

Create a Role (Log-Agent-Role) with EC2 and integrated permissions with

Permissions policies (4)
You can attach up to 10 managed policies.

<input type="checkbox"/>	Policy name ↗	Type	Description
<input type="checkbox"/>	AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 via the AWS Management Console.
<input type="checkbox"/>	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via the AWS Management Console.
<input type="checkbox"/>	CloudWatchFullAccess	AWS managed	Provides full access to CloudWatch.
<input type="checkbox"/>	CloudWatchLogsFullAccess	AWS managed	Provides full access to CloudWatch Logs

Make Instance in Ohio Region

Instances (1) [Info](#) [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 DI
<input type="checkbox"/>	Ohio-instance	i-0e5422ec7807e1b59	Running	t2.micro	Initializing	No alarms +	us-east-2b	ec2-18-216-21

Attach Log-Agent-Role to the ec2 instance Modify Role

[EC2](#) > [Instances](#) > [i-0e5422ec7807e1b59](#) > [Modify IAM role](#)

Modify IAM role [Info](#)
Attach an IAM role to your instance.

Instance ID
 i-0e5422ec7807e1b59 (Ohio-instance)

IAM role
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

[Refresh](#) [Create new IAM role](#)

[Cancel](#) [Save](#)

Now get instance SSH into Moba

Steps for installation CloudWatch Agent (For Running Instance)

```
# sudo yum update -y
```

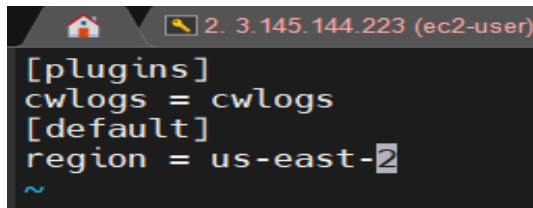
```
# sudo yum install -y awslogs
```

```
# sudo vim /etc/awslogs/awslogs.conf
```

```
[/var/log/messages]
datetime_format = %b %d %H:%M:%S
file = /var/log/messages
buffer_duration = 5000
log_stream_name = i-0e5422ec7807e1b59
initial_position = start_of_file
log_group_name = /var/log/messages
~
```

here bottom of this configuration file **Mention Instance ID** in log_stream_name

```
# sudo vim /etc/awslogs/awscli.conf
```



```
[plugins]
cwlogs = cwlogs
[default]
region = us-east-2
~
```

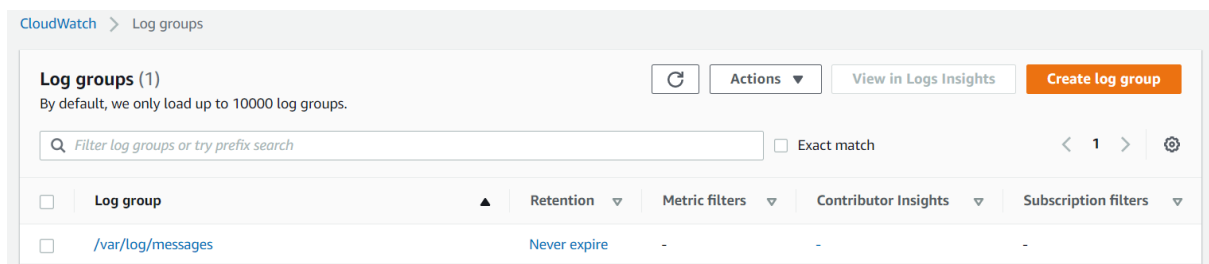
Here mention the AWS instance Region as we have Ohio region **us-east-2**

```
# sudo systemctl start awslogsd
```

```
# sudo systemctl enable awslogsd.service
```

```
# sudo systemctl status awslogsd.service
```

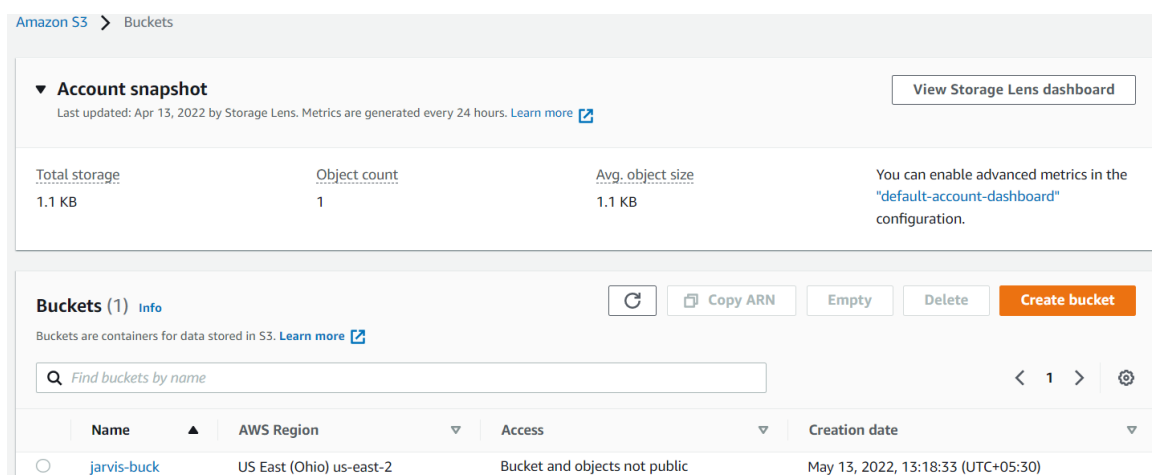
Now, Open AWS CloudWatch service and check in **Log Groups** where group are created or not



refer amazon Docs link:-

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/QuickStartEC2Instance.html>

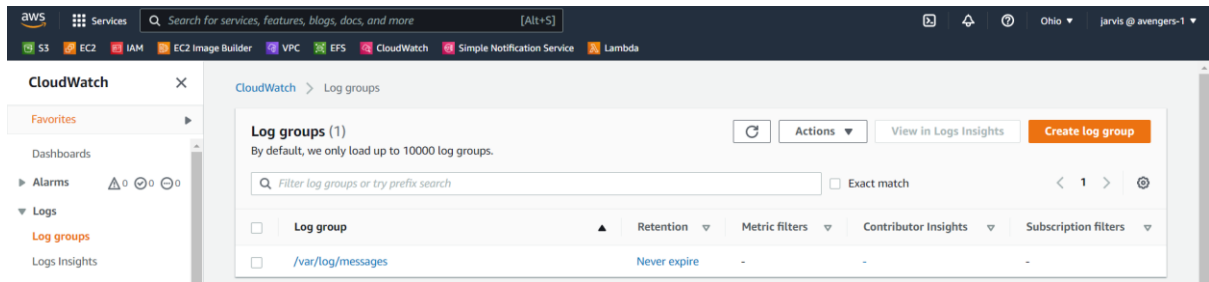
Now create S3 Bucket in **same Ohio Region** & Change the bucket policy from permissions



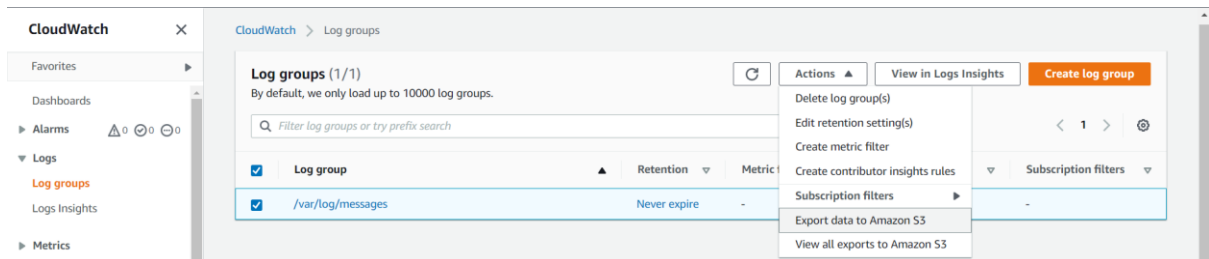
Change the bucket policy

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "logs.us-east-2.amazonaws.com"  
      },  
      "Action": "s3:GetBucketAcl",  
      "Resource": "arn:aws:s3:::jarvis-buck"  
    },  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "logs.us-east-2.amazonaws.com"  
      },  
      "Action": "s3:PutObject",  
      "Resource": "arn:aws:s3:::jarvis-buck/*",  
      "Condition": {  
        "StringEquals": {  
          "s3:x-amz-acl": "bucket-owner-full-control"  
        }  
      }  
    }  
  ]  
}
```

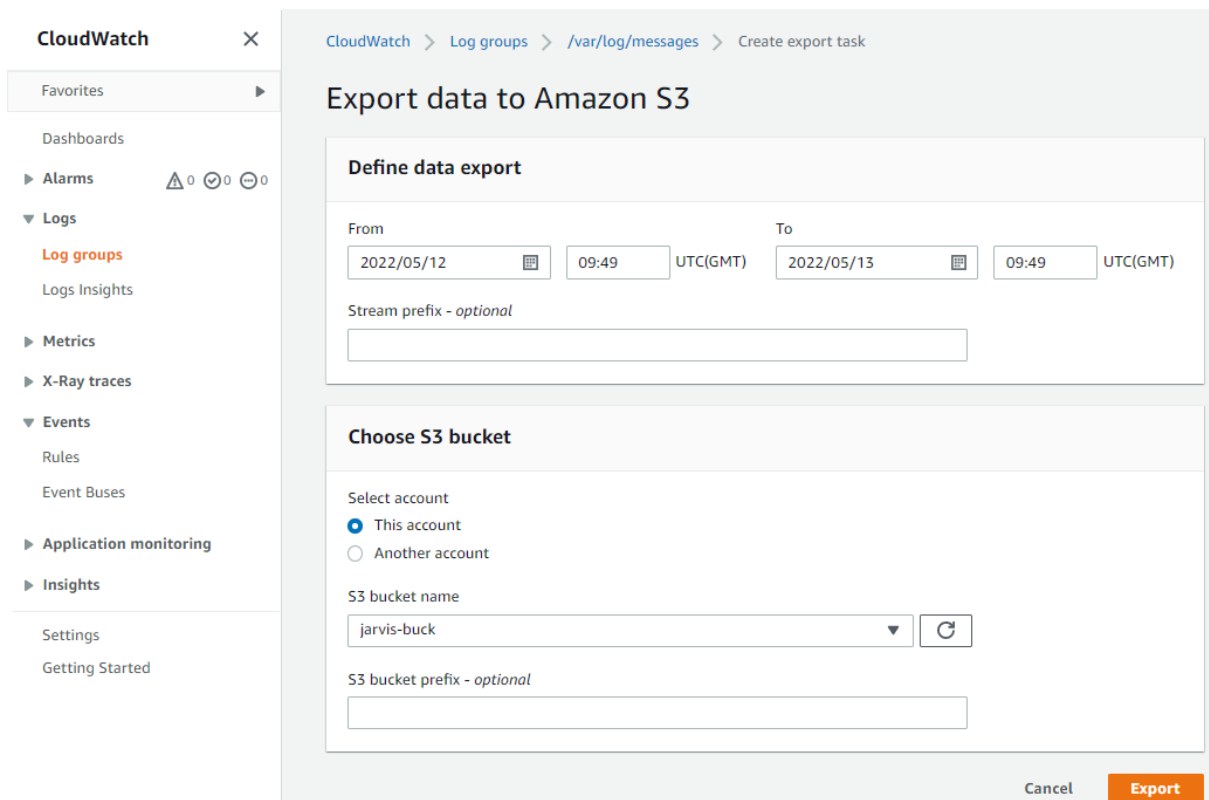
Now go to **AWS CloudWatch service** check logs group where it created or not?



Export Data to Amazon S3



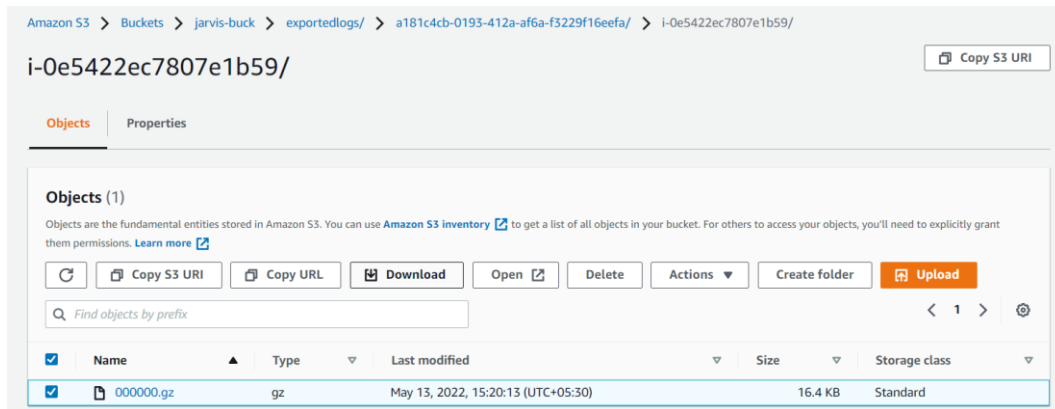
Select bucket in same region where our instance is also running



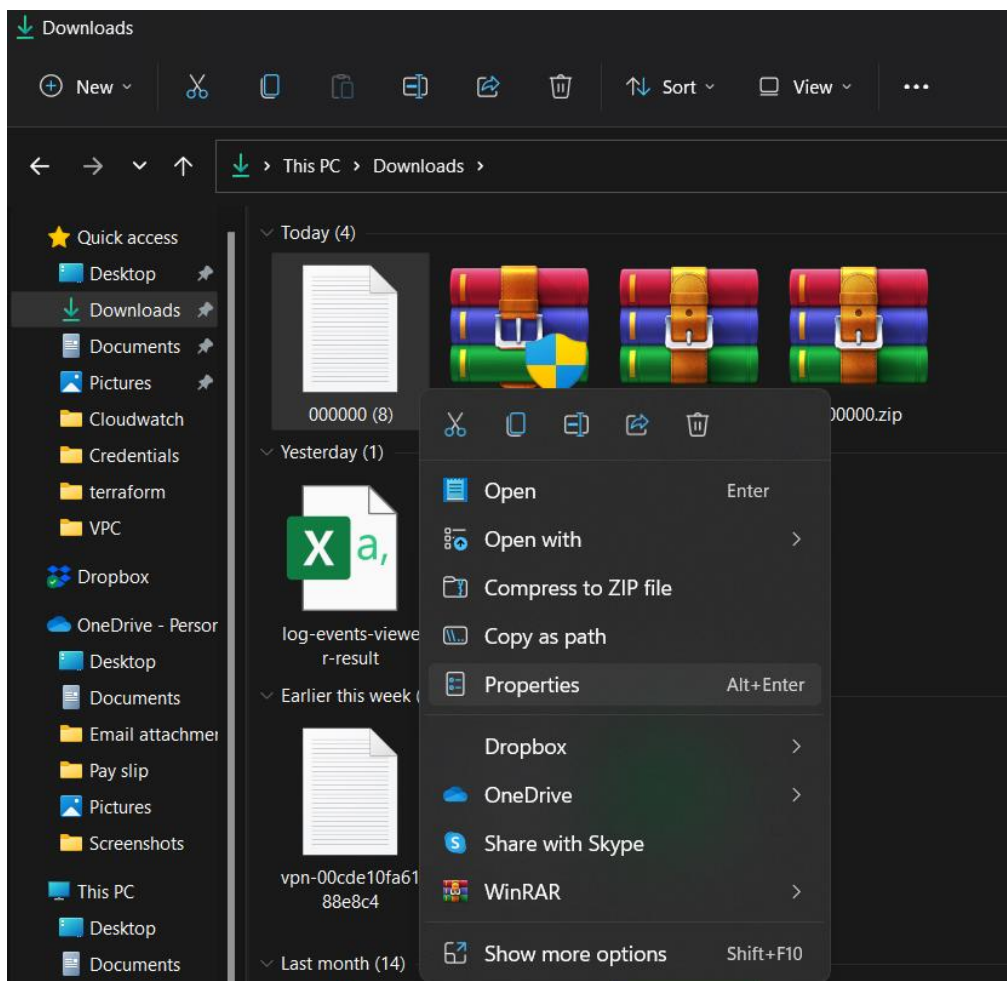
Open S3 bucket open exportedlogs folders till our instance-id's .gz file not found

exportedlogs/ → a181c4cb-0193-412a-af6a-f3229f16eefa/ → i-0e5422ec7807e1b59/

Download the our .gz **instance log files**



Extract the downloaded file through WinRAR



Extract and open it via Notepad

```
000000 (8) - Notepad
File Edit View

2022-05-13T07:59:10.000Z May 13 07:59:10 ip-172-31-16-173 dhclient[2861]: XMT: Solicit on eth0, interval 8960ms.
2022-05-13T08:07:20.000Z May 13 08:07:20 ip-172-31-16-173 dhclient[2861]: XMT: Solicit on eth0, interval 123190ms.
2022-05-13T09:03:32.000Z May 13 09:03:32 ip-172-31-16-173 dhclient[2865]: XMT: Solicit on eth0, interval 66520ms.
2022-05-13T09:14:34.000Z May 13 09:14:34 ip-172-31-16-173 dhclient[2865]: XMT: Solicit on eth0, interval 130590ms.
2022-05-13T09:35:04.000Z May 13 09:35:04 ip-172-31-16-173 dhclient[2865]: XMT: Solicit on eth0, interval 113360ms.
2022-05-13T07:59:12.000Z May 13 07:59:12 ip-172-31-16-173 systemd: Started Dynamically Generate Message Of The Day.
2022-05-13T07:59:12.000Z May 13 07:59:12 ip-172-31-16-173 systemd: Reached target Multi-User System.
2022-05-13T07:59:12.000Z May 13 07:59:12 ip-172-31-16-173 systemd: Reached target Graphical Interface.
2022-05-13T07:59:12.000Z May 13 07:59:12 ip-172-31-16-173 systemd: Reached target Cloud-init target.
2022-05-13T07:59:12.000Z May 13 07:59:12 ip-172-31-16-173 systemd: Starting Update UTMP about System Runlevel Changes...
2022-05-13T07:59:12.000Z May 13 07:59:12 ip-172-31-16-173 systemd: Started Update UTMP about System Runlevel Changes.
2022-05-13T07:59:12.000Z May 13 07:59:12 ip-172-31-16-173 systemd: Startup finished in 1.723s (kernel) + 1.119s (initrd) + 13.970s (userspace) = 16.813s.
2022-05-13T07:59:16.000Z May 13 07:59:16 ip-172-31-16-173 systemd: Created slice User Slice of ec2-user.
2022-05-13T07:59:16.000Z May 13 07:59:16 ip-172-31-16-173 systemd-logind: New session 1 of user ec2-user.
2022-05-13T07:59:16.000Z May 13 07:59:16 ip-172-31-16-173 systemd: Started Session 1 of user ec2-user.
2022-05-13T07:59:19.000Z May 13 07:59:19 ip-172-31-16-173 dhclient[2861]: XMT: Solicit on eth0, interval 18510ms.
2022-05-13T08:00:14.000Z May 13 08:00:14 ip-172-31-16-173 dhclient[2861]: XMT: Solicit on eth0, interval 75030ms.
2022-05-13T08:09:24.000Z May 13 08:09:24 ip-172-31-16-173 dhclient[2861]: XMT: Solicit on eth0, interval 117580ms.
2022-05-13T09:02:35.000Z May 13 09:02:35 ip-172-31-16-173 systemd: Started Dynamically Generate Message Of The Day.
2022-05-13T09:02:35.000Z May 13 09:02:35 ip-172-31-16-173 systemd: Reached target Multi-User System.
2022-05-13T09:02:35.000Z May 13 09:02:35 ip-172-31-16-173 systemd: Reached target Cloud-init target.
2022-05-13T09:02:35.000Z May 13 09:02:35 ip-172-31-16-173 systemd: Reached target Graphical Interface.
2022-05-13T09:02:35.000Z May 13 09:02:35 ip-172-31-16-173 systemd: Starting Update UTMP about System Runlevel Changes...
2022-05-13T09:02:35.000Z May 13 09:02:35 ip-172-31-16-173 systemd: Started Update UTMP about System Runlevel Changes.
2022-05-13T09:02:35.000Z May 13 09:02:35 ip-172-31-16-173 systemd: Startup finished in 1.873s (kernel) + 1.165s (initrd) + 13.160s (userspace) = 16.198s.
2022-05-13T09:20:44.000Z May 13 09:20:44 ip-172-31-16-173 dhclient[2865]: XMT: Solicit on eth0, interval 125410ms.
2022-05-13T07:59:38.000Z May 13 07:59:38 ip-172-31-16-173 dhclient[2861]: XMT: Solicit on eth0, interval 36160ms.
2022-05-13T08:05:16.000Z May 13 08:05:16 ip-172-31-16-173 dhclient[2861]: XMT: Solicit on eth0, interval 123820ms.
2022-05-13T09:12:35.000Z May 13 09:12:35 ip-172-31-16-173 dhclient[2865]: XMT: Solicit on eth0, interval 118140ms.
2022-05-13T09:22:50.000Z May 13 09:22:50 ip-172-31-16-173 dhclient[2865]: XMT: Solicit on eth0, interval 128830ms.
2022-05-13T09:40:01.000Z May 13 09:40:01 ip-172-31-16-173 systemd: Created slice User Slice of root.
2022-05-13T09:40:01.000Z May 13 09:40:01 ip-172-31-16-173 systemd: Started Session 5 of user root.
2022-05-13T09:40:01.000Z May 13 09:40:01 ip-172-31-16-173 systemd: Removed slice User Slice of root.
2022-05-13T09:02:58.000Z May 13 09:02:58 ip-172-31-16-173 dhclient[2865]: XMT: Solicit on eth0, interval 34100ms.
2022-05-13T09:24:59.000Z May 13 09:24:59 ip-172-31-16-173 dhclient[2865]: XMT: Solicit on eth0, interval 110860ms.
2022-05-13T09:31:33.000Z May 13 09:31:33 ip-172-31-16-173 dhclient[2818]: DHCPREQUEST on eth0 to 172.31.16.1 port 67 (xid=0x6e8aba48)
2022-05-13T09:31:33.000Z May 13 09:31:33 ip-172-31-16-173 dhclient[2818]: DHCPACK from 172.31.16.1 (xid=0x6e8aba48)
2022-05-13T09:31:33.000Z May 13 09:31:33 ip-172-31-16-173 NET: dhclient: Locked /run/dhclient/resolv.lock
2022-05-13T09:31:33.000Z May 13 09:31:33 ip-172-31-16-173 dhclient[2818]: bound to 172.31.16.173 -- renewal in 1656 seconds
```

Amazon Docs link for export CloudWatch logs into S3:-

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/S3ExportTasksConsole.html>

We also can extract via cli

gunzip /<filename>tar.gz