



DEPI AWS Project Documentation

Presented By:

Noha Ashraf Abdel Baky
Ali Mohsen Ali Saleh

Under supervision of / NTI

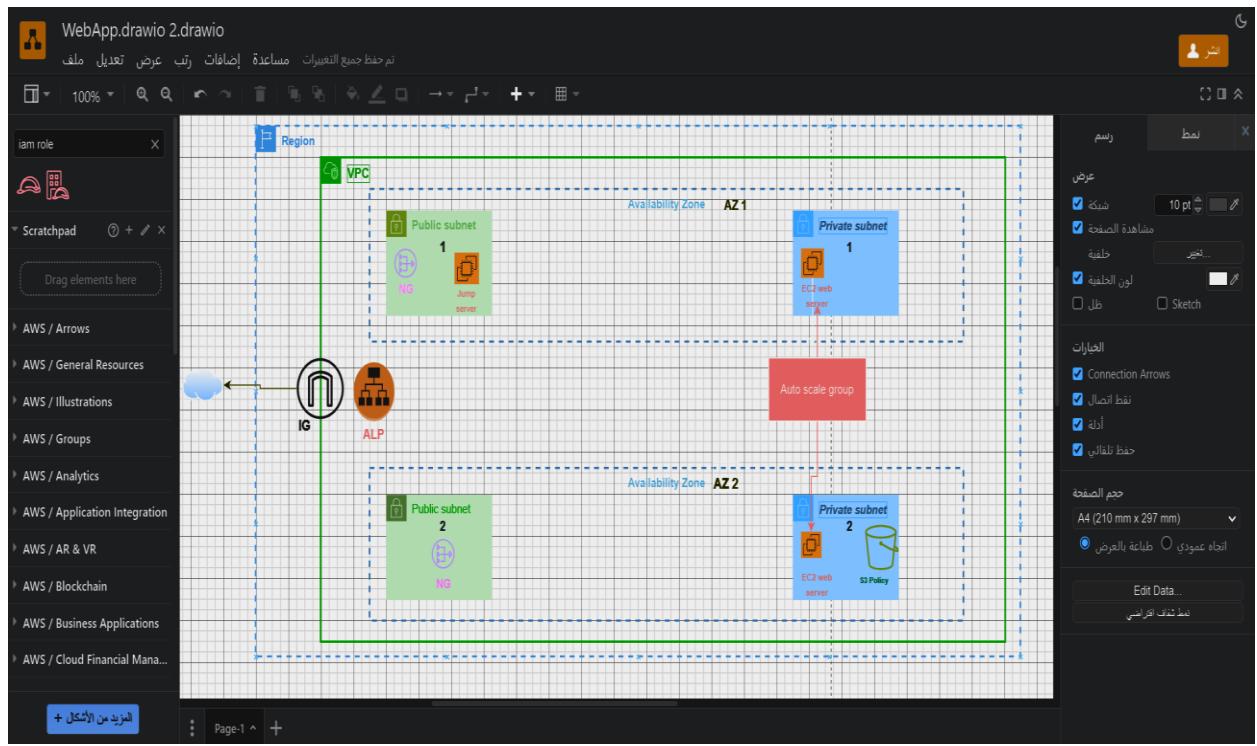
Project Objectives:

- Create Network Environment with Infrastructure as a Code.
- Host your web app on EC2 or using micro services.
- Store App static content on external storage not on EBS.
- Monitoring your servers with integrated notifications while metrics exceed specific limit.
- Automatic remediation if web service disabled.
- Noted that the environment must be [Secure - Highly Available - Scalable - Disaster Recovery needed].
- Design your Architecture on Draw IO.
- Documentation your steps.

Additional Projects:

- Enable Redirection on Load balancer from HTTP to HTTPS.
- Mount S3 on EC2.
- Use API Gateway to view image on S3.

1) Project Architecture using Draw IO



- Routing tables
- Public Routing Table

Network	Next hop
0.0.0.0	IGW

- Private Routing Table

Network	Next hop
0.0.0.0	NAT GW

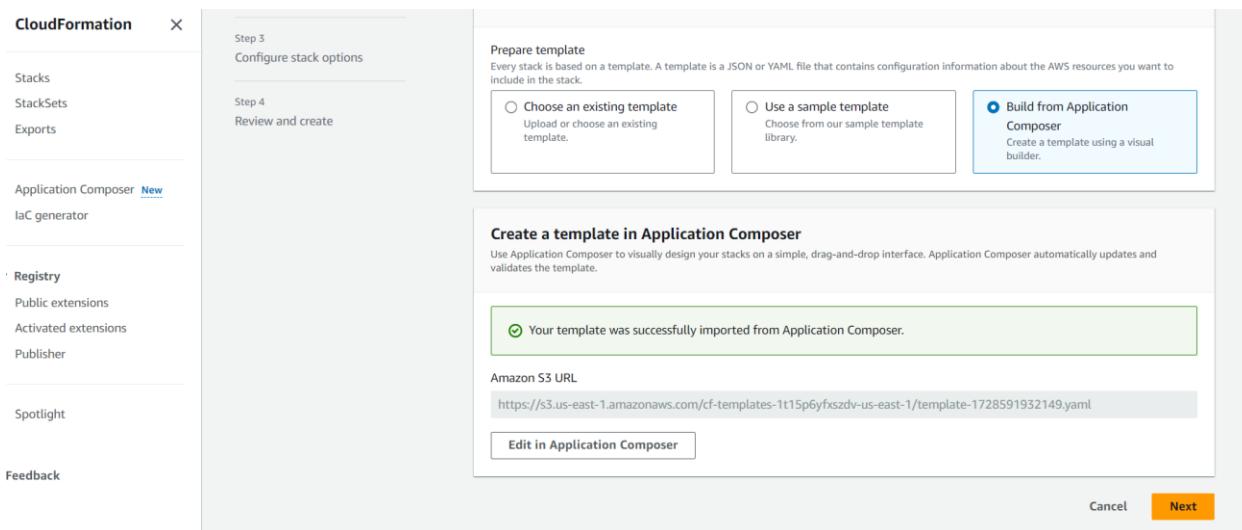
- **Subnets in availability zones**

Public subnet AZ1	Private subnet AZ1	Public subnet AZ2	Private subnet AZ2
10.0.1.0/24	10.0.3.0/24	10.0.2.0/24	10.0.4.0/24

- **Project Steps**

Task 1 : Create Network Environment with Infrastructure as a Code.

CloudFormation console > Create Stack > Build from Application Composer



Template used:

AWSTemplateFormatVersion: "2010-09-09"

Description: CloudFormation Template to Create a VPC with Public and Private Subnets, Internet Gateway, NAT Gateway, and Security Groups

Resources:

VPC

MyVPC:

Type: "AWS::EC2::VPC"

Properties:

CidrBlock: "10.0.0.0/16"

EnableDnsSupport: true

EnableDnsHostnames: true

Tags:

- Key: Name

- Value: MyVPC

Internet Gateway

MyInternetGateway:

Type: "AWS::EC2::InternetGateway"

Properties:

Tags:

- Key: Name

- Value: MyInternetGateway

AttachGateway:

Type: "AWS::EC2::VPCGatewayAttachment"

Properties:

VpcId: !Ref MyVPC

InternetGatewayId: !Ref MyInternetGateway

Public Subnet 1 (AZ1)

PublicSubnet1:

Type: "AWS::EC2::Subnet"

Properties:

VpcId: !Ref MyVPC

CidrBlock: "10.0.1.0/24"

AvailabilityZone: !Select [0, !GetAZs]

MapPublicIpOnLaunch: true

Tags:

- Key: Name

- Value: PublicSubnet1

Public Subnet 2 (AZ2)

PublicSubnet2:

Type: "AWS::EC2::Subnet"

Properties:

VpcId: !Ref MyVPC

```
CidrBlock: "10.0.2.0/24"
AvailabilityZone: !Select [ 1, !GetAZs " ]
MapPublicIpOnLaunch: true
Tags:
- Key: Name
  Value: PublicSubnet2
```

Private Subnet 1 (AZ1)

```
PrivateSubnet1:
Type: "AWS::EC2::Subnet"
Properties:
VpcId: !Ref MyVPC
CidrBlock: "10.0.3.0/24"
AvailabilityZone: !Select [ 0, !GetAZs " ]
MapPublicIpOnLaunch: false
Tags:
- Key: Name
  Value: PrivateSubnet1
```

Private Subnet 2 (AZ2)

```
PrivateSubnet2:
Type: "AWS::EC2::Subnet"
Properties:
VpcId: !Ref MyVPC
CidrBlock: "10.0.4.0/24"
AvailabilityZone: !Select [ 1, !GetAZs " ]
MapPublicIpOnLaunch: false
Tags:
- Key: Name
  Value: PrivateSubnet2
```

Public Route Table

```
PublicRouteTable:
Type: "AWS::EC2::RouteTable"
Properties:
VpcId: !Ref MyVPC
Tags:
- Key: Name
  Value: PublicRouteTable
```

Route for Public Route Table to Internet Gateway

```
PublicRoute:
Type: "AWS::EC2::Route"
Properties:
```

```
RouteTableId: !Ref PublicRouteTable
DestinationCidrBlock: "0.0.0.0/0"
GatewayId: !Ref MyInternetGateway
```

Associate Public Route Table with Public Subnet 1

```
PublicSubnet1RouteTableAssociation:
  Type: "AWS::EC2::SubnetRouteTableAssociation"
  Properties:
    SubnetId: !Ref PublicSubnet1
    RouteTableId: !Ref PublicRouteTable
```

Associate Public Route Table with Public Subnet 2

```
PublicSubnet2RouteTableAssociation:
  Type: "AWS::EC2::SubnetRouteTableAssociation"
  Properties:
    SubnetId: !Ref PublicSubnet2
    RouteTableId: !Ref PublicRouteTable
```

NAT Gateway

```
EIPForNATGateway:
  Type: "AWS::EC2::EIP"
  Properties:
    Domain: "vpc"

NATGateway:
  Type: "AWS::EC2::NatGateway"
  Properties:
    AllocationId: !GetAtt EIPForNATGateway.AllocationId
    SubnetId: !Ref PublicSubnet1
    Tags:
      - Key: Name
        Value: NATGateway
```

Private Route Table

```
PrivateRouteTable:
  Type: "AWS::EC2::RouteTable"
  Properties:
    VpcId: !Ref MyVPC
    Tags:
      - Key: Name
        Value: PrivateRouteTable
```

Route for Private Route Table to NAT Gateway

```
PrivateRoute:
```

Type: "AWS::EC2::Route"
Properties:
 RouteTableId: !Ref PrivateRouteTable
 DestinationCidrBlock: "0.0.0.0/0"
 NatGatewayId: !Ref NATGateway

Associate Private Route Table with Private Subnet 1

PrivateSubnet1RouteTableAssociation:
Type: "AWS::EC2::SubnetRouteTableAssociation"
Properties:
 SubnetId: !Ref PrivateSubnet1
 RouteTableId: !Ref PrivateRouteTable

Associate Private Route Table with Private Subnet 2

PrivateSubnet2RouteTableAssociation:
Type: "AWS::EC2::SubnetRouteTableAssociation"
Properties:
 SubnetId: !Ref PrivateSubnet2
 RouteTableId: !Ref PrivateRouteTable

--- Security Groups ---

Public Security Group (Web Servers)

PublicSecurityGroup:
Type: "AWS::EC2::SecurityGroup"
Properties:
 GroupDescription: Enable inbound traffic for web servers in the public subnet
 VpcId: !Ref MyVPC
 SecurityGroupIngress:
 - IpProtocol: tcp
 FromPort: 80
 ToPort: 80
 CidrIp: 0.0.0.0/0
 - IpProtocol: tcp
 FromPort: 443
 ToPort: 443
 CidrIp: 0.0.0.0/0
 SecurityGroupEgress:
 - IpProtocol: -1
 CidrIp: 0.0.0.0/0
 Tags:
 - Key: Name
 Value: PublicSecurityGroup

Private Security Group (Application/DB Servers)

PrivateSecurityGroup:

Type: "AWS::EC2::SecurityGroup"

Properties:

GroupDescription: Enable inbound traffic for internal resources in private subnet

VpcId: !Ref MyVPC

SecurityGroupIngress:

- IpProtocol: tcp

- FromPort: 3306

- ToPort: 3306

- SourceSecurityGroupId: !Ref PublicSecurityGroup # Access from web servers

- IpProtocol: tcp

- FromPort: 22

- ToPort: 22

- CidrIp: 10.0.0.0/16 # Internal SSH access

SecurityGroupEgress:

- IpProtocol: -1

- CidrIp: 0.0.0.0/0

Tags:

- Key: Name

- Value: PrivateSecurityGroup

Outputs:

VPCID:

Description: The VPC ID

Value: !Ref MyVPC

PublicSubnet1ID:

Description: Public Subnet 1 ID

Value: !Ref PublicSubnet1

PublicSubnet2ID:

Description: Public Subnet 2 ID

Value: !Ref PublicSubnet2

PrivateSubnet1ID:

Description: Private Subnet 1 ID

Value: !Ref PrivateSubnet1

PrivateSubnet2ID:

Description: Private Subnet 2 ID

Value: !Ref PrivateSubnet2

PublicSecurityGroupID:

Description: Public Security Group ID

Value: !Ref PublicSecurityGroup

PrivateSecurityGroupID:

Description: Private Security Group ID

Value: !Ref PrivateSecurityGroup

- **Explanation of the Template:**

- **VPC:** A VPC with a CIDR block of `10.0.0.0/16` is created.
- **Subnets:** Two public subnets (`10.0.1.0/24`, `10.0.2.0/24`) and two private subnets (`10.0.3.0/24`, `10.0.4.0/24`) are created, each in different availability zones to ensure high availability.
- **Internet Gateway:** An Internet Gateway is created and attached to the VPC.
- **NAT Gateway:** A NAT Gateway is created in the first public subnet to allow instances in private subnets to access the internet.
- **Route Tables:**
 - A public route table is created and associated with the public subnets, with a route to the Internet Gateway.
 - A private route table is created and associated with the private subnets, with a route to the NAT Gateway for outbound internet access.

* **Explanation of Security Groups:**

1. **Public Security Group (PublicSecurityGroup):**

- Allows inbound HTTP (port 80) and HTTPS (port 443) traffic from any IP (`0.0.0.0/0`).
- Allows all outbound traffic (-1 protocol and `0.0.0.0/0` for egress).
- This is typically used for web servers hosted in public subnets (e.g., EC2 instances running a web application).

2. **Private Security Group (PrivateSecurityGroup):**

- Allows inbound MySQL (port 3306) traffic only from instances within the **PublicSecurityGroup**, meaning web servers can communicate with database servers.
- Allows SSH (port 22) from within the VPC (`10.0.0.0/16`), limiting access to internal users or a bastion host.
- Allows all outbound traffic (-1 for egress).
- This group is typically used for internal resources such as application or database servers hosted in private subnets.
- **Outputs:** The VPC ID, public subnet IDs, and private subnet IDs are output for reference, which can be used when deploying other resources in this network.

You are screen sharing

CloudFormation > Infrastructure Composer

CloudFormation console mode Menu

Canvas Template YAML JSON

Validate Create template

Infrastructure Composer List Resources

Search for a resource Enhanced components (14)

- API Gateway
- Cognito UserPool
- Cognito UserPoolClient
- DynamoDB Table
- EventBridge Event rule
- EventBridge Schedule

Model Template description

```
1 AWSTemplateFormatVersion: '2010-09-09'
2 Description: 'Create a VPC, subnets, and internet gateway'
3
4 Resources:
5   VPC:
6     Type: AWS::VPC
7     Properties:
8       CidrBlock: 10.0.0.0/16
9       Tags:
10      - Key: Name
11        Value: MyVPC
12
13   SubnetPublic1:
14     Type: AWS::EC2::Subnet
15     Properties:
16       CidrBlock: 10.0.0.0/24
17       AvailabilityZone: !Select [0, !GetAZs]
18       VpcId: !Ref VPC
19       Tags:
20         - Key: Name
21           Value: PublicSubnet1
```

No template validation errors

CloudFormation Stacks StackSets Exports

Application Composer New IaC generator

Registry Public extensions Activated extensions Publisher

Spotlight Feedback

CloudFormation > Stacks > Create stack

Step 1 Create stack

Step 2 Specify stack details

Step 3 Configure stack options

Step 4 Review and create

Specify stack details

Provide a stack name

Stack name Project-Stack

Stack name must be 1 to 128 characters, start with a letter, and only contain alphanumeric characters. Character count: 13/128.

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

No parameters

There are no parameters defined in your template

Cancel Previous Next

CloudFormation

- Stacks
- StackSets
- Exports
- Application Composer [New](#)
- IaC generator
- Registry
 - Public extensions
 - Activated extensions
 - Publisher
- Spotlight
- Feedback

Advanced options

Delete all newly created resources
Deletes created resources during a rollback regardless of their attached deletion policy.

Stack policy - optional
Defines the resources that you want to protect from unintentional updates during a stack update.

Rollback configuration - optional
Specify alarms for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back.

Notification options - optional
Specify a new or existing Amazon Simple Notification Service topic where notifications about stack events are sent.

Stack creation options - optional
Specify the timeout and termination protection options for stack creation.

Cancel [Previous](#) [Next](#)

CloudFormation

- Stacks
- StackSets
- Exports
- Application Composer [New](#)
- IaC generator
- Registry
 - Public extensions
 - Activated extensions
 - Publisher
- Spotlight
- Feedback

SNS topic ARN

No notification options
There are no notification options defined

Stack creation options

Timeout
-

Termination protection
Deactivated

Quick-create link

Use quick-create links to get stacks up and running quickly from the AWS CloudFormation console with the same basic configuration as this stack. Copy the URL on the link to share. [Learn more](#)

[Open quick-create link](#)

[Create change set](#)

Cancel [Previous](#) [Submit](#)

CloudFormation

- Stacks
- Stack details**
- Drifts
- StackSets
- Exports
- Application Composer [New](#)
- IaC generator
- Registry
 - Public extensions
 - Activated extensions
 - Publisher
- Spotlight

CloudFormation > Stacks > Project-Stack

Project-Stack

Timestamp	Logical ID	Status	Detailed status
2024-10-10 23:42:51 UTC+0300	Project-Stack	CREATE_IN_PROGRESS	-
2024-10-10 22:57:52 UTC+0300	c133617a3383146l7917522t1w636013029017	CREATE_COMPLETE	-

Events (1)

Timestamp	Logical ID	Status	Detailed status
2024-10-10 23:42:51 UTC+0300	Project-Stack	CREATE_IN_PROGRESS	-

Timestamp	Logical ID	Status	Detailed status
2024-10-10 23:45:15 UTC+0300	Project-Stack	CREATE_COMPLETE	-
2024-10-10 23:45:14 UTC+0300	PrivateRoute	CREATE_COMPLETE	-

Task 2: Host your web app on EC2 or using micro services.

EC2 > Launch Instance

The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with navigation links like EC2 Dashboard, EC2 Global View, Events, Console-to-Code (with a 'Preview' link), Instances (with sub-links for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, and Capacity Reservations), and Images (with sub-links for AMIs and AMI Catalog). The main content area has a header 'Resources' with buttons for EC2 Global View, settings, and refresh. Below it, a message says 'You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:' followed by a grid of resource counts: Instances (running) 0, Auto Scaling Groups 0, Capacity Reservations 0, Dedicated Hosts 0, Elastic IPs 1, Instances 0, Key pairs 1, Load balancers 0, Placement groups 0, Security groups 4, Snapshots 0, and Volumes 0. To the right, there's a 'Launch instance' section with a large orange 'Launch instance' button and a 'Migrate a server' button. Further right is a 'Service health' section showing 'Region: US East (N. Virginia)' and 'Status: This service is operating normally.' with a green checkmark icon.

AWS Services Search [Alt+S] N. Virginia vclabs/ EC2

Name: Project Instance Add additional tags

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Li [Browse more AMIs](#) Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI ami-0fff1b9a61dec8a5f (64-bit (x86), uefi-preferred) / ami-0621e09dc8263acc3 (64-bit (Arm), uefi) Virtualization: hvm ENA enabled: true Root device type: ebs Free tier eligible

Summary

Number of instances | [Info](#) 1

Software Image (AMI) Amazon Linux 2023 AMI 2023.5.2...read more ami-0fff1b9a61dec8a5f

Virtual server type (instance type) t2.micro

Firewall (security group) New security group

Storage (volumes) 1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t2.micro in the Regions in which you launch)

Cancel Launch instance Preview code

Choosing AMI & Image type

AWS Services Search [Alt+S] EC2

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI ami-0fff1b9a61dec8a5f (64-bit (x86), uefi-preferred) / ami-0621e09dc8263acc3 (64-bit (Arm), uefi) Virtualization: hvm ENA enabled: true Root device type: ebs Free tier eligible

Description

Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Architecture	Boot mode	AMI ID	Username
64-bit (x86)	uefi-preferred	ami-0fff1b9a61dec8a5f	ec2-user

Instance type Info | Get advice

Instance type

t2.micro Family: t2 1 vCPU 1 GiB Memory Current generation: true On-Demand Windows base pricing: 0.0162 USD per Hour On-Demand SUSE base pricing: 0.0116 USD per Hour On-Demand RHEL base pricing: 0.026 USD per Hour On-Demand Linux base pricing: 0.0116 USD per Hour Free tier eligible

All generations Compare instance types

aws Services Search [Alt+S] EC2

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

MyKeyPair

Network settings Info

VPC - required Info

vpc-0762aa5c869e1ab9e (MyVPC)
10.0.0.0/16

Subnet Info

subnet-0a3b02a013554ce55 PublicSubnet1
VPC: vpc-0762aa5c869e1ab9e Owner: 636013029017 Availability Zone: us-east-1a
Zone type: Availability Zone IP addresses available: 250 CIDR: 10.0.1.0/24

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

Advanced network configuration

Configure storage Info Advanced

1x GiB Root volume (Not encrypted)

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.5.2...read more
ami-0ff1b9a61dec8a5f

Virtual server type (instance type)

t2.micro

Firewall (security group)

Project-Stack-PublicSecurityGroup-9CSldO2ZxHy4

Storage (volumes)

1 volume(s) - 8 GiB

Cancel

Instances (1/1) [Info](#)

Last updated 2 minutes ago [Connect](#) [Instance state](#) Actions [Launch instances](#)

[Find Instance by attribute or tag \(case-sensitive\)](#) All states

<input checked="" type="checkbox"/> Name	Instance ID	Instance state	Instance type	Status check	Alarms
<input checked="" type="checkbox"/> Project Instance	i-0d5ac97807f07ec59	Running	t2.micro	2/2 checks passed	View

EC2

[EC2](#) > [Security Groups](#) > [sg-001a12a8ef3b1877 - Project-Stack-PublicSecurityGroup-9CSldO22xHy4](#) > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

Security group rule ID	Type Info	Protocol Info	Port range	Source Info	Description - optional Info
sgr-01da738fbfc7070a	HTTP	TCP	80	Custom	<input type="text"/> 0.0.0.0/0 Delete
sgr-0d1ed8e787e7f3dad	HTTPS	TCP	443	Custom	<input type="text"/> 0.0.0.0/0 Delete
-	SSH	TCP	22	Anywh...	<input type="text"/> 0.0.0.0/0 Delete
-	Custom TCP	TCP	0	Custom	<input type="text"/> 0.0.0.0/0 Delete

[Add rule](#)

```

Installing : mod_lua-2.4.62-1.amzn2023.x86_64
Installing : generic-logos-https-18.0.0-12.amzn2023.0.3.noarch
Installing : httpd-2.4.62-1.amzn2023.x86_64
Running scriptlet: httpd-2.4.62-1.amzn2023.x86_64
Verifying   : apr-1.7.2-2.amzn2023.0.2.x86_64
Verifying   : apr-util-1.6.3-1.amzn2023.0.1.x86_64
Verifying   : generic-logos-https-18.0.0-12.amzn2023.0.3.noarch
Verifying   : httpd-2.4.62-1.amzn2023.x86_64
Verifying   : httpd-core-2.4.62-1.amzn2023.x86_64
Verifying   : httpd-filesystem-2.4.62-1.amzn2023.noarch
Verifying   : httpd-tools-2.4.62-1.amzn2023.x86_64
Verifying   : libbrotli-1.0.9-4.amzn2023.0.2.x86_64
Verifying   : mailcap-2.1.49-3.amzn2023.0.3.noarch
Verifying   : mod_http2-2.0.27-1.amzn2023.0.3.x86_64
Verifying   : mod_lua-2.4.62-1.amzn2023.x86_64

Installed:
apr-1.7.2-2.amzn2023.0.2.x86_64           apr-util-1.6.3-1.amzn2023.0.1.x86_64
generic-logos-https-18.0.0-12.amzn2023.0.3.noarch    httpd-2.4.62-1.amzn2023.x86_64
httpd-filesystem-2.4.62-1.amzn2023.noarch      httpd-tools-2.4.62-1.amzn2023.x86_64
mailcap-2.1.49-3.amzn2023.0.3.noarch        mod_http2-2.0.27-1.amzn2023.0.3.x86_64
mod_lua-2.4.62-1.amzn2023.x86_64

Complete!
ec2-user@ip-10-0-1-196 ~]$ sudo systemctl start httpd
ec2-user@ip-10-0-1-196 ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
ec2-user@ip-10-0-1-196 ~]$ 

```

Task 3: Store App static content on external storage not on EBS.

Create an S3 bucket

The screenshot shows the 'Create an S3 bucket' wizard in the AWS Management Console. The top navigation bar includes 'EC2', 'Amazon S3', and 'Amazon S3'. The left sidebar lists 'Buckets', 'Access Grants', 'Access Points', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', 'IAM Access Analyzer for S3', 'Block Public Access settings for this account', 'Storage Lens' (with 'Dashboards', 'Storage Lens groups', and 'AWS Organizations settings'), and a 'Feature spotlight' section.

The main content area displays the 'General purpose buckets' list, showing two existing buckets:

Name	AWS Region	IAM Access Analyzer	Creation date
cf-templates-1bi42o7m3ffz1-us-east-1	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 10, 2024, 23:16:13 (UTC+03:00)
cf-templates-1t15p6yfxs2dv-us-east-1	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 10, 2024, 23:25:31 (UTC+03:00)

Bucket type (Info):
The 'General purpose' option is selected. It is described as recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

Bucket name (Info):
The bucket name is set to 'MyAppStaticContent'. A note states that the bucket name must be unique within the global namespace and follow the bucket naming rules. A link to 'See rules for bucket naming' is provided.

Copy settings from existing bucket - optional:
Only the bucket settings in the following configuration are copied.
Choose bucket
Format: s3://bucket/prefix

Object Ownership (Info):
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

ACLs disabled (recommended):
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

ACLs enabled:
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

Block public access to buckets and objects granted through new access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

Block public access to buckets and objects granted through any access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

Block public access to buckets and objects granted through new public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

Block public and cross-account access to buckets and objects through any public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.



Turning off block all public access might result in this bucket and the objects within becoming public

AWS recommends that you turn on block all public access, unless public access is required for specific

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)

Server-side encryption with Amazon S3 managed keys (SSE-S3)

Server-side encryption with AWS Key Management Service keys (SSE-KMS)

Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the Storage tab of the [Amazon S3 pricing page](#).

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

Disable

Enable

► Advanced settings

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel

Create bucket

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting
Enabled

Hosting type
Bucket hosting

Bucket website endpoint
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)

<http://my-app-static-content.s3-website-us-east-1.amazonaws.com>

Amazon S3 > Buckets

Account snapshot - updated every 24 hours [All AWS Regions](#)

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

[View Storage Lens dashboard](#)

[General purpose buckets](#) [Directory buckets](#)

General purpose buckets (3) [Info](#) [All AWS Regions](#)

Buckets are containers for data stored in S3.

Find buckets by name				
				< 1 >
Name	AWS Region	IAM Access Analyzer	Creation date	
cf-templates-1bi42o7m3ffz1-us-east-1	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 10, 2024, 23:16:13 (UTC+03:00)	
cf-templates-1t15p6yfxszdv-us-east-1	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 10, 2024, 23:25:31 (UTC+03:00)	
my-app-static-content	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 11, 2024, 01:25:32 (UTC+03:00)	

Objects (10) [Info](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix						< 1 >		
<input type="checkbox"/> Name	Type	Last modified	Size	Storage class				
Cafe-Owners.png	png	October 11, 2024, 03:55:54 (UTC+03:00)	2.7 MB	Standard				
Cake-Vitrine.png	png	October 11, 2024, 03:55:57 (UTC+03:00)	3.8 MB	Standard				
Coffee-and-Pastries.png	png	October 11, 2024, 03:55:56 (UTC+03:00)	3.1 MB	Standard				
Coffee-Shop.png	png	October 11, 2024, 03:55:53 (UTC+03:00)	726.8 KB	Standard				
Cookies.png	png	October 11, 2024, 03:55:55 (UTC+03:00)	1.4 MB	Standard				
Cup-of-Hot-Chocolate.png	png	October 11, 2024, 03:55:50 (UTC+03:00)	3.6 MB	Standard				
index.html	html	October 11, 2024, 03:36:35 (UTC+03:00)	2.9 KB	Standard				
Strawberry-& Blueberry-	png	October 11, 2024, 03:55:52 (UTC+03:00)	2.9 MB	Standard				

Café



The Café offers an assortment of delicious and delectable pastries and coffees that will put a smile on your face. From cookies to croissants, tarts and cakes, each treat is special day!

Frank bakes a rich variety of cookies. Try them all!	Tea Coffee Latte Hot Chocolate Yes, we have it!	Our tarts are always a customer favorite!
--	---	---

About Us

Frank and Martha have been adding sweetness to their customers's lives since 2016. Both of them will personally greet you with a welcoming smile when you visit! Frank's simple and fresh ingredients to produce delightful flavors.

Contact Us



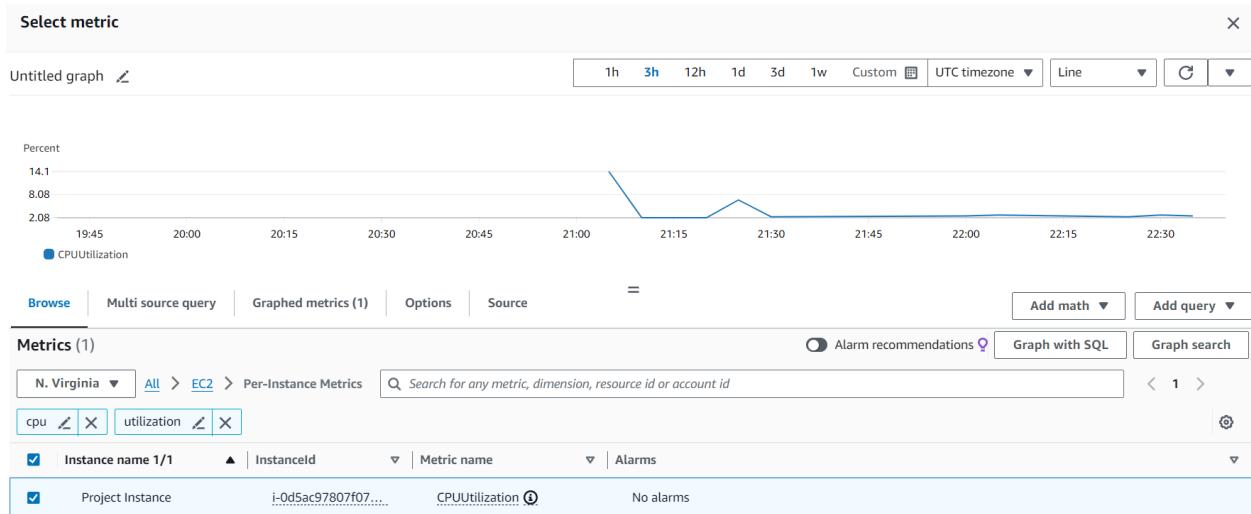
123 Sweet Tooth St.
London SW1A 0AA, UK
Tel: +44-12-12345678

Hours

Task 4: Monitoring your servers with integrated notifications while metrics exceed specific limit.

Create an alarm on Cloud Formation to monitor CPU utilization

The screenshot shows the AWS CloudWatch Metrics Alarms interface. The left sidebar includes links for CloudWatch, Favorites and recent, Dashboards, Alarms (0), All alarms, Logs, Metrics, X-Ray traces, Events, Application Signals, Network monitoring, Insights, Settings, Getting Started, and What's new. The main pane displays a table titled 'Alarms (0)' with columns for Name, State, Last state update (UTC), Conditions, and Actions. A message at the top states 'No alarms' and 'No alarms to display'. A 'Create alarm' button is located at the bottom right of the table area.



CloudWatch > Alarms > Create alarm

Step 1 Specify metric and conditions

Step 2 Configure actions

Step 3 Add name and description

Step 4 Preview and create

Specify metric and conditions

Step 1 Specify metric and conditions

Metric

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.

Percent

14.1

8.08

2.08

20:00 21:00 22:00

■ CPUUtilization

Namespace AWS/EC2

Metric name

Instanceld

Instance name Project Instance

Statistic Average

Conditions

Threshold type

Static
Use a value as a threshold

Anomaly detection
Use a band as a threshold

Whenever CPUUtilization is...

Define the alarm condition.

Greater
> threshold

Greater/Equal
>= threshold

Lower/Equal
<= threshold

Lower
< threshold

than...

Define the threshold value.

80

Must be a number

▶ Additional configuration

Cancel **Next**

Step 2
Configure actions

Step 3
Add name and description

Step 4
Preview and create

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

Create a new topic...

The topic name must be unique.

Default_CloudWatch_Alarms_Topic

SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).

Email endpoints that will receive the notification...

Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

noha.ashraf171@gmail.com

user1@example.com, user2@example.com

Create topic

Add name and description

Name and description

Alarm name

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

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

CPU utilization is in alarm or insufficient data

Up to 1024 characters (48/1024)

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

[Cancel](#)

[Previous](#)

[Next](#)

Notification

When Insufficient data, send a notification to "Default_CloudWatch_Alarms_Topic"

Step 3: Add name and description

[Edit](#)

Name and description

Name

CPUUtilization

Description

CPU utilization is in alarm or insufficient data

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

[Cancel](#)

[Previous](#)

[Create alarm](#)

Alarms (1)					
<input type="checkbox"/> Hide Auto Scaling alarms		<input type="button" value="Clear selection"/>		<input type="button" value="Create composite alarm"/>	
<input type="button" value="Actions"/>		<input type="button" value="Create alarm"/>			
<input type="text" value="Search"/>		<input type="button" value="Alarm state: Any"/>		<input type="button" value="Alarm type: Any"/>	
<input type="checkbox"/>	Name	<input type="button" value="State"/>	Last state update (UTC)	<input type="button" value="Conditions"/>	<input type="button" value="Actions"/>
<input type="checkbox"/>	CPUUtilization	<input type="button" value="Insufficient data"/>	2024-10-10 22:49:12	CPUUtilization > 80 for 1 datapoints within 5 minutes	<input checked="" type="checkbox"/> Actions enabled

Sample of the alarm notification received

INSUFFICIENT_DATA: "CPUUtilization" in US East (N. Virginia) [!\[\]\(8992432513afb96f45a69bb5f0f74668_img.jpg\)](#) [Inbox](#) [!\[\]\(419bdabe89357d973a7d75a1c51ef8f0_img.jpg\)](#)

AWS Notifications <no-reply@sns.amazonaws.com>

to me [!\[\]\(e33149aa5dfd0c44da8a965ac6e384f7_img.jpg\)](#)

You are receiving this email because your Amazon CloudWatch Alarm "CPUUtilization" in the US East (N. Virginia) region has entered the INSUFFICIENT_DATA state. The last datapoint was unknown." at "Friday 11 October, 2024 00:11:50 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/CPUUtilization>

Alarm Details:

- Name: CPUUtilization
- Description: CPU utilization is in alarm or insufficient data
- State Change: OK -> INSUFFICIENT_DATA
- Reason for State Change: Insufficient Data: 1 datapoint was unknown.
- Timestamp: Friday 11 October, 2024 00:11:50 UTC
- AWS Account: 636013029017
- Alarm Arn: arn:aws:cloudwatch:us-east-1:636013029017:alarm:CPUUtilization

Threshold:

- The alarm is in the ALARM state when the metric is GreaterThanThreshold 80.0 for at least 1 of the last 1 period(s) of 300 seconds.

Monitored Metric:

- MetricNamespace: AWS/EC2
- MetricName: CPUUtilization
- Dimensions: [InstanceId = i-0d5ac97807f07ec59]
- Period: 300 seconds
- Statistic: Average
- Unit: not specified

Task 5: Automatic remediation if web service disabled.

Select metric

Untitled graph 1h 3h 12h 1d 3d 1w Custom UTC timezone Line

Count
1
0.5
0
20:15 20:30 20:45 21:00 21:15 21:30 21:45 22:00 22:15 22:30 22:45 23:00

Browse Multi source query Graphed metrics (1) Options Source = Add math Add query

Metrics (19)
N. Virginia All > EC2 > Per-Instance Metrics < 1 >

Instance name 19/19	Instanceld	Metric name	Alarms
Project Instance	i-0d5ac97807f07...	StatusCheckFailed_Instance	No alarms
<input checked="" type="checkbox"/> Project Instance	i-0d5ac97807f07...	StatusCheckFailed	No alarms
Project Instance	i-0d5ac97807f07...	StatusCheckFailed_System	No alarms

Cancel Select metric

Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 minute.

Count
1
0.5
0
21:00 22:00 23:00

Namespace AWS/EC2

Metric name StatusCheckFailed

Instanceld i-0d5ac97807f07ec59

Instance name Project Instance

Statistic Average

Period 1 minute

Conditions

Threshold type

Static

Use a value as a threshold

Anomaly detection

Use a band as a threshold

Whenever StatusCheckFailed is...

Define the alarm condition.

Greater

> threshold

Greater/Equal

\geq threshold

Lower/Equal

\leq threshold

Lower

$<$ threshold

than...

Define the threshold value.

1

Must be a number

[Remove](#)

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.

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

Create a new topic...

The topic name must be unique.

StatusCheckFailed

SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).

Email endpoints that will receive the notification...

Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

noha.ashraf171@gmail.com

user1@example.com, user2@example.com

[Create topic](#)

Add name and description

Name and description

Alarm name

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

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

Status Check Failed

Up to 1024 characters (19/1024)

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

[Cancel](#)

[Previous](#)

[Next](#)

Actions

Notification

When In alarm, send a notification to "StatusCheckFailed"

Step 3: Add name and description

Edit

Name and description

Name

UnhealthyInstance

Description

Status Check Failed

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

Cancel

Previous

Create alarm

Lambda

[Lambda](#) > Functions

Dashboard

Applications

Functions

Additional resources

Code signing configurations

Event source mappings

Layers

Replicas

Related AWS resources

Step Functions state machines

Functions (5)

Last fetched 1 minute ago

[Actions](#)

[Create function](#)

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Function name	Description	Package type	Runtime	Last modified	
<input type="checkbox"/>	ModLabRole	updates LabRole to allow it to assume itself	Zip	Python 3.9	3 hours ago	Edit
<input type="checkbox"/>	MainMonitoringFunction	-	Zip	Python 3.9	3 hours ago	Edit
<input type="checkbox"/>	RedshiftEventSubscription	Create Redshift event subscription to SNS Topic.	Zip	Python 3.9	3 hours ago	Edit
<input type="checkbox"/>	RoleCreationFunction	Create SLR if absent	Zip	Python 3.9	3 hours ago	Edit
<input type="checkbox"/>	RedshiftOverwat	Deletes Redshift Cluster if the	Zip	Python 3.9	2 hours ago	Edit

Basic information

Function name

Enter a name that describes the purpose of your function.

AutomaticRemediationForWebService

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.

Node.js 20.x



Architecture [Info](#)

Choose the instruction set architecture you want for your function code.

x86_64

arm64

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

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

Role creation might take a few minutes. Please do not delete the role or edit the trust or permissions policies in this role.

Lambda will create an execution role named AutomaticRemediationForWebService-role-qjomgr6t, with permission to upload logs to Amazon CloudWatch Logs.

▼ Additional Configurations

Use additional configurations to set up code signing, function URL, tags, and Amazon VPC access for your function.

Enable Code signing [Info](#)

Use code signing configurations to ensure that the code has been signed by an approved source and has not been altered since signing.

Enable function URL [Info](#)

Use function URLs to assign HTTP(S) endpoints to your Lambda function.

Enable tags [Info](#)

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources, track your AWS costs, and enforce attribute-based access control.

Enable VPC [Info](#)

Connect your function to a VPC to access private resources during invocation.

▼ Additional Configurations

Use additional configurations to set up code signing, function URL, tags, and Amazon VPC access for your function.

Enable Code signing Info

Use code signing configurations to ensure that the code has been signed by an approved source and has not been altered since signing.

Enable function URL Info

Use function URLs to assign HTTP(S) endpoints to your Lambda function.

Enable tags Info

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources, track your AWS costs, and enforce attribute-based access control.

Enable VPC Info

Connect your function to a VPC to access private resources during invocation.

[Cancel](#)

[Create function](#)

Identity and Access Management (IAM)

IAM > Roles

Roles (19) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.



[Delete](#)

[Create role](#)

< 1 >

Role name

▲ Trusted entities

Last activity

[AWSServiceRoleForAWSCloud9](#)

AWS Service: cloud9 (Service-Linked)

-

[AWSServiceRoleForCloudWatchEvents](#)

AWS Service: events (Service-Linked)

-

[AWSServiceRoleForElastiCache](#)

AWS Service: elasticache (Service-Linked)

-

[AWSServiceRoleForOrganizations](#)

AWS Service: organizations (Service-Linked)

-

[AWSServiceRoleForSupport](#)

AWS Service: support (Service-Linked)

-

[AWSServiceRoleForTrustedAdvisor](#)

AWS Service: trustedadvisor (Service-Linked)

-

[c133617a3383146l7917522t1w63601302901-LambdaSLRRole-hKYTkixFktbk](#)

AWS Service: lambda

3 hours ago

[EMR_AutoScaling_DefaultRole](#)

AWS Service: application-autoscaling

-

[EMR_DefaultRole](#)

AWS Service: elasticmapreduce

-

[EMR_EC2_DefaultRole](#)

AWS Service: ec2

-

<input checked="" type="radio"/> AWS service Allow AWS services like EC2, Lambda, or others to perform actions in this account.	<input type="radio"/> AWS account Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.	<input type="radio"/> Web identity Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
<input type="radio"/> SAML 2.0 federation Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.	<input type="radio"/> Custom trust policy Create a custom trust policy to enable others to perform actions in this account.	

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

Lambda

Choose a use case for the specified service.

Use case

Lambda

Allows Lambda functions to call AWS services on your behalf.

Filter by Type

Policy name	Type	Description
<input type="checkbox"/> AmazonEC2ContainerRegistryFullAccess	AWS managed	Provides administrative access to Amazon EC2 Container Registry.
<input type="checkbox"/> AmazonEC2ContainerRegistryPowerUser	AWS managed	Provides full access to Amazon EC2 Container Registry.
<input type="checkbox"/> AmazonEC2ContainerRegistryPullOnly	AWS managed	Provides access to pull images from Amazon ECR.
<input type="checkbox"/> AmazonEC2ContainerRegistryReadOnly	AWS managed	Provides read-only access to Amazon ECR.
<input type="checkbox"/> AmazonEC2ContainerServiceAutoscale...	AWS managed	Policy to enable Task Autoscaling for Amazon ECS.
<input type="checkbox"/> AmazonEC2ContainerServiceEventsRole	AWS managed	Policy to enable CloudWatch Events for Amazon ECS.
<input type="checkbox"/> AmazonEC2ContainerServiceforEC2Role	AWS managed	Default policy for the Amazon EC2 Role for Amazon ECS.
<input type="checkbox"/> AmazonEC2ContainerServiceRole	AWS managed	Default policy for Amazon ECS service role.
<input checked="" type="checkbox"/> AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 via the AWS Lambda service.
<input type="checkbox"/> AmazonEC2ReadOnlyAccess	AWS managed	Provides read only access to Amazon EC2.
<input type="checkbox"/> AmazonEC2TaskExecutionRole	AWS managed	Provides EC2 task execution role.

Role details

Role name

Enter a meaningful name to identify this role.

LambdaEC2AccessRole

Maximum 64 characters. Use alphanumeric and '+=_,@-_` characters.

Description

Add a short explanation for this role.

Allows Lambda functions to call AWS services on your behalf.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: +=_,@-_`!#\$%^*(),;,.~`

Not authorized to create an IAM role

Option # 2 on AWS config

AWS Config > Set up AWS Config

Step 1
Settings

Step 2
Rules

Step 3
Review

Recording method

Recording strategy
Customize AWS Config to record configuration changes for all supported resource types, or for only the supported resource types that are relevant to you. Globally recorded resources (RDS global clusters and IAM users, groups, roles, and customer managed policies) may be recorded in more than this Region. [Learn more](#). You are charged based on the number of configuration items recorded. [Pricing details](#).

All resource types with customizable overrides
AWS Config will record all current and future supported resource types in this Region. You can override the recording frequency for specific resource types or exclude specific resource types from recording.

Specific resource types
AWS Config will only record the resource types that you specify.

Resource types to record [Info](#)
Choose a resource type to record and its frequency. It also impacts the costs to your bill. If you change the recording frequency for a resource type, the configuration items that were already recorded will remain unchanged.

Resource type	Frequency
AWS EC2 Instance	Continuous

[Add resource type](#)
No limits if all resource types have the same frequency.

Delivery method

Amazon S3 bucket

Create a bucket Choose a bucket from your account Choose a bucket from another account

Ensure appropriate permissions are available in this S3 bucket's policy. [Learn more](#).

S3 Bucket name (required)
config-bucket-636013029017 **Prefix (optional)** /AWSLogs/636013029017/Config/
us-east-1

Amazon SNS topic

Stream configuration changes and notifications to an Amazon SNS topic.
If you choose email as the notification endpoint for your SNS topic, this can cause a high volume of email. [Learn more](#).

Create a topic Choose a topic from your account Choose a topic from another account

Ensure appropriate permissions are available in this SNS topic's policy. [Learn more](#).

SNS topic name
StatusCheckFailed

[Cancel](#) [Next](#)

Recording method

Recording strategy
Record specific resource types.

▶ Recorded resource types (1)

Delivery method

S3 bucket name
config-bucket-636013029017
SNS topic name
StatusCheckFailed

▼ AWS Config rules (2)

ec2-instance-detailed-monitoring-enabled
ec2-instance-managed-by-systems-manager

Cancel Previous Confirm

Create an Automation Document in AWS System Manager

AWS Systems Manager > Documents

Owned by Amazon Owned by me Shared with me Favorites - new All documents

Categories info Filter

Filter by selecting either document type or available categories of single document type.

- Automation documents ▲ 12 categories
- Command documents ▲ 9 categories
- Policy documents No categories for this document type.
- Session documents No categories for this document type.
- Conformance Pack Template documents No categories for this document type.

Documents Preferences Actions Create document

Search by keyword or filter by tag or attributes

Document type: Automation X Clear filters

Document Type	Owner	Platform Types	Default Version
AWS-ASGEnterStandby	Automation Amazon	Windows, Linux, MacOS	1
AWS-ASGExitStandby	Automation Amazon	Windows, Linux, MacOS	1
AWS-AddOpsItemDedupStringToEventBridgeRule	Automation Amazon	Windows, Linux, MacOS	1
AWS-ArchiveEBSVolumeSnapshot	Automation Amazon	Windows, Linux, MacOS	1

The screenshot shows the 'NewRunbook' interface. On the left, there's a code editor with JSON code for a runbook. On the right, there's a visual editor showing a flowchart with nodes like 'Start', 'aws:runCommand startWebService', and 'End'.

```

1 {
2   "schemaVersion": "0.3",
3   "description": "Start web service if it is stopped",
4   "mainSteps": [
5     {
6       "action": "aws:runCommand",
7       "name": "startWebService",
8       "inputs": {
9         "DocumentName": "AWS-RunShellScript",
10        "InstancesIds": ["i-0d5ac9780f07ec59"],
11        "Parameters": {
12          "commands": ["sudo systemctl start your-web-service"]
13        }
14      }
15    }
16  ]
17 }

```

Manage remediation in AWS Config

The screenshot shows the 'Select remediation method' section. It includes options for 'Automatic remediation' (selected) and 'Manual remediation'. Below this, there's a note about auto-remediation and a settings section for retries. Further down, the 'Remediation action details' section shows a dropdown for 'Choose remediation action' set to 'NewRunbook'.

Select remediation method

- Automatic remediation
The remediation action gets triggered automatically when the resources in scope become noncompliant.
- Manual remediation
You have to manually choose to remediate the noncompliant resources.

If a resource is still non-compliant after auto-remediation, you can set this rule to try again. Note, there are costs associated with running a remediation script.

Retries in Seconds

5 60

Remediation action details

The execution of remediation actions is achieved using AWS Systems Manager Automation

Choose remediation action

NewRunbook

Start web service if it is stopped

ec2-instance-managed-by-systems-manager

Rule details		
Description Checks if your Amazon EC2 instances are managed by AWS Systems Manager (SSM Agent). The rule is NON_COMPLIANT if the EC2 instance previously associated with an SSM Agent instance inventory becomes unreachable or is not managed by SSM Agent.	Enabled evaluation mode • DETECTIVE	Detective evaluation trigger type • Oversized configuration changes • Configuration changes
Config rule ARN arn:aws:config:us-east-1:636013029017:config-rule/config-rule-uv9ia5	Last successful detective evaluation ⌚ Not available	Scope of changes Resources
		Resource types • EC2 Instance • SSM ManagedInstanceInventory
Remediation action		
Remediation action NewRunbook	Description Start web service if it is stopped	Edit Delete

Extra Task:Enable Redirection on Load balancer from HTTP to HTTPS.

EC2 > Load balancers

Name	DNS name	State	VPC ID	Availability Zones	Type
No load balancers You don't have any load balancers in us-east-1					
0 load balancers selected					
Select a load balancer above.					

Load Balancing

- Load Balancers**
- Target Groups
- Trust Stores [New](#)

Auto Scaling

▶ How Application Load Balancers work

Basic configuration

Load balancer name

Name must be unique within your AWS account and can't be changed after the load balancer is created.

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme | [Info](#)

Scheme can't be changed after the load balancer is created.

Internet-facing

An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. [Learn more](#) 

Internal

An internal load balancer routes requests from clients to targets using private IP addresses. Compatible with the **IPv4** and **Dualstack IP** address types.

Load balancer IP address type | [Info](#)

Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Put an additional cost.

IPv4

Includes only IPv4 addresses.

Dualstack

Includes IPv4 and IPv6 addresses.

Dualstack without public IPv4

Security groups



Project-Stack-PublicSecurityGroup-9CSldO2ZxHy4 
sg-001a12a8efd3b1877 VPC: vpc-0762aa5c869e1ab9e

Listeners and routing [Info](#)

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener **HTTP:80**

[Remove](#)

Protocol	Port
HTTP	<input type="text" value="80"/> : 80

Default action	Info
Forward to	<input type="text" value="Select a target group"/> 

[Create target group](#) 

Basic configuration

Settings in this section can't be changed after the target group is created.

Choose a target type

Instances

- Supports load balancing to instances within a specific VPC.
- Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.

IP addresses

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

Target group name

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol : Port

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation



1-65535

IP address type

Only targets with the indicated IP address type can be registered to this target group.

IPv4

Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.

IPv6

Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). [Learn more](#)

VPC

Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

vinc-0762aa5c869e1ab9e

IPv4 VPC CIDR: 10.0.0.0/16

Protocol version

Register targets

This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

Available instances (1)			
<input type="button" value="Create target group"/>			
<input type="text" value="Filter instances"/>			
<input type="checkbox"/>	Instance ID	Name	State
<input type="checkbox"/>	i-0d5ac97807f07ec59	Project Instance	Running

EC2 > Target groups > NewTargetGroup

NewTargetGroup

Details

Target type Instance	Protocol : Port HTTP: 80	Protocol version HTTP1	VPC vpc-0762aa5c869e1ab9e		
IP address type IPv4	Load balancer None associated				
0 Total targets	0 Healthy	0 Unhealthy	0 Unused	0 Initial	0 Draining
	0 Anomalous				

EC2 > Load balancers > NewLoadBalancer

NewLoadBalancer

▼ Details

Load balancer type Application	Status Provisioning	VPC vpc-0762aa5c869e1ab9e	Load balancer IP address type IPv4
Scheme Internet-facing	Hosted zone Z35SXDOTRQ7X7K	Availability Zones subnet-0a3b02a013554ce55 us-east-1a (use1-az4) subnet-0a05cfef988f77c74b us-east-1b (use1-az6)	Date created October 11, 2024, 04:47 (UTC+03:00)
Load balancer ARN arn:aws:elasticloadbalancing:us-east-1:636013029017:loadbalancer/app/NewLoadBalancer/75e4eb88e062f26		DNS name Info NewLoadBalancer-1272292230.us-east-1.elb.amazonaws.com (A Record)	

EC2 > Load balancers > NewLoadBalancer

NewLoadBalancer

▼ Details

Load balancer type Application	Status 🕒 Provisioning	VPC vpc-0762aa5c869e1ab9e
Scheme Internet-facing	Hosted zone Z35SXDOTRQ7X7K	Availability Zones subnet-0a3b02a013554ce55 us-east-1a (use1-az4) subnet-0a05cf988f77c74b us-east-1b (use1-az6)
Load balancer ARN arn:aws:elasticloadbalancing:us-east-1:636013029017:loadbalancer/app/NewLoadBalancer/75e4eb88e062f26	DNS name Info NewLoadBalancer-1272292230.us-east-1.elb.amazonaws.com (A Record)	

Actions ▲

- Edit IP address type
- Edit subnets
- Add listener
- Edit security groups
- Edit load balancer attributes
- Manage tags
- Delete load balancer
- Start zonal shift (Route 53 ARC) [Edit](#)

Listeners and rules [Info](#)

A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.

Listeners and rules (1) [Info](#)

<input type="checkbox"/>	Protocol:Port	Default action	Rules	ARN	Security policy	Default
<input type="checkbox"/>	HTTP:80	Forward to target group <ul style="list-style-type: none">• NewTargetGroup: 1 (100%)• Target group stickiness: Off	1 rule	ARN	Not applicable	Not app

Listener details: HTTPS:443

A listener checks for connection requests using the protocol and port that you configure. The default action and any additional rules that you create determine how the Application Load Balancer routes requests to its registered targets.

Listener configuration

The listener will be identified by the protocol and port.

Protocol

Used for connections from clients to the load balancer.

HTTPS	▼
-------	---

Port

The port on which the load balancer is listening for connections.

443

1-65535

Default actions | [Info](#)

The default action is used if no other rules apply. Choose the default action for traffic on this listener.

Authentication | [Info](#)

Authentication requires IPv4 connectivity to authentication endpoints. [Learn more](#)

Use OpenID or Amazon Cognito

Include authentication using either OpenID Connect (OIDC) or Amazon Cognito.

Routing actions

Forward to target groups

Redirect to URL

Return fixed response

Forward to target group | [Info](#)

Choose a target group and specify routing weight or [Create target group](#)

Target group

Weight Percent

Security policy | [Info](#)

Your load balancer uses a Secure Socket Layer (SSL) negotiation configuration called a security policy to manage SSL connections with clients. [Compare security policies](#)

Security category

Policy name

All security policies

ELBSecurityPolicy-TLS13-1-2-2021-06 (recommended)

Default SSL/TLS server certificate

The certificate used if a client connects without SNI protocol, or if there are no matching certificates. You can source this certificate from AWS Certificate Manager (ACM), Amazon Identity and Access Management (IAM), or import a certificate. This certificate will automatically be added to your listener certificate list.

Certificate source

From ACM

From IAM

Import certificate

Certificate (from ACM)

The selected certificate will be applied as the default SSL/TLS server certificate for this load balancer's secure listeners.

Select a certificate



[Request new ACM certificate](#)

Client certificate handling | [Info](#)

Client certificates are used to make authenticated requests to remote servers. [Learn more](#)

Mutual authentication (mTLS)

Mutual TLS (Transport Layer Security) authentication offers two-way peer authentication. It adds a layer of security over TLS and allows your services to verify the client that's making the connection.

Request public certificate

Domain names

Provide one or more domain names for your certificate.

Fully qualified domain name | [Info](#)

NewLoadBalancer-1272292230.us-east-1.elb.amazonaws.com

[Add another name to this certificate](#)

Validation method [Info](#)

Select a method for validating domain ownership.

DNS validation - recommended

Choose this option if you are authorized to modify the DNS configuration for the domains in your certificate request.

Email validation

Choose this option if you do not have permission or cannot obtain permission to modify the DNS configuration for the domains in your certificate request.

Validation domains

The validation domain will act as the email address suffix that will receive validation emails for the requested certificate domain name. This must be the same as the domain name or a superdomain of the domain name.

Domain name

NewLoadBalancer-1272292230.us-east-

Validation domain - *optional*

NewLoadBalancer-1272292230.us-east-

Listener details: HTTP:80

A listener checks for connection requests using the protocol and port that you configure. The default action and any additional rules that you create determine how the Application Load Balancer routes requests to its registered targets.

Listener configuration

The listener will be identified by the protocol and port.

Protocol

Used for connections from clients to the load balancer.

Port

The port on which the load balancer is listening for connections.

HTTP

80

1-65535

Default actions [Info](#)

The default action is used if no other rules apply. Choose the default action for traffic on this listener.

Routing actions

Forward to target groups

Redirect to URL

Return fixed response

Redirect to URL [Info](#)

Redirect client requests from one URL to another. You cannot redirect HTTPS to HTTP. To avoid a redirect loop, you must modify at least one of the following components: protocol, port, hostname or path. Components that you do not modify retain their original values.

URI parts

Full URL

Protocol

Used for connections from clients to the load balancer.

Port

The port on which the load balancer is listening for connections.

HTTPS

443

1-65535 or to retain the original port enter #[port]

Protocol

Used for connections from clients to the load balancer.

Port

The port on which the load balancer is listening for connections.

▼

1-65535 or to retain the original port enter #[port]

 Custom host, path, query

Select to modify host, path and query. If no changes are made, settings from the request URL are retained.

Host

Specify a host or retain the original host by using #{host}. Not case sensitive.

Maximum 128 characters. Allowed characters are a-z, A-Z, 0-9; the following special characters: -.; and wildcards (* and ?). At least one "." is required. Only alphabetical characters are allowed after the final "." character.

Path

Specify a path or retain the original path by using #{path}. Case sensitive.

Maximum 128 characters. Allowed characters are a-z, A-Z, 0-9; the following special characters: _-.\$/~`:@:+; & (using &); and wildcards (* and ?).

Query - optional

Specify a query or retain the original query by using #{query}. Not case sensitive.

Maximum 128 characters.

Status code▼

Thank you