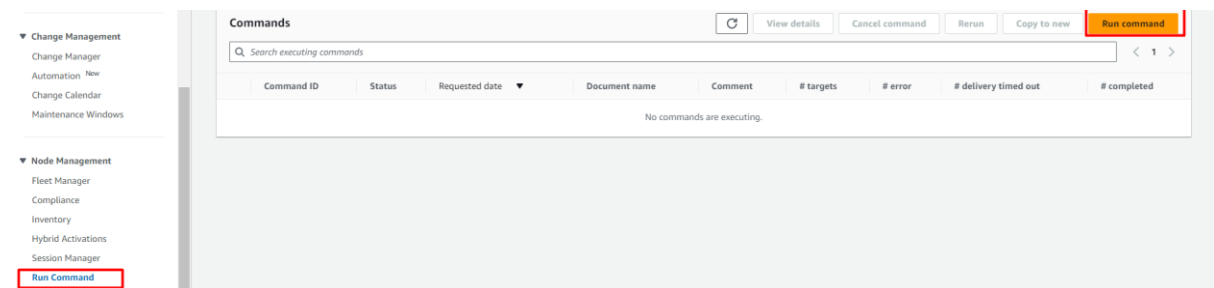
- Hence, we have configure everything
- Now exit from the Windows server.

STEP 8: Now run the CloudWatch Agent

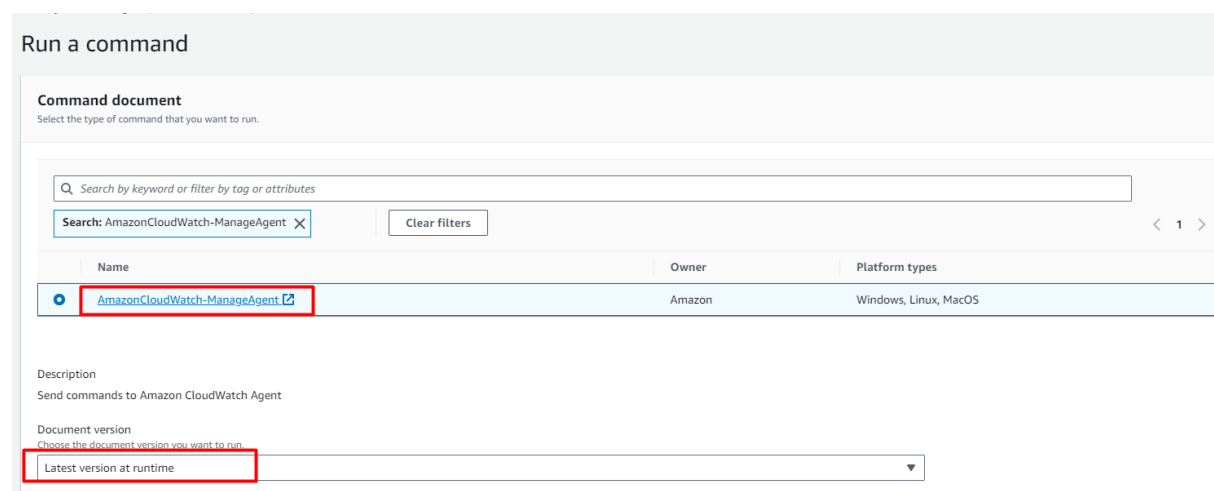
- Open Session Manager
- Go to parameter Store
- Hence we can see the Parameter for Windows Server has been Created for Cloudwatch Agent



- Then Click on Run Command



- Search for “AmazonCloudWatch-ManagedAgent”
- And Choose it
- And in Document version Choose Latest Version



- And scroll down to Optional configuration source :
- Enter the Parameter Store name : “AmazonCloudWatch-windows”

Command parameters

Action
The action CloudWatch Agent should take.

configure

Mode
Controls platform-specific default behavior such as whether to include EC2 Metadata in metrics.

ec2

Optional Configuration Source
Only for 'configure' related actions. Use 'ssm' to apply a ssm parameter as config. Use 'default' to apply default config for amazon-cloudwatch-agent. Use 'all' with 'configure (remove)' to clean all agent.

ssm

Optional Configuration Location
Only for 'configure' related actions. Only needed when Optional Configuration Source is set to 'ssm'. The value should be a ssm parameter name.

AmazonCloudWatch-windows

Optional Restart
Only for 'configure' related actions. If 'yes', restarts the agent to use the new configuration. Otherwise the new config will only apply on the next agent restart.

yes

- Choose your instance where you want to run this command
- And Run the Command

Target selection

Target selection
Choose a method for selecting targets.

☐ Specify instance tags
Specify one or more tag key-value pairs to select instances that share those tags.

☒ Choose instances manually
Manually select the instances you want to register as targets.

☐ Choose a resource group
Choose a resource group that includes the resources you want to target.

i-0271f209cc440f863

Instances

1

	Name	Instance ID	Instance state	Availability zone	Ping status	Last ping time
<input checked="" type="checkbox"/>	WINDOWS SERVER (SYSTEM MANAGER)	i-0271f209cc440f863	running	ap-south-1a	Online	4/21/2024 at 17:43:0

- Wait for 5-10 min till the process is going on
- Once it success

Command ID: 54303d13-bd83-499f-90e7-79f3b21760ab

Cancel command

Command status

Overall status	Detailed status	# targets	# completed	# error
Success	Success	1	1	0

Targets and outputs

Search command invocations

	Instance ID	Instance name	Status	Detailed Status	Start time	
<input type="radio"/>	i-0271f209cc440f863	EC2AMAZ-65CV4FD.WORKGROUP	Success	Success	Sun, 21 Apr 2024 12:19:33 GMT	S

STEP 9: Open CloudWatch to check Metrics of this Instance

- Go to CloudWatch
- Then in CloudWatch go to All metric
- Copy the Instance ID and paste the ID in the search bar of the Metric,
- Hence we can see the Disk , memory Metric is Visible .

The screenshot shows the AWS CloudWatch Metrics console. At the top, there's a search bar with the instance ID 'i-0271f209cc440f863' entered. Below the search bar, the 'Custom namespaces' section is highlighted with a red box. It contains two entries: 'CWAgent > InstanceId' with 2 metrics and 'CWAgent > ImageId, InstanceId, InstanceType, objectname' with 1 metric. Below this, the 'AWS namespaces' section shows 'EC2 > Per-Instance Metrics' with 17 metrics.

STEP 10: Check the Logs are coming in the Log group

- Go to Log group in CloudWatch
- Hence, we can see the Log group has been created for Windows logs

The screenshot shows the AWS CloudWatch Log groups console. It displays a list of log groups. The log group '/var/logs/systemwindows' is highlighted with a red box. Below it, the log group 'System-Windows' is also highlighted with a red box. The table shows the following log groups:

Log group	Log class	Anomaly d...	Data pro
/aws/lambda/StartEC2Instance	Standard	Configure	-
/aws/lambda/StopEC2Instances	Standard	Configure	-
/var/logs/systemwindows	Standard	Configure	-
Security	Standard	Configure	-
System-Windows	Standard	Configure	-
demo	Standard	Configure	-

Reference Link:

YOUTUBE : https://youtu.be/vAnIhIwE5hY?si=T494Z0Aa6y_whW9x