



Academic Year: 2025-26

Semester: V

Class / Branch/ Div: TEIT C

Subject: ADL

Name of Student: Deep Varkute

Student ID:24204010

Roll No.60

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**

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
nagios-master	i-0ae05f518a2969e19	Running	t3.micro	Initializing	View alarms +	ap-south-1b	ec2-13-204
nagios-agent	i-020678f0b714d4651	Running	t3.micro	Initializing	View alarms +	ap-south-1b	ec2-3-108-1

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

**Security group inbound rules:**

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sg-0481bc62914e993c3	SSH	TCP	22	Custom 0.0.0.0/0	
sg-065d27d49622829a5	HTTPS	TCP	443	Custom 0.0.0.0/0	
sg-0b97b1b95b800c005	HTTP	TCP	80	Custom 0.0.0.0/0	
-	All traffic	All	All	Custom 0.0.0.0/0	



PARSHVANATH CHARITABLE TRUST'S

**A. P. SHAH INSTITUTE OF TECHNOLOGY**

**Department of Information Technology**

**(NBA Accredited)**



**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:

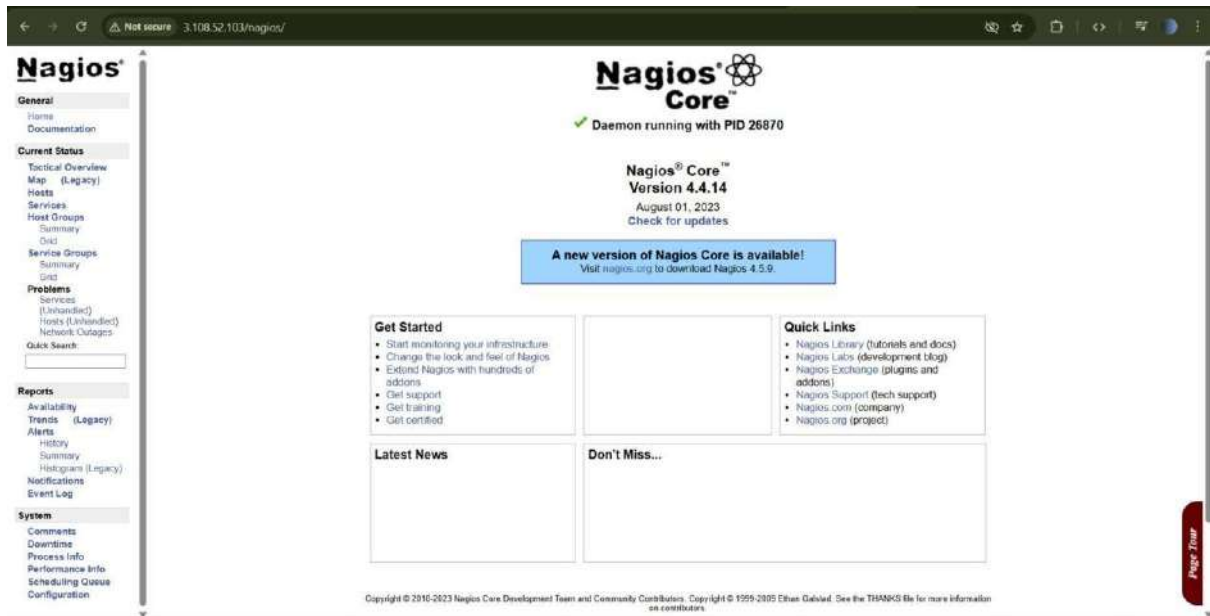
`http://<MASTER_PUBLIC_IP>/nagios`

**SIT**

**Department of Information Technology | AP**



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>
```



PARSHVANATH CHARITABLE TRUST'S

**A. P. SHAH INSTITUTE OF TECHNOLOGY**

**Department of Information Technology**

**(NBA Accredited)**



**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
}
```

**SIT**

**Department of Information Technology | AP**

**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

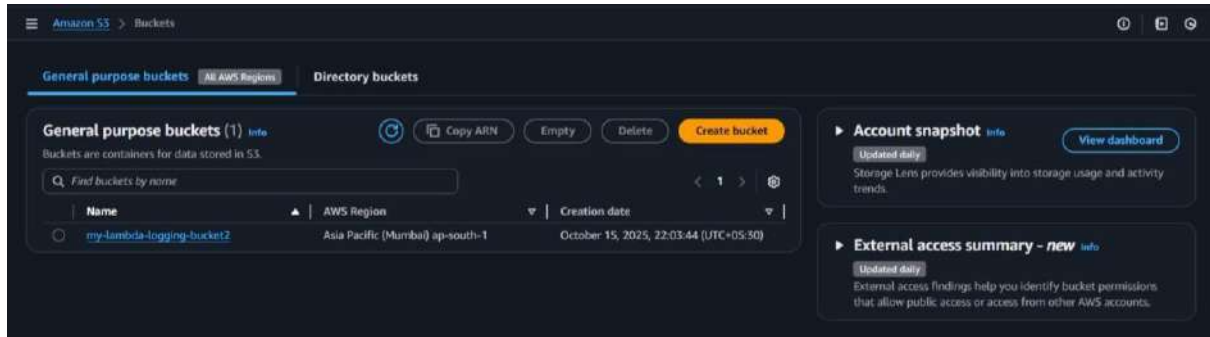


**Q. 2 Create a Lambda function which will log the content to add an object to a specific bucket.**

## Step 1: Create an S3 bucket

Bucket name: my-lambda-logging-bucket

Uncheck “Block all public access”

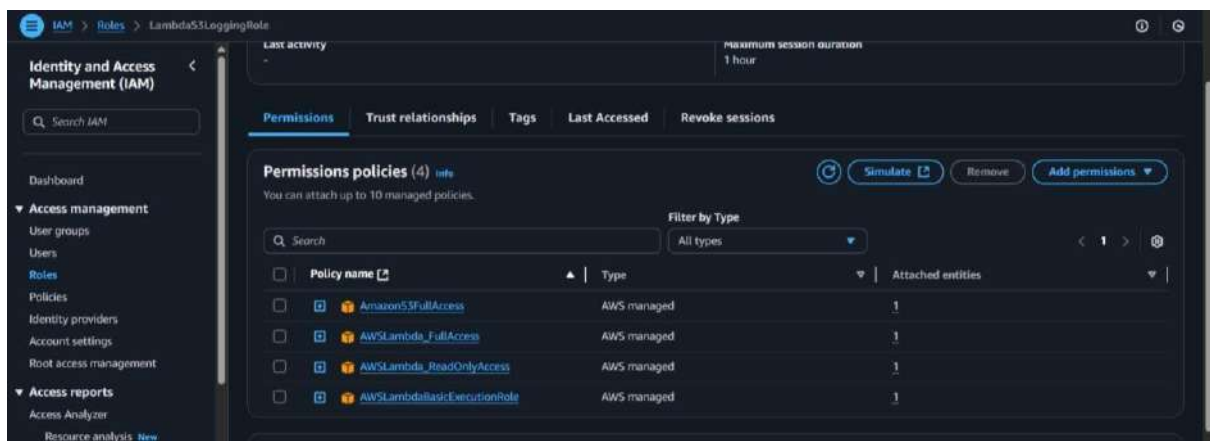


## Step 2: Create an IAM Role for Lambda

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.





PARSHVANATH CHARITABLE TRUST'S  
**A. P. SHAH INSTITUTE OF TECHNOLOGY**  
Department of Information Technology  
(NBA Accredited)



**Basic Information**

**Function name**  
Enter a name that describes the purpose of your function.  
  
Function name must be 1 to 64 characters, must be unique to the Region, and can't include spaces. Valid characters are a-z, A-Z, 0-9, hyphens (-), and underscores (\_).

**Runtime** Info  
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.

**Architecture** Info  
Choose the instruction set architecture you want for your function code.  
☐ arm64  
☒ x86\_64

**Permissions** Info  
By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

**▼ Change default execution role**

**Execution role**  
Choose a role that defines the permissions of your function. To create a custom role, go to the [IAM console](#).  
☐ Create a new role with basic Lambda permissions  
☒ Use an existing role  
☐ Create a new role from AWS policy templates

**Existing role**  
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.

View the LambdaS3LoggingRole role in the IAM console.

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

**Code source** Info

[Open in Visual Studio Code](#) [Upload from](#)

**EXPLORER**

- ▼ S3OBJECTLOGGER
  - lambda\_function.py
- ▼ DEPLOY
  - Deploy (Ctrl+Shift+D)
  - Test (Ctrl+Shift+Q)
- ▼ TEST EVENTS (NONE SELECTED)
  - + Create new test event

**lambda\_function.py**

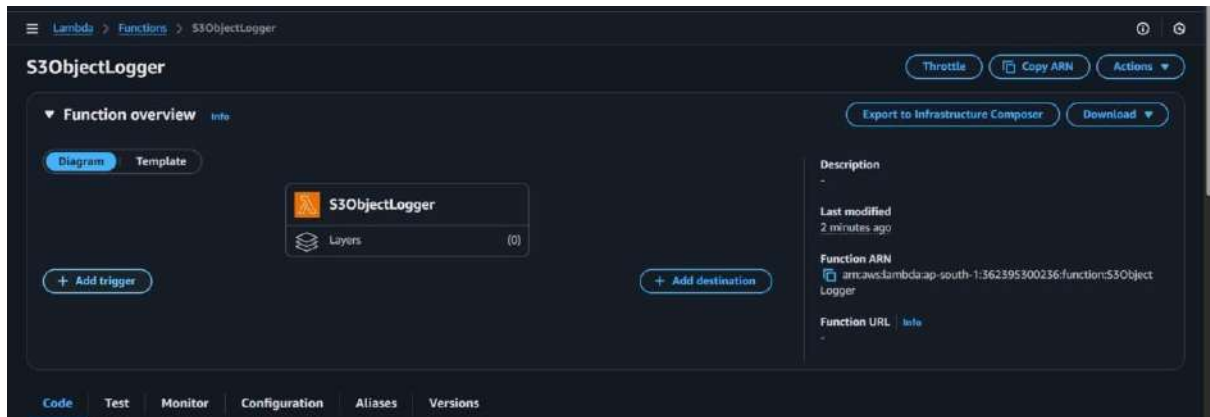
```
1 import json
2 import logging
3
4 logger = logging.getLogger()
5 logger.setLevel(logging.INFO)
6
7 def lambda_handler(event, context):
8     # Log the received event
9     logger.info("Received event: " + json.dumps(event, indent=2))
10
11     # Get bucket name and object key
12     bucket = event['Records'][0]['s3']['bucket']['name']
13     key = event['Records'][0]['s3']['object']['key']
14
15     logger.info(f"new object added to bucket: {bucket}, key: {key}")
16
17     return {
18         'statusCode': 200,
19         'body': json.dumps(f"Logged object {key} in bucket {bucket}")
20     }
21
```

Amazon Q Tip 1/3: Start typing to get suggestions ([ESC] to exit)

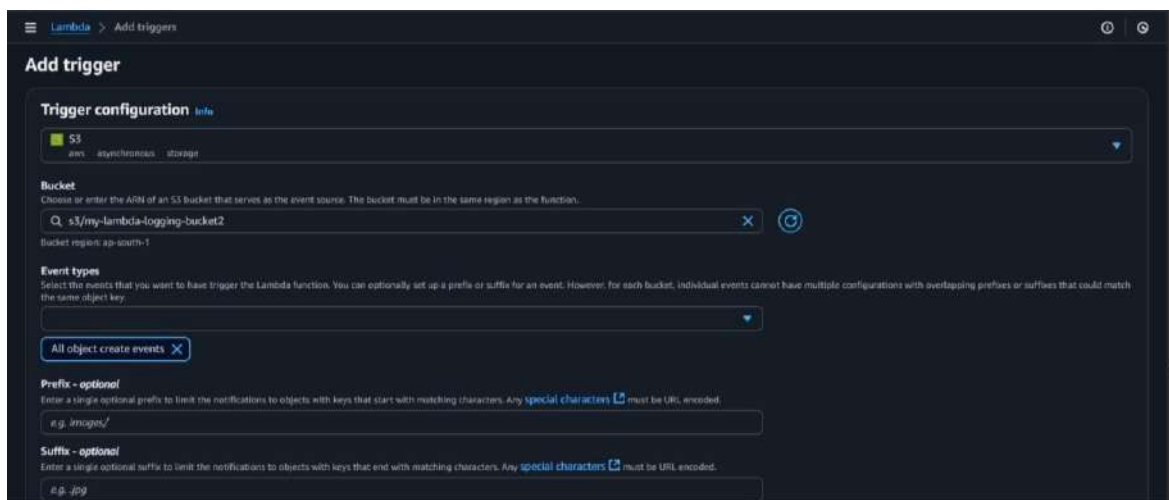
**Step 5: Add S3 trigger to Lambda**

**SIT**

**Department of Information Technology | AP**



Click on Add trigger



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

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





PARSHVANATH CHARITABLE TRUST'S  
**A. P. SHAH INSTITUTE OF TECHNOLOGY**  
Department of Information Technology  
(NBA Accredited)



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_vedanttense_exp12.p...	-	application/pdf	1016.1 KB	Succeeded	-

CloudWatch > Log groups > /aws/lambda/S3ObjectLogger > 2025/10/15/[\$LATEST]9146bf794705471790c84f1bb7bccc83

**CloudWatch**

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](#)

Filter events - press enter to search

Clear 1m 30m 1h 12h Custom UTC timezone

Display

No older events at this moment. [Retry](#)

Timestamp	Message
2025-10-15T16:50:52.118Z	INIT_START Runtime Version: python3.11.v96 Runtime Version ABI: armv7l-aws-lambda-rp-south-1::runtimeid6033992cdd8c573adb7ac8214699...
2025-10-15T16:50:52.204Z	START RequestId: a6286194-fa9d-4ab1-9f50-734fa7c07a88 Version: \$LATEST
2025-10-15T16:50:52.204Z	[INFO] 2025-10-15T16:50:52.204Z a6286194-fa9d-4ab1-9f50-734fa7c07a88 Received event: { "Records": [ { "s3": { "bucket": { "name": "...
2025-10-15T16:50:52.204Z	[INFO] 2025-10-15T16:50:52.204Z a6286194-fa9d-4ab1-9f50-734fa7c07a88 New object added to bucket: my-lambda-logging-bucket, key: tes...
2025-10-15T16:50:52.217Z	END RequestId: a6286194-fa9d-4ab1-9f50-734fa7c07a88
2025-10-15T16:50:52.217Z	REPORT RequestId: a6286194-fa9d-4ab1-9f50-734fa7c07a88 Duration: 3.55 ms Billed Duration: 84 ms Memory Size: 128 MB Max Memory Used...
2025-10-15T16:52:41.817Z	START RequestId: eabdd0f-cab4-4179-9801-acea5c09659d Version: \$LATEST
2025-10-15T16:52:41.819Z	[INFO] 2025-10-15T16:52:41.819Z eabdd0f-cab4-4179-9801-acea5c09659d Received event: { "Records": [ { "eventVersion": "2.1", "event...
2025-10-15T16:52:41.819Z	[INFO] 2025-10-15T16:52:41.819Z eabdd0f-cab4-4179-9801-acea5c09659d New object added to bucket: my-lambda-logging-bucket2, key: 23...
2025-10-15T16:52:41.819Z	[INFO] 2025-10-15T16:52:41.819Z eabdd0f-cab4-4179-9801-acea5c09659d New object added to bucket: my-lambda-logging-bucket2, key: 23104195_vedanttense_exp12.pdf