Little bit Advanced

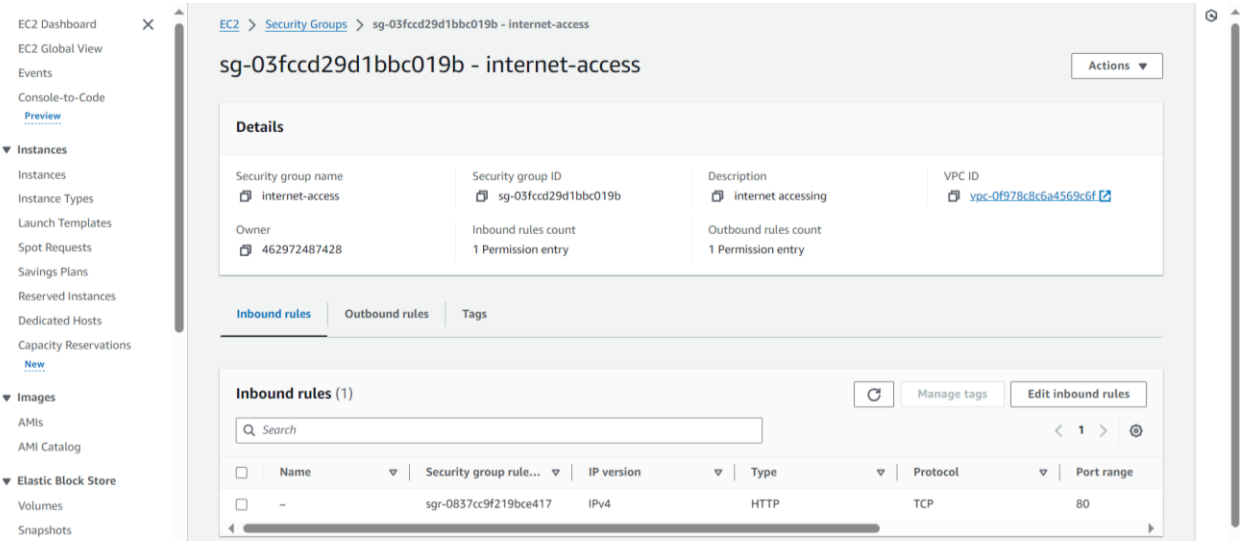
Q1. EC2 with ELB and ASG

Objective: Learn how to create a scalable and highly available web application environment using Amazon EC2 instances, ELB, and ASG.

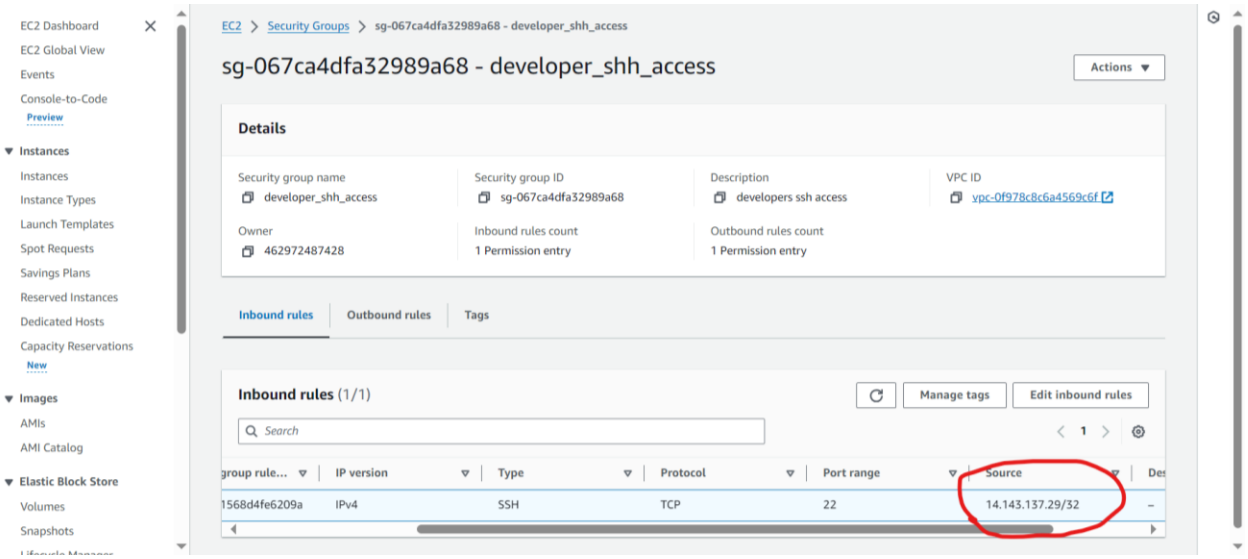
Approach:

1. Launch EC2 Instances: Start by launching two or more EC2 instances. These instances will run a simple web application (e.g., a "Hello World" page or any basic web service).
2. Configure Load Balancer: Set up an Elastic Load Balancer (ELB) to distribute incoming web traffic across your EC2 instances. This step ensures high availability and fault tolerance.
3. Set Up Auto Scaling Group (ASG): Create an ASG that uses the launched EC2 instances. Configure ASG policies to automatically scale the number of instances up or down based on criteria like CPU usage or network traffic.
4. Test Your Setup: Simulate traffic to test the scaling policies and the load balancer. Observe how ASG adds or removes instances and how ELB distributes traffic.
5. Verify Website Functionality: Ensure that the website hosted on EC2 instances remains accessible and functional during scaling operations.

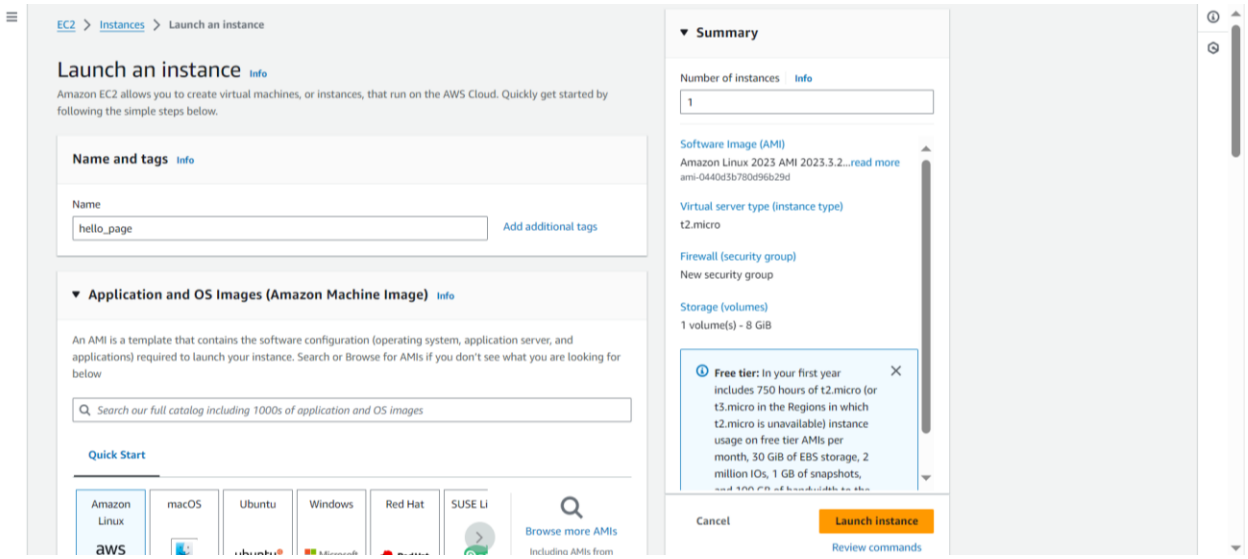
Goal: By the end of this lab, students will have a hands-on understanding of setting up a load-balanced and auto-scaled web application using AWS services.

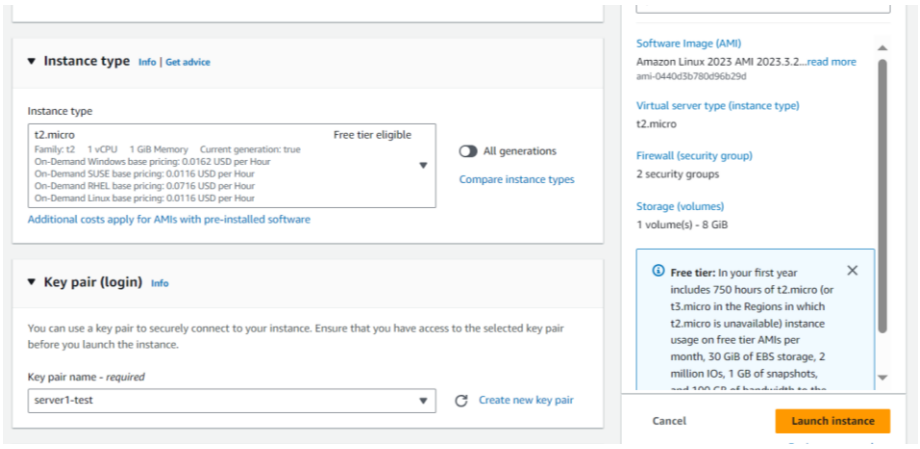


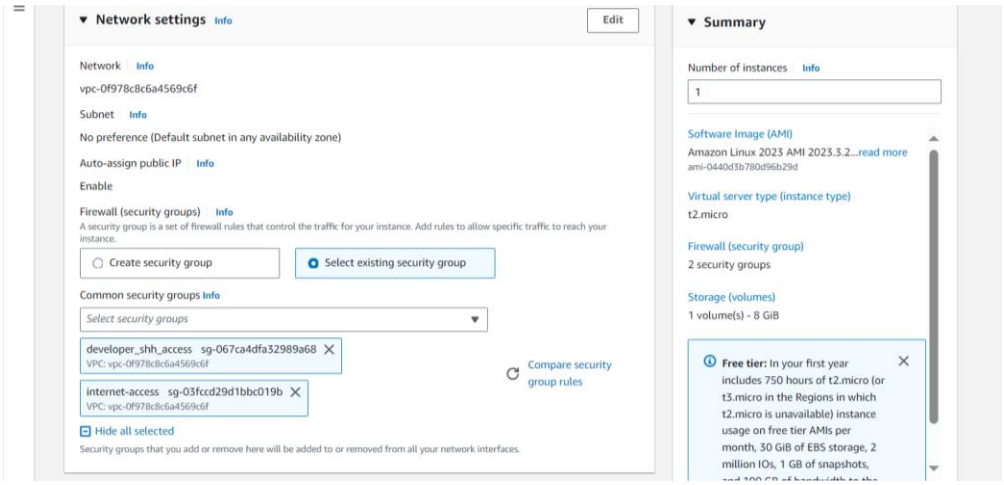
Creating security group for connecting with SSH

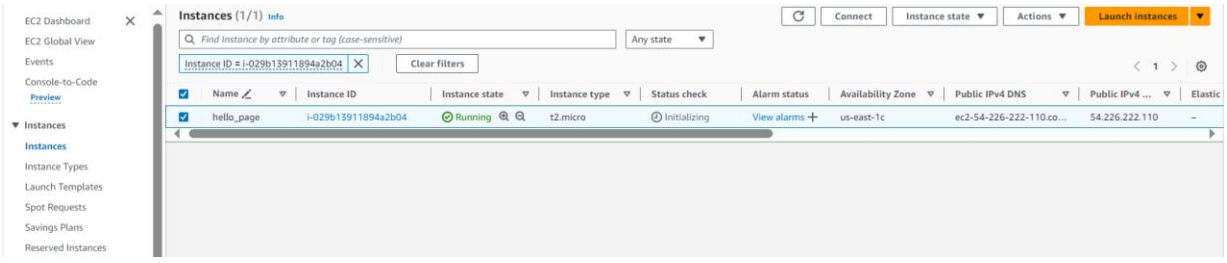


Creating EC2 instance

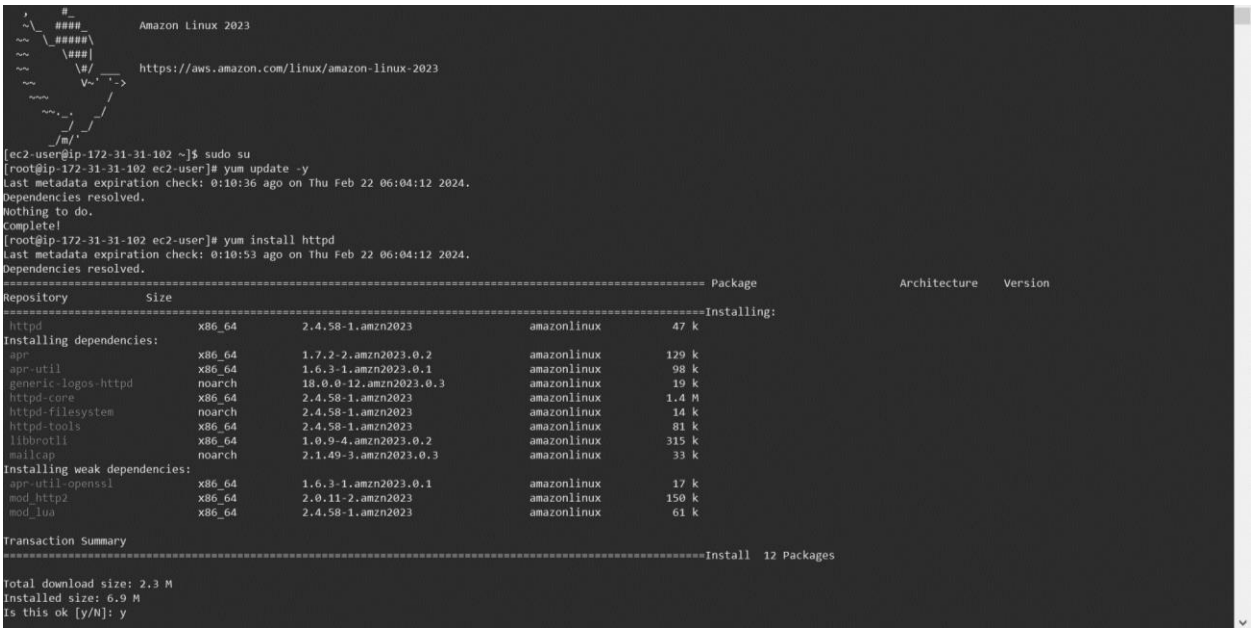



Instance type Info | Get advice
Instance type
t2.micro
Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.0716 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour
All generations
Compare instance types
Additional costs apply for AMIs with pre-installed software
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
server1-test
Create new key pair
Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...read more
ami-0440d3b780d96b29d
Virtual server type (instance type)
t2.micro
Firewall (security group)
2 security groups
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots,
Cancel
Launch instance

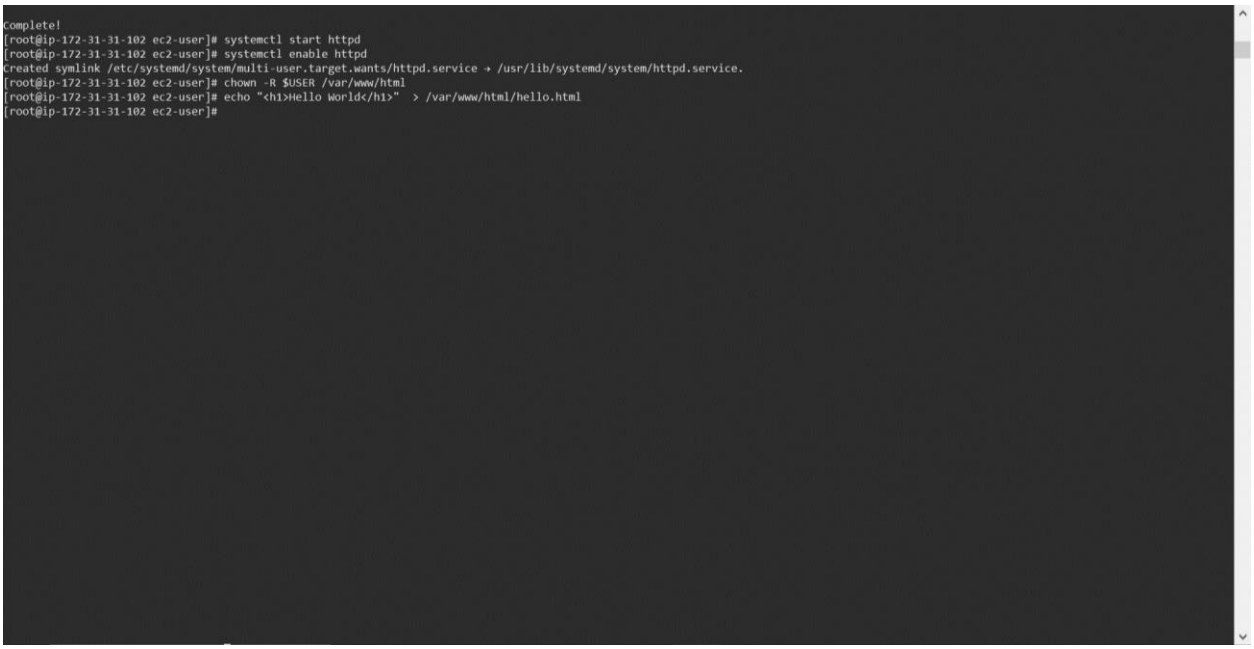

Network settings Info
Edit
Network Info
vpc-0f978c8c6a4569c6f
Subnet Info
No preference (Default subnet in any availability zone)
Auto-assign public IP Info
Enable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Common security groups Info
Select security groups
developer_shh_access sg-067ca4dfa32989a68
VPC: vpc-0f978c8c6a4569c6f
internet-access sg-03fccd29d1bbc019b
VPC: vpc-0f978c8c6a4569c6f
Compare security group rules
Hide all selected
Security groups that you add or remove here will be added to or removed from all your network interfaces.
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...read more
ami-0440d3b780d96b29d
Virtual server type (instance type)
t2.micro
Firewall (security group)
2 security groups
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots,


EC2 Dashboard
EC2 Global View
Events
Console-to-Code
Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Instances (1/1) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
Any state
Instance ID = i-029b13911894a2b04
Clear filters
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic
hello_page
i-029b13911894a2b04
Running
t2.micro
Initializing
View alarms
us-east-1c
ec2-54-226-222-110.co...
54.226.222.110

Connecting EC2 instance with SSH

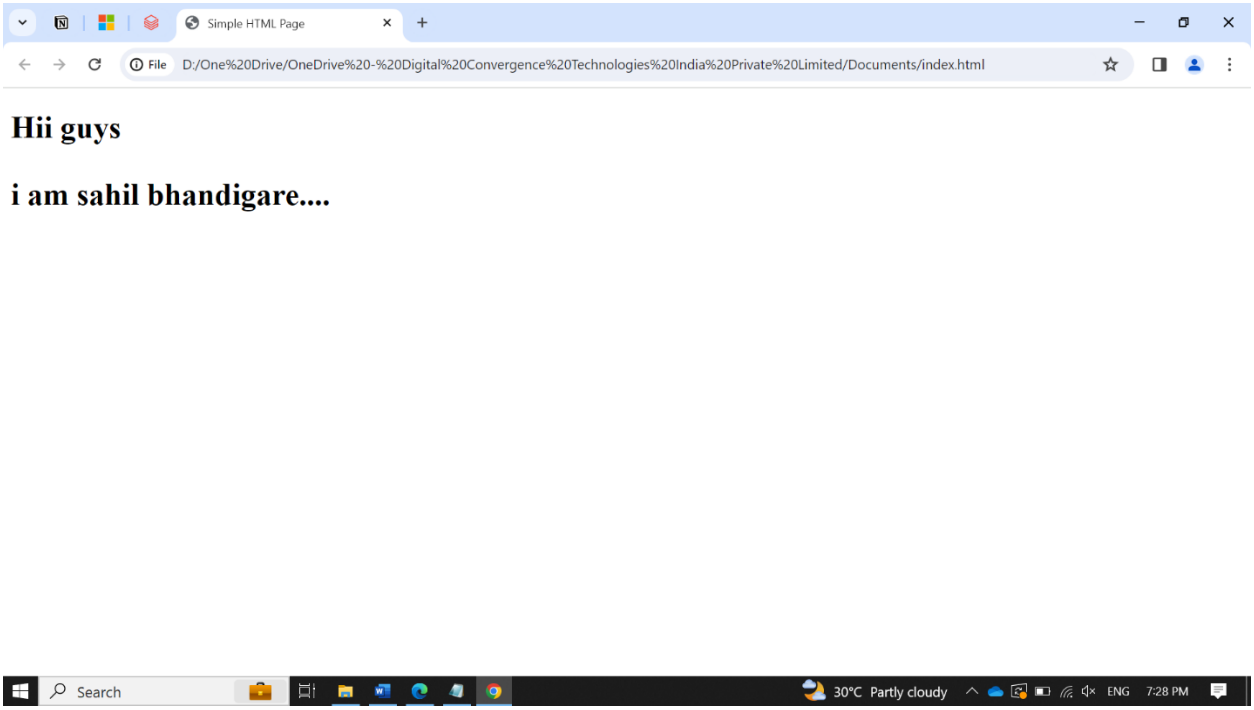


```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-172-31-31-102 ~]$ sudo su
[root@ip-172-31-31-102 ec2-user]# yum update -y
Last metadata expiration check: 0:10:36 ago on Thu Feb 22 06:04:12 2024.
Dependencies resolved.
Nothing to do.
Complete!
[root@ip-172-31-31-102 ec2-user]# yum install httpd
Last metadata expiration check: 0:10:53 ago on Thu Feb 22 06:04:12 2024.
Dependencies resolved.
================================================================================ Package                    Architecture    Version
Repository            Size
================================================================================Installing:
 httpd                x86_64          2.4.58-1.amzn2023               amazonlinux          47 k
Installing dependencies:
 apr                  x86_64          1.7.2-2.amzn2023.0.2            amazonlinux         129 k
 apr-util             x86_64          1.6.3-1.amzn2023.0.1            amazonlinux          98 k
 generic-logos-httpd  noarch          18.0.0-12.amzn2023.0.3          amazonlinux          19 k
 httpd-core           x86_64          2.4.58-1.amzn2023               amazonlinux         1.4 M
 httpd-filesystem     noarch          2.4.58-1.amzn2023               amazonlinux          14 k
 httpd-tools          x86_64          2.4.58-1.amzn2023               amazonlinux          81 k
 libbrotli            x86_64          1.0.9-4.amzn2023.0.2            amazonlinux         315 k
 mailcap              noarch          2.1.49-3.amzn2023.0.3           amazonlinux          33 k
Installing weak dependencies:
 apr-util-openssl     x86_64          1.6.3-1.amzn2023.0.1            amazonlinux          17 k
 mod_http2            x86_64          2.0.11-2.amzn2023               amazonlinux         150 k
 mod_lua              x86_64          2.4.58-1.amzn2023               amazonlinux          61 k

Transaction Summary
================================================================================Install  12 Packages

Total download size: 2.3 M
Installed size: 6.9 M
Is this ok [y/N]: y
```

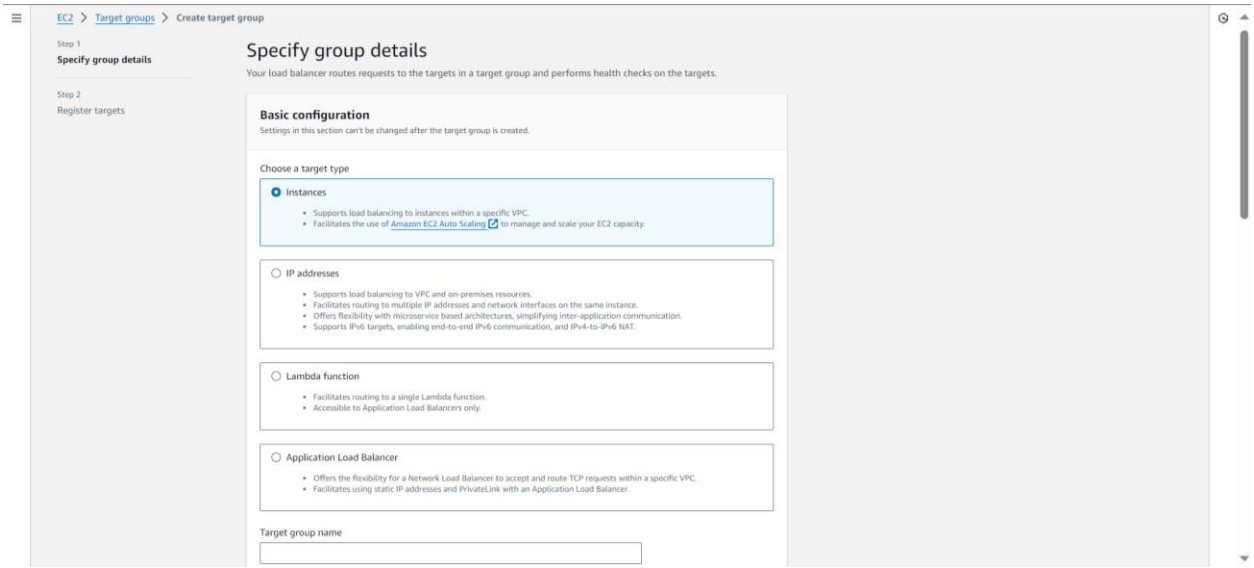


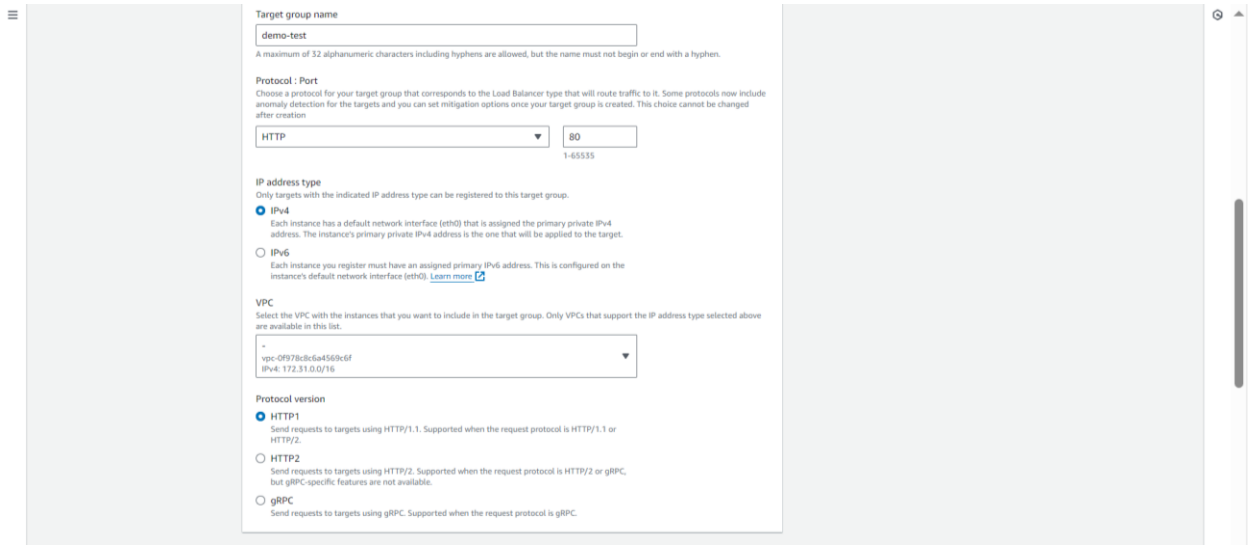
```
Complete!
[root@ip-172-31-31-102 ec2-user]# systemctl start httpd
[root@ip-172-31-31-102 ec2-user]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@ip-172-31-31-102 ec2-user]# chown -R $USER /var/www/html
[root@ip-172-31-31-102 ec2-user]# echo "<h1>Hello World</h1>"  > /var/www/html/hello.html
[root@ip-172-31-31-102 ec2-user]#
```

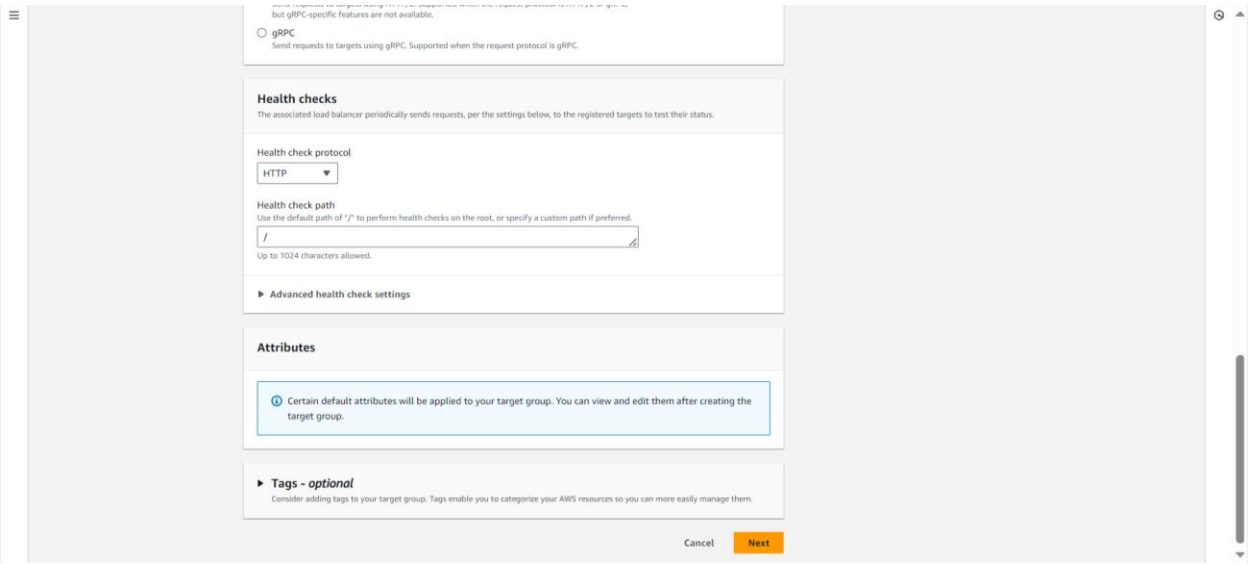
Opening web page with Public-IP

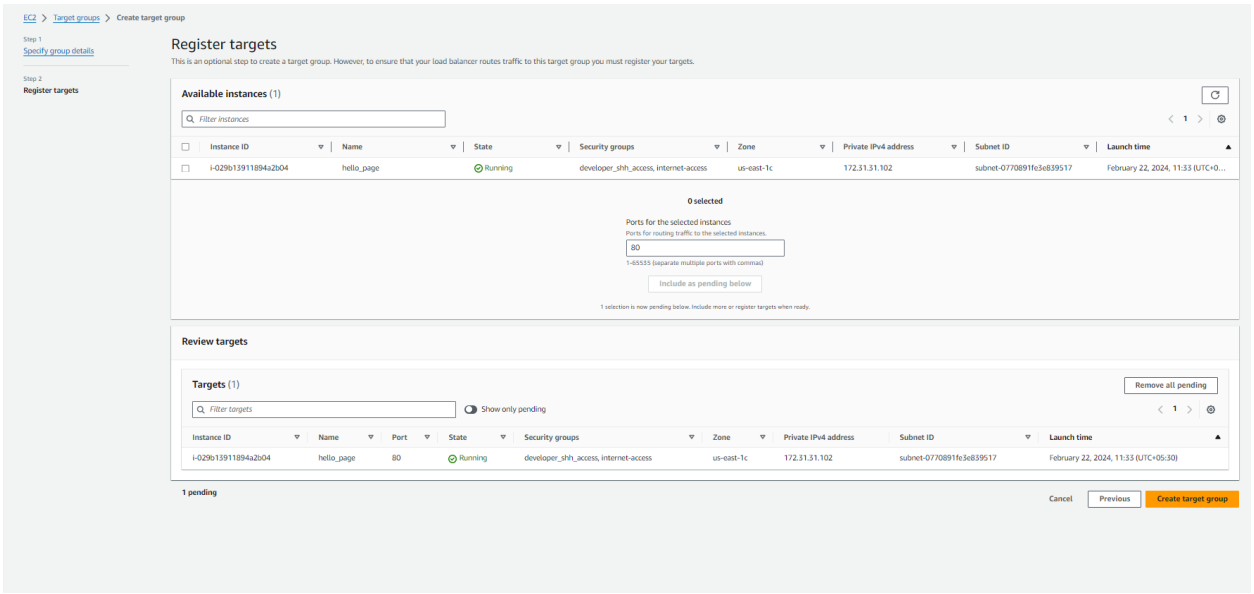


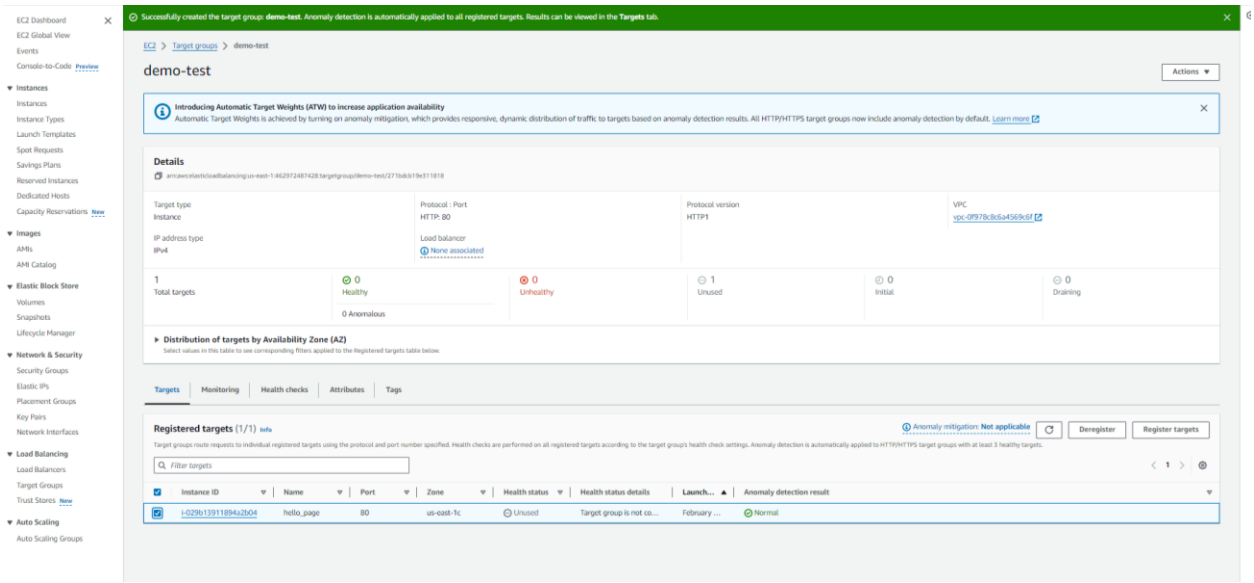
Creating target group before load balancer to allocate EC2 as a target



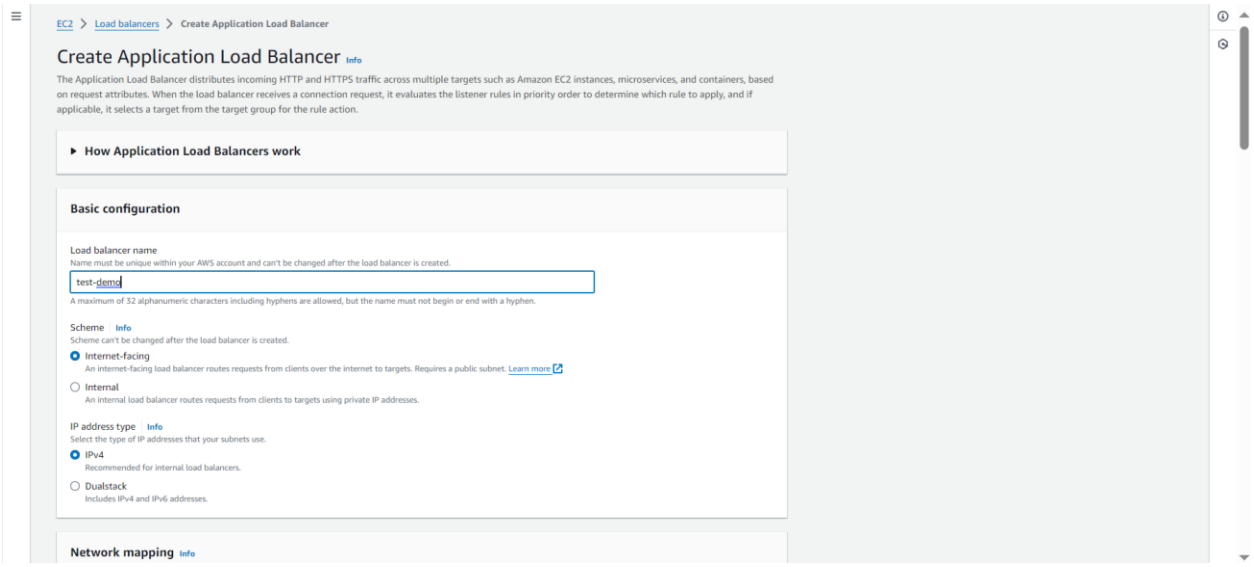

Target group name
demo-test
A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.
Protocol : Port
Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation
HTTP
80
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.
-
vpc-0f978c8c6a4569c6f
IPv4: 172.31.0.0/16
Protocol version
HTTP1
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.
HTTP2
Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.
gRPC
Send requests to targets using gRPC. Supported when the request protocol is gRPC.

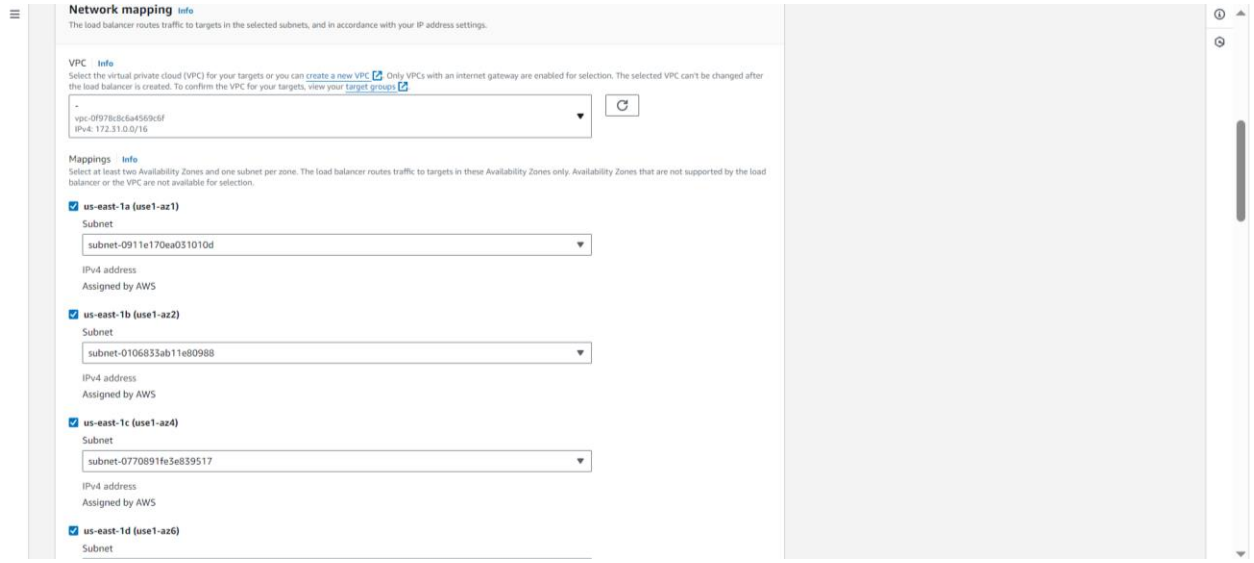

but gRPC-specific features are not available.
gRPC
Send requests to targets using gRPC. Supported when the request protocol is gRPC.
Health checks
The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.
Health check protocol
HTTP
Health check path
Use the default path of "/" to perform health checks on the root, or specify a custom path if preferred.
/
Up to 1024 characters allowed.
Advanced health check settings
Attributes
Certain default attributes will be applied to your target group. You can view and edit them after creating the target group.
Tags - optional
Consider adding tags to your target group. Tags enable you to categorize your AWS resources so you can more easily manage them.
Cancel
Next


EC2 > Target groups > Create target group
Step 1
Specify group details
Step 2
Register targets
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)
Filter instances
Instance ID
Name
State
Security groups
Zone
Private IPv4 address
Subnet ID
Launch time
i-029b13911894a2b04
hello_page
Running
developer_shh_access, internet-access
us-east-1c
172.31.31.102
subnet-0770891fe3e839517
February 22, 2024, 11:33 (UTC+0...
0 selected
Ports for the selected instances
Ports for routing traffic to the selected instances.
80
1-65535 (separate multiple ports with commas)
Include as pending below
1 selection is now pending below. Include more or register targets when ready.
Review targets
Targets (1)
Remove all pending
Filter targets
Show only pending
Instance ID
Name
Port
State
Security groups
Zone
Private IPv4 address
Subnet ID
Launch time
i-029b13911894a2b04
hello_page
80
Running
developer_shh_access, internet-access
us-east-1c
172.31.31.102
subnet-0770891fe3e839517
February 22, 2024, 11:33 (UTC+05:30)
1 pending
Cancel
Previous
Create target group

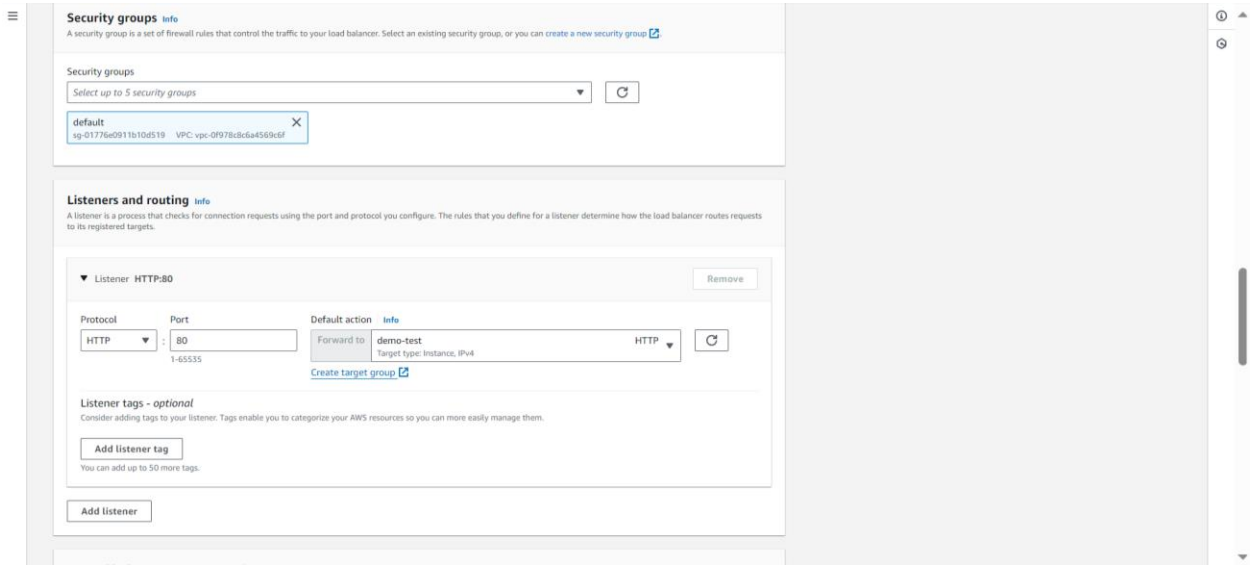

Successfully created the target group: demo-test. Anomaly detection is automatically applied to all registered targets. Results can be viewed in the Targets tab.
EC2 > Target groups > demo-test
demo-test
Actions
Introducing Automatic Target Weights (ATW) to increase application availability
Automatic Target Weights is achieved by turning on anomaly mitigation, which provides responsive, dynamic distribution of traffic to targets based on anomaly detection results. All HTTP/HTTPS target groups now include anomaly detection by default. Learn more
Details
Target type
Instance
Protocol : Port
HTTP: 80
Protocol version
HTTP1
VPC
vpc-0f978c8c6a4569c6f
IP address type
IPv4
Load balancer
None associated
1
Total targets
0
Healthy
0 Anomalous
0
Unhealthy
1
Unused
0
Initial
0
Draining
Distribution of targets by Availability Zone (AZ)
Targets
Monitoring
Health checks
Attributes
Tags
Registered targets (1/1)
Anomaly mitigation: Not applicable
Deregister
Register targets
Filter targets
Instance ID
Name
Port
Zone
Health status
Health status details
Launch...
Anomaly detection result
i-029b13911894a2b04
hello_page
80
us-east-1c
Unused
Target group is not co...
February ...
Normal

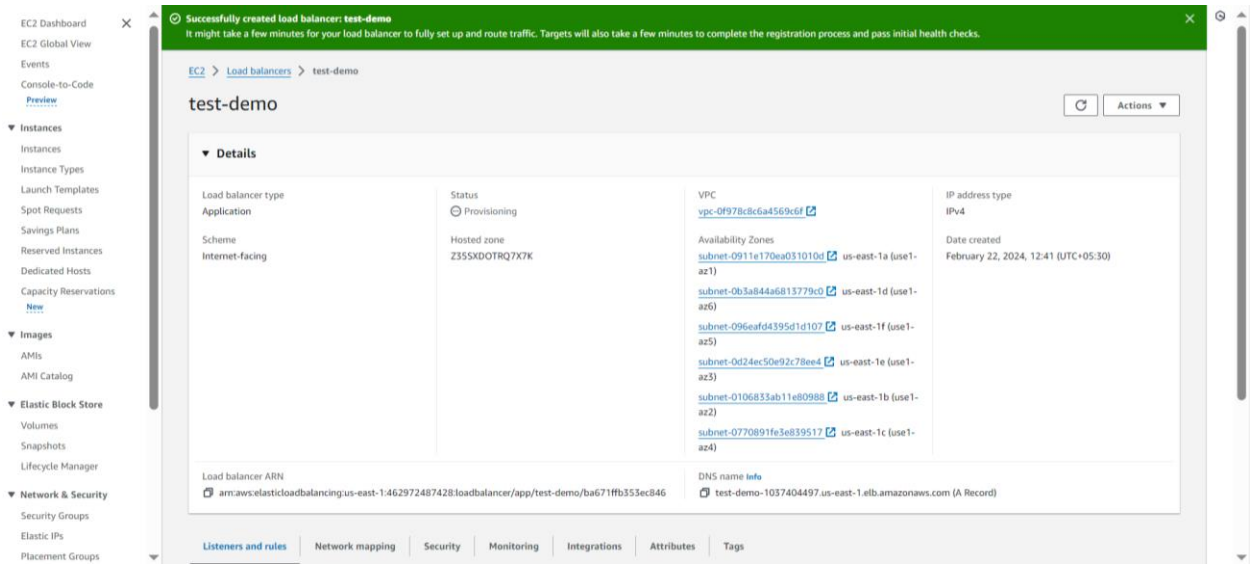
Creating application load balancer



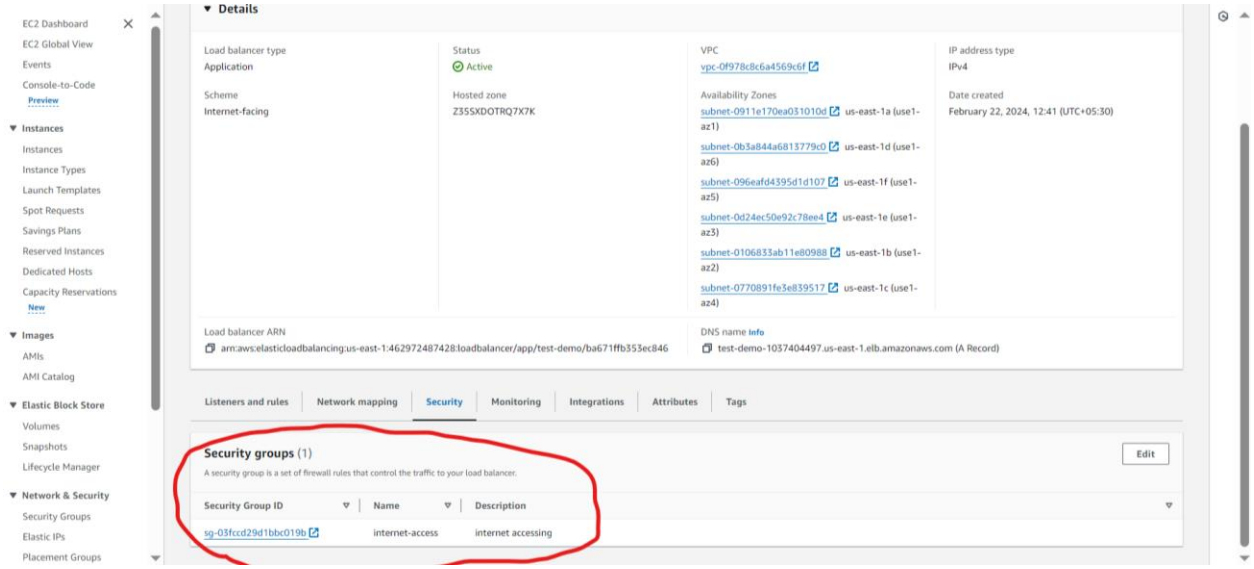


Creating security group

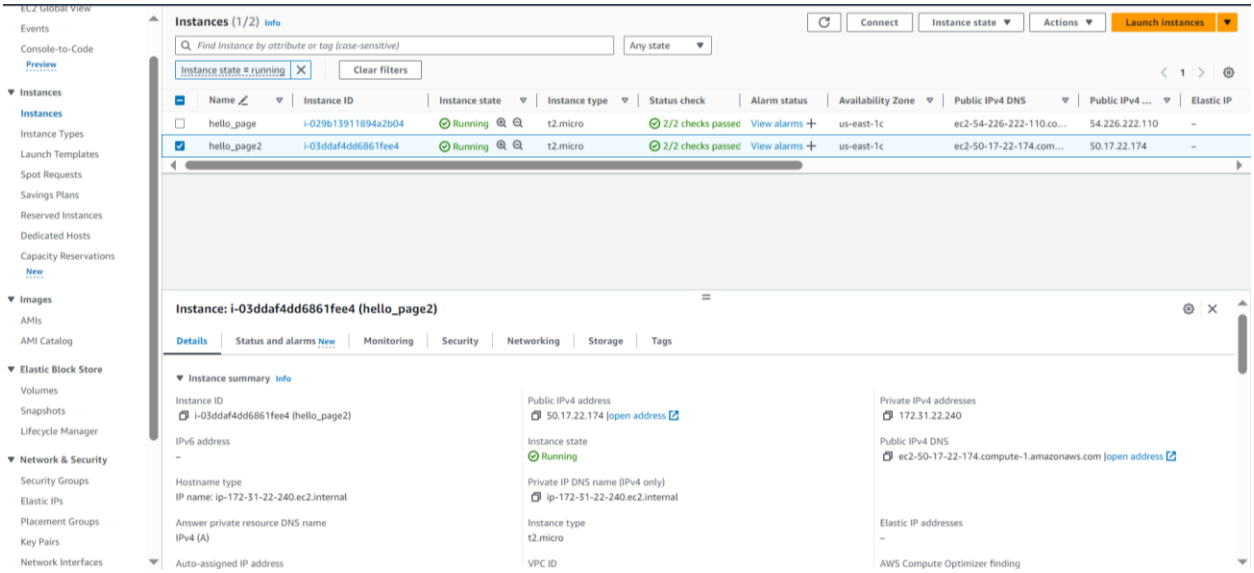


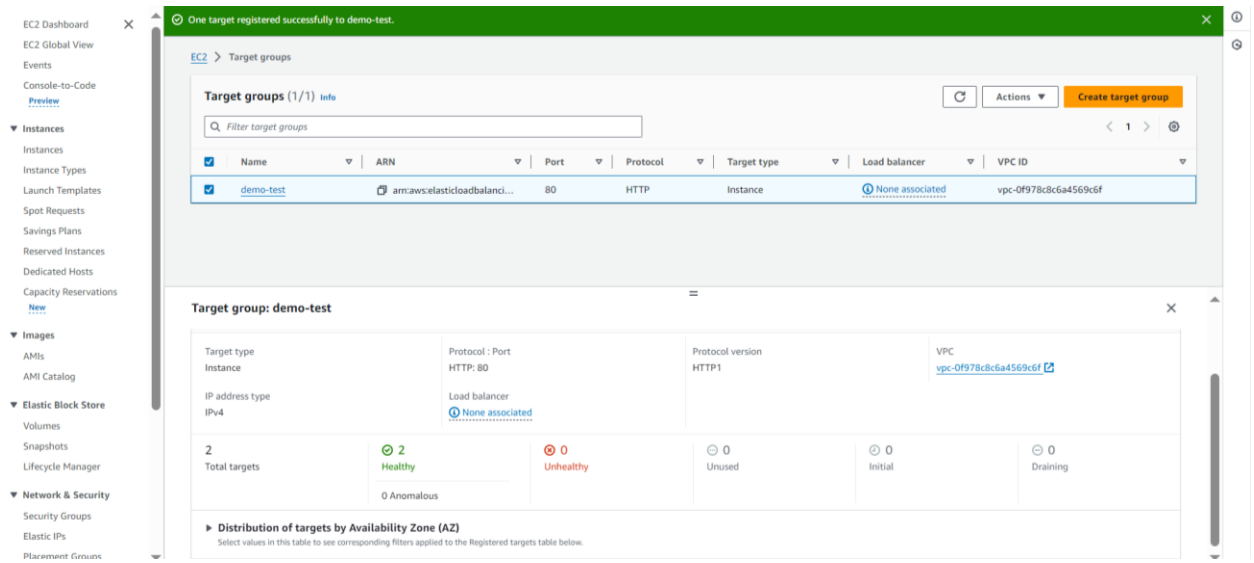


Adding security group

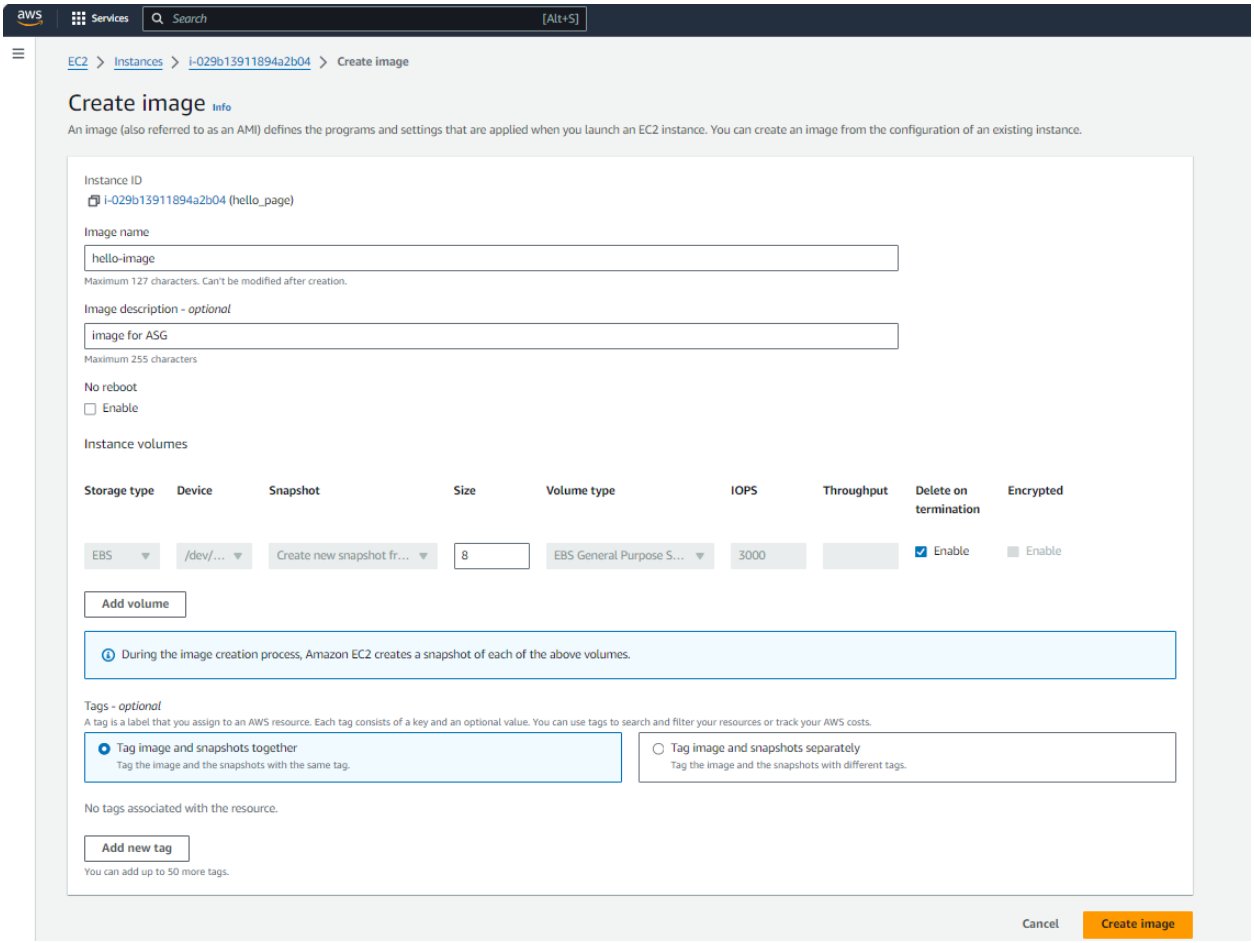


Creating another EC2

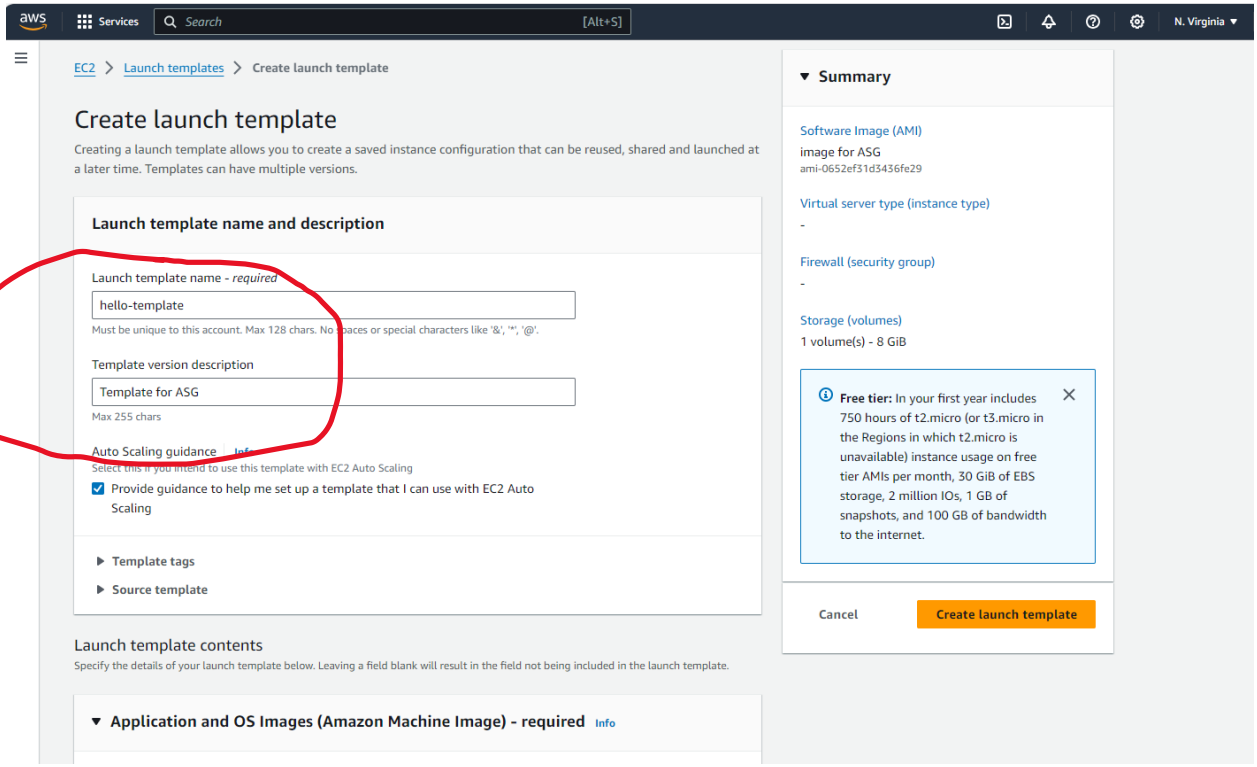


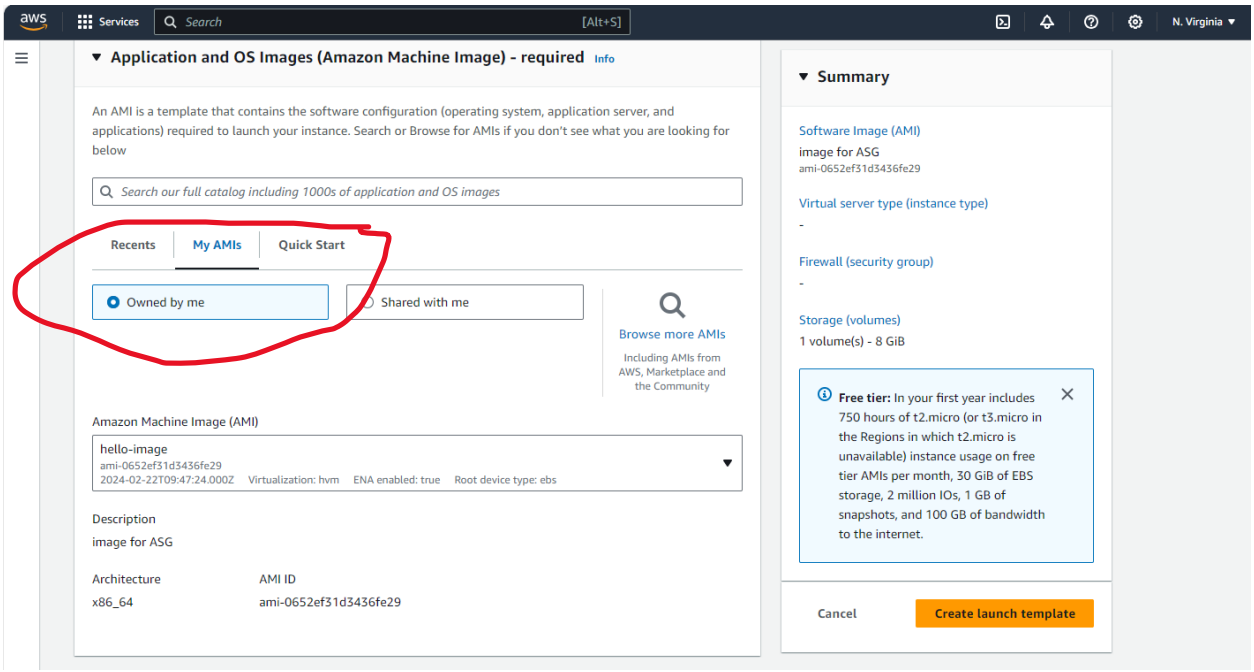


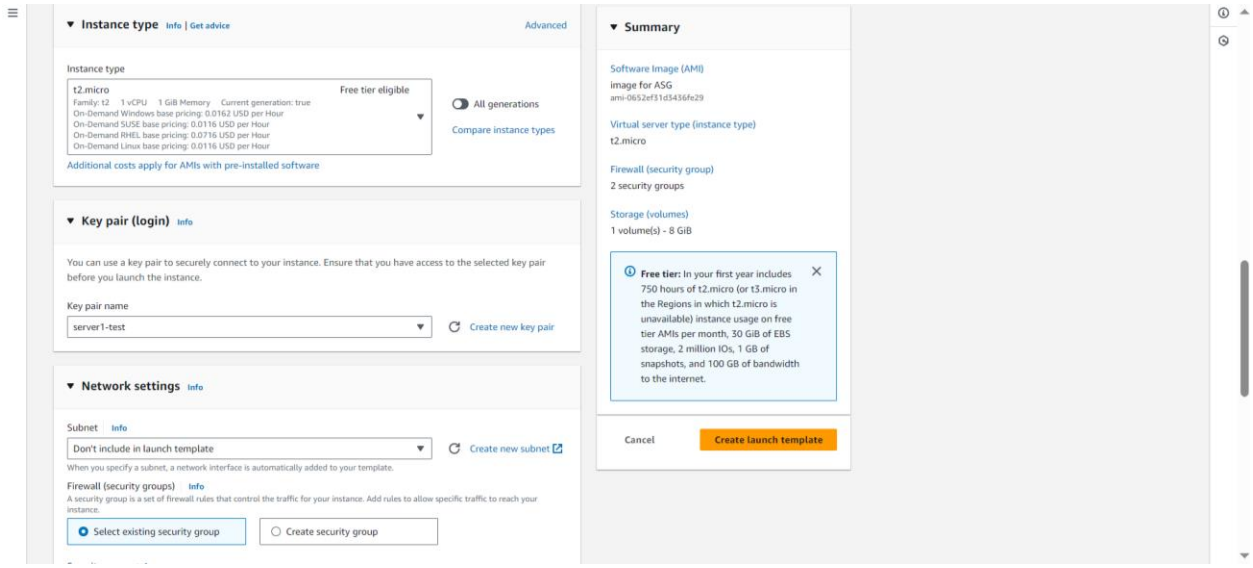
Creating image

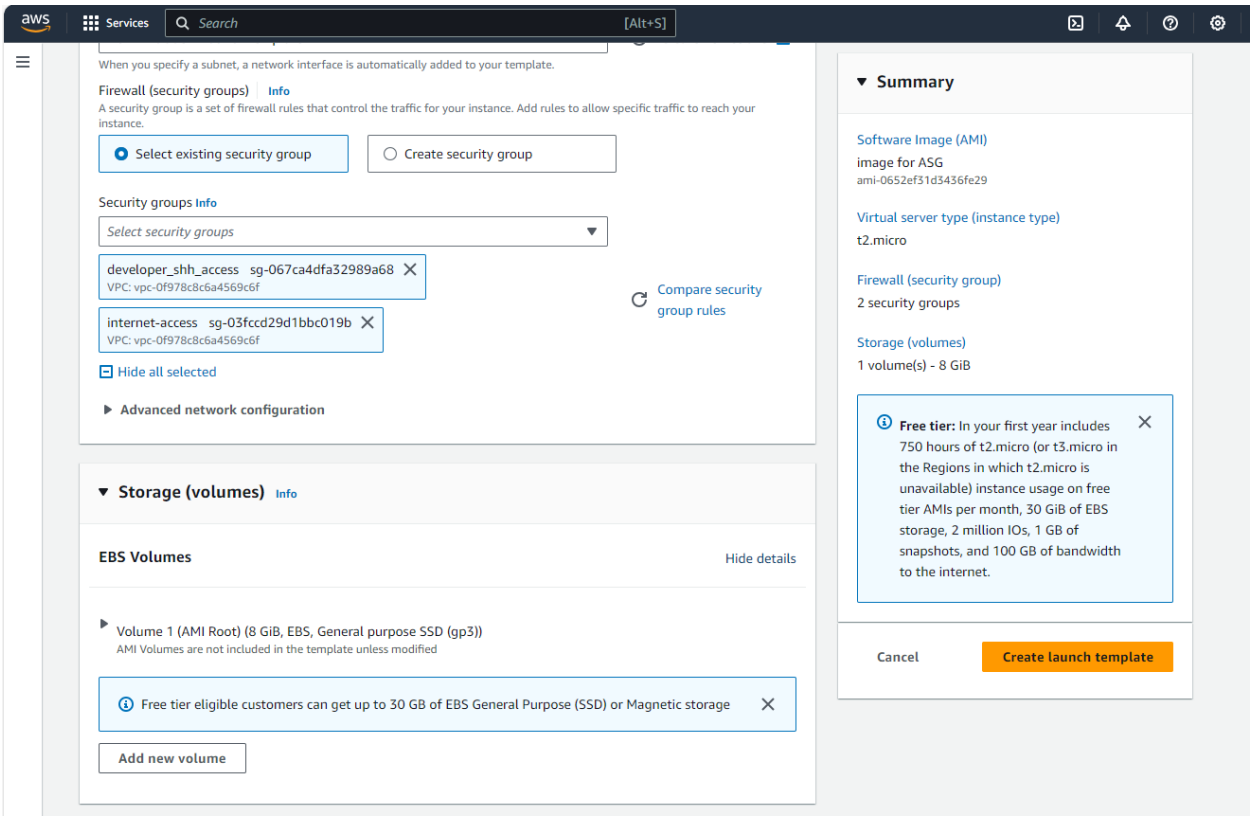


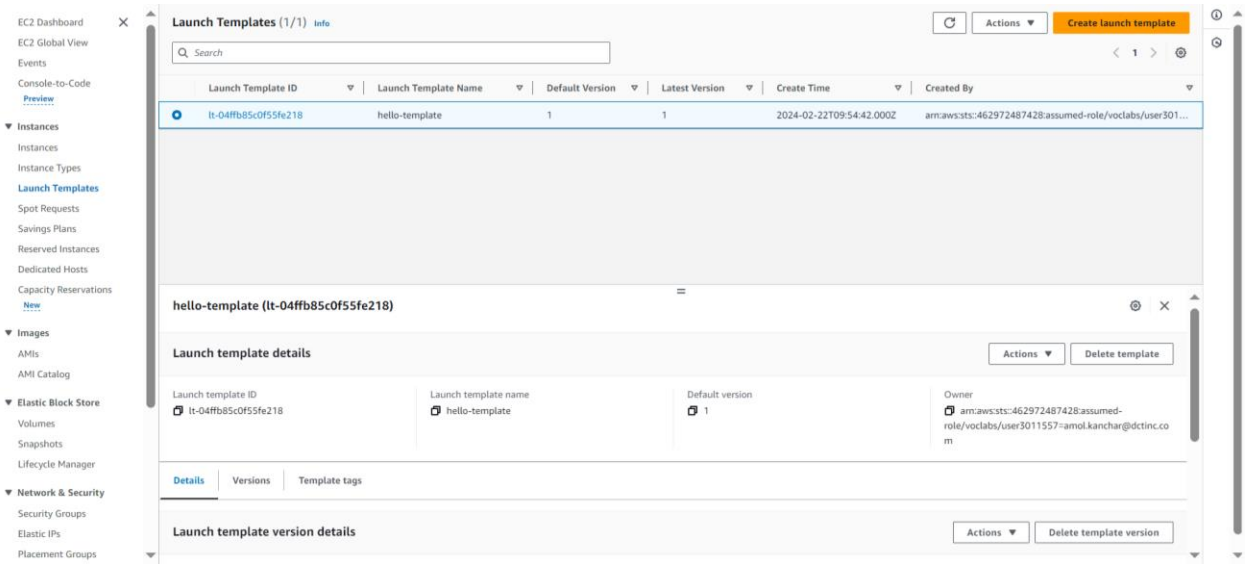
Creating Template for ASG



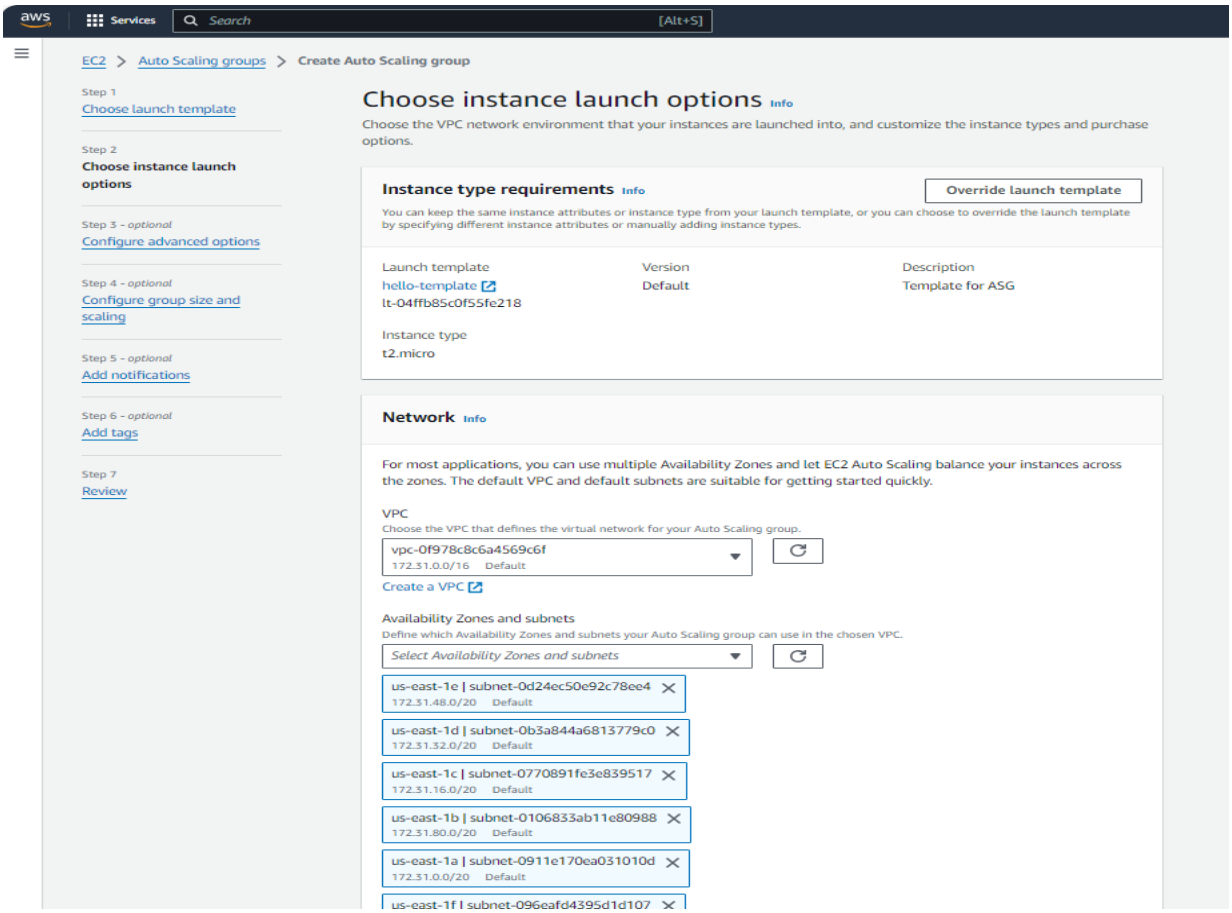


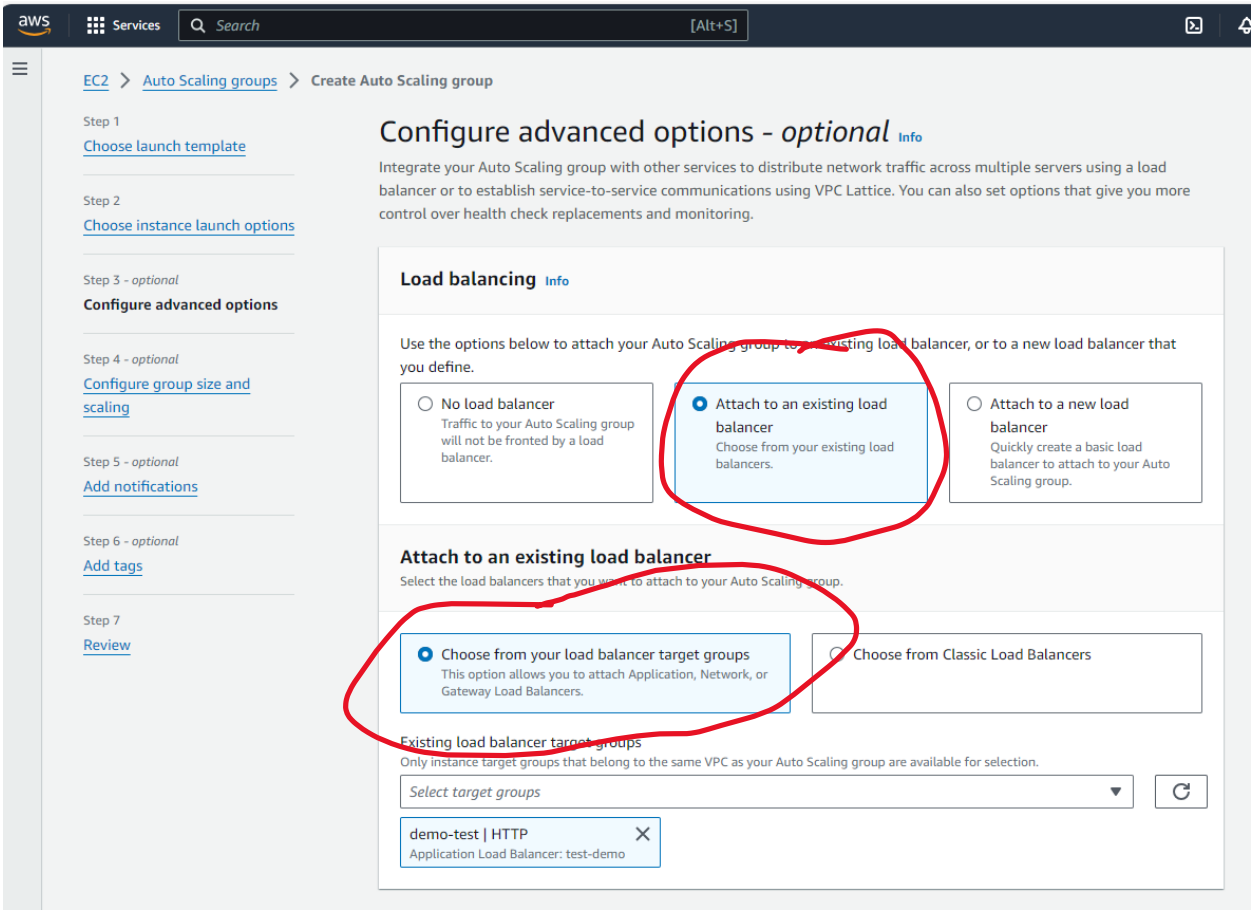

Instance type Info | Get advice
Advanced
Instance type
t2.micro
Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.0716 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour
All generations
Compare instance types
Additional costs apply for AMIs with pre-installed software
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
server1-test
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
Summary
Software Image (AMI)
image for ASG
ami-0652ef31d3436fe29
Virtual server type (instance type)
t2.micro
Firewall (security group)
2 security groups
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.
Cancel
Create launch template

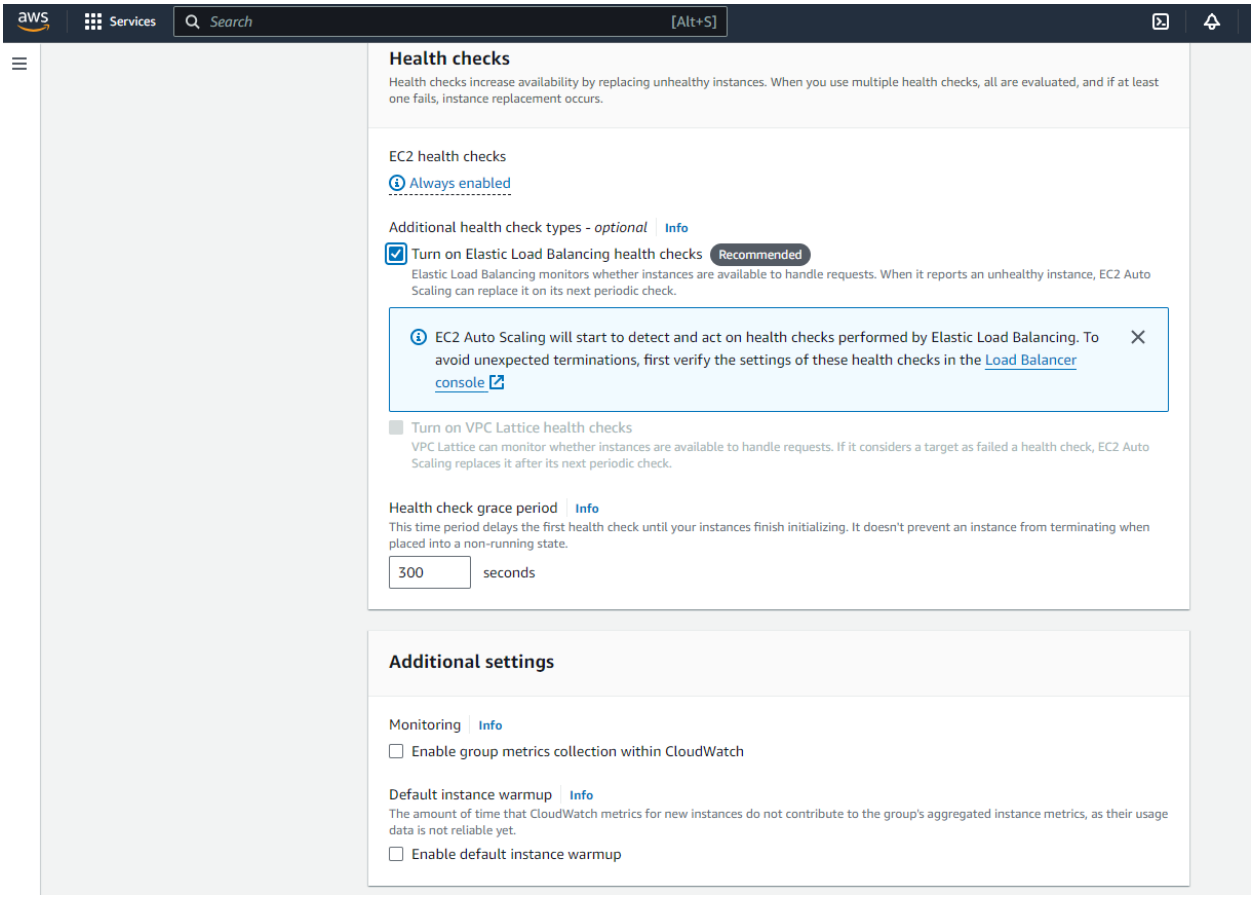

aws
Services
Search
[Alt+S]
When you specify a subnet, a network interface is automatically added to your template.
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Select existing security group
Create security group
Security groups Info
Select security groups
developer_shh_access sg-067ca4dfa32989a68
VPC: vpc-0f978c8c6a4569c6f
internet-access sg-03fccd29d1bbc019b
VPC: vpc-0f978c8c6a4569c6f
Compare security group rules
Hide all selected
Advanced network configuration
Storage (volumes) Info
EBS Volumes
Hide details
Volume 1 (AMI Root) (8 GiB, EBS, General purpose SSD (gp3))
AMI Volumes are not included in the template unless modified
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage
Add new volume
Summary
Software Image (AMI)
image for ASG
ami-0652ef31d3436fe29
Virtual server type (instance type)
t2.micro
Firewall (security group)
2 security groups
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.
Cancel
Create launch template

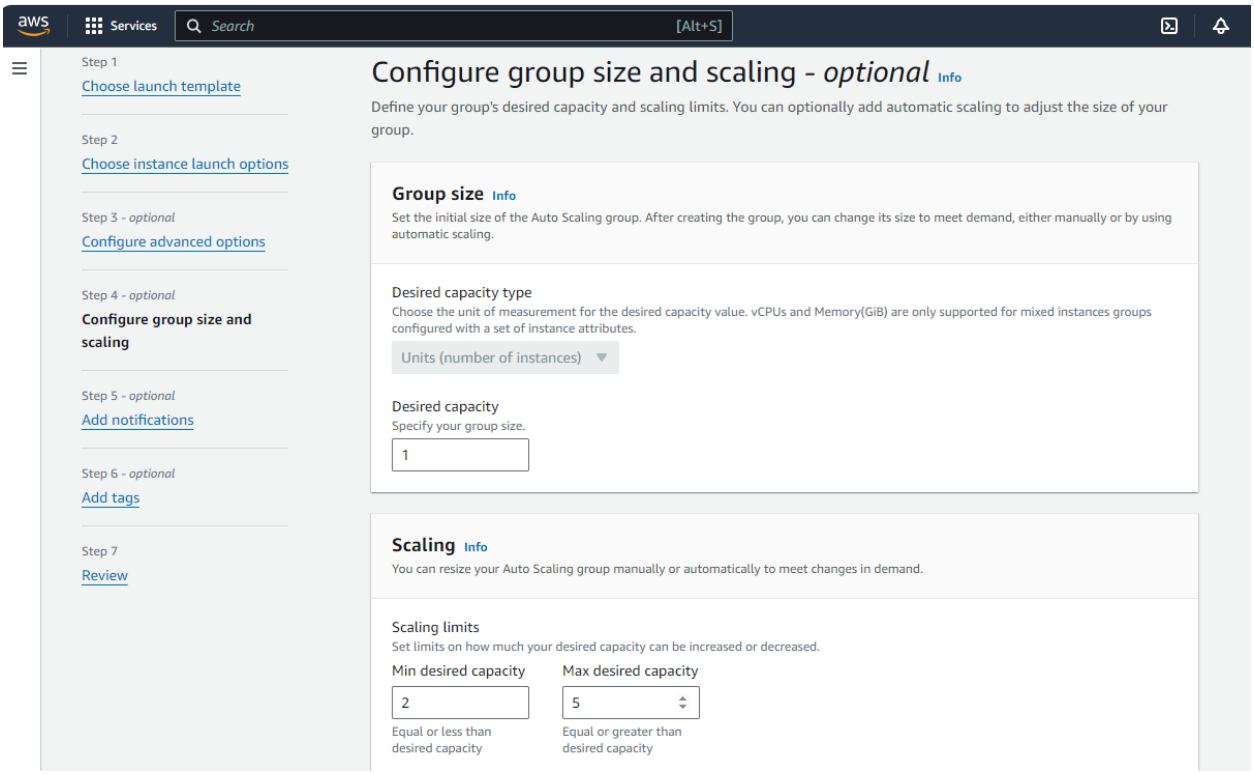

EC2 Dashboard
EC2 Global View
Events
Console-to-Code
Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Launch Templates (1/1) Info
Actions
Create launch template
Search
1
Launch Template ID
Launch Template Name
Default Version
Latest Version
Create Time
Created By
lt-04ffb85c0f55fe218
hello-template
1
1
2024-02-22T09:54:42.000Z
arn:aws:sts::462972487428:assumed-role/voclabs/user301...
hello-template (lt-04ffb85c0f55fe218)
Launch template details
Actions
Delete template
Launch template ID
lt-04ffb85c0f55fe218
Launch template name
hello-template
Default version
1
Owner
arn:aws:sts::462972487428:assumed-role/voclabs/user3011557=amol.kanchar@dctinc.com
Details
Versions
Template tags
Launch template version details
Actions
Delete template version

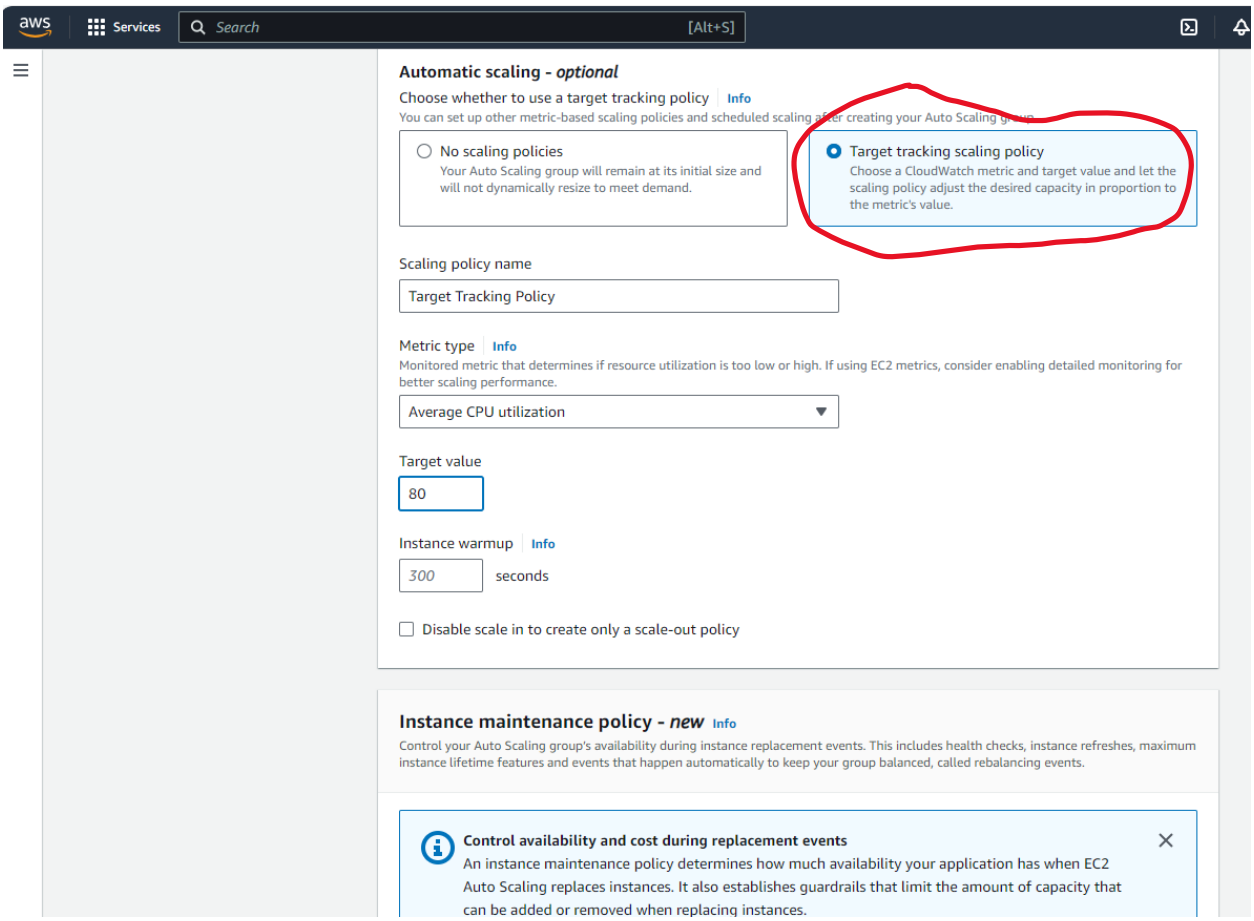
Creating ASG

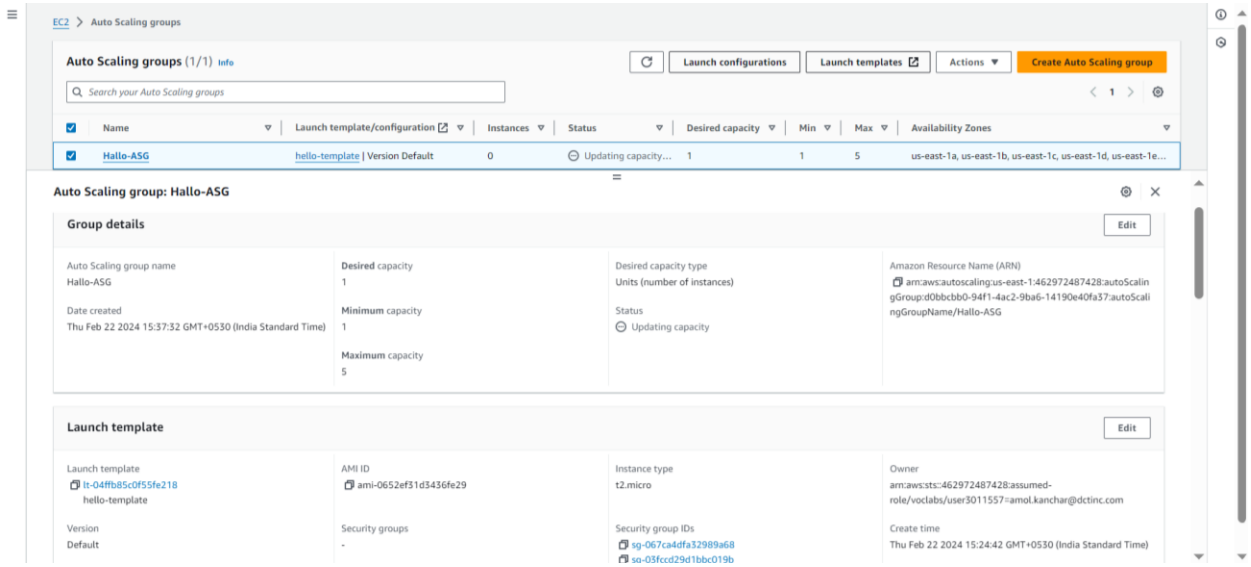


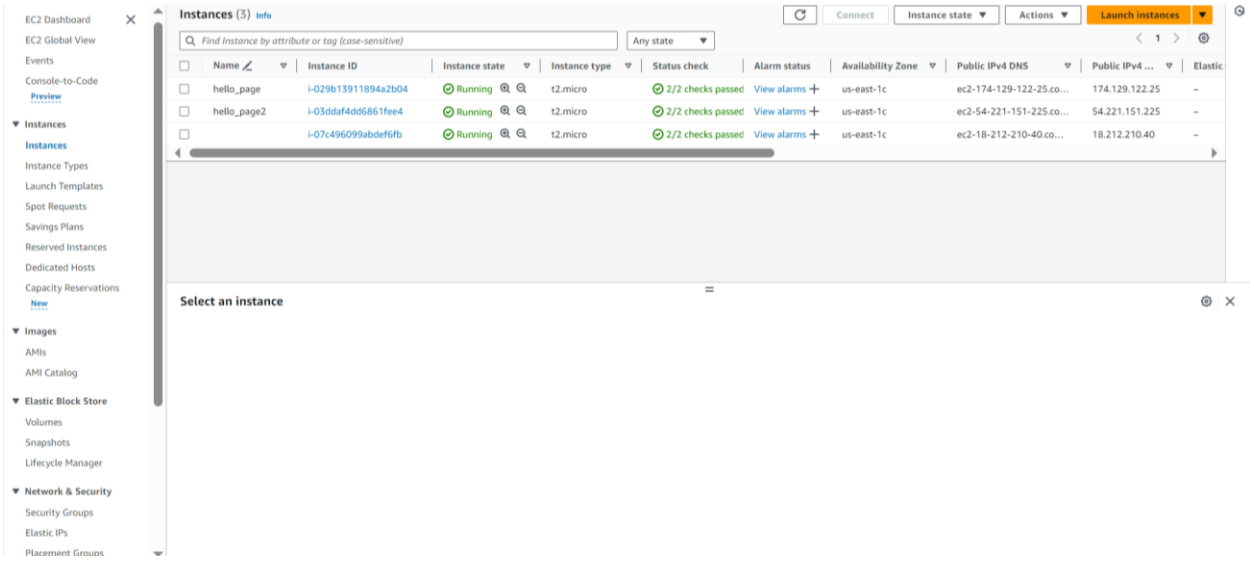

aws
Services
Search
[Alt+S]
EC2 > Auto Scaling groups > Create Auto Scaling group
Step 1
Choose launch template
Step 2
Choose instance launch options
Step 3 - optional
Configure advanced options
Step 4 - optional
Configure group size and scaling
Step 5 - optional
Add notifications
Step 6 - optional
Add tags
Step 7
Review
Configure advanced options - optional Info
Integrate your Auto Scaling group with other services to distribute network traffic across multiple servers using a load balancer or to establish service-to-service communications using VPC Lattice. You can also set options that give you more control over health check replacements and monitoring.
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 an existing load balancer
Select the load balancers that you want to attach to your Auto Scaling group.
Choose from your load balancer target groups
This option allows you to attach Application, Network, or Gateway Load Balancers.
Choose from Classic Load Balancers
Existing load balancer target groups
Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.
Select target groups
demo-test | HTTP
Application Load Balancer: test-demo

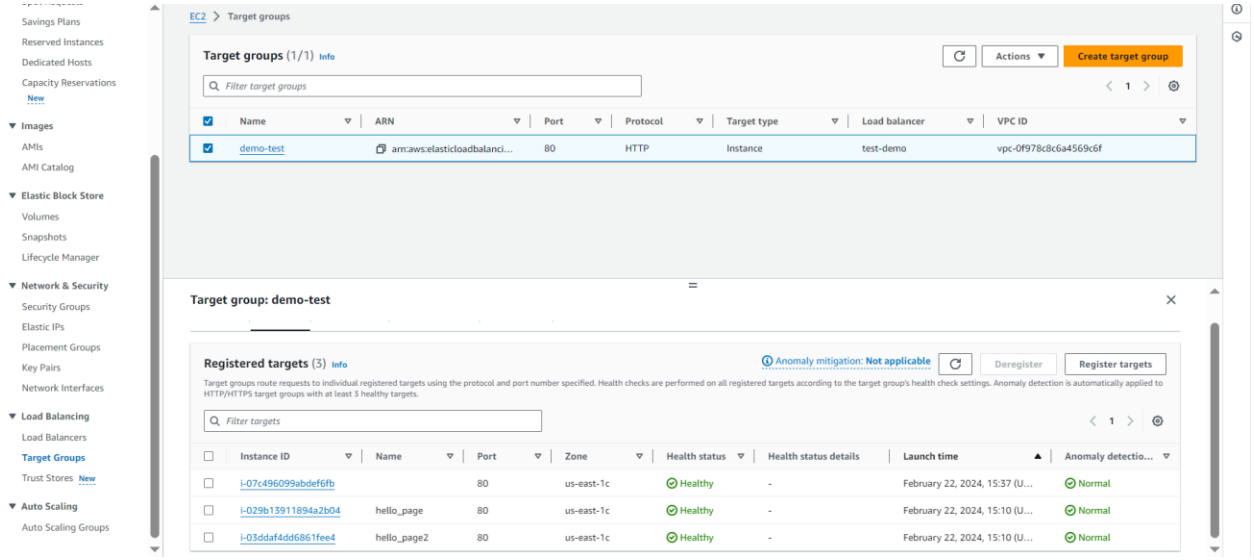

aws
Services
Search
[Alt+S]
Health checks
Health checks increase availability by replacing unhealthy instances. When you use multiple health checks, all are evaluated, and if at least one fails, instance replacement occurs.
EC2 health checks
Always enabled
Additional health check types - optional
Info
Turn on Elastic Load Balancing health checks
Recommended
Elastic Load Balancing monitors whether instances are available to handle requests. When it reports an unhealthy instance, EC2 Auto Scaling can replace it on its next periodic check.
EC2 Auto Scaling will start to detect and act on health checks performed by Elastic Load Balancing. To avoid unexpected terminations, first verify the settings of these health checks in the Load Balancer console
Turn on VPC Lattice health checks
VPC Lattice can monitor whether instances are available to handle requests. If it considers a target as failed a health check, EC2 Auto Scaling replaces it after its next periodic check.
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.
300
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.
Enable default instance warmup


aws
Services
Search
[Alt+S]
Step 1
Choose launch template
Step 2
Choose instance launch options
Step 3 - optional
Configure advanced options
Step 4 - optional
Configure group size and scaling
Step 5 - optional
Add notifications
Step 6 - optional
Add tags
Step 7
Review
Configure group size and scaling - optional Info
Define your group's desired capacity and scaling limits. You can optionally add automatic scaling to adjust the size of your group.
Group size Info
Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.
Desired capacity type
Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.
Units (number of instances)
Desired capacity
Specify your group size.
1
Scaling Info
You can resize your Auto Scaling group manually or automatically to meet changes in demand.
Scaling limits
Set limits on how much your desired capacity can be increased or decreased.
Min desired capacity
2
Equal or less than desired capacity
Max desired capacity
5
Equal or greater than desired capacity


aws
Services
Search
[Alt+S]
Automatic scaling - optional
Choose whether to use a target tracking policy Info
You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.
No scaling policies
Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.
Target tracking scaling policy
Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.
Scaling policy name
Target Tracking Policy
Metric type Info
Monitored metric that determines if resource utilization is too low or high. If using EC2 metrics, consider enabling detailed monitoring for better scaling performance.
Average CPU utilization
Target value
80
Instance warmup Info
300
seconds
Disable scale in to create only a scale-out policy
Instance maintenance policy - new Info
Control your Auto Scaling group's availability during instance replacement events. This includes health checks, instance refreshes, maximum instance lifetime features and events that happen automatically to keep your group balanced, called rebalancing events.
Control availability and cost during replacement events
An instance maintenance policy determines how much availability your application has when EC2 Auto Scaling replaces instances. It also establishes guardrails that limit the amount of capacity that can be added or removed when replacing instances.


EC2 > Auto Scaling groups
Auto Scaling groups (1/1) Info
Launch configurations
Launch templates
Actions
Create Auto Scaling group
Search your Auto Scaling groups
Name
Launch template/configuration
Instances
Status
Desired capacity
Min
Max
Availability Zones
Hallo-ASG
hello-template | Version Default
0
Updating capacity...
1
1
5
us-east-1a, us-east-1b, us-east-1c, us-east-1d, us-east-1e...
Auto Scaling group: Hallo-ASG
Group details
Edit
Auto Scaling group name
Hallo-ASG
Date created
Thu Feb 22 2024 15:37:32 GMT+0530 (India Standard Time)
Desired capacity
1
Minimum capacity
1
Maximum capacity
5
Desired capacity type
Units (number of instances)
Status
Updating capacity
Amazon Resource Name (ARN)
arn:aws:autoscaling:us-east-1:462972487428:autoScalingGroup:d0bbcbb0-94f1-4ac2-9ba6-14190e40fa37:autoScalingGroupName/Hallo-ASG
Launch template
Edit
Launch template
lt-04ffb85c0f55fe218
hello-template
Version
Default
AMI ID
ami-0652ef31d3436fe29
Security groups
-
Instance type
t2.micro
Security group IDs
sg-067ca4dfa32989a68
sg-03fccd29d1bbc019b
Owner
arn:aws:sts::462972487428:assumed-role/voclabs/user3011557=amol.kanchar@dctinc.com
Create time
Thu Feb 22 2024 15:24:42 GMT+0530 (India Standard Time)


EC2 Dashboard
EC2 Global View
Events
Console-to-Code
Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Instances (3) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
Any state
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic
hello_page
i-029b13911894a2b04
Running
t2.micro
2/2 checks passed
View alarms
us-east-1c
ec2-174-129-122-25.co...
174.129.122.25
hello_page2
i-03ddaf4dd6861fee4
Running
t2.micro
2/2 checks passed
View alarms
us-east-1c
ec2-54-221-151-225.co...
54.221.151.225
i-07c496099abdef6fb
Running
t2.micro
2/2 checks passed
View alarms
us-east-1c
ec2-18-212-210-40.co...
18.212.210.40
Select an instance


Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Load Balancing
Load Balancers
Target Groups
Trust Stores New
Auto Scaling
Auto Scaling Groups
EC2 > Target groups
Target groups (1/1) Info
Actions
Create target group
Filter target groups
Name
ARN
Port
Protocol
Target type
Load balancer
VPC ID
demo-test
arn:aws:elasticloadbalanci...
80
HTTP
Instance
test-demo
vpc-0f978c8c6a4569c6f
Target group: demo-test
Registered targets (3) Info
Anomaly mitigation: Not applicable
Deregister
Register targets
Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.
Filter targets
Instance ID
Name
Port
Zone
Health status
Health status details
Launch time
Anomaly detectio...
i-07c496099abdef6fb
80
us-east-1c
Healthy
-
February 22, 2024, 15:37 (U...
Normal
i-029b13911894a2b04
hello_page
80
us-east-1c
Healthy
-
February 22, 2024, 15:10 (U...
Normal
i-03ddaf4dd6861fee4
hello_page2
80
us-east-1c
Healthy
-
February 22, 2024, 15:10 (U...
Normal

Q2. Hosting a Static Portfolio Website on S3

Objective: Learn to host a static website (such as a personal portfolio) on Amazon S3.

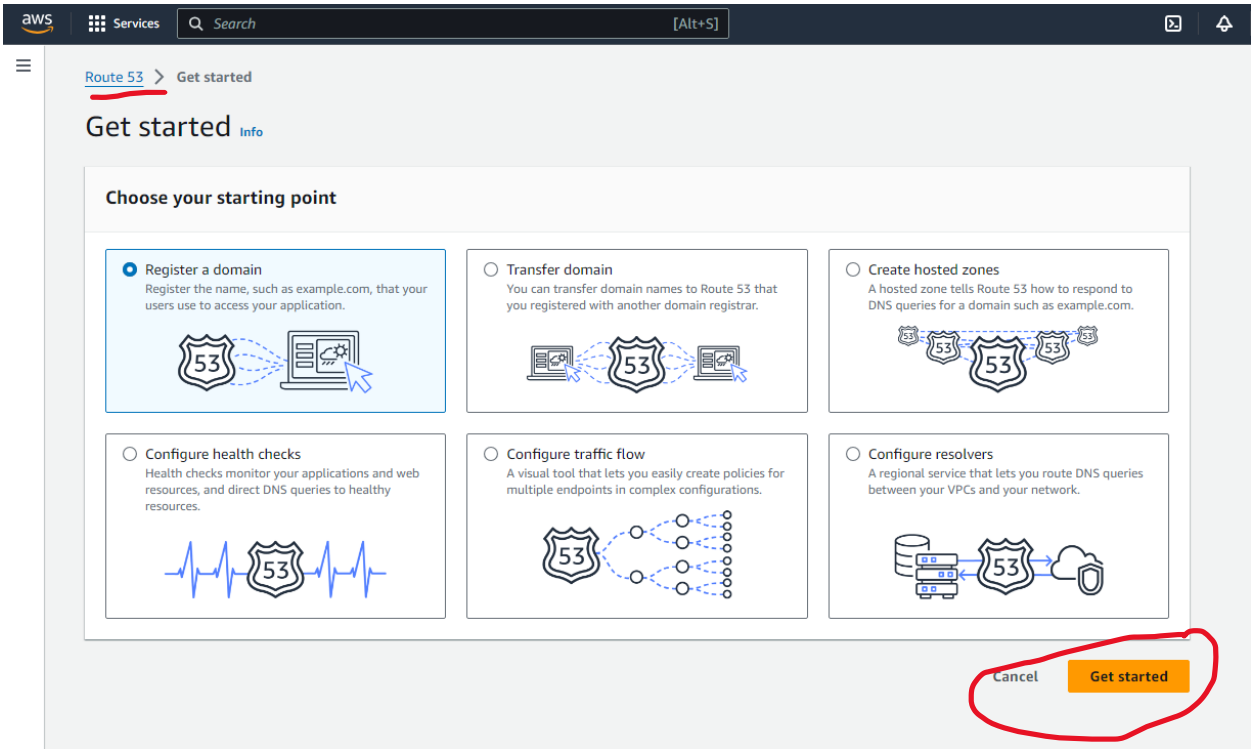
Approach:

1. Create an S3 Bucket: Start by creating a new S3 bucket. Configure the bucket for website hosting, which includes setting permissions to make the content publicly accessible.
2. Upload Website Files: Upload the static files of your portfolio website (HTML, CSS, JavaScript, images) to the S3 bucket.
3. Configure DNS: Use Amazon Route 53 or another DNS service to point a domain name to the S3 bucket. This makes the website accessible via a user-friendly URL.
4. Enable Additional Features (Optional): Implement features like HTTPS for secure access and CloudFront for content delivery optimization.

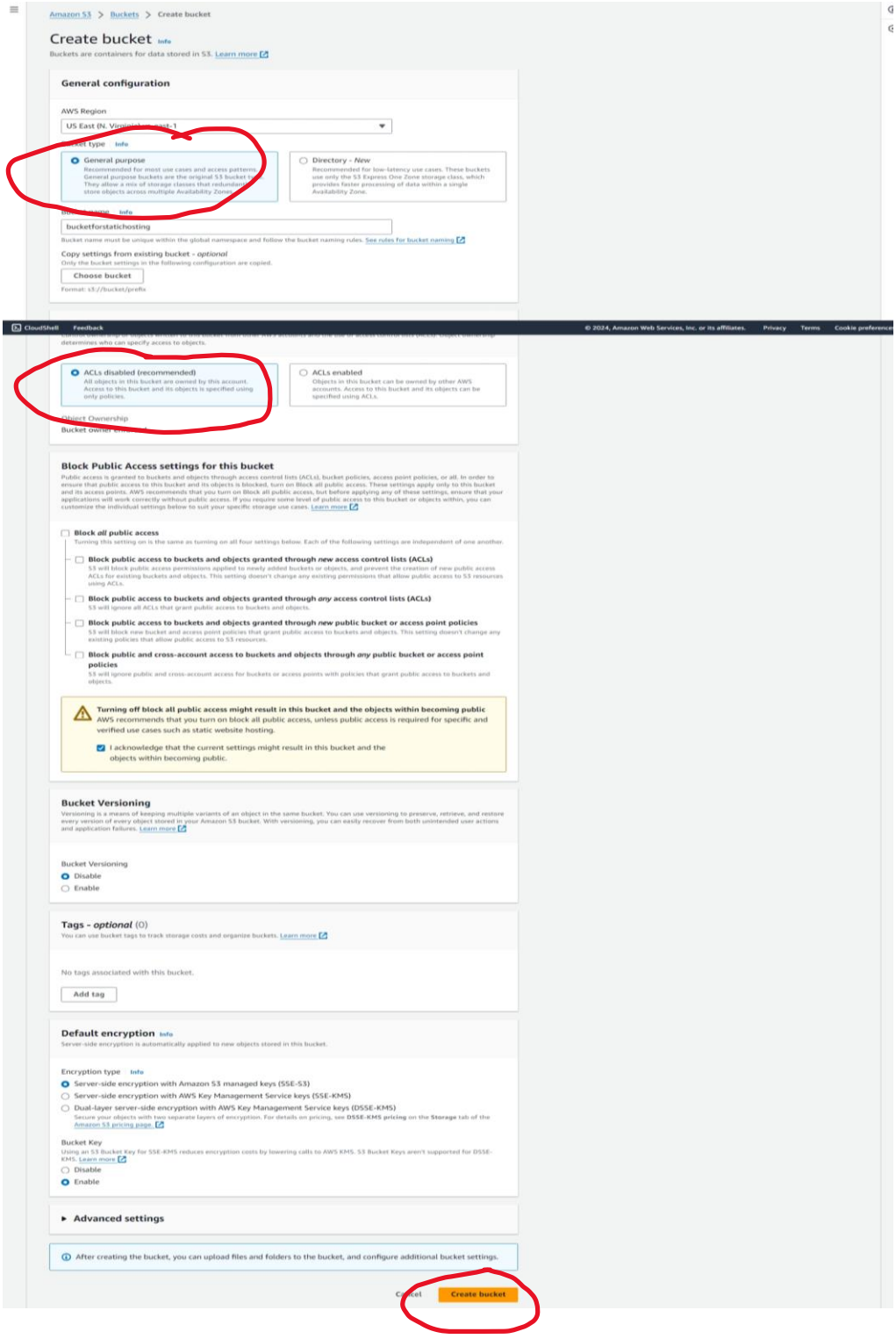
Goal: Students will understand how to use S3 for hosting static websites, manage bucket permissions, and integrate with other AWS services for a complete web hosting solution.

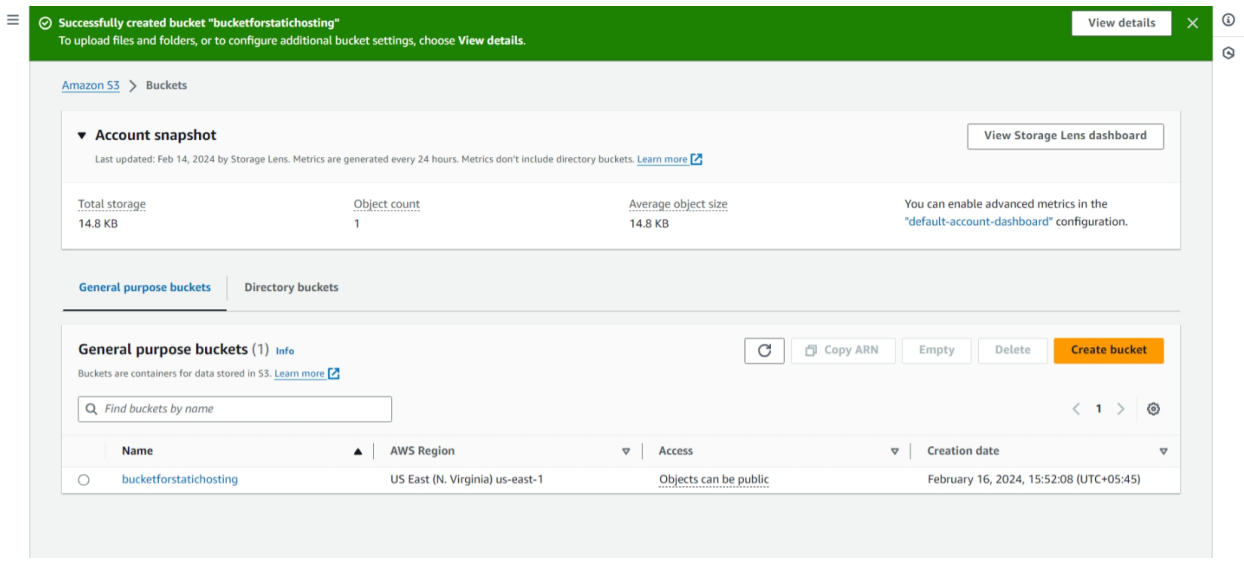
Steps:

1. To configure DNS we use Amazon Route 53
    - Click on get started in Amazon Route 53

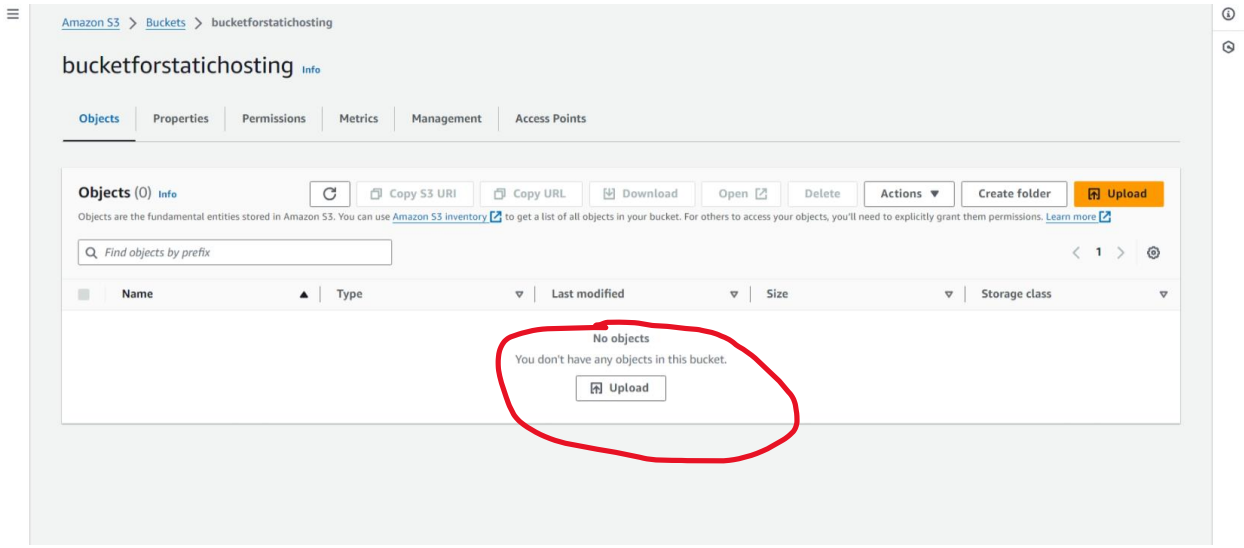


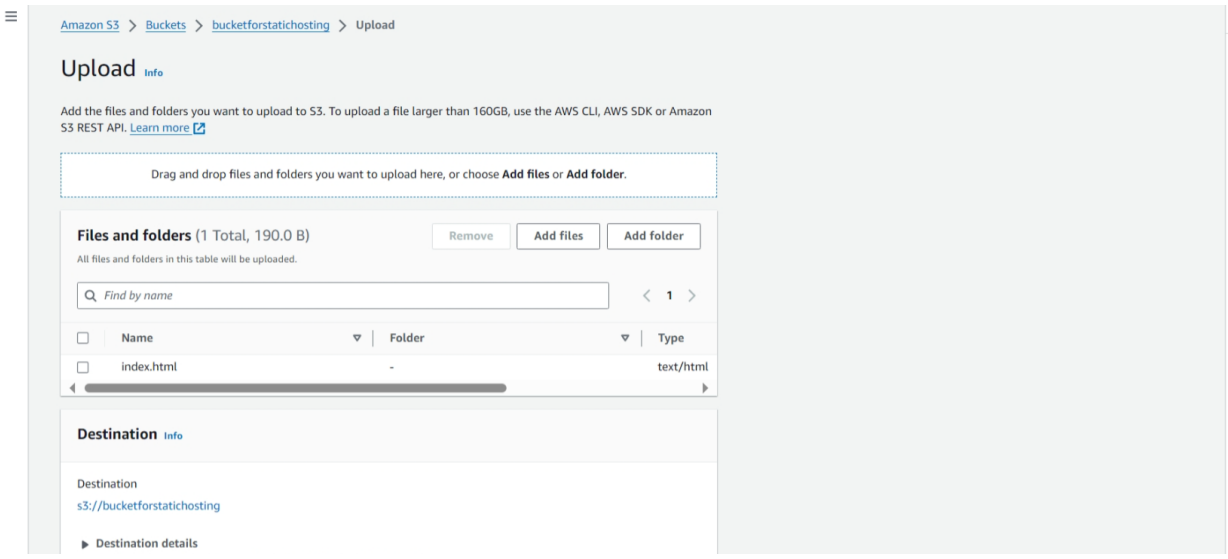
Creating S3 bucket

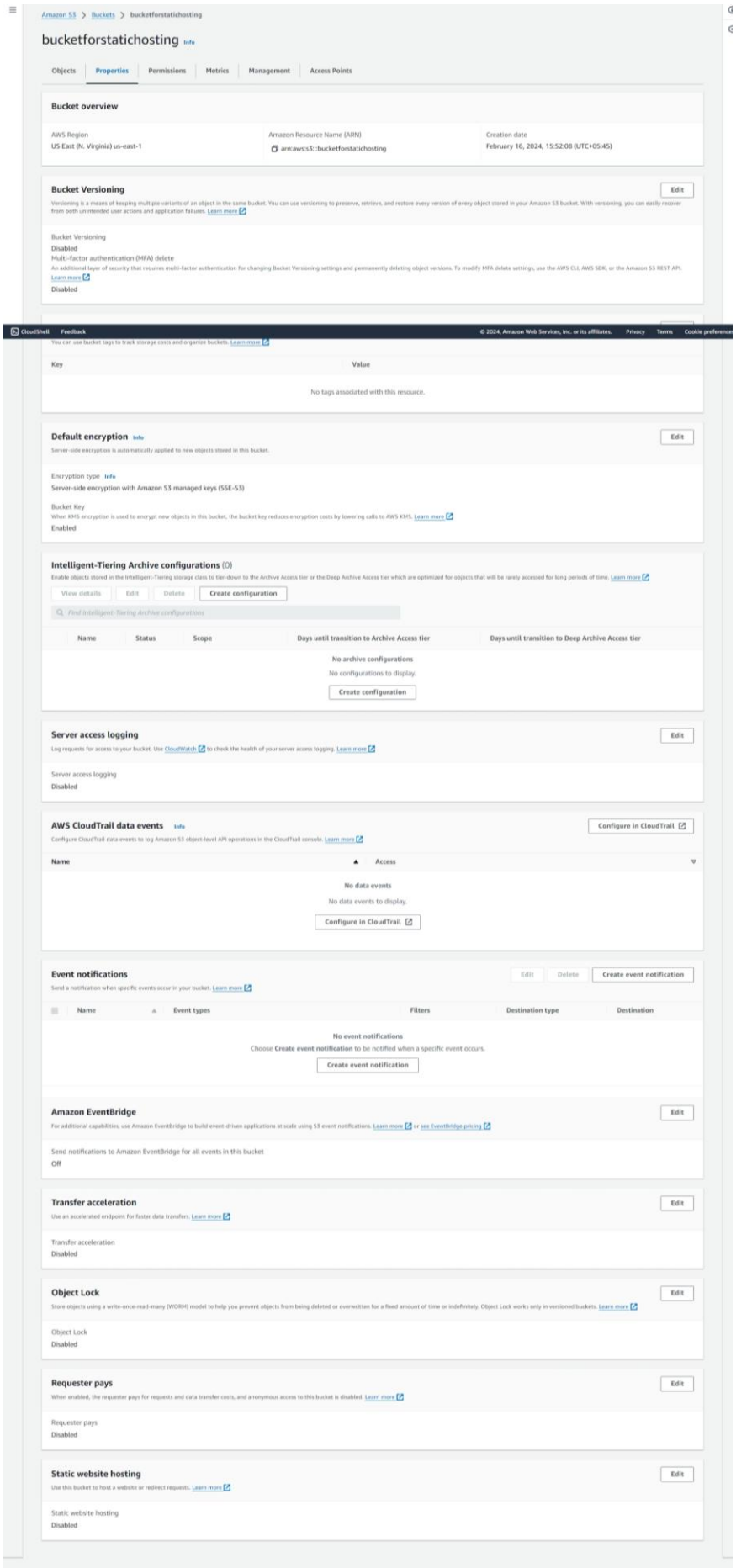


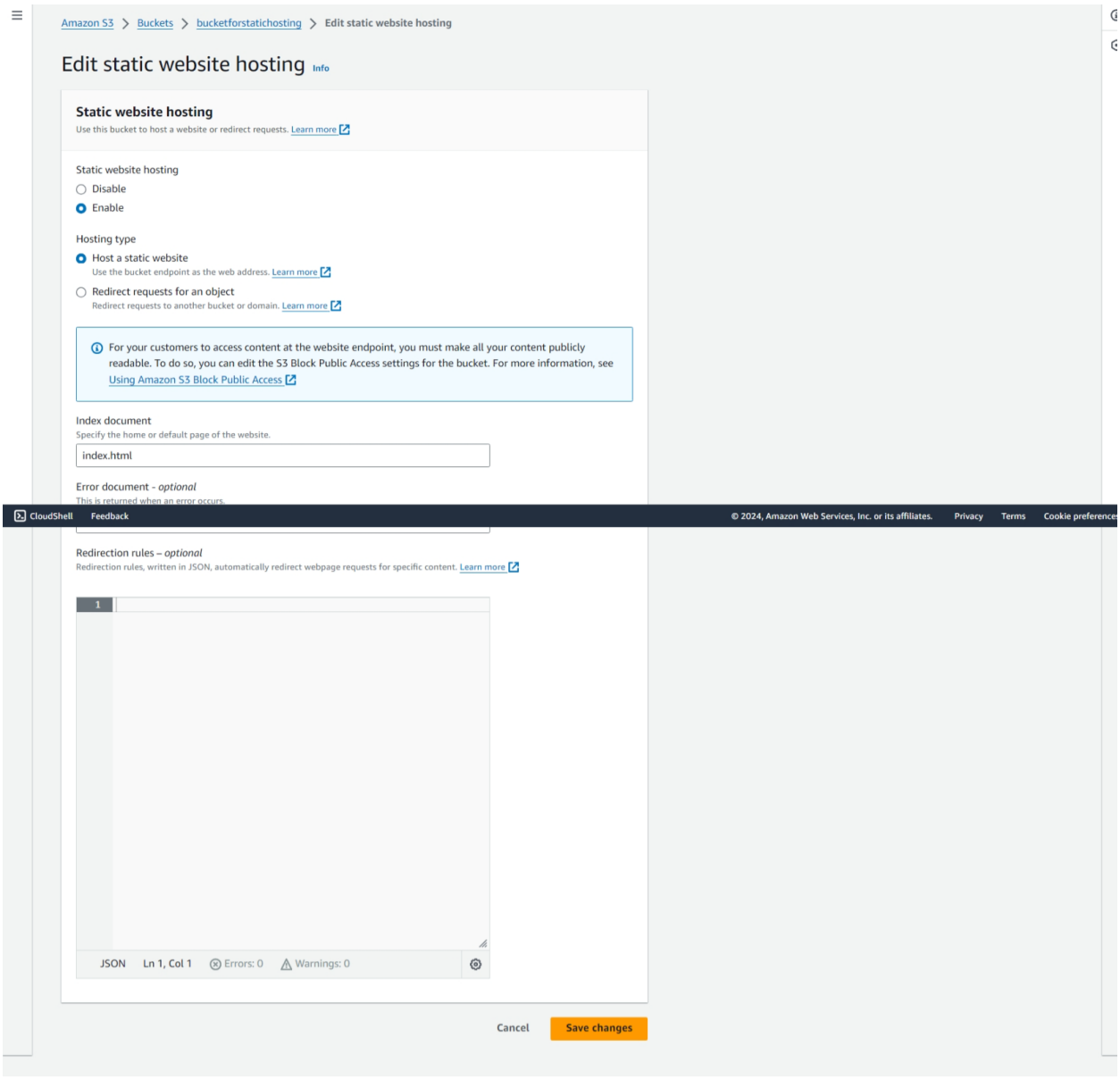


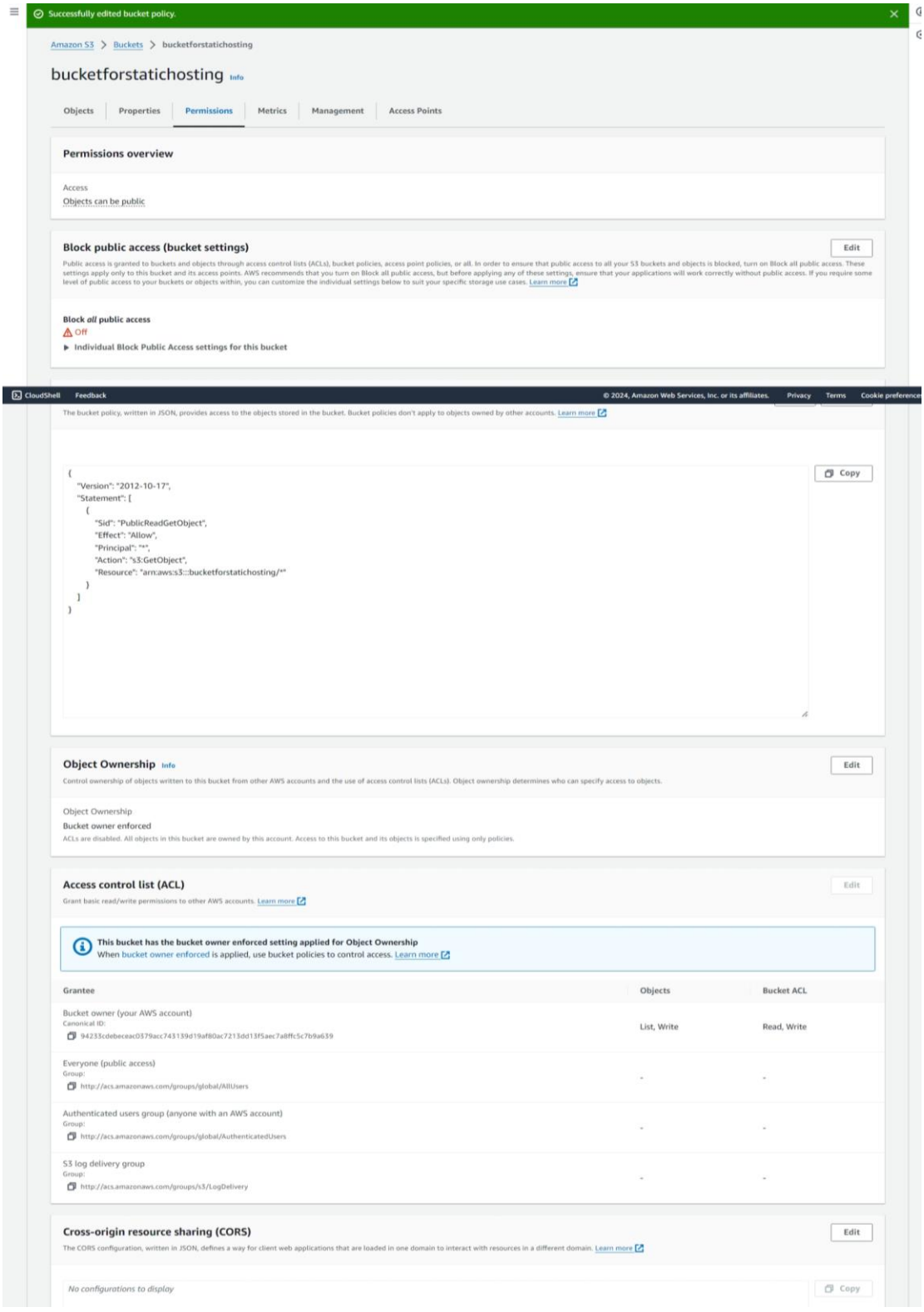
Upload static website



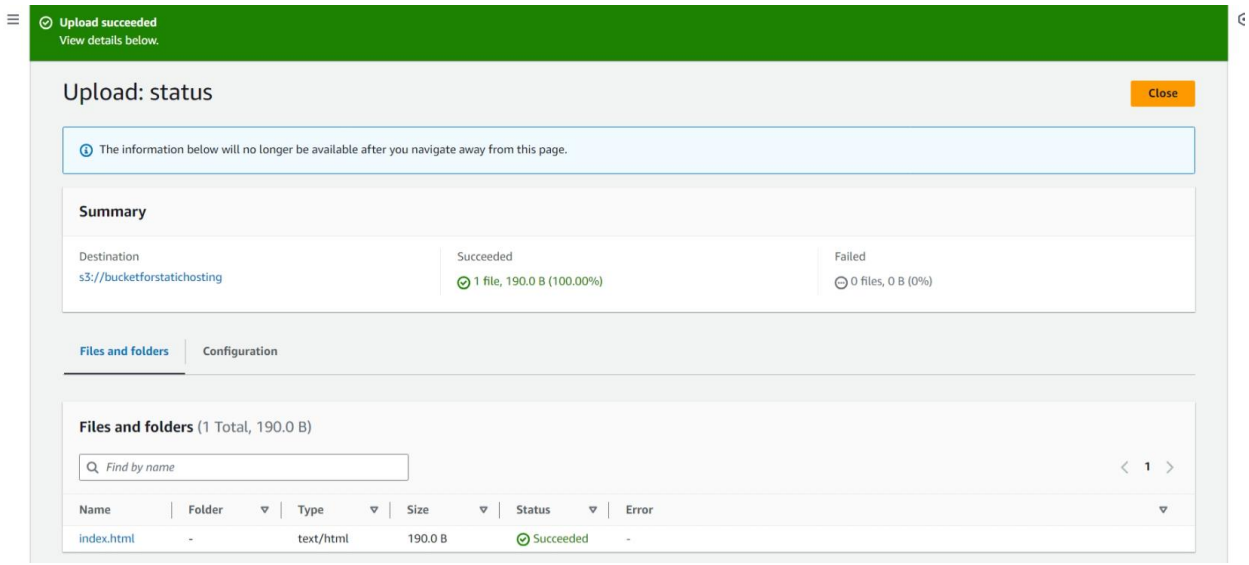

Amazon S3 > Buckets > bucketforstatichosting > Upload
Upload Info
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files or Add folder.
Files and folders (1 Total, 190.0 B)
Remove
Add files
Add folder
All files and folders in this table will be uploaded.
Find by name
1
Name
Folder
Type
index.html
-
text/html
Destination Info
Destination
s3://bucketforstatichosting
Destination details


Amazon S3 > Buckets > bucketforstatichosting
bucketforstatichosting Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Bucket overview
AWS Region
US East (N. Virginia) us-east-1
Amazon Resource Name (ARN)
arn:aws:s3:::bucketforstatichosting
Creation date
February 16, 2024, 15:52:08 (UTC+05:45)
Bucket Versioning
Edit
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more
Bucket Versioning
Disabled
Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
You can use bucket tags to track storage costs and organize buckets. Learn more
Key
Value
No tags associated with this resource.
Default encryption Info
Edit
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)
Bucket Key
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. Learn more
Enabled
Intelligent-Tiering Archive configurations (0)
Enable objects stored in the Intelligent-Tiering storage class to tier-down to the Archive Access tier or the Deep Archive Access tier which are optimized for objects that will be rarely accessed for long periods of time. Learn more
View details
Edit
Delete
Create configuration
Find Intelligent-Tiering Archive configurations
Name
Status
Scope
Days until transition to Archive Access tier
Days until transition to Deep Archive Access tier
No archive configurations
No configurations to display.
Create configuration
Server access logging
Edit
Log requests for access to your bucket. Use CloudWatch to check the health of your server access logging. Learn more
Server access logging
Disabled
AWS CloudTrail data events Info
Configure in CloudTrail
Configure CloudTrail data events to log Amazon S3 object-level API operations in the CloudTrail console. Learn more
Name
Access
No data events
No data events to display.
Configure in CloudTrail
Event notifications
Edit
Delete
Create event notification
Send a notification when specific events occur in your bucket. Learn more
Name
Event types
Filters
Destination type
Destination
No event notifications
Choose Create event notification to be notified when a specific event occurs.
Create event notification
Amazon EventBridge
Edit
For additional capabilities, use Amazon EventBridge to build event-driven applications at scale using S3 event notifications. Learn more or see EventBridge pricing
Send notifications to Amazon EventBridge for all events in this bucket
Off
Transfer acceleration
Edit
Use an accelerated endpoint for faster data transfers. Learn more
Transfer acceleration
Disabled
Object Lock
Edit
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. Learn more
Object Lock
Disabled
Requester pays
Edit
When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. Learn more
Requester pays
Disabled
Static website hosting
Edit
Use this bucket to host a website or redirect requests. Learn more
Static website hosting
Disabled


Amazon S3 > Buckets > bucketforstatichosting > Edit static website hosting
Edit static website hosting Info
Static website hosting
Use this bucket to host a website or redirect requests. Learn more
Static website hosting
Disable
Enable
Hosting type
Host a static website
Use the bucket endpoint as the web address. Learn more
Redirect requests for an object
Redirect requests to another bucket or domain. Learn more
For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access
Index document
Specify the home or default page of the website.
index.html
Error document - optional
This is returned when an error occurs.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Redirection rules – optional
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. Learn more
1
JSON
Ln 1, Col 1
Errors: 0
Warnings: 0
Cancel
Save changes


Successfully edited bucket policy.
Amazon S3 > Buckets > bucketforstatichosting
bucketforstatichosting Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Permissions overview
Access
Objects can be public
Block public access (bucket settings)
Edit
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 all your S3 buckets and 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Off
Individual Block Public Access settings for this bucket
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "PublicReadGetObject",
"Effect": "Allow",
"Principal": "*",
"Action": "s3:GetObject",
"Resource": "arn:aws:s3:::bucketforstatichosting/*"
}
]
}
Copy
Object Ownership Info
Edit
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.
Object Ownership
Bucket owner enforced
ACLs are disabled. All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
Access control list (ACL)
Edit
Grant basic read/write permissions to other AWS accounts. Learn more
This bucket has the bucket owner enforced setting applied for Object Ownership
When bucket owner enforced is applied, use bucket policies to control access. Learn more
Grantee
Objects
Bucket ACL
Bucket owner (your AWS account)
Canonical ID:
94233cdebeceac0379acc743139d19af80ac7213dd13f5aec7a8ffc5c7b9a639
List, Write
Read, Write
Everyone (public access)
Group:
http://acs.amazonaws.com/groups/global/AllUsers
-
-
Authenticated users group (anyone with an AWS account)
Group:
http://acs.amazonaws.com/groups/global/AuthenticatedUsers
-
-
S3 log delivery group
Group:
http://acs.amazonaws.com/groups/s3/LogDelivery
-
-
Cross-origin resource sharing (CORS)
Edit
The CORS configuration, written in JSON, defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. Learn more
No configurations to display
Copy

Here we see the index file uploaded



Here we can see the website hosted from amazon s3