.

Academic Year: 2025-26 | **Name of Student: Deep Varkute**
Semester: V | **Student ID:24204010**
Class / Branch/ Div: TEIT C | **Roll No.60**
Subject: ADL | **Date of Submission:15/10/25**

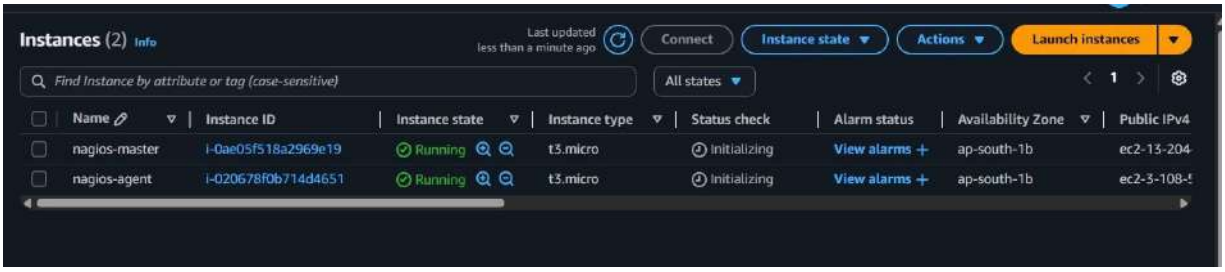
Assignment No 2

Q. 1 Make use of NRPE (Nagios Remote Plugin Executor) for continuous monitoring and reducing application vulnerabilities.

STEP 1: Launch the two EC2 instances

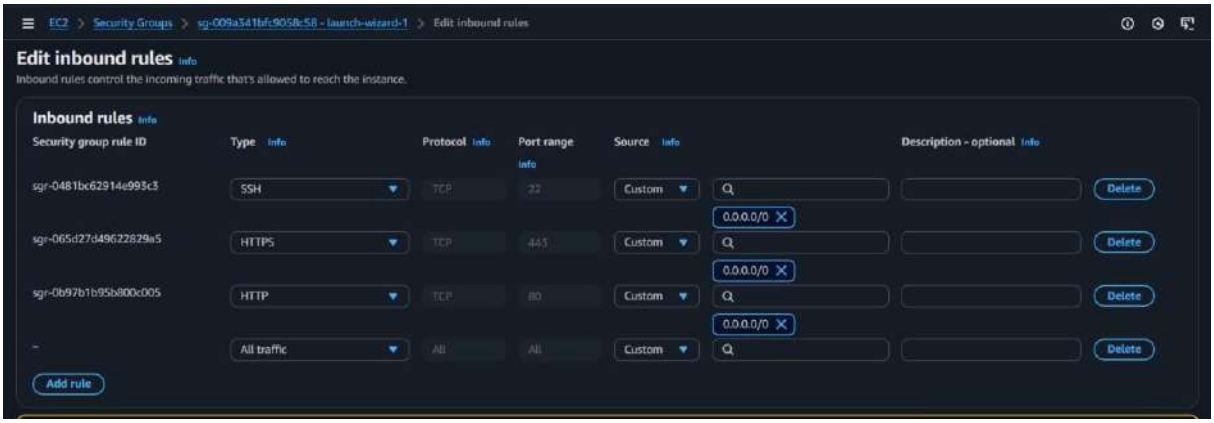
Instance 1 — Nagios Server Instance

2 — NRPE Client



Make sure both Instances are on Same Security group (same network)

Security group inbound rules:



Now connect to both instances

STEP 2: Update both instances Run on both instances : sudo apt update && sudo apt upgrade -y

STEP 3: Install Nagios Core (on MASTER only)

3.1 Install dependencies

```
sudo apt install -y autoconf gcc make wget unzip apache2 php libapache2-mod-php php-gd libgd-dev
sudo apt install -y openssl libssl-dev daemon wget apache2-utils
```

3.2 Create Nagios user and group

```
sudo useradd nagios
sudo usermod -a -G nagios www-data
```

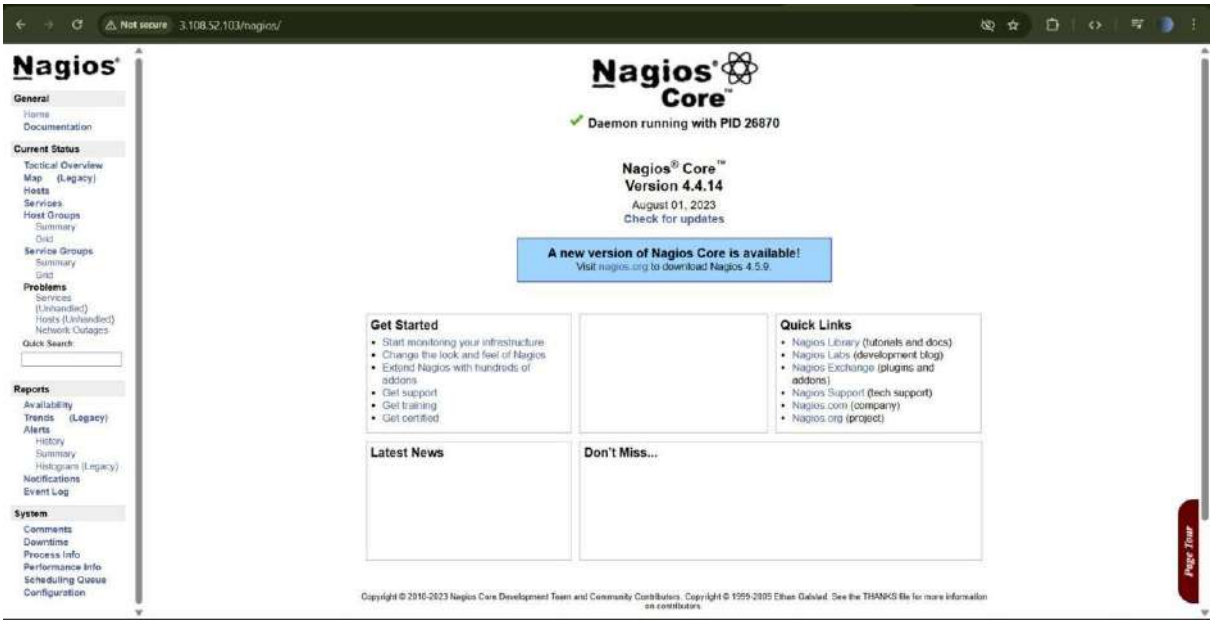
3.3 Download and install Nagios Core cd /tmp wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.14.tar.g z tar -xvzf nagios-4.4.14.tar.gz cd nagios-4.4.14 ./configure --with-httpd-conf=/etc/apache2/sites-enabled make all sudo make install sudo make install-init sudo make install-commandmode sudo make install-config sudo make install-webconf **3.4 Create web admin user** sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin # set password (e.g., admin123)

3.5 Enable Apache modules and start services

```
sudo a2enmod rewrite cgi sudo systemctl restart apache2 sudo systemctl enable apache2 sudo systemctl start nagios sudo systemctl enable nagios
```

✓ Now Nagios dashboard will be available at:
http://<MASTER_PUBLIC_IP>/nagios

Login with user: `nagiosadmin` and password you created.



STEP 4: Install NRPE on the AGENT 4.1 Install NRPE and Nagios plugins `sudo apt install -y nagios-nrpe-server nagios-plugins`

4.2 Configure NRPE

Edit the config file:

```
sudo nano /etc/nagios/nrpe.cfg
```

Find this line:

```
allowed_hosts=127.0.0.1
```

Replace it with your Nagios master's private IP, e.g.:

```
allowed_hosts=127.0.0.1,172.31.12.45
```

Then restart NRPE:

```
sudo systemctl restart nagios-nrpe-server sudo
systemctl enable nagios-nrpe-server
```

💻 STEP 5: Install NRPE plugin on MASTER 5.1 Install NRPE plugin

```
sudo apt install -y nagios-nrpe-plugin nagios-plugins
```

5.2 Test NRPE connectivity

```
/usr/lib/nagios/plugins/check_nrpe -H <AGENT_PRIVATE_IP>
```

You should see:

```
ubuntu@nagios-master:~$ /usr/lib/nagios/plugins/check_nrpe -H 172.31.11.198
NRPE v4.1.0
ubuntu@nagios-master:~$
```

STEP 6: Add Agent to Nagios Configuration On MASTER:

```
sudo                                    nano
/usr/local/nagios/etc/servers/agent.cfg
```

If `servers` directory doesn't exist, create it:

```
sudo mkdir /usr/local/nagios/etc/servers
```

Add:

```
define host {
    use                     linux-server
    host_name               nagios-agent
    alias                   nagios-agent
    address                 <AGENT_PRIVATE_IP>
    max_check_attempts      5
    check_period            24x7
    notification_interval   30
    notification_period     24x7
}

define service {

    use                     generic-service
    host_name               nagios-agent
    service_description     PING
    check_command           check_ping!100.0,20%!500.0,60%
}
define service {
    use                     generic-service
    host_name               nagios-agent
    service_description     Check NRPE
    check_command           check_nrpe!check_load
}
```

Now include this directory in main config:

```
sudo nano /usr/local/nagios/etc/nagios.cfg
```

Uncomment or add:

```
cfg_dir=/usr/local/nagios/etc/servers
```

Then restart Nagios:

```
sudo systemctl restart nagios
```

🌐 STEP 7: Access the Dashboard Go to:

```
http://<MASTER_PUBLIC_IP>/nagios
```

Login with `nagiosadmin`.

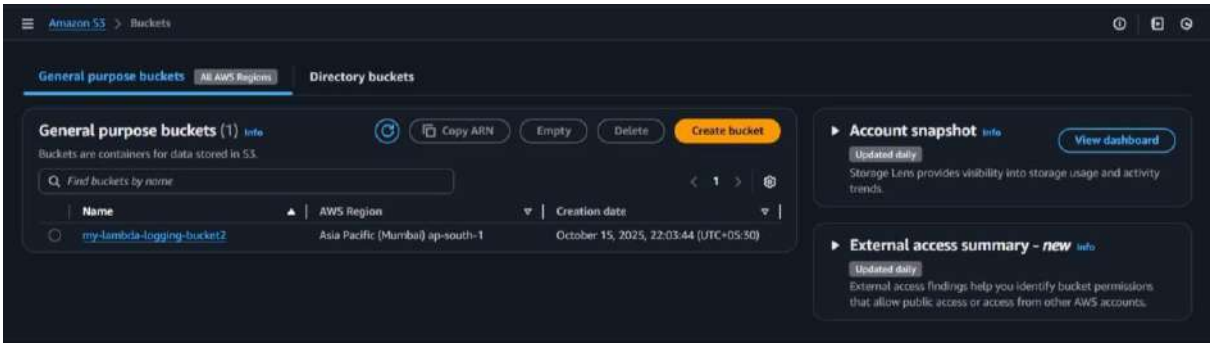
Go to:
Hosts → nagios-agent → Services

Q. 2 Create a Lambda function which will log the content to add an object to a specific bucket.

Step 1: Create an S3 bucket

Bucket name: `my-lambda-logging-bucket`

Uncheck "Block all public access"



Step 2: Create an IAM Role for Lambda

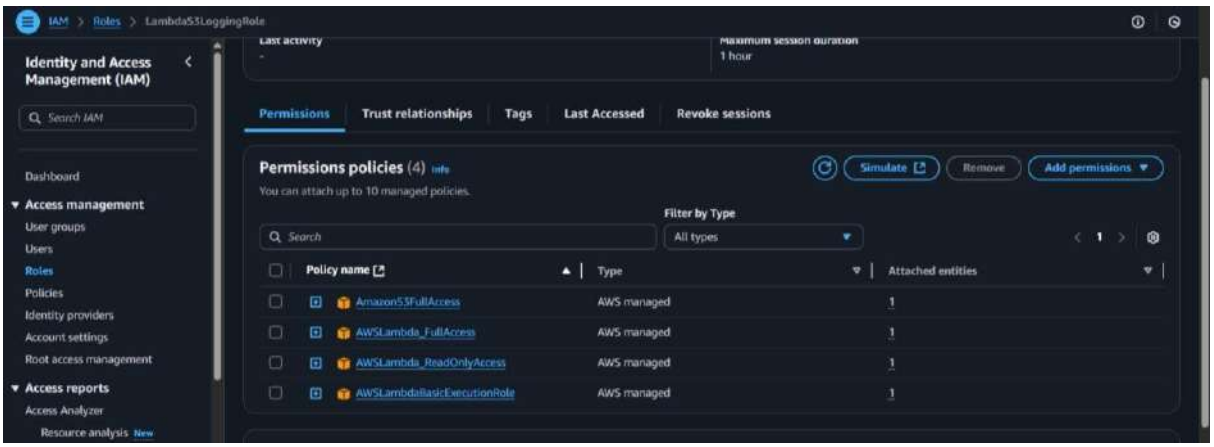
Go to Services → IAM → Roles → Create Role.

- Select type of trusted entity → Lambda. Click Next.
- Attach policies:

  AWSLambdaBasicExecutionRole

  AmazonS3FullAccess

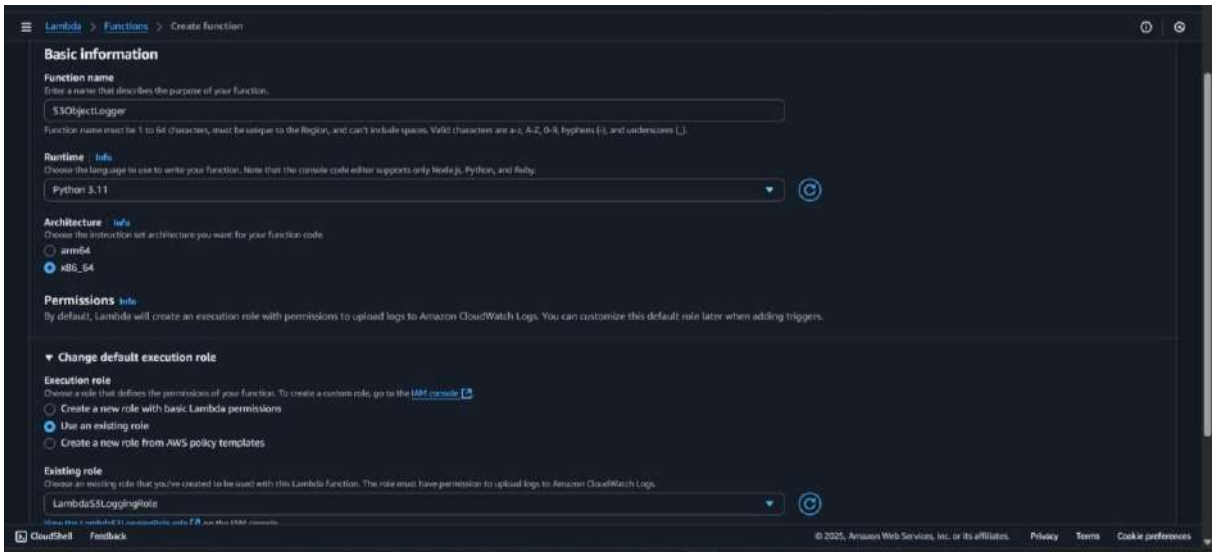
Next → Name the role → e.g., `LambdaS3LoggingRole`.

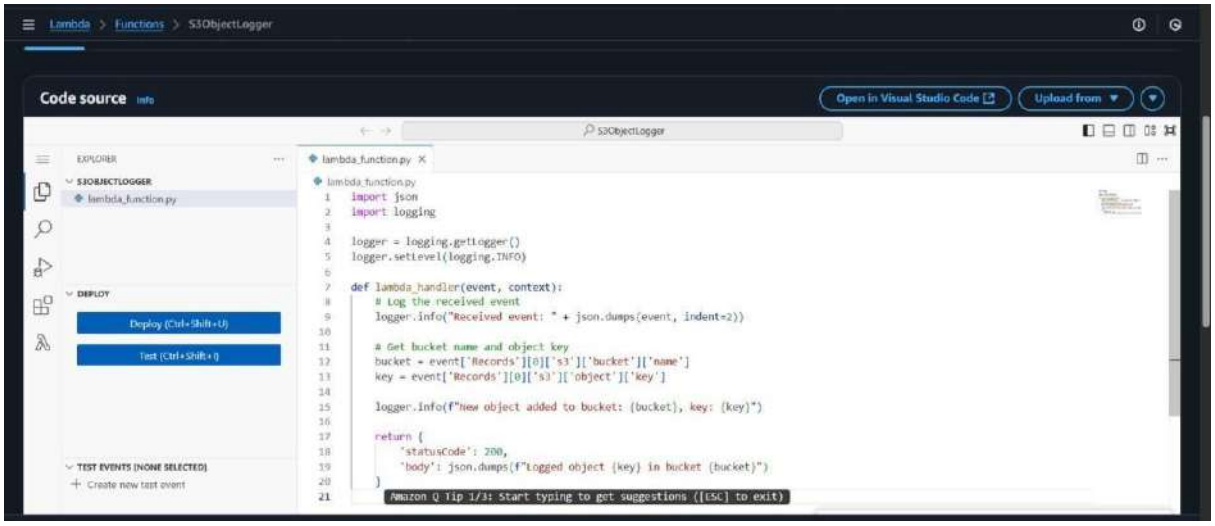


Step 4: Create Lambda function

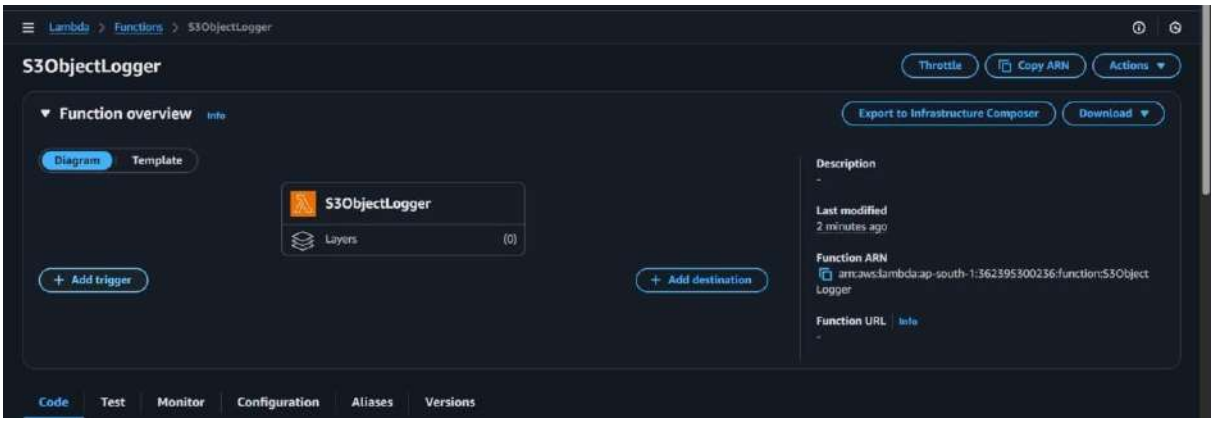
1. Go to Services → Lambda → Create function.
2. Select Author from scratch.

.

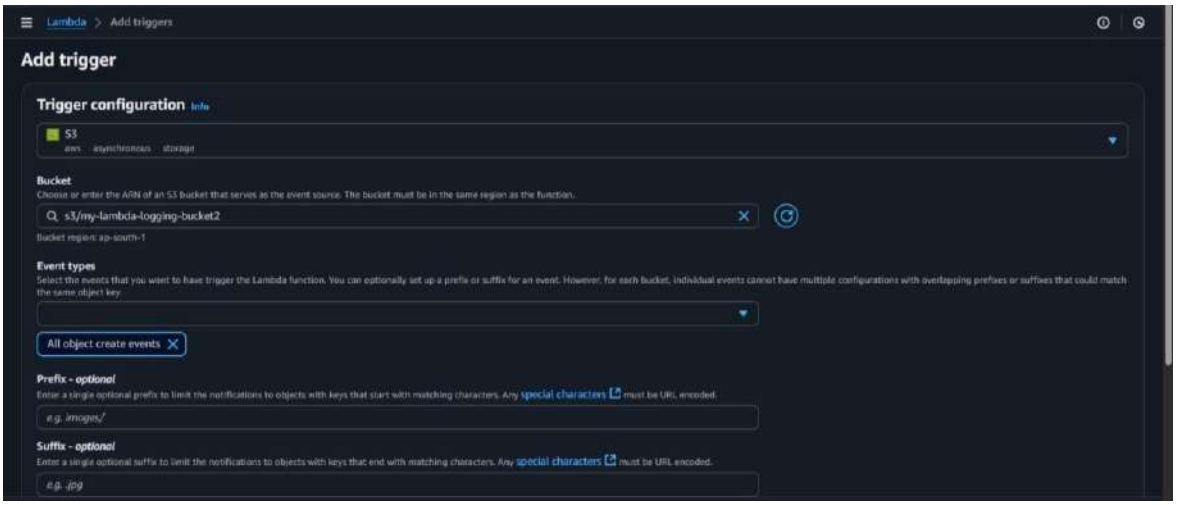




Step 5: Add S3 trigger to Lambda



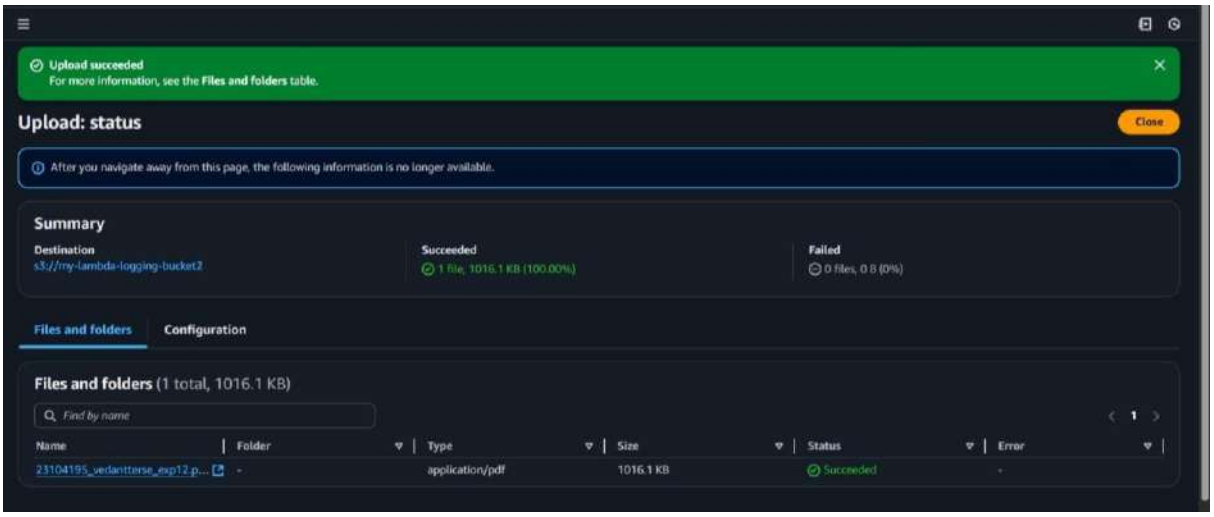
Click on Add trigger

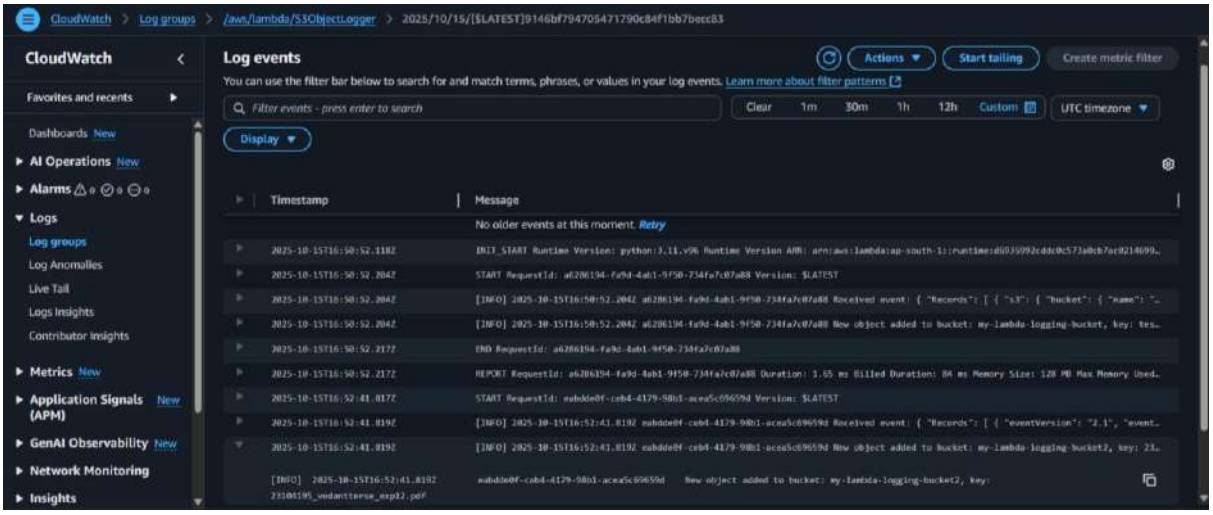


Go to S3 → my-lambda-logging-bucket → Upload.

- **Upload any small file (`test.txt` for example).**

.


Upload succeeded
For more information, see the Files and folders table.
Upload: status
Close
After you navigate away from this page, the following information is no longer available.
Summary
Destination
s3://my-lambda-logging-bucket2
Succeeded
1 file, 1016.1 KB (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 total, 1016.1 KB)
Find by name
Name
Folder
Type
Size
Status
Error
23104195_vedantterse_exp12.p...
application/pdf
1016.1 KB
Succeeded


CloudWatch
Log groups
/aws/lambda/S3ObjectLogger
2025/10/15/[$LATEST]9146bf7947054471790c84f1bb7beecc83
CloudWatch
Favorites and recents
Dashboards New
AI Operations New
Alarms
Logs
Log groups
Log Anomalies
Live Tail
Logs Insights
Contributor Insights
Metrics New
Application Signals (APM) New
GenAI Observability New
Network Monitoring
Insights
Log events
You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns
Actions
Start tailing
Create metric filter
Filter events - press enter to search
Clear
1m
30m
1h
12h
Custom
UTC timezone
Display
Timestamp
Message
No older events at this moment. Retry