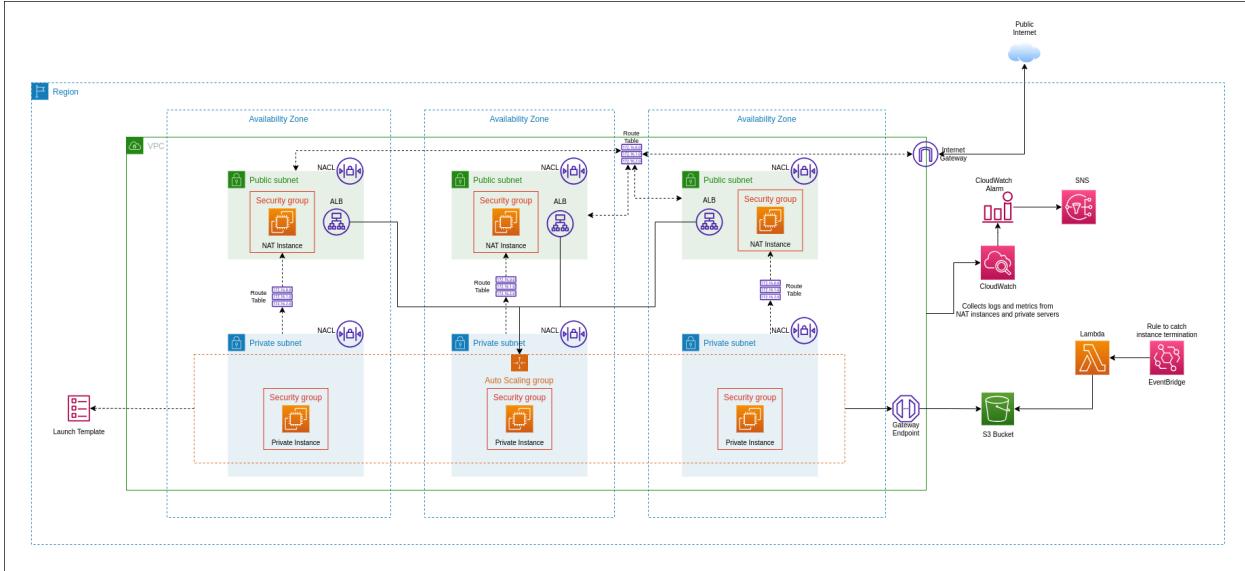


Demo project for AWS



Architecture Diagram for the Solution

Step 1 - Create a VPC with the CIDR range of “172.168.0.0/16”

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

VPC only VPC and more

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.

Project-VPC

IPv4 CIDR block [Info](#)
 IPv4 CIDR manual input
 IPAM-allocated IPv4 CIDR block

IPv4 CIDR
172.168.0.0/16

IPv6 CIDR block [Info](#)
 No IPv6 CIDR block
 IPAM-allocated IPv6 CIDR block
 Amazon-provided IPv6 CIDR block
 IPv6 CIDR owned by me

Tenancy [Info](#)
Default

vpc-03da74872e88be55a / Project-VPC			
Details		Actions	
VPC ID vpc-03da74872e88be55a	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-d7a20ee76c28599c	Main route table rtb-042b7a6579fd03688	Main network ACL acl-0965545c6c096d97c
Default VPC No	IPv4 CIDR 172.168.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups Failed to load rule groups	Owner ID 237042273450	

Step 2 - Create three public and three private subnets across three availability zones.

Subnets (6) Info											
Q Find resources by attribute or tag Actions Create subnet											
<input type="text" value="Subnet ID = subnet-0d4fb0f09e6227e1e"/> X <input type="text" value="Subnet ID = subnet-0b822cf2c0ed21c10"/> X <input type="text" value="Subnet ID = subnet-0a9ebf9449d745906"/> X Show more (+3) Clear filters											
Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 ...	Available I...	Availability Zone		Availability Zone		Availability Zone
Project-VPC-Private-1a	subnet-0d0191134f25185e	Available	vpc-03da74872e88be55a Proj...	172.168.4.0/24	-	251	us-east-1a		use1-az1		
Project-VPC-Private-1c	subnet-0e602f51fd6a63f7	Available	vpc-03da74872e88be55a Proj...	172.168.6.0/24	-	251	us-east-1c		use1-az4		
Project-VPC-Private-1b	subnet-01848f693e9b8798f	Available	vpc-03da74872e88be55a Proj...	172.168.5.0/24	-	251	us-east-1b		use1-az2		
Project-VPC-Public-1a	subnet-0d4fb0f09e6227e1e	Available	vpc-03da74872e88be55a Proj...	172.168.1.0/24	-	251	us-east-1a		use1-az1		
Project-VPC-Public-1b	subnet-0b822cf2c0ed21c10	Available	vpc-03da74872e88be55a Proj...	172.168.2.0/24	-	251	us-east-1b		use1-az2		
Project-VPC-Public-1c	subnet-0a9ebf9449d745906	Available	vpc-03da74872e88be55a Proj...	172.168.3.0/24	-	251	us-east-1c		use1-az4		

Step 3 - Create an Internet gateway and attach it to the VPC.

VPC > Internet gateways > igw-04e52390847cebbd3 / Project-VPC-IGW							
Actions							
Details Info							
Internet gateway ID igw-04e52390847cebbd3	State Detached	VPC ID -	Owner 237042273450				
Tags <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> Q Search tags </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Key</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Name</td> <td>Project-VPC-IGW</td> </tr> </tbody> </table> Manage tags				Key	Value	Name	Project-VPC-IGW
Key	Value						
Name	Project-VPC-IGW						

VPC > Internet gateways > Attach to VPC (igw-04e52390847cebbd3)

Attach to VPC (igw-04e52390847cebbd3) [Info](#)

VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs
Attach the internet gateway to this VPC.

[▶ AWS Command Line Interface command](#)

[Cancel](#) [Attach internet gateway](#)

Step 4 - Create a route table for the public subnets.

VPC > Route tables > Create route table

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings	
Name - optional	Create a tag with a key of 'Name' and a value that you specify.
<input type="text" value="Project-VPC-PublicRT"/>	
VPC	The VPC to use for this route table.
<input type="text" value="vpc-03da74872e88be55a (Project-VPC)"/>	

Edit the subnet association for the public route table to attach the three public subnets.

Routes | **Subnet associations** | Edge associations | Route propagation | Tags

Explicit subnet associations (3)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
Project-VPC-Public-1a	subnet-0d4fb0f09e6227e1e	172.168.1.0/24	-
Project-VPC-Public-1b	subnet-0b822cf2c0ed21c10	172.168.2.0/24	-
Project-VPC-Public-1c	subnet-0a9ebf9449d745906	172.168.3.0/24	-

Edit the route of the table to forward the internet faced traffic to the internet gateway as a target.

VPC > Route tables > rtb-0666535f17e0b5476 > Edit routes

Edit routes

Destination	Target	Status	Propagated
172.168.0.0/16	Q local	Active	No
Q 0.0.0.0/0	Q igw-04e52390847cebbdd	-	No

Step 5 - Create a Security group for the NAT instance, which will be created in the public subnet.

Basic details

Security group name Info

Name cannot be edited after creation.

Description Info

VPC Info

The security group allows incoming traffic for HTTP, HTTPS, SSH, and all ICMP from anywhere.

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-0dc59ad063ef05a33	HTTP	TCP	80	Custom	0.0.0.0/0
sgr-0e7abb4d49b1f9d45	HTTPS	TCP	443	Custom	0.0.0.0/0
sgr-02cc4eb3ff7df86bf	SSH	TCP	22	Custom	0.0.0.0/0
sgr-0b150bd0ce05e39e9	All ICMP - IPv4	ICMP	All	Custom	0.0.0.0/0

Step 6 - Launch an EC2 instance in one of the public subnets. Choose the AWS managed NAT AMI.

Catalog	Published	Architecture	Virtualization	Root device type	ENA Enabled
Community AMIs	2023-06-06T19:49:10.000Z	x86_64	hvm	ebs	Yes

▼ Instance type [Info](#)

Instance type

t2.micro Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand RHEL pricing: 0.0716 USD per Hour
On-Demand Linux pricing: 0.0116 USD per Hour

All generations

[Compare instance types](#)

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

NAT-instance [Create new key pair](#)

Attach the previously created security group to the instance.

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-03da74872e88be55a (Project-VPC)
172.168.0.0/16

Subnet Info

subnet-0d4fb0f09e6227e1e Project-VPC-Public-1a
VPC: vpc-03da74872e88be55a Owner: 237042273450
Availability Zone: us-east-1a IP addresses available: 251 CIDR: 172.168.1.0/24 [Create new subnet](#)

Auto-assign public IP [Info](#)

Enable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

Common security groups [Info](#)

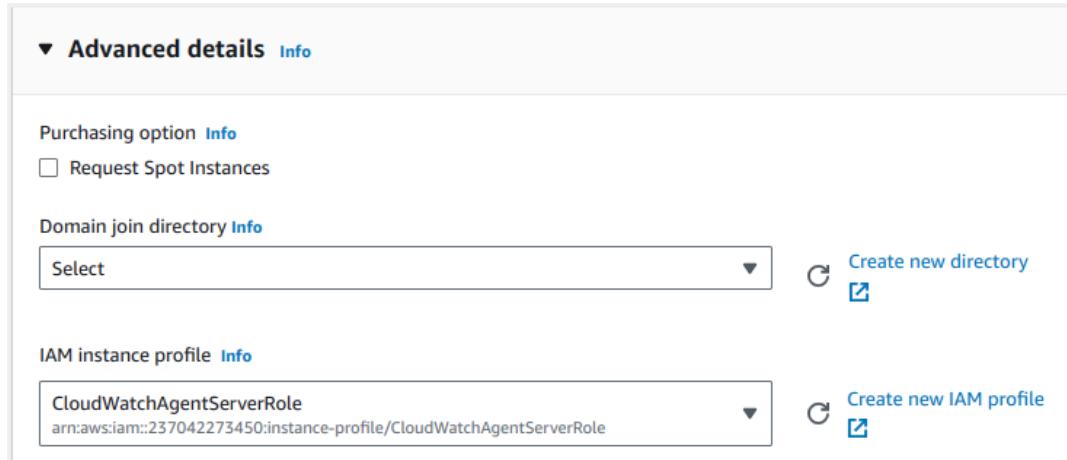
Select security groups

Project-VPC-NAT-SG sg-08408dfa060a543b3 X
VPC: vpc-03da74872e88be55a [Compare security group rules](#)

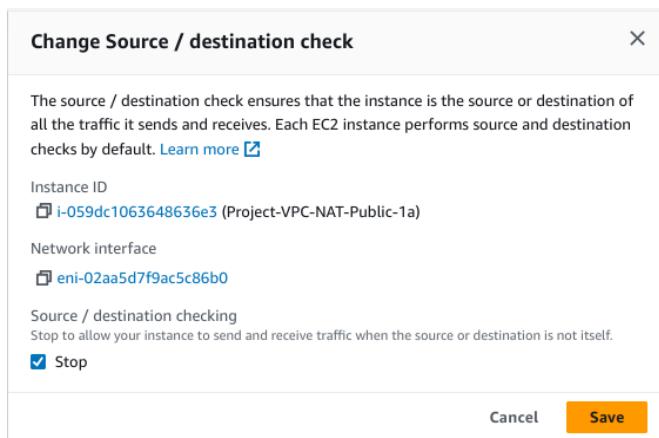
Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

Attach the “CloudWatchAgentServerRole” role to the instance profile, it will allow the instance to send logs and metrics to cloudwatch using cloudwatch agent.



After the NAT instance is launched, stop the source/destination checking on the instance. It will allow the instance to send and receive the traffic when it is not the source and destination for that traffic.

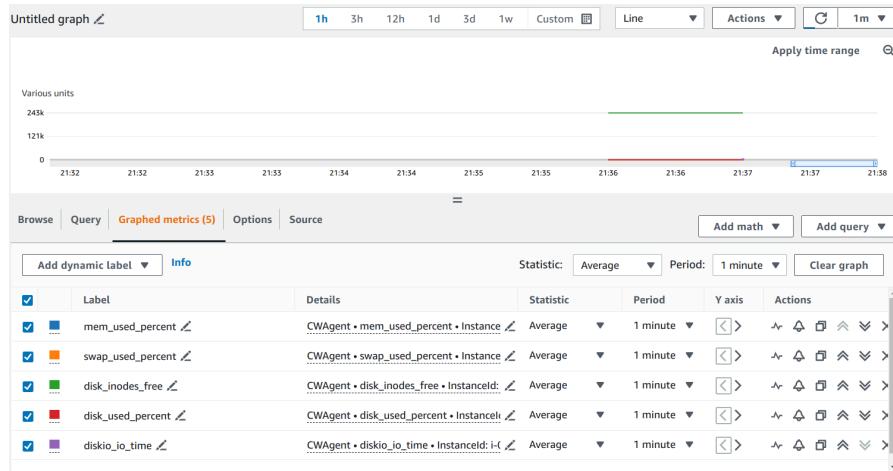


Step 7 - SSH into the NAT instance and configure the CloudWatch agent in it to send CPU, disk, and memory metrics to cloudwatch.

```
[ec2-user@ip-172-168-1-147 ~]$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json
***** processing amazon-cloudwatch-agent *****
I! Trying to detect region from ec2 D! [EC2] Found active network interface Successfully fetched the config and saved in /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp
Start Configuration Validation...
2023/08/07 16:06:37 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp ...
2023/08/07 16:06:37 D! append_dimensions required because append_dimensions is set
2023/08/07 16:06:37 D! delta_processor required because metrics with diskio or net are set
2023/08/07 16:06:37 D! ec2tagger processor required because append_dimensions is set
2023/08/07 16:06:37 Configuration validation first phase succeeded
I! Detecting run as user...
I! Trying to detect region from ec2
D! [EC2] Found active network interface
/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -schematest -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml
Configuration validation second phase succeeded
Configuration validation succeeded
amazon-cloudwatch-agent stop/waiting
amazon-cloudwatch-agent start/running, process 19291
[ec2-user@ip-172-168-1-147 ~]$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a status
{
    "status": "running",
    "starttime": "2023-08-07T16:06:38+0000",
    "configstatus": "configured",
    "version": "1.300026.1b168"
}
```

The above snapshot shows that the cloudwatch agent is running in the instance.

It is seen that the metrics of the NAT instance are available in the cloudwatch.



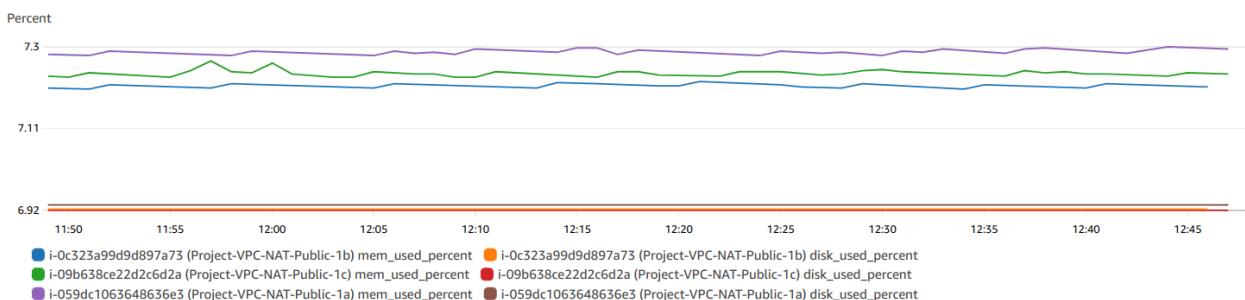
Step 8 - Create AMI of the above instance and launch NAT instances in other two subnets.

This screenshot shows the 'Configure Image' step of the AWS Create Image wizard. It includes fields for Instance ID, Image name, Image description, No reboot, and Instance volumes. The instance volume configuration table is shown below:

Storage type	Device	Snapshot	Size	Volume type	IOPS	Throughput	Delete on termination	Encrypted
EBS	/dev/...	Create new snapshot fr...	8	Magnetic - standard	2000		<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

Launch two more NAT instances using the above AMI in different subnets.

The snapshot shows that the metrics from all the three NAT instances are available in cloudwatch.



Step 9 - Create a route table for one of the private subnets.

The screenshot shows the 'Details' tab of a route table named 'rtb-0579e91fb17dff72'. The table has the following details:

Route table ID rtb-0579e91fb17dff72	Main No	Explicit subnet associations subnet-0d0191134f251c85e / Project-VPC-Private-1a	Edge associations -
VPC vpc-03da74872e88be55a Project-VPC	Owner ID 237042273450		

Edit the route to forward the internet facing traffic to the NAT instance hosted in the public subnet of the same AZ. This will allow the instances in the private subnet to access the public internet for updates and downloads.

The screenshot shows the 'Routes' and 'Subnet associations' tabs for the route table.

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	eni-02aa5d7f9ac5c86b0	Active	No
172.168.0.0/16	local	Active	No

Subnet associations (1)

Name	Subnet ID	IPv4 CIDR
Project-VPC-Private-1a	subnet-0d0191134f251c85e	172.168.4.0/24

Create two more route tables for the other two private subnets and edit their route and subnet association. The route table forwards the internet facing traffic from the instances in those subnets to the NAT instances in the public subnet of the same AZ.

Step 10 - Create NACL for the public subnets.

The screenshot shows the 'Network ACL settings' page for creating a new Network ACL.

Name - optional
Creates a tag with a key of 'Name' and a value that you specify.

VPC
VPC to use for this network ACL.

Allow inbound and outbound rules to allow only SSH, HTTP, HTTPS, and all ICMP traffic.

Outbound rules (5)

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	SSH (22)	TCP (6)	22	0.0.0.0/0	<input checked="" type="radio"/> Allow
101	HTTP (80)	TCP (6)	80	0.0.0.0/0	<input checked="" type="radio"/> Allow
102	HTTPS (443)	TCP (6)	443	0.0.0.0/0	<input checked="" type="radio"/> Allow
103	All ICMP - IPv4	ICMP (1)	All	0.0.0.0/0	<input checked="" type="radio"/> Allow
*	All traffic	All	All	0.0.0.0/0	<input checked="" type="radio"/> Deny

Associate the public subnets to the NACL.

Subnet associations (3)

Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IPv6 CIDR
Project-VPC-Public-1a	subnet-0d4fb0f09e6227e1e	acl-0d7bbfd9fdf94fae / Project-VPC-P...	us-east-1a	172.168.1.0/24	-
Project-VPC-Public-1c	subnet-0a9ebf9449d745906	acl-0d7bbfd9fdf94fae / Project-VPC-P...	us-east-1c	172.168.3.0/24	-
Project-VPC-Public-1b	subnet-0b822cf2c0ed21c10	acl-0d7bbfd9fdf94fae / Project-VPC-P...	us-east-1b	172.168.2.0/24	-

Step 11 - Create NACL for the private subnets.

acl-07710b914bb352407 / Project-VPC-Private-NACL

Details [Info](#)

Network ACL ID acl-07710b914bb352407	Associated with 3 Subnets	Default No	VPC ID vpc-03da74872e88be55a / Project-VPC
Owner 237042273450			

Inbound rules (6)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	172.168.0.0/16	<input checked="" type="radio"/> Allow
101	HTTP (80)	TCP (6)	80	0.0.0.0/0	<input checked="" type="radio"/> Allow
102	HTTPS (443)	TCP (6)	443	0.0.0.0/0	<input checked="" type="radio"/> Allow
103	All TCP	TCP (6)	All	0.0.0.0/0	<input checked="" type="radio"/> Allow
104	All ICMP - IPv4	ICMP (1)	All	0.0.0.0/0	<input checked="" type="radio"/> Allow
*	All traffic	All	All	0.0.0.0/0	<input checked="" type="radio"/> Deny

Inbound rules	Outbound rules	Subnet associations	Tags																																										
Outbound rules (6)			Run Reachability Analyzer X																																										
Filter outbound rules <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Rule number</th><th>Type</th><th>Protocol</th><th>Port range</th><th>Destination</th><th>Allow/Deny</th></tr> </thead> <tbody> <tr><td>100</td><td>All traffic</td><td>All</td><td>All</td><td>172.168.0.0/16</td><td></td></tr> <tr><td>101</td><td>HTTP (80)</td><td>TCP (6)</td><td>80</td><td>0.0.0.0/0</td><td></td></tr> <tr><td>102</td><td>HTTPS (443)</td><td>TCP (6)</td><td>443</td><td>0.0.0.0/0</td><td></td></tr> <tr><td>103</td><td>All TCP</td><td>TCP (6)</td><td>All</td><td>0.0.0.0/0</td><td></td></tr> <tr><td>104</td><td>All ICMP - IPv4</td><td>ICMP (1)</td><td>All</td><td>0.0.0.0/0</td><td></td></tr> <tr><td>*</td><td>All traffic</td><td>All</td><td>All</td><td>0.0.0.0/0</td><td></td></tr> </tbody> </table>				Rule number	Type	Protocol	Port range	Destination	Allow/Deny	100	All traffic	All	All	172.168.0.0/16		101	HTTP (80)	TCP (6)	80	0.0.0.0/0		102	HTTPS (443)	TCP (6)	443	0.0.0.0/0		103	All TCP	TCP (6)	All	0.0.0.0/0		104	All ICMP - IPv4	ICMP (1)	All	0.0.0.0/0		*	All traffic	All	All	0.0.0.0/0	
Rule number	Type	Protocol	Port range	Destination	Allow/Deny																																								
100	All traffic	All	All	172.168.0.0/16																																									
101	HTTP (80)	TCP (6)	80	0.0.0.0/0																																									
102	HTTPS (443)	TCP (6)	443	0.0.0.0/0																																									
103	All TCP	TCP (6)	All	0.0.0.0/0																																									
104	All ICMP - IPv4	ICMP (1)	All	0.0.0.0/0																																									
*	All traffic	All	All	0.0.0.0/0																																									

Inbound rules	Outbound rules	Subnet associations	Tags																								
Subnet associations (3)			Edit subnet associations X																								
Filter subnet associations <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Name</th><th>Subnet ID</th><th>Associated with</th><th>Availability Zone</th><th>IPv4 CIDR</th><th>IPv6 CIDR</th></tr> </thead> <tbody> <tr><td>Project-VPC-Private-1b</td><td>subnet-01848f693e9b8798f</td><td>acl-07710b914bb352407 / Project-VPC...</td><td>us-east-1b</td><td>172.168.5.0/24</td><td>-</td></tr> <tr><td>Project-VPC-Private-1c</td><td>subnet-0e602f51fd6da63f7</td><td>acl-07710b914bb352407 / Project-VPC...</td><td>us-east-1c</td><td>172.168.6.0/24</td><td>-</td></tr> <tr><td>Project-VPC-Private-1a</td><td>subnet-0d0191134f251c85e</td><td>acl-07710b914bb352407 / Project-VPC...</td><td>us-east-1a</td><td>172.168.4.0/24</td><td>-</td></tr> </tbody> </table>				Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IPv6 CIDR	Project-VPC-Private-1b	subnet-01848f693e9b8798f	acl-07710b914bb352407 / Project-VPC...	us-east-1b	172.168.5.0/24	-	Project-VPC-Private-1c	subnet-0e602f51fd6da63f7	acl-07710b914bb352407 / Project-VPC...	us-east-1c	172.168.6.0/24	-	Project-VPC-Private-1a	subnet-0d0191134f251c85e	acl-07710b914bb352407 / Project-VPC...	us-east-1a	172.168.4.0/24	-
Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IPv6 CIDR																						
Project-VPC-Private-1b	subnet-01848f693e9b8798f	acl-07710b914bb352407 / Project-VPC...	us-east-1b	172.168.5.0/24	-																						
Project-VPC-Private-1c	subnet-0e602f51fd6da63f7	acl-07710b914bb352407 / Project-VPC...	us-east-1c	172.168.6.0/24	-																						
Project-VPC-Private-1a	subnet-0d0191134f251c85e	acl-07710b914bb352407 / Project-VPC...	us-east-1a	172.168.4.0/24	-																						

Step 12 - Create an IAM role for the private instances.

The policies attached to the roles allows the instances to describe other instances, perform actions with S3, send logs to cloudwatch, and SSM connection.

ApacheServer-Role

Delete

Allows EC2 instances to call AWS services on your behalf.

Summary

Edit

Creation date	ARN	Instance profile ARN
August 04, 2023, 12:40 (UTC+05:30)	arn:aws:iam::237042273450:role/ApacheServer-Role	arn:aws:iam::237042273450:instance-profile/ApacheServer-Role
Last activity	Maximum session duration	
2 hours ago	1 hour	

Permissions

Trust relationships

Tags

Access Advisor

Revoke sessions

Permissions policies (4) Info

You can attach up to 10 managed policies.

 Simulate Remove Add permissions ▾
< 1 >
Edit

<input type="checkbox"/>	Policy name	Type	Description
<input type="checkbox"/>	describeEC2	Customer managed	
<input type="checkbox"/>	EC2_S3_ReadWriteAccess	Customer managed	
<input type="checkbox"/>	CloudWatchAgentServerPolicy	AWS managed	Permissions required to use AmazonCloudWatchAgent on servers
<input type="checkbox"/>	AmazonSSMManagedInstanceC...	AWS managed	The policy for Amazon EC2 Role to enable AWS Systems Manager service core functionality.

Step 13 - Launch EC2 instance in one of the private subnets.

Instance summary for i-0da22e3f609d4989d (Project-VPC-PrivateServer-1a) [Info](#)

Updated less than a minute ago

Instance ID i-0da22e3f609d4989d (Project-VPC-PrivateServer-1a)	Public IPv4 address -	Private IPv4 addresses 172.168.4.193															
IPv6 address -	Instance state Running	Public IPv4 DNS -															
Hostname type IP name: ip-172-168-4-193.ec2.internal	Private IP DNS name (IPv4 only) ip-172-168-4-193.ec2.internal	Elastic IP addresses -															
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more															
Auto-assigned IP address -	VPC ID vpc-03da74872e88be55a (Project-VPC)	Auto Scaling Group name -															
IAM Role ApacheServer-Role	Subnet ID subnet-0d0191134f251c85e (Project-VPC-Private-1a)																
IMDSv2 Optional																	
Details Security Networking Storage Status checks Monitoring Tags																	
▼ Instance details Info <table border="1"> <tbody> <tr> <td>Platform Amazon Linux (Inferred)</td> <td>AMI ID ami-09538990a0c4fe9be</td> <td>Monitoring disabled</td> </tr> <tr> <td>Platform details Linux/UNIX</td> <td>AMI name amzn2-ami-kernel-5.10-hvm-2.0.20230727.0-x86_64-gp2</td> <td>Termination protection Disabled</td> </tr> <tr> <td>Stop protection Disabled</td> <td>Launch time Fri Aug 04 2023 16:55:57 GMT+0530 (India Standard Time) (16 minutes)</td> <td>AMI location amazon/amzn2-ami-kernel-5.10-hvm-2.0.20230727.0-x86_64-gp2</td> </tr> <tr> <td>Instance auto-recovery Default</td> <td>Lifecycle normal</td> <td>Stop-hibernate behavior disabled</td> </tr> <tr> <td>AMI Launch index 0</td> <td>Key pair assigned at launch privateInstancePEM</td> <td>State transition reason -</td> </tr> </tbody> </table>			Platform Amazon Linux (Inferred)	AMI ID ami-09538990a0c4fe9be	Monitoring disabled	Platform details Linux/UNIX	AMI name amzn2-ami-kernel-5.10-hvm-2.0.20230727.0-x86_64-gp2	Termination protection Disabled	Stop protection Disabled	Launch time Fri Aug 04 2023 16:55:57 GMT+0530 (India Standard Time) (16 minutes)	AMI location amazon/amzn2-ami-kernel-5.10-hvm-2.0.20230727.0-x86_64-gp2	Instance auto-recovery Default	Lifecycle normal	Stop-hibernate behavior disabled	AMI Launch index 0	Key pair assigned at launch privateInstancePEM	State transition reason -
Platform Amazon Linux (Inferred)	AMI ID ami-09538990a0c4fe9be	Monitoring disabled															
Platform details Linux/UNIX	AMI name amzn2-ami-kernel-5.10-hvm-2.0.20230727.0-x86_64-gp2	Termination protection Disabled															
Stop protection Disabled	Launch time Fri Aug 04 2023 16:55:57 GMT+0530 (India Standard Time) (16 minutes)	AMI location amazon/amzn2-ami-kernel-5.10-hvm-2.0.20230727.0-x86_64-gp2															
Instance auto-recovery Default	Lifecycle normal	Stop-hibernate behavior disabled															
AMI Launch index 0	Key pair assigned at launch privateInstancePEM	State transition reason -															

The security group attached to the private instance allows incoming HTTP, ICMP, SSH, and HTTPS traffic from the security group of the NAT instance only.

[Details](#) | [Security](#) | [Networking](#) | [Storage](#) | [Status checks](#) | [Monitoring](#) | [Tags](#)

▼ Security details

IAM Role ApacheServer-Role	Owner ID 237042273450	Launch time Fri Aug 04 2023 16:55:57 GMT+0530 (India Standard Time)
Security groups sg-04036e3a9cf0b54c4 (Project-VPC-PrivateServer-SG)		

▼ Inbound rules

Filter rules						
Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
-	sgr-0e155ff818c7473d	443	TCP	sg-08408dfa060a543b3	Project-VPC-PrivateServer-SG	-
-	sgr-0ac743f863225467c	All	ICMP	sg-08408dfa060a543b3	Project-VPC-PrivateServer-SG	-
-	sgr-03bcefa02b7c82a0	22	TCP	sg-08408dfa060a543b3	Project-VPC-PrivateServer-SG	-
-	sgr-0d0fd1db1f301962b	80	TCP	sg-08408dfa060a543b3	Project-VPC-PrivateServer-SG	-

▼ Networking details [Info](#)

Public IPv4 address -	Private IPv4 addresses 172.168.4.193	VPC ID vpc-03da74872e88be55a (Project-VPC)
Public IPv4 DNS -	Private IP DNS name (IPv4 only) ip-172-168-4-193.ec2.internal	Secondary private IPv4 addresses -
Subnet ID subnet-0d0191134f251c85e (Project-VPC-Private-1a)	IPV6 addresses -	Outpost ID -
Availability zone us-east-1a	Carrier IP addresses (ephemeral) -	
Use RDN as guest OS hostname Disabled	Answer RDN DNS hostname IPv4 Disabled	

Step 14 - Connect to the NAT instance using SSH or Session manager.

To SSH the private instance from the NAT instance, copy the content of the key pair attached to the private instance and paste it into a new file created in the NAT instance.

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEowIBAAKCAQEauk6RSvt3G4grXpxKR5P4GYlkZdCLt+ikAoDTgx48iKFQbN99  
0Gx726r4t9urur/Js00f2Ywjisld/PdgPbB/1rBNhElD/01LJnb8mz5GQ+KfjvK  
6pxl3PkcxklP62hRQXnB6SehrgAFRA0xkXEv4kLfT4TPf2p6WTD02jHq/blsZPqc  
E9TBASiS/_0NOEU4nDZfugvqKTR+F2H3HxGak1f0ghHRmh4qlT9C0Pdf1SRsK5lDx  
VBVb3MM5YHw1jhk3D3KN5dq+oC7k9LMFj/VL+HbKdRUfJYouM0bs5TK4SrWlcKTJ  
NNbAoZqrxiUiyeCdA8yFteydK+qQ36pSzt7JNwIDAQABoIBAB0VnNr+zMZQiKy5  
a2Mn2kNKM44M0efmtMFN3/VnY+a10pXzV2cme1eEHvrYDDEngFW6MHnJjs+Lkq  
CS0404zRcxh9s9hiQbVOG6cJ2g10fsrchj5n8gMAJLzTxu58M1u65WxaS0Xtbq7  
d0IGsHn7BI+OZTI39iesW90g09Yc7xDtex1ewQnREYw4UkZVDgQZYXmoIXJMR6eC  
y33kWK8W249ojoVagVcb71c3k/Z/G0E1rob98wydG5rf94Zayg/zm1HeUGE3QPvt  
gSWtjq1MSxS3fLBi6g6STPjM/7eadmYCIBxvkKEIBy8zaBxjoU/QgRvSR/WnQKzK  
UxjMYAEcgYEATxntanXnXY9LkZ+jLOYNydbIP0q0VTxKo/B3LFAQHJRNFNCx2ZCm  
yhnzeZ4i4bC1mTBVMn/DdGUkCY5TyGx0ZmxrU5E4w52Wjj9v+SRMaLMJag55e04y  
nzIXkhaZw2Cj3KxcV14ecLvajHMsw8e/+knB4ugEUsZL29DYfljtcAEcgYEAx3lt  
ukOP30Tx/4b2x+YutwOhoS6fuZi1NK8wIz9G0DZ7oy/Kafrede1vQzozRWm3kPKGd  
+DaFsraA+f53Sl0eW0/zXJ17nACbC0i/h6uj8kjR6jb2LhmsXV1GL8pAX4VtwLAjH  
tBuJfgYBtk0TqxBysUddWRs9mJe1M75AG-XruTcCgYAgbDykhn5ksohMagBfm0at  
YyG+a2bHqiH+Mf0Zr4kp/qGasImRZZIe6JnkIkcx7E0d9xlv6uKghUNXK6B00fj  
c7p0F7hB1oHPAk011LVECcSSDCpvDRi50+G0Xro1I0q1Ju55rqGkG0QRXiDaxUiE  
MTJiBvkwZ15zmUvCpoQAQKBgF/oHD/0dagJU+k9501b2N4Zmt66YgWEtKuWB5kK  
1SI13+AoHDQ0b8Td81k9D3KZG8GjGya6YDH31zTYluYxfyQ8ft3pHTvPZyBT8VSO  
yREqtjnsBMeMnd5b0OPBMBokMs6aIhqOp1zyWnRiTrCS3XHr9ADhvg3d6hjiwkQn  
mdyLAoGBAO6cZABTAF3wKwk0Wx05WrLU3qnM7MeL9fYbXA09he0ozNIcirpespq  
WR6nyfDU3CYe4v1hpoIz6kctKwlmokMJncGuCk4fXmqi+E4tnmixHc1RuWK2BcUq6  
U63Egr/xU5TRIZmMeLYiBoLN9w0DVGYBQ3zJlqmXIgFBriW0mBR6  
-----END RSA PRIVATE KEY-----  
~  
~
```

```
shreyaskayarkar@rahulraj-TravelMate-P214-53:~$ ssh -i "Downloads/NAT-instance.pem" ec2-user@52.3.223.244  
Last login: Fri Aug 4 09:45:27 2023 from 106.51.73.138  
  
_ _| _ _| )  
_ | ( _ _ / Amazon Linux AMI  
__| \ _ _|_|  
  
https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/  
8 package(s) needed for security, out of 12 available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-172-168-1-147 ~]$ hostname  
ip-172-168-1-147  
[ec2-user@ip-172-168-1-147 ~]$ █
```

After pasting the content of the private instance key pair to a new file, use the “chmod” command to change the permissions of the file.

```
[ec2-user@ip-172-168-1-147 ~]$ sudo vi privateInstancePEM.pem  
[ec2-user@ip-172-168-1-147 ~]$ sudo chmod 400 privateInstancePEM.pem  
[ec2-user@ip-172-168-1-147 ~]$ █
```

SSH into the private instance.

```
[ec2-user@ip-172-168-1-147 ~]$ sudo ssh -i privateInstancePEM.pem ec2-user@172.168.4.193
The authenticity of host '172.168.4.193 (172.168.4.193)' can't be established.
ECDSA key fingerprint is SHA256:cJwxh0QUP1qifWNjljcbuHa3GSIDCH+c5sUfDhf1IJE.
ECDSA key fingerprint is MD5:72:21:41:d9:29:38:40:cd:06:1a:64:b0:7f:02:9b:4d.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.168.4.193' (ECDSA) to the list of known hosts.

 _ _ | _ _ ) )
 _ | ( _ _ /   Amazon Linux 2 AMI
 _ _ \_ | _ |

https://aws.amazon.com/amazon-linux-2/
No packages needed for security; 2 packages available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-168-4-193 ~]$ clear
```

Step 15 - Install apache in the private instance then start and enable the apache service (httpd.service)

```
[root@ip-172-168-4-193 ec2-user]# systemctl start httpd
[root@ip-172-168-4-193 ec2-user]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@ip-172-168-4-193 ec2-user]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2023-08-04 11:46:30 UTC; 14s ago
     Docs: man:httpd.service(8)
 Main PID: 3672 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec: 0 B/sec"
   CGroup: /system.slice/httpd.service
           ├─3672 /usr/sbin/httpd -DFOREGROUND
           ├─3673 /usr/sbin/httpd -DFOREGROUND
           ├─3674 /usr/sbin/httpd -DFOREGROUND
           ├─3675 /usr/sbin/httpd -DFOREGROUND
           ├─3676 /usr/sbin/httpd -DFOREGROUND
           └─3677 /usr/sbin/httpd -DFOREGROUND

Aug 04 11:46:30 ip-172-168-4-193.ec2.internal systemd[1]: Starting The Apache HTTP Server...
Aug 04 11:46:30 ip-172-168-4-193.ec2.internal systemd[1]: Started The Apache HTTP Server.
```

Navigate to the document root file, which is index.html here. Edit the index.html file.

```
[ec2-user@ip-172-168-4-79 ~]$ cd /
[ec2-user@ip-172-168-4-79 /]$ cd var/www/html
[ec2-user@ip-172-168-4-79 html]$ ls
[ec2-user@ip-172-168-4-79 html]$ sudo vi index.html
[ec2-user@ip-172-168-4-79 html]$
```

Curl the private ip of the instance in the nat instance to check if the apache server is working correctly.

```
[ec2-user@ip-172-168-1-147 ~]$ curl 172.168.4.193
<!doctype html>
<html lang=en>
<head>
<meta charset=utf-8>
<title>Group 1 Project</title>
</head>
<body>
<h1>Axcess.io</h1>
<p>Akash</p>
<p>Shreyas</p>
<p>Cloud Engineers</p>
</body>
</html>

[ec2-user@ip-172-168-1-147 ~]$
```

Step 16 - Configure the cloudwatch agent in the private instance.

```
[ec2-user@ip-172-168-4-79 /]$ sudo yum install amazon-cloudwatch-agent -y
Last metadata expiration check: 0:11:03 ago on Fri Aug 4 10:21:28 2023.
Dependencies resolved.
=====
 Package                               Architecture      Version
=====
 Installing:
  amazon-cloudwatch-agent            x86_64          1.300025.0
Transaction Summary
=====
 Install 1 Package
```

```
[ec2-user@ip-172-168-4-193 ~]$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard
=====
= 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: [1]:
1
Trying to fetch the default region based on ec2 metadata...
Are you using EC2 or On-Premises hosts?
1. EC2
2. On-Premises
default choice: [1]:
1
Which user are you planning to run the agent?
1. root
2. cwagent
3. others
default choice: [1]:
1
Do you want to turn on StatsD daemon?
1. yes
2. no
default choice: [1]:
2
Do you want to monitor metrics from CollectD? WARNING: CollectD must be installed or the Agent will fail to start
1. yes
2. no
default choice: [1]:
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
```

```
Do you want to add ec2 dimensions (ImageId, InstanceId, InstanceType, AutoScalingGroupName) into all of your metrics if the info is available?
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 enables sub-minute resolution for all metrics, but you can customize for specific metrics in the output json file.
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]:
2
[...]
```

```
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
Do you have any existing CloudWatch Log Agent (http://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AgentReference.html) configuration file to import for migration?
1. yes
2. no
default choice: [2]:
2
Do you want to monitor any log files?
1. yes
2. no
default choice: [1]:
1
Log file path:
/var/log/httpd/access_log
Log group name:
default choice: [access_log]
/var/log/httpd/access_log
Log stream name:
default choice: [{instance_id}]
{instance_id}/httpd/access_log
```

```
22. 3288
23. 3653
default choice: [1]:
5
Do you want to specify any additional log files to monitor?
1. yes
2. no
default choice: [1]:
1
Log file path:
/var/log/httpd/error_log
Log group name:
default choice: [error_log]
/var/log/httpd/error_log
Log stream name:
default choice: [{instance_id}]
{instance_id}/httpd/error_log
```

```
default choice: [1]:
5
Do you want to specify any additional log files to monitor?
1. yes
2. no
default choice: [1]:
1
Log file path:
/var/log/messages
Log group name:
default choice: [messages]
/var/log/messages
Log stream name:
default choice: [{instance_id}]
{instance_id}/systemLogs/messages
```

```
default choice: [1]:  
5  
Do you want to specify any additional log files to monitor?  
1. yes  
2. no  
default choice: [1]:  
2  
Saved config file to /opt/aws/amazon-cloudwatch-agent/bin/config.json successfully.
```

```
Please check the above content of the config.  
The config file is also located at /opt/aws/amazon-cloudwatch-agent/bin/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  
Program exits now.
```

Edit the configuration file to group the metrics based on the ASG.

```
[ec2-user@ip-172-168-4-193 ~]$ sudo vi /opt/aws/amazon-cloudwatch-agent/bin/config.json
```

```
  "agent": {  
    "metrics_collection_interval": 60,  
    "run_as_user": "root"  
  },  
  "logs": {  
    "logs_collected": {  
      "files": [  
        "collect_list": [  
          {  
            "file_path": "/var/log/httpd/access_log",  
            "log_group_name": "/var/log/httpd/access_log",  
            "log_stream_name": "[{instance_id}]/httpd/access_log",  
            "retention_in_days": 7,  
            "timestamp_format": "%Y-%m-%d %H:%M:%S"  
          },  
          {  
            "file_path": "/var/log/httpd/error_log",  
            "log_group_name": "/var/log/httpd/error_log",  
            "log_stream_name": "[{instance_id}]/httpd/error_log",  
            "retention_in_days": 7,  
            "timestamp_format": "%Y-%m-%d %H:%M:%S"  
          },  
          {  
            "file_path": "/var/log/messages",  
            "log_group_name": "/var/log/messages",  
            "log_stream_name": "[{instance_id}]/systemLogs/messages",  
            "retention_in_days": 7,  
            "timestamp_format": "%Y-%m-%d %H:%M:%S"  
          }  
        ]  
      }  
    }  
  },  
},  
}
```

```

    "metrics": {
        "aggregation_dimensions": [
            [
                "InstanceId"
            ]
        ],
        "append_dimensions": [
            "AutoScalingGroupName": "${aws:AutoScalingGroupName}",
            "InstanceId": "${aws:InstanceId}"
        ],
        "metrics_collected": {
            "cpu": {
                "measurement": [
                    "cpu_usage_idle",
                    "cpu_usage_iowait",
                    "cpu_usage_user",
                    "cpu_usage_system"
                ],
                "metrics_collection_interval": 60,
                "totalcpu": false
            },
            "disk": {
                "measurement": [
                    "used_percent",
                    "inodes_free"
                ],
                "metrics_collection_interval": 60,
                "resources": [
                    "*"
                ]
            },
            "diskio": {
                "measurement": [
                    "io_time"
                ],
                "metrics_collection_interval": 60,
                "resources": [
                    "*"
                ]
            },
            "mem": {
                "measurement": [
                    "mem_used_percent"
                ]
            }
        }
    }
}

```

```

        "swap": {
            "measurement": [
                "swap_used_percent"
            ],
            "metrics_collection_interval": 60
        }
    }
}

```

Start the CloudWatch agent. Check if it's running or not.

```

[ec2-user@ip-172-168-4-193 ~]$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json
***** processing amazon-cloudwatch-agent *****
I: Trying to detect region from ec2 D! [EC2] Found active network interface Successfully fetched the config and saved in /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp
Start configuration validation...
2023/08/04 16:28:38 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp ...
2023/08/04 16:28:38 I! Valid Json input schema.
2023/08/04 16:28:38 D! ec2tagger processor required because append_dimensions is set
2023/08/04 16:28:38 D! delta processor required because metrics with diskio or net are set
2023/08/04 16:28:38 D! ec2tagger processor required because append_dimensions is set
2023/08/04 16:28:38 Configuration validation first phase succeeded
I: Detecting aws_as_user...
I: Trying to detect region from ec2
D! [EC2] Found active network interface
/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -schematest -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml
Configuration validation second phase succeeded
amazon-cloudwatch-agent has already been stopped
Created symlink from /etc/systemd/system/multi-user.target.wants/amazon-cloudwatch-agent.service to /etc/systemd/system/amazon-cloudwatch-agent.service.
[ec2-user@ip-172-168-4-193 ~]$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a status
{
    "status": "running",
    "starttime": "2023-08-04T16:20:39+0000",
    "configstatus": "configured",
    "version": "1.300025.0"
}

```

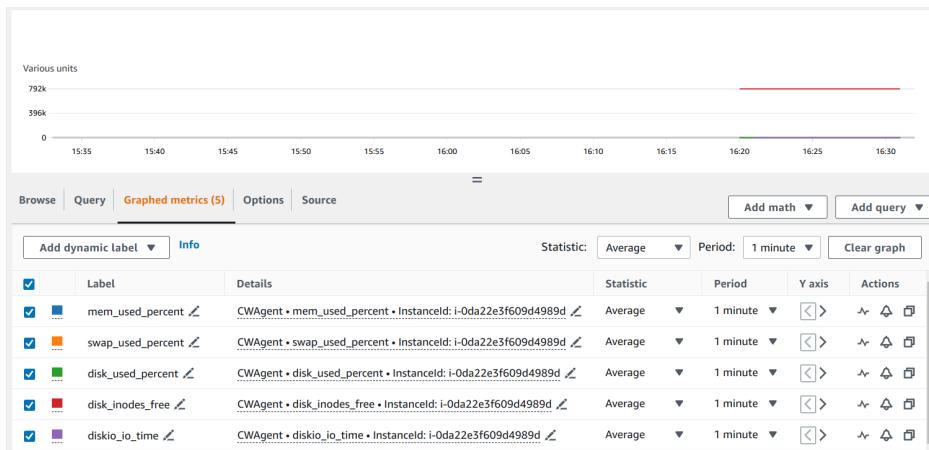
Step 17 - Check the cloudwatch for the logs.

The first screenshot shows the 'Log groups' page with three entries: '/var/log/httpd/access_log', '/var/log/httpd/error_log', and '/var/log/messages'. Each entry has a checkbox, a dropdown for 'Data protection', a dropdown for 'Sensitive data...', a dropdown for 'Retention' set to '1 week', a dropdown for 'Metric filters', and a dropdown for 'Contributor Insights'.

The second screenshot shows the 'Log streams' page with one entry: 'i-Oda22e3f609d4989d/httpd/access_log'. It includes a 'Last event time' of '2023-08-04 21:50:46 (UTC+05:30)'.

The third screenshot shows the 'Log events' page for the '/var/log/httpd/access_log' stream. It displays a single event from '2023-08-04T21:50:46.155+05:30' with the message: '172.168.1.147 - - [04/Aug/2023:11:49:04 +0000] "GET / HTTP/1.1" 200 192 "-" "curl/7.61.1"'. There is a 'Copy' button next to the message.

Metrics collected from the instance.



Step 18 - Create an AMI of the instance. This AMI will be used in the launch template of the ASG.

The screenshot shows the 'Create Image' step in the AWS EC2 console. The instance ID is listed as i-0da2e3f609d4989d (Project-VPC-PrivateServer-1a). The image name is set to 'Project-VPC-ApacheServer-AMI'. The image description is 'Linux 2 with Apache server and CloudWatch agent configured.' Under 'No reboot', the 'Enable' checkbox is checked. In the 'Instance volumes' section, there is one volume listed: an EBS volume of size 8 GB, type General Purpose S., IOPS 100, Throughput 100, Delete on termination enabled, and Encrypted disabled. A note at the bottom states: 'During the Image creation process, Amazon EC2 creates a snapshot of each of the above volumes.'

Step 19 - Create an S3 bucket which will be used to store the private IP addresses of the instances launched in the ASG.

The screenshot shows the 'Create bucket' step in the AWS S3 console. The bucket name is 'project-vpc-apache-asg-bucket'. The AWS Region is set to 'US East (N. Virginia) us-east-1'. Under 'Copy settings from existing bucket - optional', there is a link to 'See rules for bucket naming'. A 'Choose bucket' button is also present.

Step 20 - Create S3 gateway endpoint.

Any traffic for S3 bucket will go through the private IP on the AWS private network instead of the public internet. This is achieved by configuring the route tables of the private subnets to route traffic which have the destination of the S3 bucket to be forwarded through the endpoint as a target.

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.

Project-VPC-S3_GatewayEndpoint

Service category
Select the service category

AWS services
Services provided by Amazon

PrivateLink Ready partner services
Services with an AWS Service Ready designation

AWS Marketplace services
Services that you've purchased through AWS Marketplace

EC2 Instance Connect Endpoint
An elastic network interface that allow you to connect to resources in a private subnet

Other endpoint services
Find services shared with you by service name

Services (1/2)

Find resources by attribute or tag

Service Name = com.amazonaws.us-east-1.s3

Service Name	Owner	Type
com.amazonaws.us-east-1.s3	amazon	Gateway
com.amazonaws.us-east-1.s3	amazon	Interface

VPC
Select the VPC in which to create the endpoint

Route tables (3/5) Info

Name	Route Table ID	Main
-	rtb-042b7a6579fd03688	Yes
<input checked="" type="checkbox"/> Project-VPC-PrivateRT-1b	rtb-0904364de9b8b1eb2 (Project-VPC-...)	No
<input checked="" type="checkbox"/> Project-VPC-PrivateRT-1a	rtb-0579e91fb17dfff72 (Project-VPC-Pr...)	No
<input type="checkbox"/> Project-VPC-PublicRT	rtb-0666535f17e0b5476 (Project-VPC-...)	No
<input checked="" type="checkbox"/> Project-VPC-PrivateRT-1c	rtb-09a78f02cef8309f5 (Project-VPC-Pr...)	No

Endpoints (1/1) Info

Name	VPC endpoint ID	VPC ID	Service name
<input checked="" type="checkbox"/> Project-VPC-S3_Gatewa...	vpce-0978da159e62b87ff	vpc-03da74872e88be55a Project-VPC	com.amazonaws.us-east-1.s3

Step 21 - Create a launch template.

Attach the AMI created from the private instance to the launch template.

Launch template name and description

Launch template name - required
Project-VPC-ApacheServer-Template

Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '*', '@'.

Template version description
Apache server.

Max 255 chars

Recents | **My AMIs** | Quick Start

Don't include in launch template Owned by me

Shared with me

Amazon Machine Image (AMI)

Project-VPC-ApacheServer-AMI
ami-0c4927c2c48712852
2023-08-04T18:30:55.000Z Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Linux 2 with Apache server and CloudWatch agent configured.

Architecture AMI ID

x86_64 ami-0c4927c2c48712852

▼ Instance type [Info](#) Advanced

Instance type

t2.micro Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand RHEL pricing: 0.0716 USD per Hour
On-Demand Linux pricing: 0.0116 USD per Hour

All generations [Compare instance types](#)

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name

privateInstancePEM [Create new key pair](#)

▼ Network settings [Info](#)

Subnet Info

Don't include in launch template Create new subnet

When you specify a subnet, a network interface is automatically added to your template.

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Select existing security group Create security group

Security groups [Info](#)

Select security groups

Project-VPC-PrivateServer-SG sg-04036e3a9cf0b54c4 X [Compare security group rules](#)

► Advanced network configuration

▼ Advanced details [Info](#)

Purchasing option [Info](#)
 Request Spot Instances

IAM instance profile [Info](#)
ApacheServer-Role
arn:aws:iam::237042273450:instance-profile/ApacheServer-Role

Hostname type [Info](#)
IP name

Create new IAM profile

User data - *optional* [Info](#)
Upload a file with your user data or enter it in the field.

Choose file

```
#!/usr/bin/env python3

import subprocess
import logging
import boto3
import time
from botocore.exceptions import ClientError

# Configure logging
logging.basicConfig(level=logging.INFO, format='%(asctime)s - %(levelname)s - %(message)s')
logger = logging.getLogger(__name__)

# Set the AWS region and the log group name
aws_region = 'us-east-1'
```

User data has already been base64 encoded

The user data is a script written in python. Here the script uses the boto3 package to interact with the AWS services. The script here on first launch retrieves the private IP of the current instance by its instance id, then stores the instance id and private ip in key:value pair in a document stored in S3 bucket. Then the instance retrieves the IP addresses from the S3 bucket and runs ping operation on those IPs. It then sends the results to the Cloudwatch logs.

```
#!/usr/bin/env python3

import subprocess
import logging
import boto3
import requests
import time
from botocore.exceptions import ClientError
```

```

# Configure logging
logging.basicConfig(level=logging.INFO, format='%(asctime)s - %(levelname)s - %
(message)s')
logger = logging.getLogger(__name__)

# Set the AWS region and the log group name
aws_region = 'us-east-1'
log_group_name = 'apacheServers/pingResponse'
s3_bucket_name = "project-vpc-apache-asg-bucket"
s3_privateIp_file = "Project-VPC-ApacheASG-PrivateIPs.txt"

s3_client = boto3.client('s3', region_name=aws_region)

# Initialize CloudWatch Logs client and log stream name
cloudwatch_client = boto3.client('logs', region_name=aws_region)
log_stream_name = None

```

```

#get IPs from S3 bucket
def retrievePrivateIps_S3():
    try:
        response = s3_client.get_object(Bucket=s3_bucket_name, Key
            =s3_privateIp_file)
        json_bytes = response['Body'].read()
        json_string = json_bytes.decode('utf-8')
        private_ips = json.loads(json_string)

        return private_ips
    except Exception as e:
        logger.error(f"Error getting private IPs from S3 bucket: {e}")
        return []

```

```

# Function to ping other instances in the ASG
def ping_other_instances():
    try:
        privateIPs_list = retrievePrivateIps_S3().values()

```

```

        for privateIP in privateIPs_list:
            if privateIP == get_private_ip(get_current_instance_id()):
                # Skip pinging the current instance itself
                continue

            ping_command = ['ping', '-c', '4', privateIP]
            result = subprocess.run(ping_command, capture_output=True, text=True)

            # Push the ping results to CloudWatch Logs
            log_message = f"Ping from {get_current_instance_id()} to {privateIP}:
            {result.stdout.strip()}"

```

```

    push_to_cloudwatch_logs(log_message)

except Exception as e:
    logger.error(f"Error: {e}")

# Function to get the current EC2 instance ID
def get_current_instance_id():
    try:
        response = requests.get('http://169.254.169.254/latest/meta-data/instance
                               -id', timeout=2)
        response.raise_for_status()
        return response.text.strip()
    except requests.exceptions.RequestException as e:
        logger.error(f"Error getting instance ID: {e}")
        return None

# Function to get the private IP of an instance
def get_private_ip(instance_id):
    ec2_resource = boto3.resource('ec2', region_name=aws_region)
    instance = ec2_resource.Instance(instance_id)
    return instance.private_ip_address

# Function to get the log stream name for the current instance
def get_log_stream_name():
    global log_stream_name

```

```

if log_stream_name is None:
    log_stream_name = get_current_instance_id()

try:
    response = cloudwatch_client.describe_log_streams(
        logGroupName=log_group_name,
        logStreamNamePrefix=log_stream_name,
        limit=1
    )
    if 'logStreams' in response:
        for stream in response['logStreams']:
            if stream['logStreamName'] == log_stream_name:
                return log_stream_name

    # If log stream doesn't exist, create a new one
    cloudwatch_client.create_log_stream(logGroupName=log_group_name,
                                         logStreamName=log_stream_name)
    return log_stream_name

except ClientError as e:
    logger.error(f"Error retrieving log stream name: {e}")

return log_stream_name

```

```

# Function to push logs to CloudWatch Logs
def push_to_cloudwatch_logs(log_message):
    log_stream_name = get_log_stream_name()

    try:
        cloudwatch_client.put_log_events(
            logGroupName=log_group_name,
            logStreamName=log_stream_name,
            logEvents=[{'timestamp': int(time.time() * 1000), 'message': log_message}]
        )
        logger.info(f"Pushed logs to CloudWatch Logs: {log_message}")
    except ClientError as e:
        logger.error(f"Error pushing logs to CloudWatch Logs: {e}")

```

```

def main():
    instance_id = get_current_instance_id()
    currentInstance_privateIP = get_private_ip(instance_id)
    objectList = s3_client.list_objects(Bucket=s3_bucket_name)
    objects = []
    try:
        for file in objectList['Contents']:
            objects.append(file['Key'])
    except KeyError as e:
        pass

    if s3_privateIp_file not in objects:
        s3_client.put_object(Bucket=s3_bucket_name, Key=s3_privateIp_file)

    response = s3_client.get_object(Bucket=s3_bucket_name, Key=s3_privateIp_file)
    json_bytes = response['Body'].read()

    # Convert bytes to a string
    json_string = json_bytes.decode('utf-8')

    # Parse the JSON string
    existingIps = json.loads(json_string)

```

```

if instance_id not in existingIps.keys():
    existingIps[instance_id] = currentInstance_privateIP
    updatedIps = json.dumps(existingIps, indent=2)
    s3_client.put_object(Bucket=s3_bucket_name, Key=s3_privateIp_file,
                         Body=updatedIps)

while True:
    ping_other_instances()

    time.sleep(60)

if __name__ == "__main__":
    main()

```

Step 22 - Create an Auto Scaling Group.

Name

Auto Scaling group name
Enter a name to identify the group.

Must be unique to this account in the current Region and no more than 255 characters.

Launch template [Info](#) [Switch to launch configuration](#)

Launch template
Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

[▼](#) [C](#)

[Create a launch template](#)

Version
 [▼](#) [C](#)

[Create a launch template version](#)

Description Apache server.	Launch template Project-VPC-ApacheServer-Template 	Instance type t2.micro
-------------------------------	---	---------------------------

Select the three private subnets for the private instances.

Network [Info](#)

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC
Choose the VPC that defines the virtual network for your Auto Scaling group.
 [▼](#) [C](#)

[Create a VPC](#)

Availability Zones and subnets
Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

[▼](#) [C](#)

us-east-1a subnet-0d0191134f251c85e (Project-VPC-Private-1a) 172.168.4.0/24	X
us-east-1b subnet-01848f693e9b8798f (Project-VPC-Private-1b) 172.168.5.0/24	X
us-east-1c subnet-0e602f51fd6da63f7 (Project-VPC-Private-1c) 172.168.6.0/24	X

[Create a subnet](#)

Create an Application Load Balancer which will distribute the incoming traffic on apache server to the instances launched in the ASG.

Load balancing [Info](#)

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

No load balancer
Traffic to your Auto Scaling group will not be fronted by a load balancer.

Attach to an existing load balancer
Choose from your existing load balancers.

Attach to a new load balancer
Quickly create a basic load balancer to attach to your Auto Scaling group.

Attach to a new load balancer

Define a new load balancer to create for attachment to this Auto Scaling group.

Load balancer type
Choose from the load balancer types offered below. Type selection cannot be changed after the load balancer is created. If you need a different type of load balancer than those offered here, visit the [Load Balancing console](#).

Application Load Balancer
HTTP, HTTPS

Network Load Balancer
TCP, UDP, TLS

Load balancer name
Name cannot be changed after the load balancer is created.

Project-VPC-Apache-ALB

Load balancer scheme
Scheme cannot be changed after the load balancer is created.

Internal

Internet-facing

Network mapping
Your new load balancer will be created using the same VPC and Availability Zone selections as your Auto Scaling group. You can select different subnets and add subnets from additional Availability Zones.

VPC
[vpc-03da74872e88be55a](#) [Project-VPC](#)

Availability Zones and subnets
You must select a single subnet for each Availability Zone enabled. Only public subnets are available for selection to support DNS resolution.

us-east-1a

us-east-1c

us-east-1b

Listeners and routing
If you require secure listeners, or multiple listeners, you can configure them from the [Load Balancing console](#) after your load balancer is created.

Protocol	Port	Default routing (forward to)
HTTP	80	<input type="text" value="Create a target group"/>

New target group name
An instance target group with default settings will be created.

Project-VPC-Apache-TG

Health check grace period | [Info](#)
 This time period delays the first health check until your instances finish initializing. It doesn't prevent an instance from terminating when placed into a non-running state.

20	seconds
----	---------

Additional settings

Monitoring | [Info](#)
 Enable group metrics collection within CloudWatch

Default instance warmup | [Info](#)
 The amount of time that CloudWatch metrics for new instances do not contribute to the group's aggregated instance metrics, as their usage data is not reliable yet.

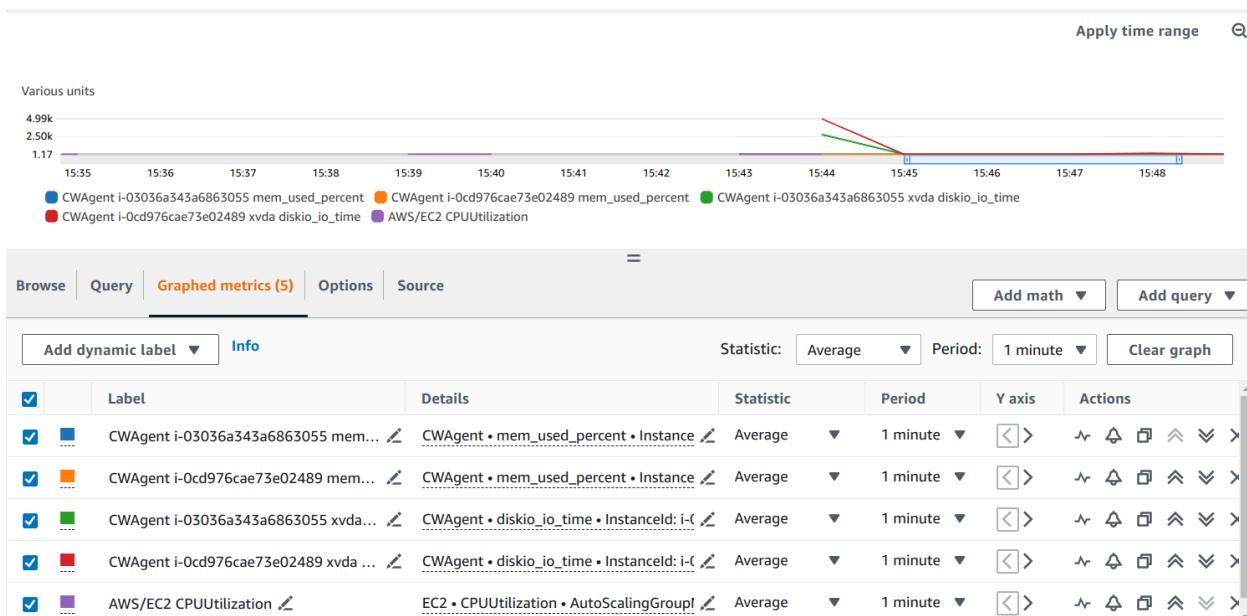
<input type="checkbox"/> Enable default instance warmup

[Cancel](#) [Skip to review](#) [Previous](#) [Next](#)

Project-VPC-ApacheASG

Details	Activity	Automatic scaling	Instance management	Monitoring	Instance refresh																								
<p>Instances (2)</p> <table border="1"> <thead> <tr> <th colspan="2"></th> <th colspan="2">Filter instances</th> <th colspan="2"></th> </tr> <tr> <th></th> <th>Instance ID</th> <th>Lifecycle</th> <th>Instance...</th> <th>Weighted...</th> <th>Launch template/configuration</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>i-03036a343a6863055</td> <td>InService</td> <td>t2.micro</td> <td>-</td> <td>Project-VPC-ApacheServer-Template Version 4 us-east-1a</td> </tr> <tr> <td><input type="checkbox"/></td> <td>i-0cd976cae73e02489</td> <td>InService</td> <td>t2.micro</td> <td>-</td> <td>Project-VPC-ApacheServer-Template Version 4 us-east-1c</td> </tr> </tbody> </table>								Filter instances					Instance ID	Lifecycle	Instance...	Weighted...	Launch template/configuration	<input type="checkbox"/>	i-03036a343a6863055	InService	t2.micro	-	Project-VPC-ApacheServer-Template Version 4 us-east-1a	<input type="checkbox"/>	i-0cd976cae73e02489	InService	t2.micro	-	Project-VPC-ApacheServer-Template Version 4 us-east-1c
		Filter instances																											
	Instance ID	Lifecycle	Instance...	Weighted...	Launch template/configuration																								
<input type="checkbox"/>	i-03036a343a6863055	InService	t2.micro	-	Project-VPC-ApacheServer-Template Version 4 us-east-1a																								
<input type="checkbox"/>	i-0cd976cae73e02489	InService	t2.micro	-	Project-VPC-ApacheServer-Template Version 4 us-east-1c																								

After the instances are launched it sends metrics to cloudwatch based on the Auto Scaling Group name. As it was configured in the custom AMI.



Log groups (4)						
By default, we only load up to 10000 log groups.						
<input type="button" value="C"/> Actions ▾		<input type="button" value="View in Logs Insights"/>		<input type="button" value="Start tailing"/>		<input type="button" value="Create log group"/>
<input type="text" value="Filter log groups or try prefix search"/> <input type="checkbox"/> Exact match ◀ 1 ▶ ⚙						
<input type="checkbox"/>	Log group	Data protection	Sensitive data...	Retention	Metric filters	Contributor
<input type="checkbox"/>	/var/log/httpd/access_log	-	-	1 week	-	-
<input type="checkbox"/>	/var/log/httpd/error_log	-	-	1 week	-	-
<input type="checkbox"/>	/var/log/messages	-	-	1 week	-	-
<input type="checkbox"/>	apacheServers/pingResponse	-	-	1 week	-	-

Application access and error logs from the Apache server running on the instance.

Log streams (2)							
CloudWatch > Log groups > /var/log/httpd/access_log > i-0cd976cae73e02489/httpd/access_log							
Log streams (2)							
<input type="text" value="Filter log streams or try prefix search"/> <input type="checkbox"/> Exact match <input type="checkbox"/> Show expired Info ◀ 1 ▶ ⚙							
<input type="checkbox"/>	Log stream	Last event time					
<input type="checkbox"/>	i-0cd976cae73e02489/httpd/access_log	2023-08-05 15:43:51 (UTC+05:30)					
<input type="checkbox"/>	i-03036a343a6863055/httpd/access_log	2023-08-05 15:43:16 (UTC+05:30)					

Log events							
CloudWatch > Log groups > /var/log/httpd/access_log > i-0cd976cae73e02489/httpd/access_log							
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 Retry							
<input type="button" value="C"/> Actions ▾	<input type="button" value="Start tailing"/>	<input type="button" value="Create metric filter"/>	<input type="text" value="Filter events"/>	<input type="button" value="Clear"/>	<input type="button" value="1m"/>	<input type="button" value="30m"/>	
<input type="text" value="Filter events"/>	<input type="button" value="Clear"/>	<input type="button" value="1m"/>	<input type="button" value="30m"/>	<input type="button" value="1h"/>	<input type="button" value="12h"/>	<input type="button" value="Custom"/> Display ▾ ⚙	
<input type="checkbox"/>	Timestamp	Message					
	No older events at this moment. Retry						
<input type="checkbox"/>	2023-08-05T15:43:46.543+05:30	172.168.2.40 - - [05/Aug/2023:10:13:46 +0000] "GET / HTTP/1.1" 200 192 "-" "ELB-HealthChecker/2.0"					
<input type="checkbox"/>	2023-08-05T15:43:46.543+05:30	172.168.1.84 - - [05/Aug/2023:10:13:46 +0000] "GET / HTTP/1.1" 200 192 "-" "ELB-HealthChecker/2.0"					
<input type="checkbox"/>	2023-08-05T15:43:51.010+05:30	172.168.3.204 - - [05/Aug/2023:10:13:46 +0000] "GET / HTTP/1.1" 200 192 "-" "ELB-HealthChecker/2.0"					
<input type="checkbox"/>	2023-08-05T15:44:16.614+05:30	172.168.1.84 - - [05/Aug/2023:10:14:16 +0000] "GET / HTTP/1.1" 200 192 "-" "ELB-HealthChecker/2.0"					

Log events							
CloudWatch > Log groups > /var/log/httpd/error_log > i-0416ed65478135536/httpd/error_log							
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 Retry							
<input type="button" value="C"/> Actions ▾	<input type="button" value="Start tailing"/>	<input type="button" value="Create metric filter"/>	<input type="text" value="Filter events"/>	<input type="button" value="Clear"/>	<input type="button" value="1m"/>	<input type="button" value="30m"/>	
<input type="text" value="Filter events"/>	<input type="button" value="Clear"/>	<input type="button" value="1m"/>	<input type="button" value="30m"/>	<input type="button" value="1h"/>	<input type="button" value="12h"/>	<input type="button" value="Custom"/> Display ▾ ⚙	
<input type="checkbox"/>	Timestamp	Message					
	No older events at this moment. Retry						
<input type="checkbox"/>	2023-08-05T19:17:32.308+05:30	[Sat Aug 05 13:47:28.346155 2023] [suexec:notice] [pid 2960] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/...					
<input type="checkbox"/>	2023-08-05T19:17:32.308+05:30	[Sat Aug 05 13:47:28.375795 2023] [lmbmethod_heartbeat:notice] [pid 2960] AH02282: No slotmem from mod_heartmonitor					
<input type="checkbox"/>	2023-08-05T19:17:32.308+05:30	[Sat Aug 05 13:47:28.376151 2023] [http2:warn] [pid 2960] AH10034: The mpm module (prefork.c) is not supported by m...					
<input type="checkbox"/>	2023-08-05T19:17:32.308+05:30	[Sat Aug 05 13:47:28.382353 2023] [mpm_prefork:notice] [pid 2960] AH00163: Apache/2.4.57 () configured -- resuming ...					

System logs from the instances.

The screenshot shows the CloudWatch Log Events interface for the log group /var/log/messages. The log entries are as follows:

Timestamp	Message
2023-08-05T15:43:16.762+05:30	Aug 5 10:13:09 ip-172-168-4-193 dhclient[2947]: XMT: Solicit on eth0, interval 2000ms.
2023-08-05T15:43:16.762+05:30	Aug 5 10:13:09 ip-172-168-4-193 dbus[2613]: [system] Activating via systemd: service name='org.freedesktop.hostname...
2023-08-05T15:43:16.762+05:30	Aug 5 10:13:09 ip-172-168-4-193 systemd[1]: Starting Hostname Service...
2023-08-05T15:43:16.762+05:30	Aug 5 10:13:10 ip-172-168-4-193 kernel: xfs filesystem being remounted at /tmp supports timestamps until 2038 (0x...

The instances ping other instances every minute and send logs to the cloudwatch.

The screenshot shows the CloudWatch Log Events interface for the log group apacheServers/pingResponse. The log entries are as follows:

Timestamp	Message
2023-08-05T15:48:34.262+05:30	Ping from i-03036a343a6863055 to 172.168.6.207: PING 172.168.6.207 (172.168.6.207) 56(84) bytes of data. --- 172...
2023-08-05T15:48:47.606+05:30	Ping from i-03036a343a6863055 to 172.168.6.5: PING 172.168.6.5 (172.168.6.5) 56(84) bytes of data. --- 172.168.6...
2023-08-05T15:50:01.463+05:30	Ping from i-03036a343a6863055 to 172.168.6.207: PING 172.168.6.207 (172.168.6.207) 56(84) bytes of data. --- 172...
2023-08-05T15:51:15.190+05:30	Ping from i-03036a343a6863055 to 172.168.6.207: PING 172.168.6.207 (172.168.6.207) 56(84) bytes of data. --- 172...

Step 23 - Create ASG memory based alarm and scaling policy to launch a new instance whenever the memory usage goes over 50% of threshold.

The screenshot shows the 'Create dynamic scaling policy' wizard. The steps completed are:

- Policy type: Simple scaling
- Scaling policy name: Project-VPC-ASG-MemoryUsage
- CloudWatch alarm: Choose an alarm that can scale capacity whenever: (dropdown menu)
- Create a CloudWatch alarm
- Take the action:
 - Add: 1 capacity units
- And then wait:
 - 20 seconds before allowing another scaling activity

After creating dynamic simple scaling policy in the ASG, create an alarm in CloudWatch.

The screenshot shows the 'Select metric' interface in the AWS CloudWatch Metrics console. At the top, there's a breadcrumb navigation: 'All > CWAgent > AutoScalingGroupName'. Below it is a search bar with placeholder text 'Search for any metric, dimension, resource id or account id'. The main area displays a list of metrics under the heading 'AutoScalingGroupName 10/10'. The metrics listed are: 'Project-VPC-ApacheASG diskio io_time', 'Project-VPC-ApacheASG mem_used_percent' (which is checked and highlighted), 'Project-VPC-ApacheASG swap_used_percent', 'Project-VPC-ApacheASG disk_used_percent', and 'Project-VPC-ApacheASG disk_inodes_free'.

The alarm will be in “in-alarm” state if the metric value crosses the threshold of 50%.

The screenshot shows the 'Conditions' step in the CloudWatch Metrics creation wizard. Under 'Threshold type', the 'Static' option is selected, with the sub-instruction 'Use a value as a threshold'. The 'Anomaly detection' option is also present but not selected. Below this, the condition 'Whenever mem_used_percent is...' is defined. The 'Greater > threshold' radio button is selected, and the value '50' is entered into the input field. The other three options ('Greater/Equal', 'Lower/Equal', 'Lower < threshold') are shown as unselected radio buttons. A note below says 'Must be a number'. At the bottom right of the step, there are 'Cancel' and 'Next' buttons.

The alarm will trigger auto scaling action.

The screenshot shows the 'Auto Scaling action' step in the CloudWatch Metrics creation wizard. Under 'Alarm state trigger', the 'In alarm' radio button is selected, with the sub-instruction 'The metric or expression is outside of the defined threshold.' The 'OK' and 'Insufficient data' options are also present but not selected. In the 'Resource type' section, 'EC2 Auto Scaling group' is selected, while 'ECS Service' is unselected. The 'Select a group' dropdown is set to 'Project-VPC-ApacheASG'. A note below says 'Only Auto Scaling groups with a simple scaling or step scaling policy in this account are available.' Under 'Take the following action...', the dropdown is set to 'Project-VPC-ASG-MemoryUsage (Add 1 instance)'. A note below says 'Only actions for the selected Auto Scaling group are available.' At the bottom right, there is an 'Add Auto Scaling action' button.

Name of the alarm.

Add name and description

Name and description

Alarm name
Project-VPC-ApacheASG-MemoryUsage

Alarm description - optional [View formatting guidelines](#)

Edit **Preview**

```
# This is an H1
**double asterisks will produce strong character**
This is [an example](https://example.com/) inline link.
```

Up to 1024 characters (0/1024)

Info Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.

CloudWatch > Alarms					
Alarms (1)		Actions		Create alarm	
<input type="checkbox"/> Search		<input type="button" value="Any state"/> <input type="button" value="Any type"/> <input type="button" value="Any actions ..."/>		<input type="button" value="Actions"/>	
<input type="checkbox"/>	Name	State	Last state update	Conditions	Actions
<input type="checkbox"/>	Project-VPC-ApacheASG-MemoryUsage	 OK	2023-08-07 05:35:42	mem_used_percent > 50 for 1 datapoints within 5 minutes	 Actions enabled

Step 24 - Create metric filters in the application log group to catch errors and exceptions.

The filter pattern will catch the logs which contain 4xx and 5xx status codes.

Define pattern

Create filter pattern
You can use metric filters to monitor events in a log group as they are sent to CloudWatch Logs. You can monitor and count specific terms or extract values from log events and associate the results with a metric. [Learn more about pattern syntax.](#)

Filter pattern
Specify the terms or pattern to match in your log events to create metrics.

```
[host, logName, user, timestamp, request, statusCode=4* || statusCode=5*, size]
```

Create filter name

Log events that match the pattern you define are recorded to the metric that you specify. You can graph the metric and set alarms to notify you.

Filter name
Project-VPC-ApacheAccessErrorFilter

Filter pattern
[host, logName, user, timestamp, request, statusCode=4* || statusCode=5*, size]

Metric details

Metric namespace
Namespaces let you group similar metrics. [Learn more](#)

Project-VPC-ApacheLogs Create new

Namespaces can be up to 255 characters long; all characters are valid except for colon(:) at the start of the name.

Metric name
Metric name identifies this metric, and must be unique within the namespace. [Learn more](#)

Project-VPC-ApacheAccess_ErrorMetric

Metric name can be up to 255 characters long; all characters are valid except for colon(:), asterisk(*), dollar(\$), and space().

Metric value
Metric value is the value published to the metric name when a Filter Pattern match occurs.

1

Valid metric values are: floating point number (1, 99.9, etc.), numeric field identifiers (\$1, \$2, etc.), or named field identifiers (e.g. \$host, \$logName, \$user, \$timestamp, \$request, \$statusCode, \$size).

Step 25 - Create an alarm on the metric filter, which will be triggered whenever the filter catches a matching event.

Metric filters (1)

[Edit](#) [Delete](#) [Create alarm](#) [Create metric filter](#)

Find metric filters

Project-VPC-ApacheAccessErrorFilter <input checked="" type="checkbox"/>
Filter pattern [host, logName, user, timestamp, request, statusCode=4* statusCode=5*, size]
Metric Project-VPC-ApacheLogs / Project-VPC-ApacheAccess_ErrorMetric
Metric value 1
Default value -
Unit -
Dimensions -
Alarms None.

Conditions

Threshold type

Static
Use a value as a threshold

Anomaly detection
Use a band as a threshold

Whenever Project-VPC-ApacheAccess_ErrorMetric is...

Define the alarm condition.

Greater
> threshold

Greater/Equal
>= threshold

Lower/Equal
<= threshold

Lower
< threshold

than...

Define the threshold value.

1

Must be a number

► Additional configuration

Cancel **Next**

Notification

Alarm state trigger

Define the alarm state that will trigger this action.

In alarm
The metric or expression is outside of the defined threshold.

OK
The metric or expression is within the defined threshold.

Insufficient data
The alarm has just started or not enough data is available.

Remove

Send a notification to the following SNS topic

Define the SNS (Simple Notification Service) topic that will receive the notification.

Select an existing SNS topic

Create new topic

Use topic ARN to notify other accounts

Send a notification to...

Project-VPC-ApacheServer_AlarmSNS

Only email lists for this account are available.

Email (endpoints)

skayarkar89@gmail.com - [View in SNS Console](#)

Add notification

Add name and description

Name and description

Alarm name

Project-VPC-ApacheAccessErrorAlarm

Alarm description - optional [View formatting guidelines](#)

Edit | Preview

Subscriptions (1)

Edit Delete Request confirmation Confirm

Search

ID	Endpoint	Status
00612938-eea9-40ec-b977-b8b...	skayarkar89@gmail.com	Confirmed

The alarm is in “in-alarm” state because previously the log group recorded one log with 404 status code, which crosses the threshold limit of 1.

Alarms (2)					<input type="checkbox"/> Hide Auto Scaling alarms	<input type="button" value="Clear selection"/>	<input type="button" value="C"/>	<input type="button" value="Create composite alarm"/>	<input type="button" value="Actions"/>	<input type="button" value=""/>
	<input type="text"/> Search	<input type="button" value="Any state"/>	<input type="button" value="Any type"/>	<input type="button" value="Any actions ..."/>						
<input type="checkbox"/>	Name	State	Last state update	Conditions						
<input type="checkbox"/>	Project-VPC-ApacheAccessErrorAlarm	⚠ In alarm	2023-08-07 06:06:50	Project-VPC-ApacheAccess_ErrorMetric >= 1 for 1 datapoints within 5 minutes						Actions enabled

ALARM: "Project-VPC-ApacheAccessErrorAlarm" in US East (N. Virginia) Inbox ×

 AWS Notifications <no-reply@sns.amazonaws.com>
to me ▾ 11:36 AM (0 minutes ago) ⚡ ⓘ ⌂ ⌃

You are receiving this email because your Amazon CloudWatch Alarm "Project-VPC-ApacheAccessErrorAlarm" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [3.0 (07/08/23 06:01:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Monday 07 August, 2023 06:06:50 UTC".

View this alarm in the AWS Management Console:
<https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarmsV2:alarm/Project-VPC-ApacheAccessErrorAlarm>

Alarm Details:

- Name: Project-VPC-ApacheAccessErrorAlarm
- Description:
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [3.0 (07/08/23 06:01:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Monday 07 August, 2023 06:06:50 UTC
- AWS Account: 237042273450
- Alarm Arn: arn:aws:cloudwatch:us-east-1:237042273450:alarm:Project-VPC-ApacheAccessErrorAlarm

Threshold:

Step 26 - Metric filter for system logs with warning and error.

/var/log/messages > Create metric filter

Define pattern

Create filter pattern
You can use metric filters to monitor events in a log group as they are sent to CloudWatch Logs. You can monitor and count specific terms or extract values from log events and associate the results with a metric. [Learn more about pattern syntax.](#) ⓘ

Filter pattern
Specify the terms or pattern to match in your log events to create metrics.
"Warning:"

Create filter name
Log events that match the pattern you define are recorded to the metric that you specify. You can graph the metric and set alarms to notify you.

Filter name
Project-VPC-ApacheSystemLog_Warnings

Filter pattern
"Warning:"

Metric details

Metric namespace
Namespaces let you group similar metrics. [Learn more](#)

 Create new
 Namespaces can be up to 255 characters long; all characters are valid except for colon(:) at the start of the name.

Metric name
Metric name identifies this metric, and must be unique within the namespace. [Learn more](#)

 Metric name can be up to 255 characters long; all characters are valid except for colon(:), asterisk(*), dollar(\$), and space().

Metric value
Metric value is the value published to the metric name when a Filter Pattern match occurs.

 Valid metric values are: floating point number (1, 99.9, etc.), numeric field identifiers (\$1, \$2, etc.), or named field identifiers (e.g.

Conditions

Threshold type

Static
Use a value as a threshold

Anomaly detection
Use a band as a threshold

Whenever Project-VPC-ApacheSystemWarningMetric is...
Define the alarm condition.

Greater
> threshold

Greater/Equal
>= threshold

Lower/Equal
<= threshold

Lower
< threshold

than...
Define the threshold value.

 Must be a number

► Additional configuration

Notification

Alarm state trigger
Define the alarm state that will trigger this action.

In alarm
The metric or expression is outside of the defined threshold.

OK
The metric or expression is within the defined threshold.

Insufficient data
The alarm has just started or not enough data is available.

Remove

Send a notification to the following SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.

Select an existing SNS topic

Create new topic

Use topic ARN to notify other accounts

Send a notification to...

Only email lists for this account are available.

Email (endpoints)
skayarkar89@gmail.com - [View in SNS Console](#)

Name and description

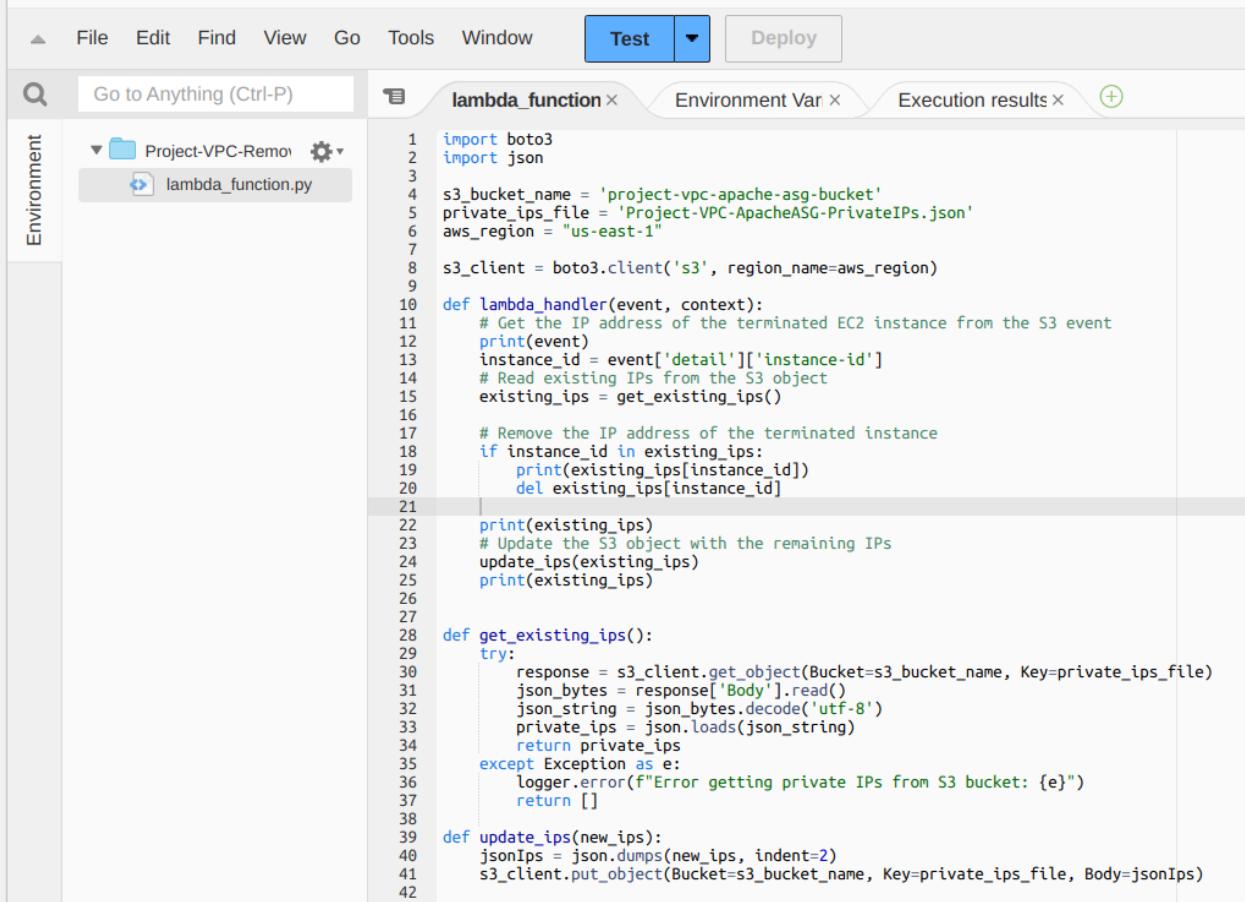
Alarm name
Project-VPC-ApacheSystemWarning_Alarm

Alarm description - optional [View formatting guidelines](#)

[Edit](#) | [Preview](#)

Step 27 - Create an event bridge rule to track EC2 termination events and delete the private IP entry for that instance from the s3 bucket.

Lambda for the event trigger. The lambda function will retrieve the instance id of the terminated instances from the event record. Then delete the matching record in the S3 document of private IPs and again upload the modified document to S3.



```

File Edit Find View Go Tools Window Test Deploy
Go to Anything (Ctrl-P)
lambda_function Environment Var Execution results +
Environment Project-VPC-Removal lambda_function.py
1 import boto3
2 import json
3
4 s3_bucket_name = 'project-vpc-apache-asg-bucket'
5 private_ips_file = 'Project-VPC-ApacheASG-PrivateIPs.json'
6 aws_region = "us-east-1"
7
8 s3_client = boto3.client('s3', region_name=aws_region)
9
10 def lambda_handler(event, context):
11     # Get the IP address of the terminated EC2 instance from the S3 event
12     print(event)
13     instance_id = event['detail']['instance-id']
14     # Read existing IPs from the S3 object
15     existing_ips = get_existing_ips()
16
17     # Remove the IP address of the terminated instance
18     if instance_id in existing_ips:
19         print(existing_ips[instance_id])
20         del existing_ips[instance_id]
21
22     print(existing_ips)
23     # Update the S3 object with the remaining IPs
24     update_ips(existing_ips)
25     print(existing_ips)
26
27
28 def get_existing_ips():
29     try:
30         response = s3_client.get_object(Bucket=s3_bucket_name, Key=private_ips_file)
31         json_bytes = response['Body'].read()
32         json_string = json_bytes.decode('utf-8')
33         private_ips = json.loads(json_string)
34         return private_ips
35     except Exception as e:
36         logger.error(f"Error getting private IPs from S3 bucket: {e}")
37         return []
38
39 def update_ips(new_ips):
40     jsonIps = json.dumps(new_ips, indent=2)
41     s3_client.put_object(Bucket=s3_bucket_name, Key=private_ips_file, Body=jsonIps)
42

```

The rule will catch instance termination events and trigger the lambda function.

Define rule detail Info

Rule detail

Name
Project-VPC-ApacheASG-TerminationRule
Maximum of 64 characters consisting of numbers, lower/upper case letters, .,-_.

Description - *optional*
Enter description

Event bus Info
Select the event bus this rule applies to, either the default event bus or a custom or partner event bus.
default

Enable the rule on the selected event bus

Rule type Info
 Rule with an event pattern A rule that runs when an event matches the defined event pattern. EventBridge sends the event to the specified target.
 Schedule A rule that runs on a schedule

Cancel **Next**

Event pattern Info

Event source
AWS service or EventBridge partner as source
AWS services

AWS service
The name of the AWS service as the event source
EC2

Event type
The type of events as the source of the matching pattern
EC2 Instance State-change Notification

Any state
 Specific state(s)

shutting-down X terminated X

Event pattern
Event pattern, or filter to match the events

```
1 {
2   "source": ["aws.ec2"],
3   "detail-type": ["EC2 Instance State-change Notificat
4   "detail": {
5     "state": ["shutting-down", "terminated"]
6   }
7 }
```

Copy **Test pattern** **Edit pattern**

Target 1

Target types
Select an EventBridge event bus, EventBridge API destination (SaaS partner), or another AWS service as a target.

- EventBridge event bus
- EventBridge API destination
- AWS service

Select a target | [Info](#)
Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule)

Lambda function ▾

Function

Project-VPC-RemoveIP ▾ [C](#)

▶ Configure version/alias

▶ Additional settings

Add another target Cancel Skip to Review and create Previous **Next**

Step 28 - Currently the file which stores the private IPs of the instances contain the following.

```
{
  "i-0fc16f1715e280016": "172.168.6.244",
  "i-0312b9ff8fea4df50": "172.168.5.124",
  "i-09df76abd2e0350ff": "172.168.4.34"
}
```

After changing the desired capacity of the ASG back to two, one of the instances will be terminated and through the event bridge rule, this event will trigger the lambda function to remove the associated IP address from the bucket object.

```

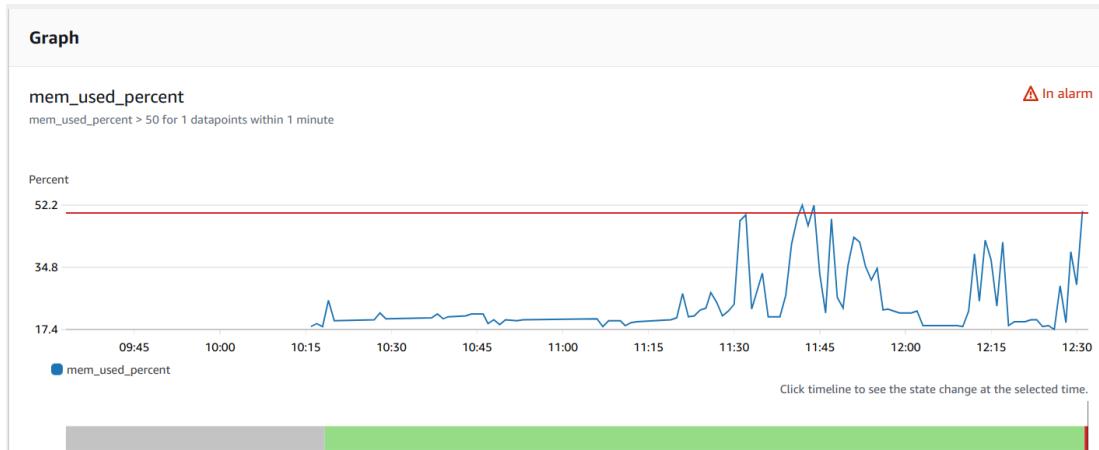
  "i-0fc16f1715e280016": "172.168.6.244",
  "i-09df76abd2e0350ff": "172.168.4.34"
```

Filter instances

<input type="checkbox"/>	Instance ID	▲	Lifecycle	▼	Instance...	▼	V
<input type="checkbox"/>	i-09df76abd2e0350ff E		InService		t2.micro		-
<input type="checkbox"/>	i-0fc16f1715e280016 E		InService		t2.micro		-

Step 29 - Check the memory based auto scaling policy. Run stress command in one of the private instances in the ASG.

```
[root@ip-172-168-5-124 /]# stress -c 2 -i 1 -m 1 --vm-bytes 558M  
stress: info: [4347] dispatching hogs: 2 cpu, 1 io, 1 vm, 0 hdd
```



The alarm turns to “in-alarm” state and triggers the auto scaling which launches one more instance.

Instances (3)										<input type="button" value="Create"/>	<input type="button" value="Actions ▾"/>		
<input type="text"/> Filter instances										<	1	>	<input type="button" value="Settings"/>
	Instance ID	Lifecycle	Instance Type	Weighted Capacity	Launch Configuration	Availability Zone	Health Status	Protected From Auto Scaling					
<input type="checkbox"/>	i-0312b9ff8fea4df50	InService	t2.micro	-	Project-VPC-Ap-	us-east-1b	Healthy	<input checked="" type="checkbox"/>					
<input type="checkbox"/>	i-09df76abd2e0350ff	InService	t2.micro	-	Project-VPC-Ap-	us-east-1a	Healthy	<input checked="" type="checkbox"/>					
<input type="checkbox"/>	i-0fc16f1715e280016	InService	t2.micro	-	Project-VPC-Ap-	us-east-1c	Healthy	<input checked="" type="checkbox"/>					

Below the table, a summary row provides details for the new instance:

- i-09df76abd2e0350ff Running t2.micro Initializing No alarms + us-east-1a