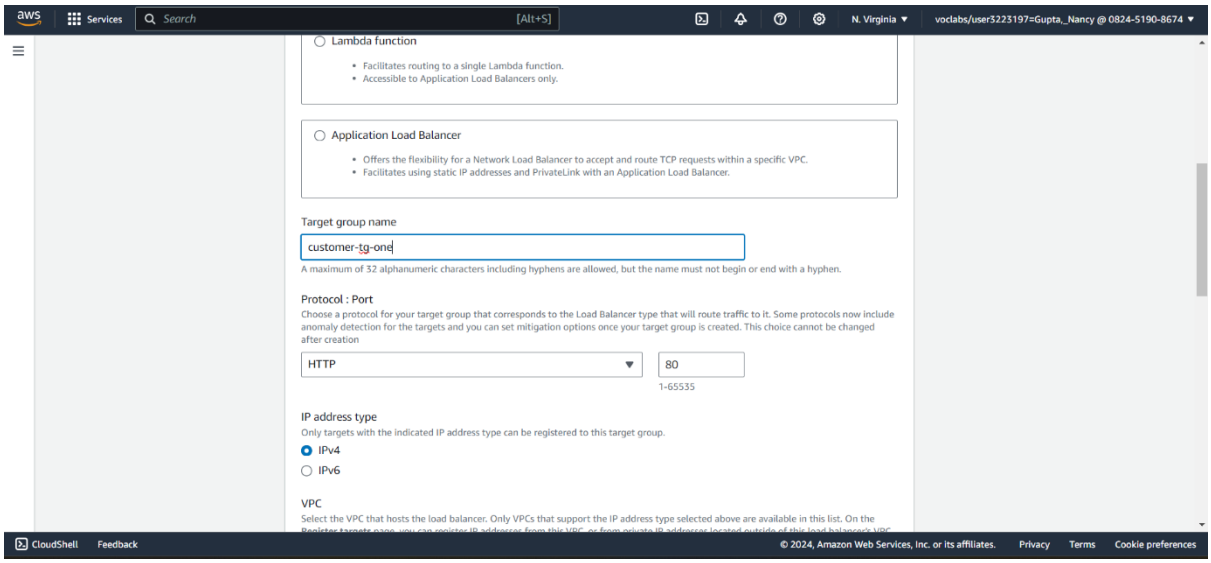
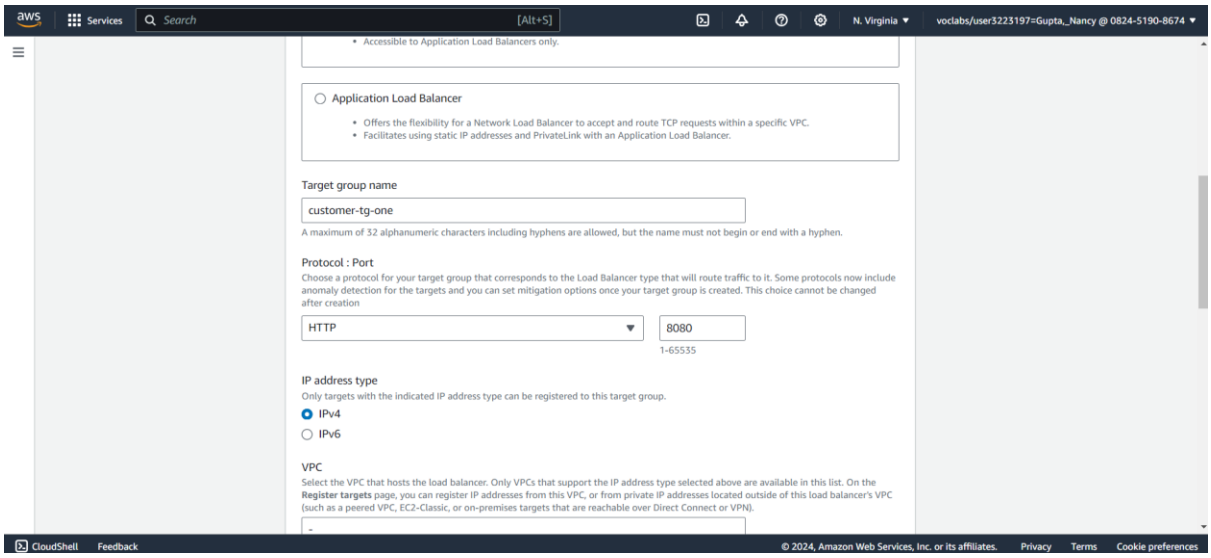
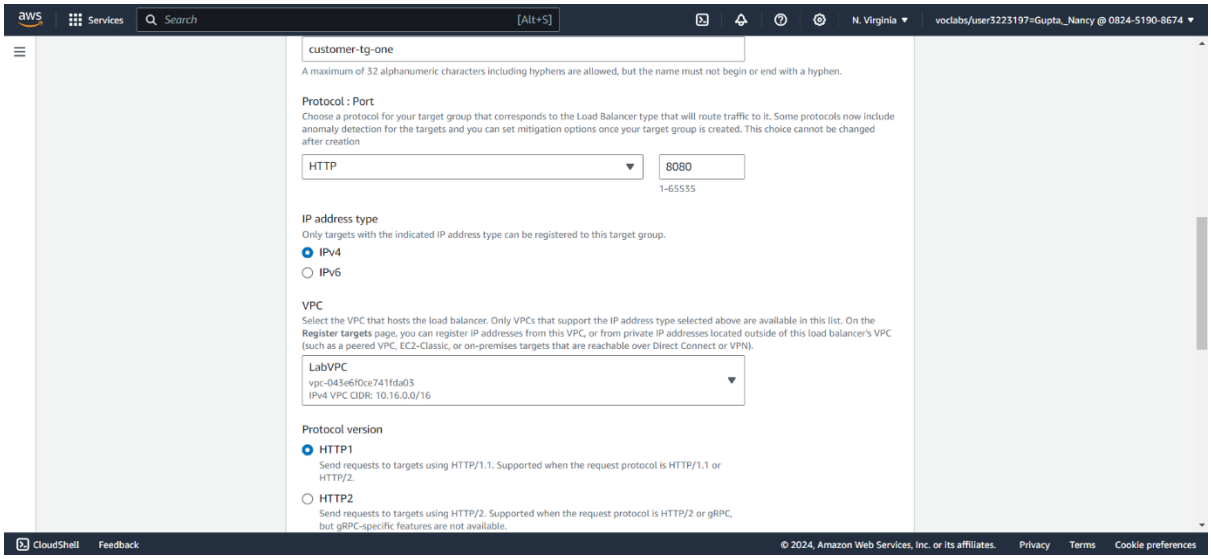
- **Protocol: Choose HTTP.**



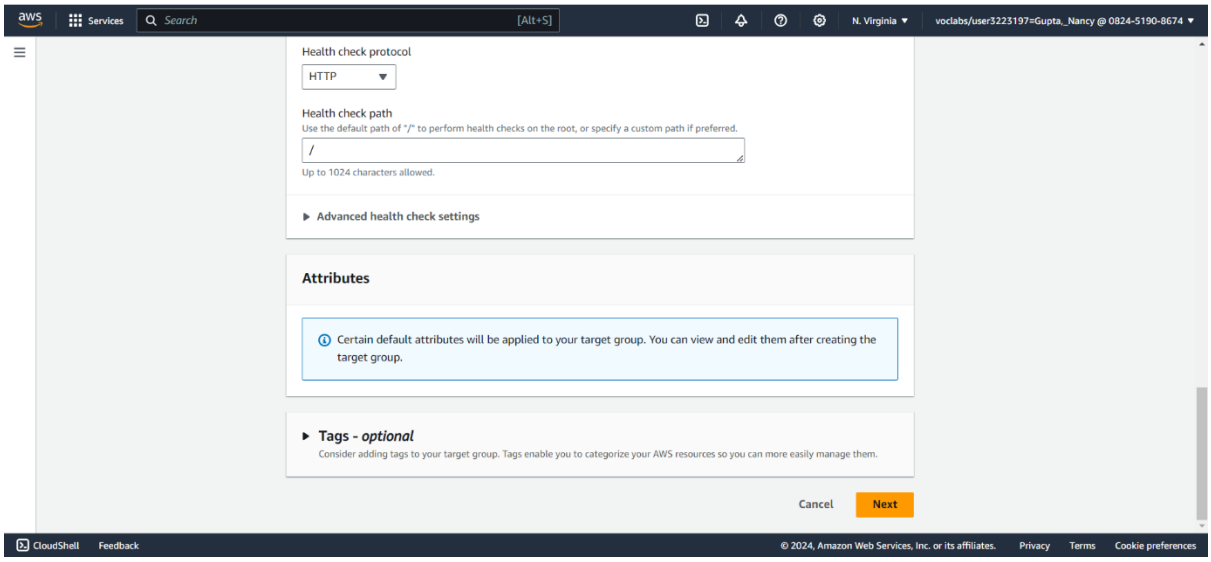
- **Port: Enter 8080**



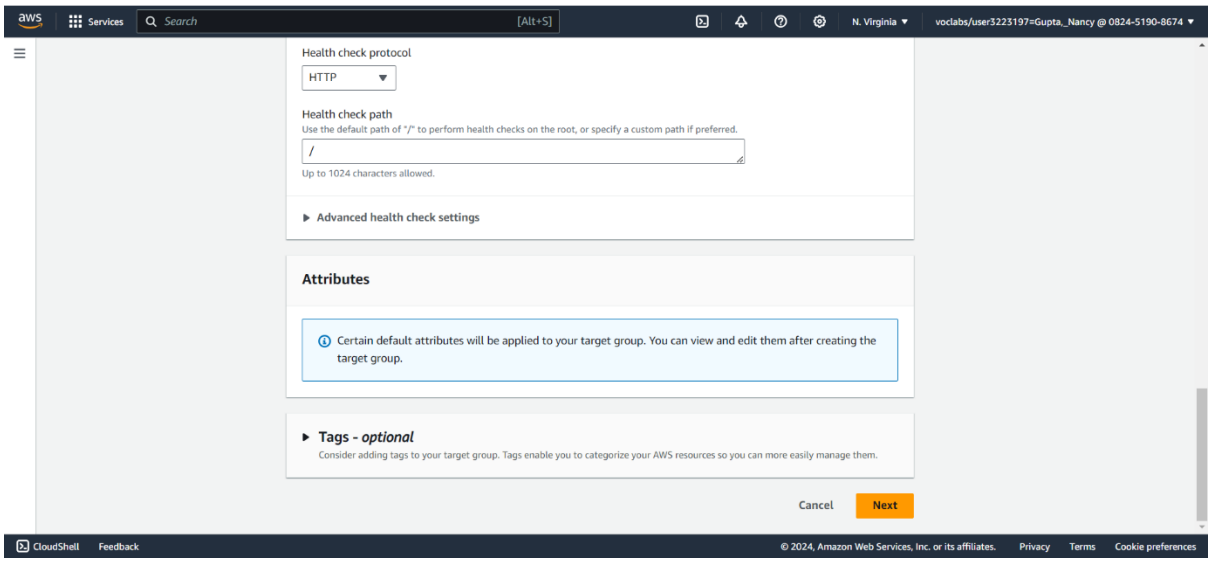
- **VPC: Choose LabVPC.**



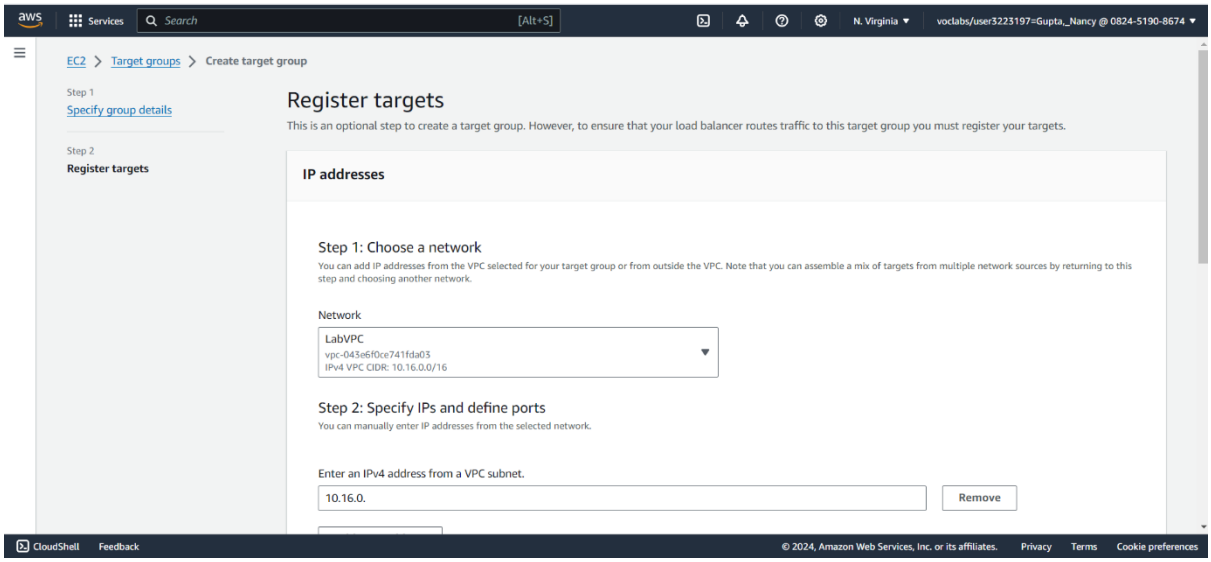
- **Health check path: Enter /**

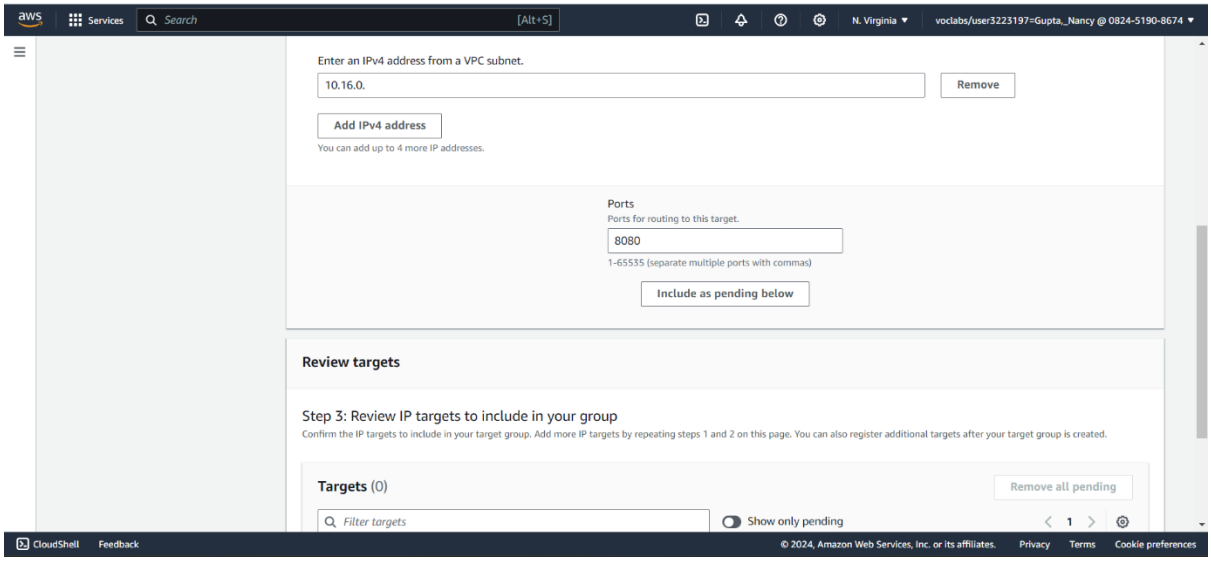


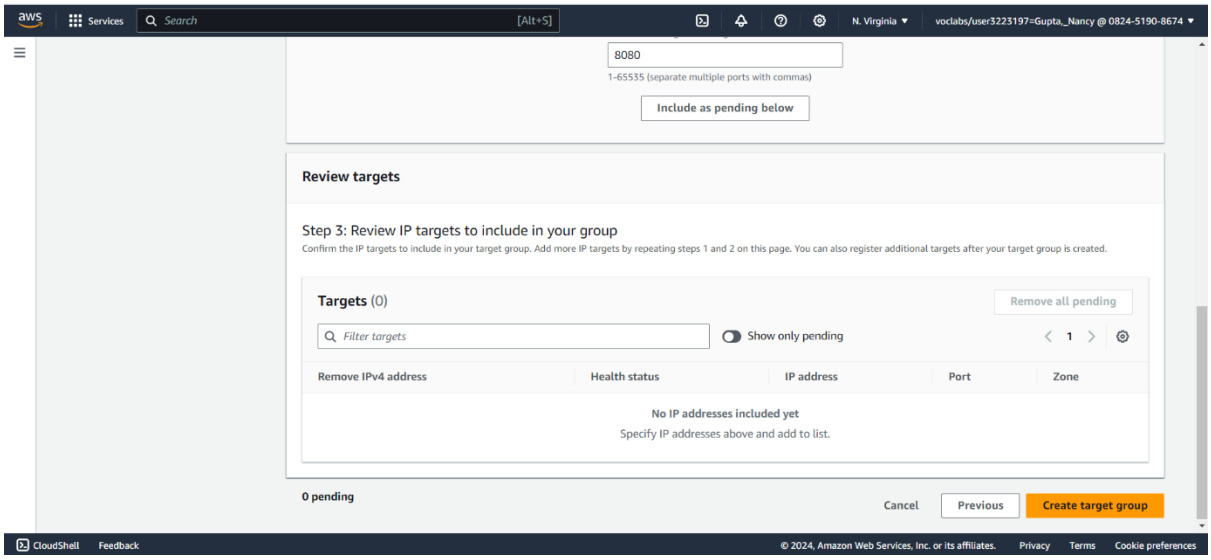
- **Choose Next.**

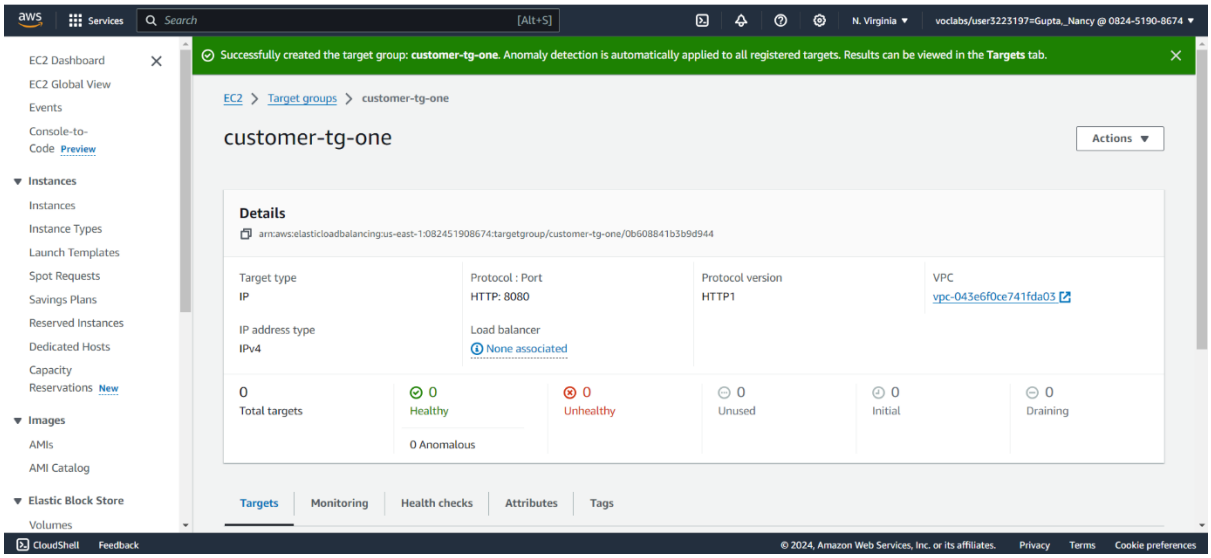


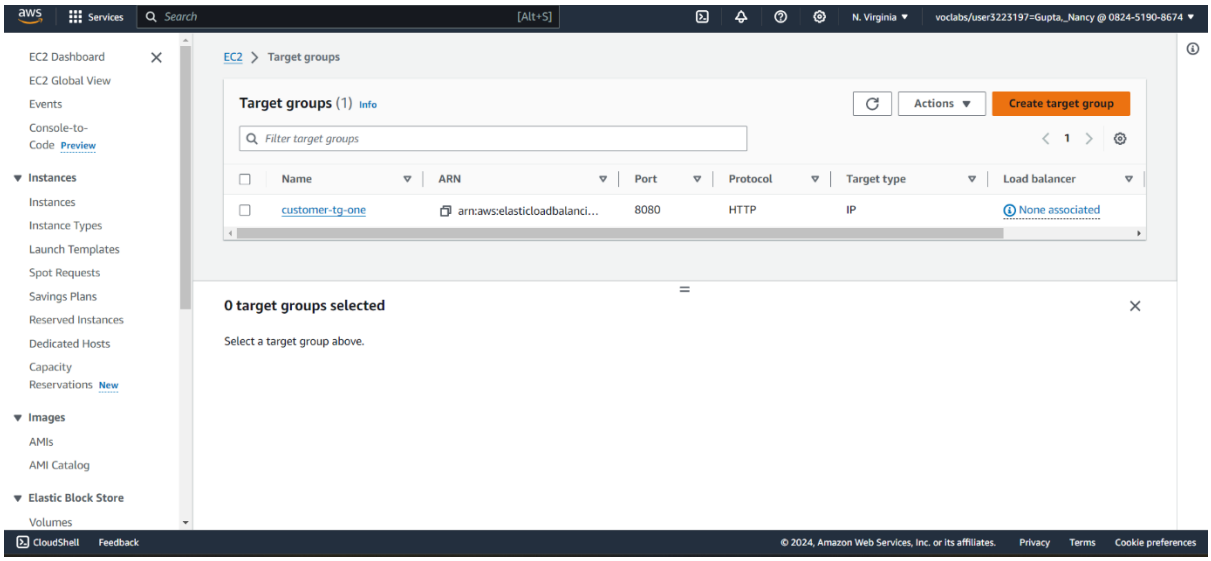
- **On the Register targets page, accept all defaults (don't register any targets), and choose Create target group.**



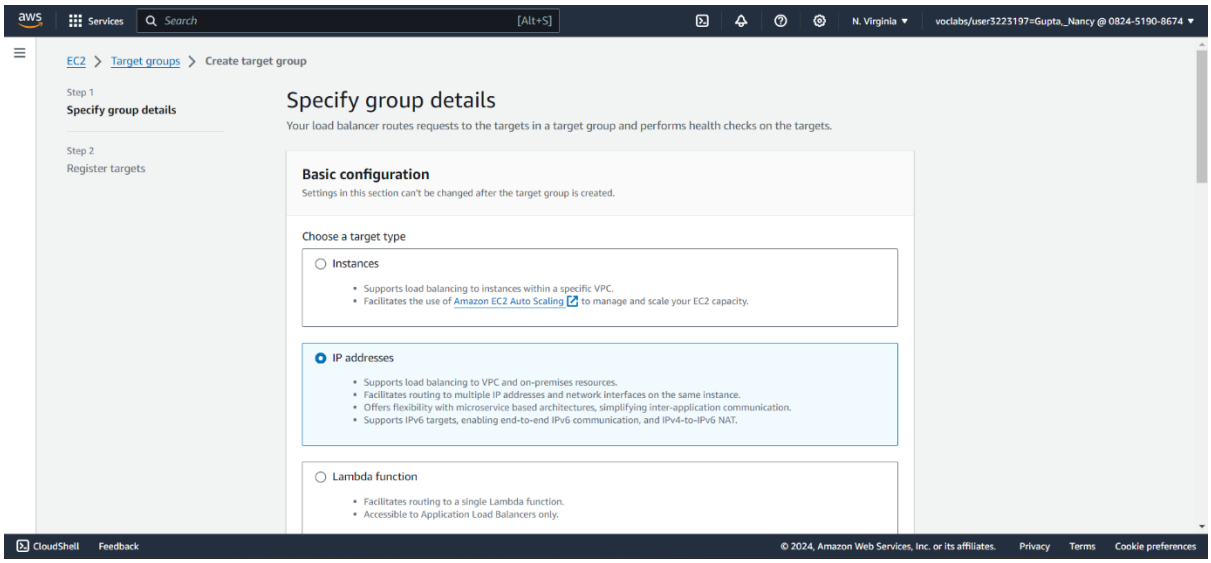


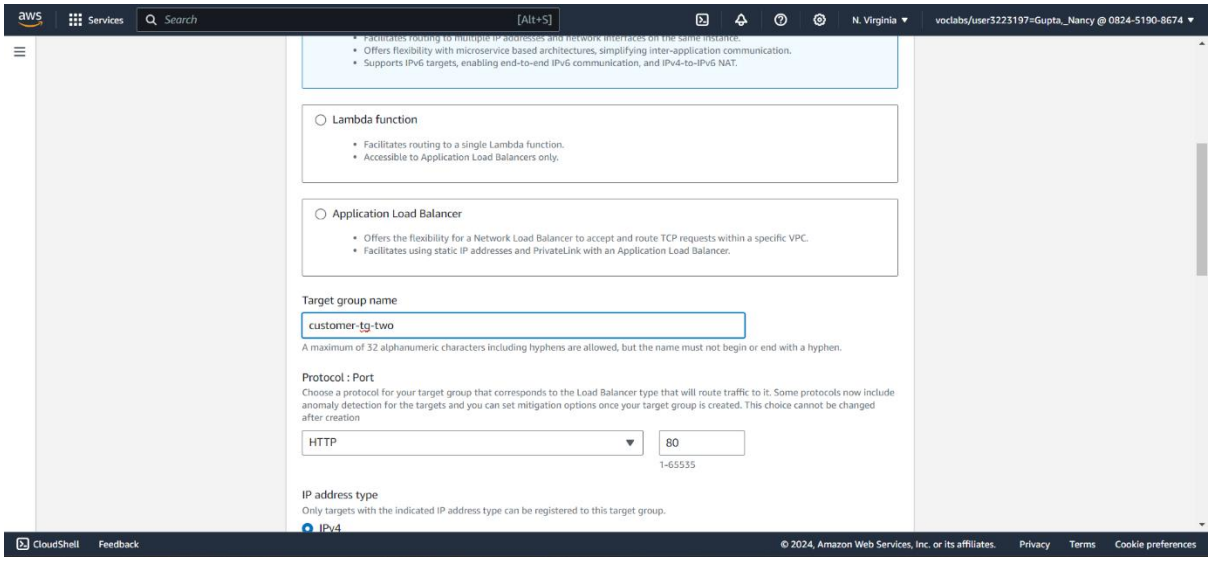


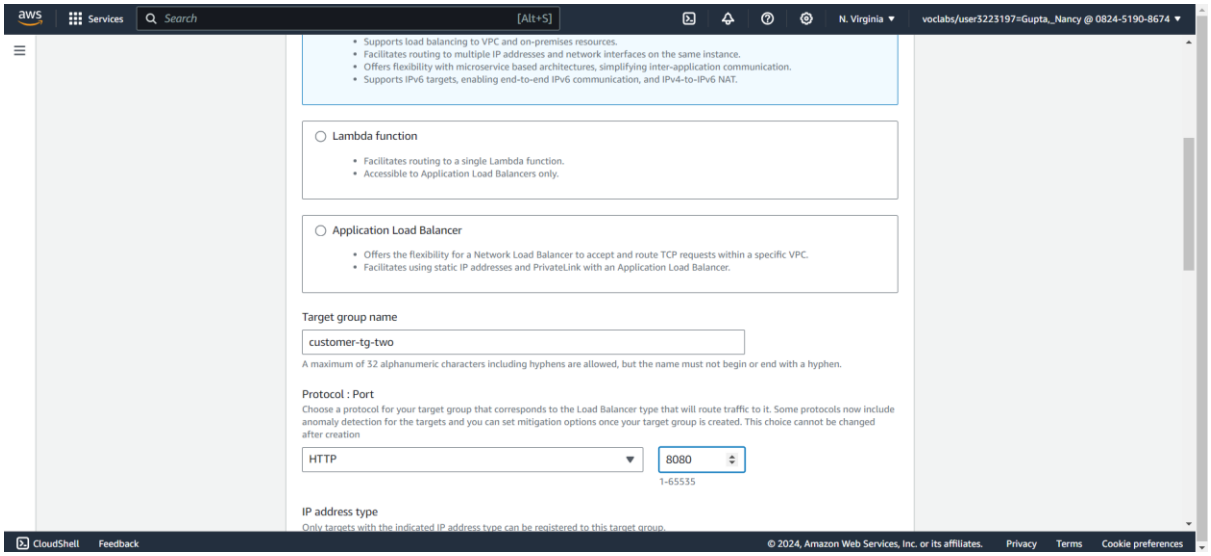


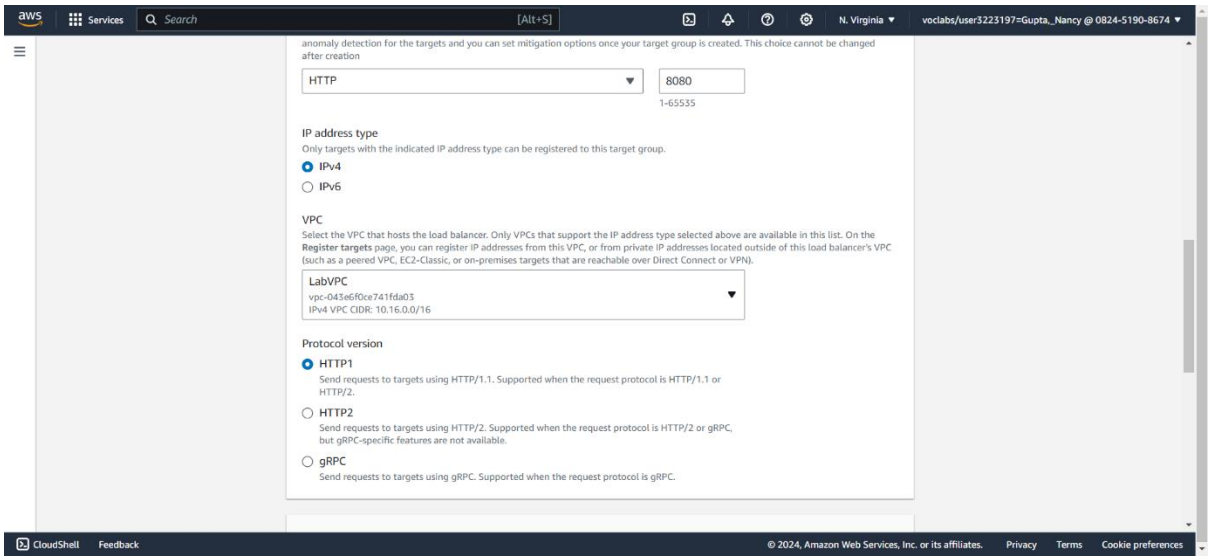


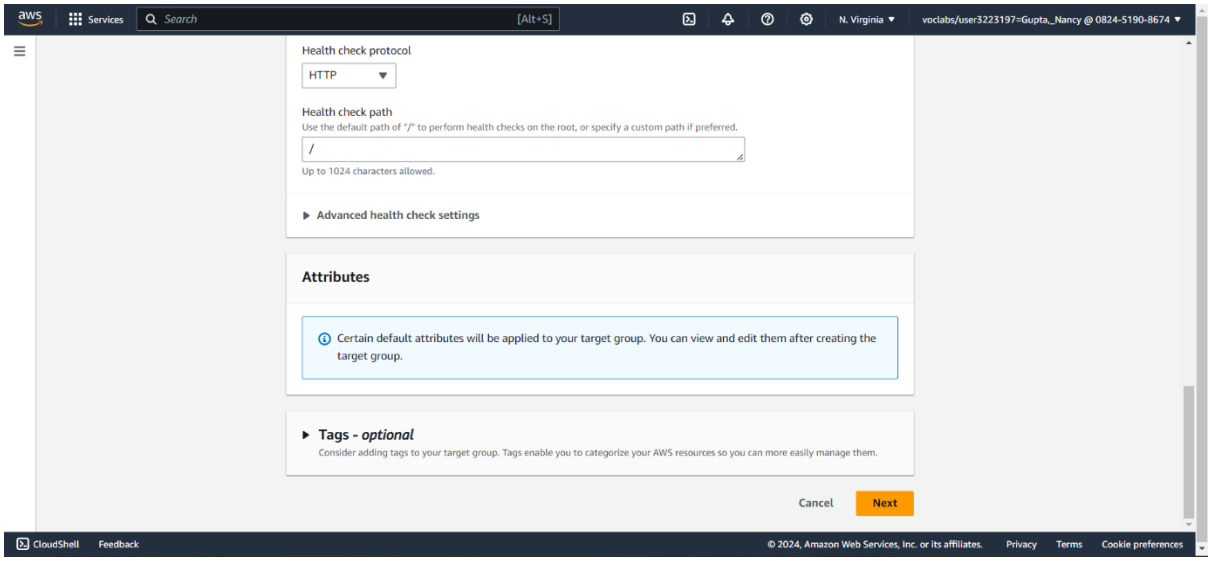
2. **Create a second target group for the *customer* microservice. Use the same settings as the first target group except use customer-tg-two as the target group name.**

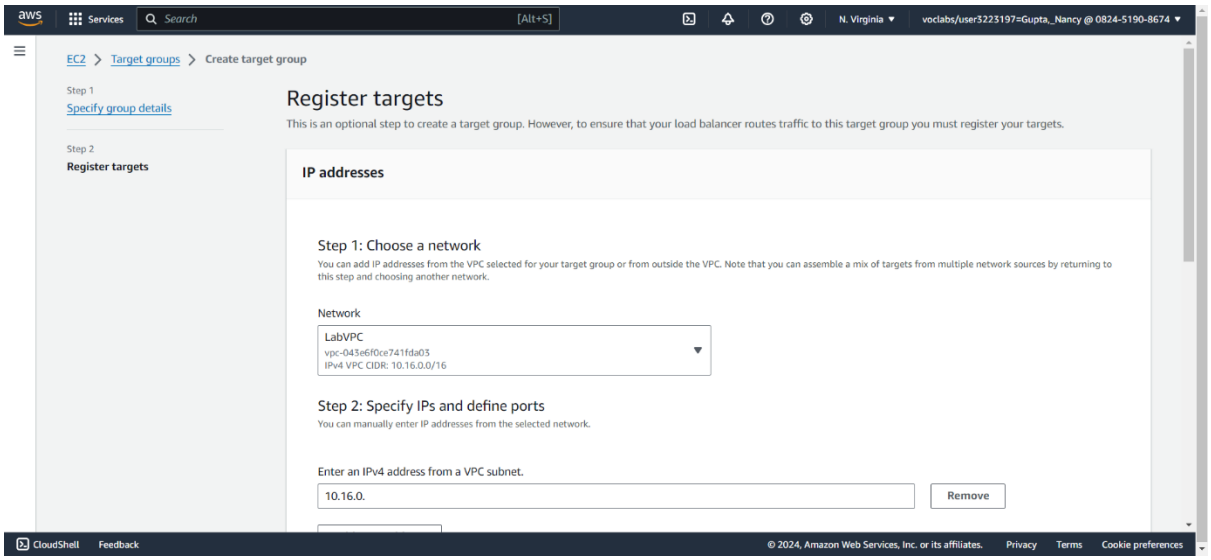


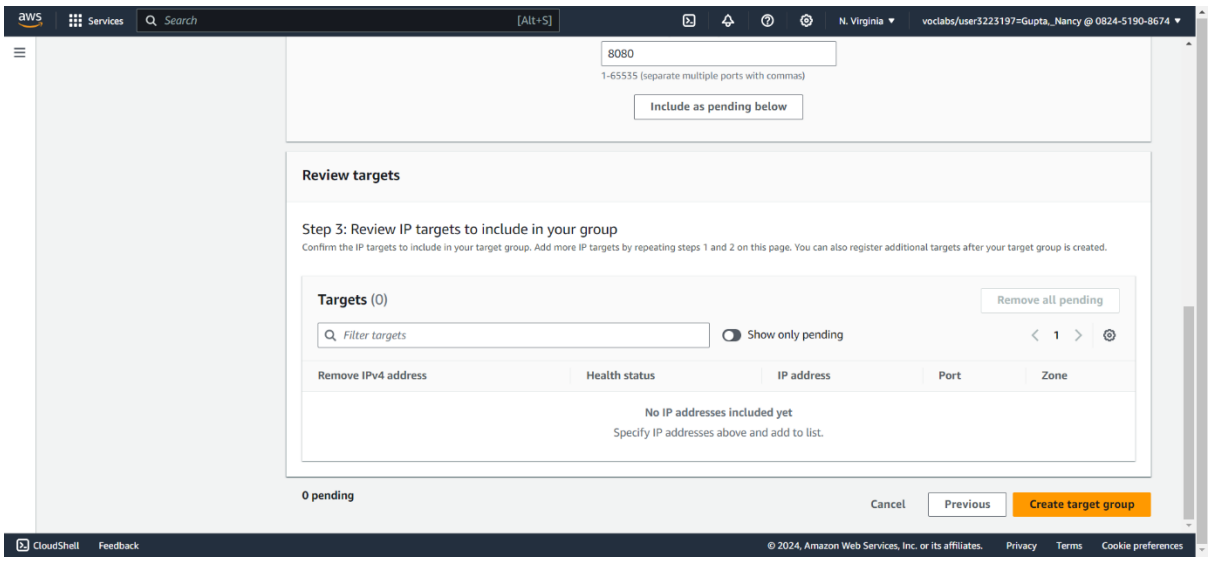

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
• Facilitates routing to multiple IP addresses and network interfaces on the same instance.
• Offers flexibility with microservice based architectures, simplifying inter-application communication.
• Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.
Lambda function
• Facilitates routing to a single Lambda function.
• Accessible to Application Load Balancers only.
Application Load Balancer
• Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
• Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.
Target group name
customer-tg-two
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

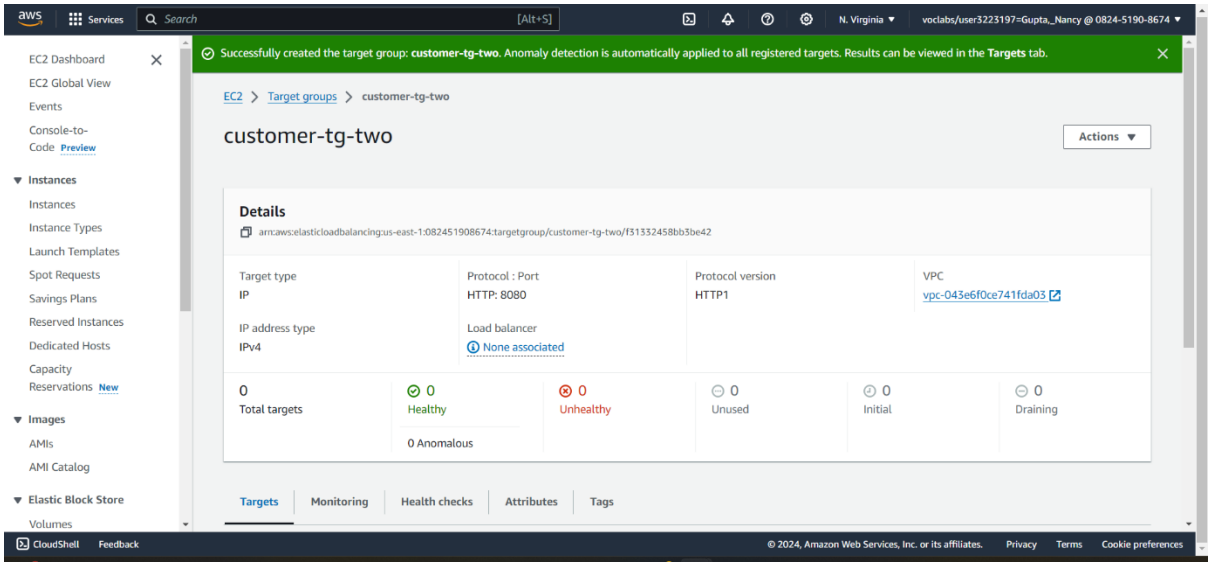

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
• Supports load balancing to VPC and on-premises resources.
• Facilitates routing to multiple IP addresses and network interfaces on the same instance.
• Offers flexibility with microservice based architectures, simplifying inter-application communication.
• Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.
Lambda function
• Facilitates routing to a single Lambda function.
• Accessible to Application Load Balancers only.
Application Load Balancer
• Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
• Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.
Target group name
customer-tg-two
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
8080
1-65535
IP address type
Only targets with the indicated IP address type can be registered to this target group.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

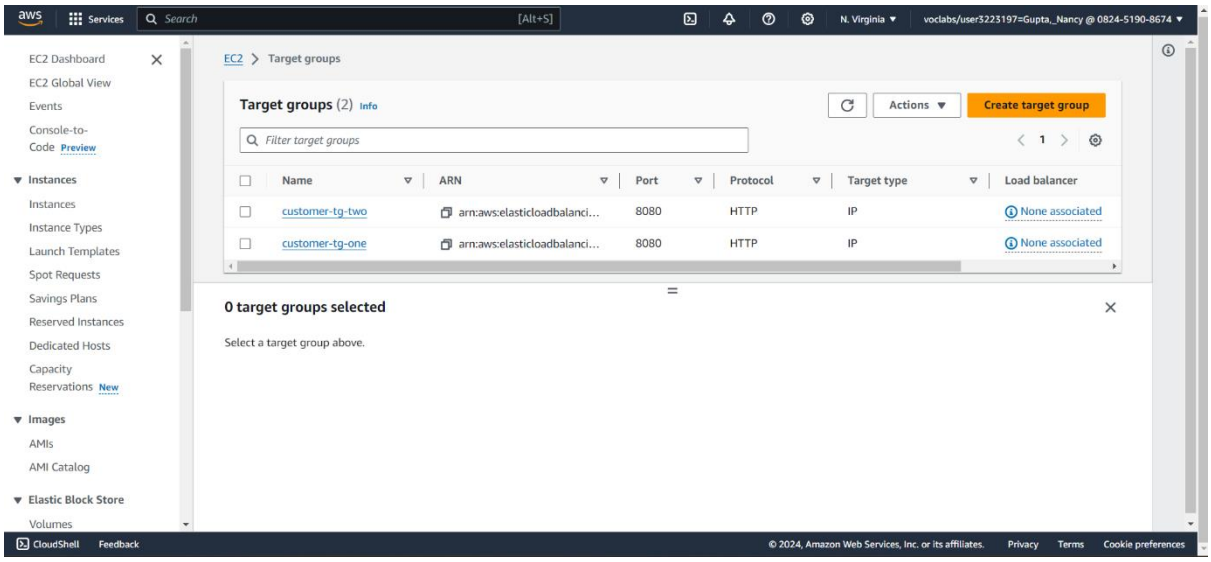

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation
HTTP
8080
1-65535
IP address type
Only targets with the indicated IP address type can be registered to this target group.
IPv4
IPv6
VPC
Select the VPC that hosts the load balancer. Only VPCs that support the IP address type selected above are available in this list. On the Register targets page, you can register IP addresses from this VPC, or from private IP addresses located outside of this load balancer's VPC (such as a peered VPC, EC2-Classic, or on-premises targets that are reachable over Direct Connect or VPN).
LabVPC
vpc-043e6f0ce741fda03
IPv4 VPC CIDR: 10.16.0.0/16
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.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


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

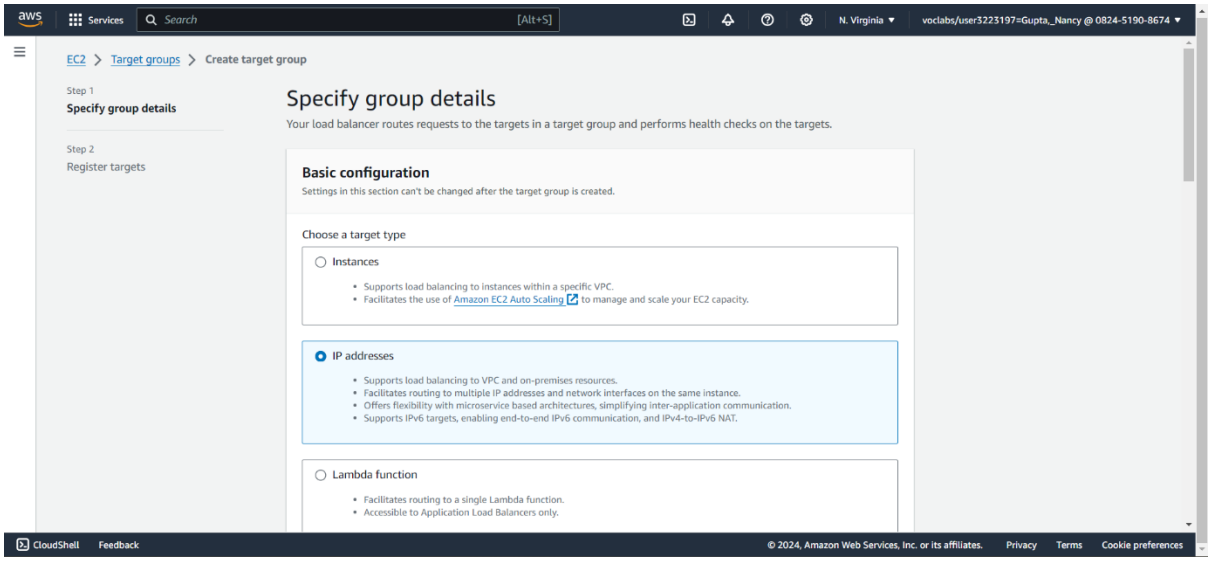

EC2 > Target groups > Create target group
Step 1
Specify group details
Step 2
Register targets
Register targets
This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.
IP addresses
Step 1: Choose a network
You can add IP addresses from the VPC selected for your target group or from outside the VPC. Note that you can assemble a mix of targets from multiple network sources by returning to this step and choosing another network.
Network
LabVPC
vpc-043e6f0ce741fda03
IPv4 VPC CIDR: 10.16.0.0/16
Step 2: Specify IPs and define ports
You can manually enter IP addresses from the selected network.
Enter an IPv4 address from a VPC subnet.
10.16.0.
Remove

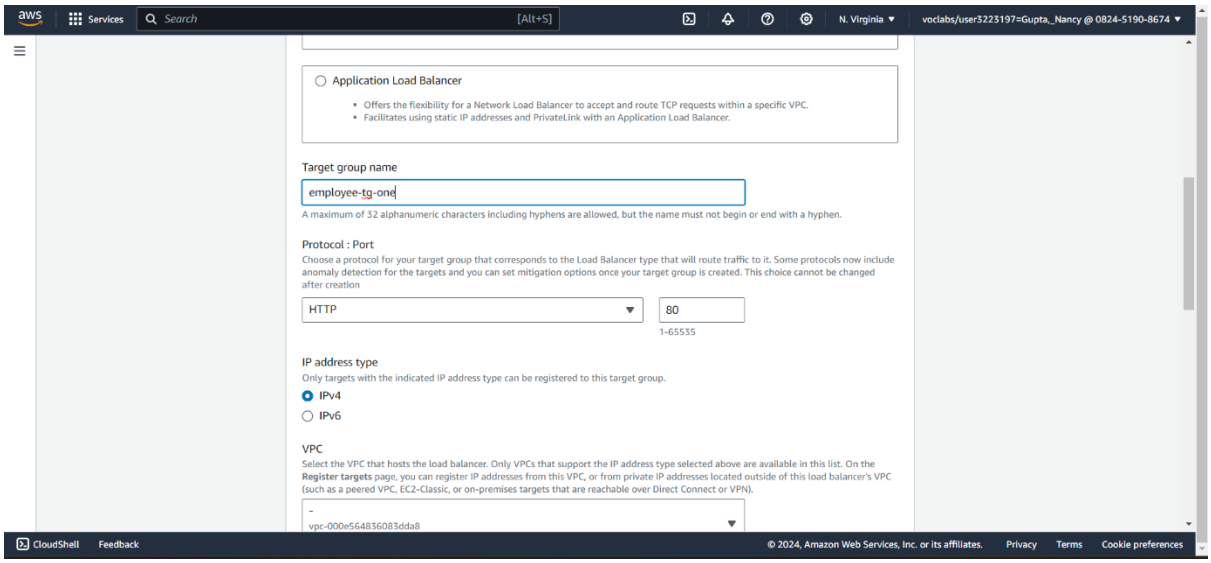

8080
1-65535 (separate multiple ports with commas)
Include as pending below
Review targets
Step 3: Review IP targets to include in your group
Confirm the IP targets to include in your target group. Add more IP targets by repeating steps 1 and 2 on this page. You can also register additional targets after your target group is created.
Targets (0)
Remove all pending
Filter targets
Show only pending
Remove IPv4 address
Health status
IP address
Port
Zone
No IP addresses included yet
Specify IP addresses above and add to list.
0 pending
Cancel
Previous
Create target group

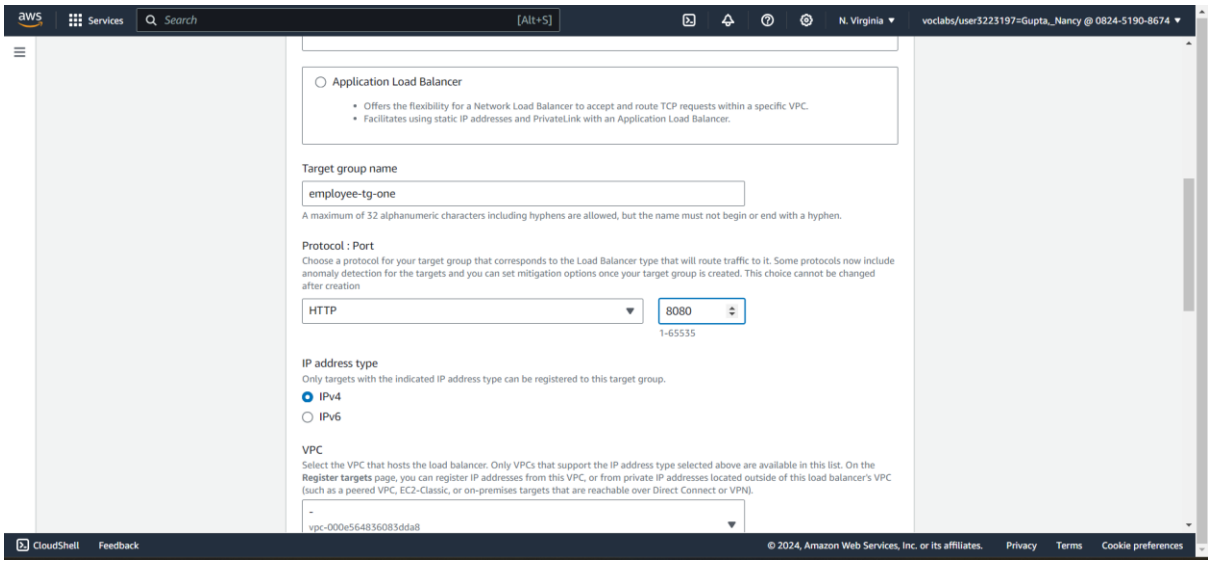


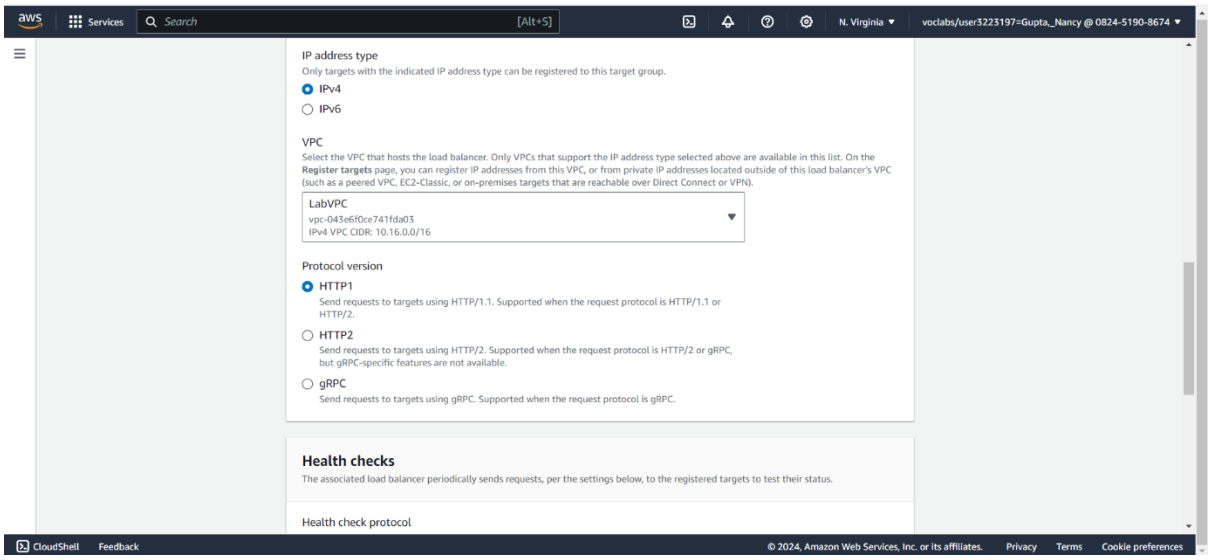


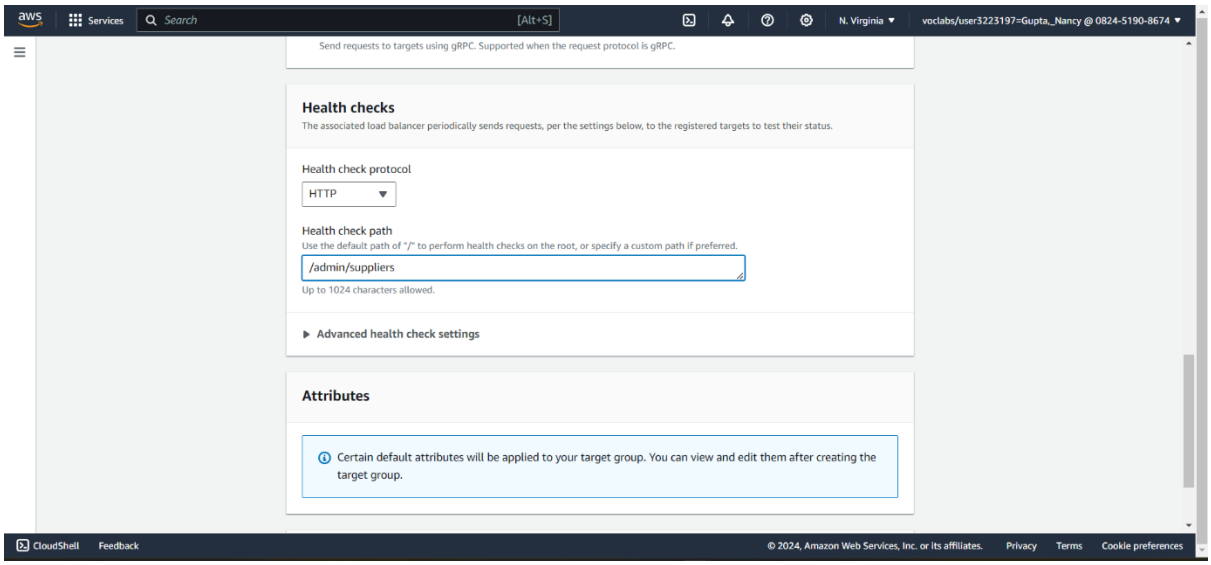
3. **Create a target group for the *employee* microservice. Use the same settings as the other target groups with the following exceptions:**
    - **Target group name: Enter employee-tg-one**
    - **Health check path: Enter /admin/suppliers**

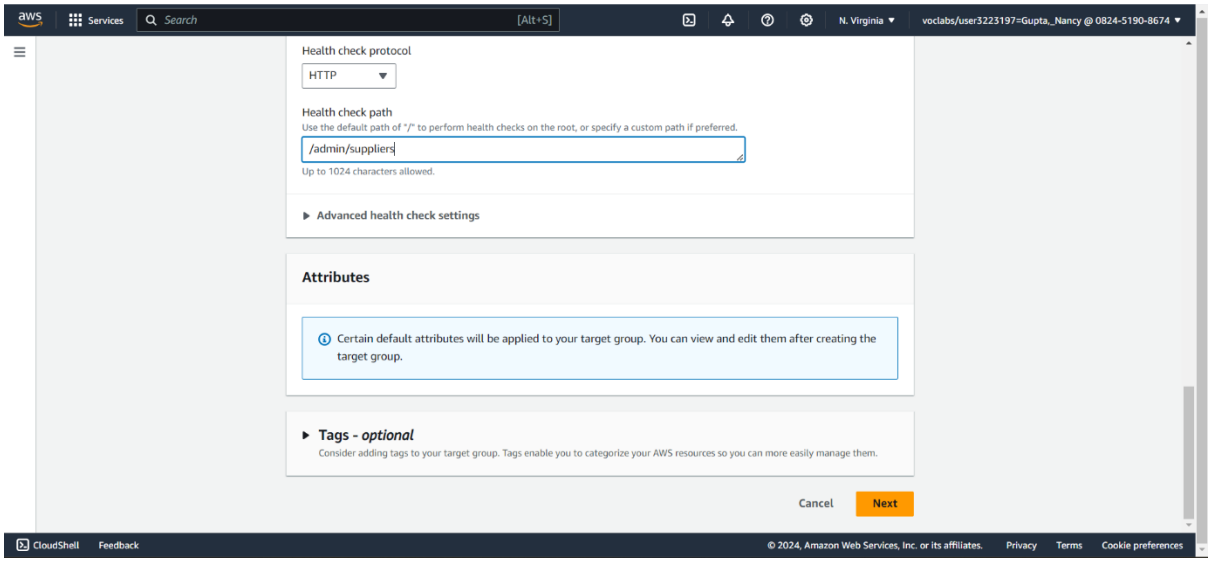

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
EC2 > Target groups > Create target group
Step 1
Specify group details
Step 2
Register targets
Specify group details
Your load balancer routes requests to the targets in a target group and performs health checks on the targets.
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.
Lambda function
Facilitates routing to a single Lambda function.
Accessible to Application Load Balancers only.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

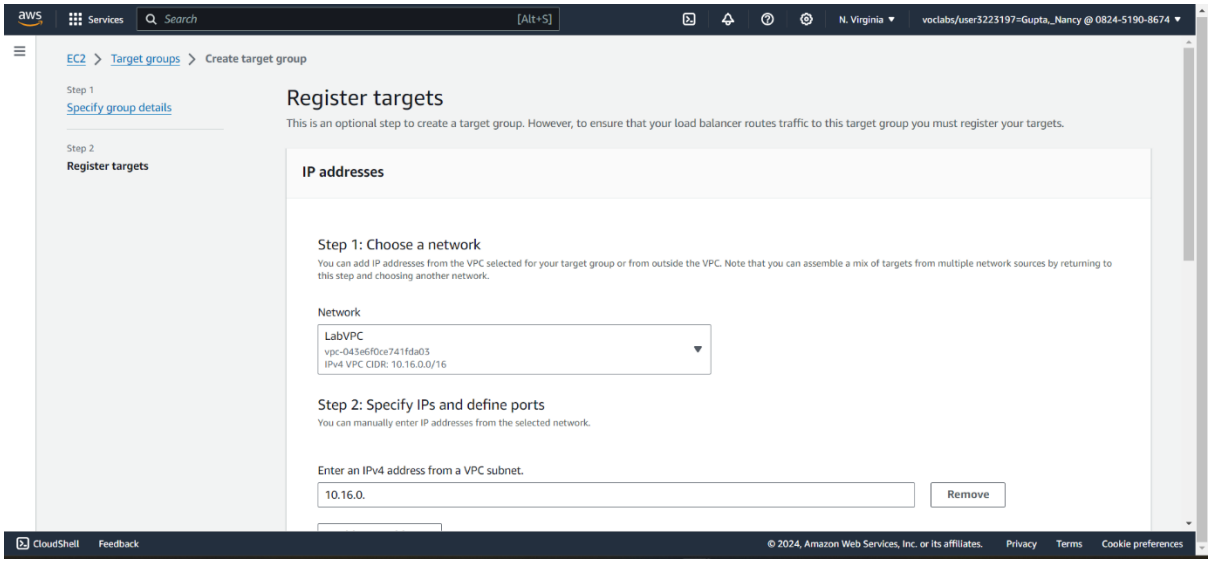

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
Application Load Balancer
Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.
Target group name
employee-tg-one
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
IPv6
VPC
Select the VPC that hosts the load balancer. Only VPCs that support the IP address type selected above are available in this list. On the Register targets page, you can register IP addresses from this VPC, or from private IP addresses located outside of this load balancer's VPC (such as a peered VPC, EC2-Classic, or on-premises targets that are reachable over Direct Connect or VPN).
-
vpc-000e564836083dda8
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

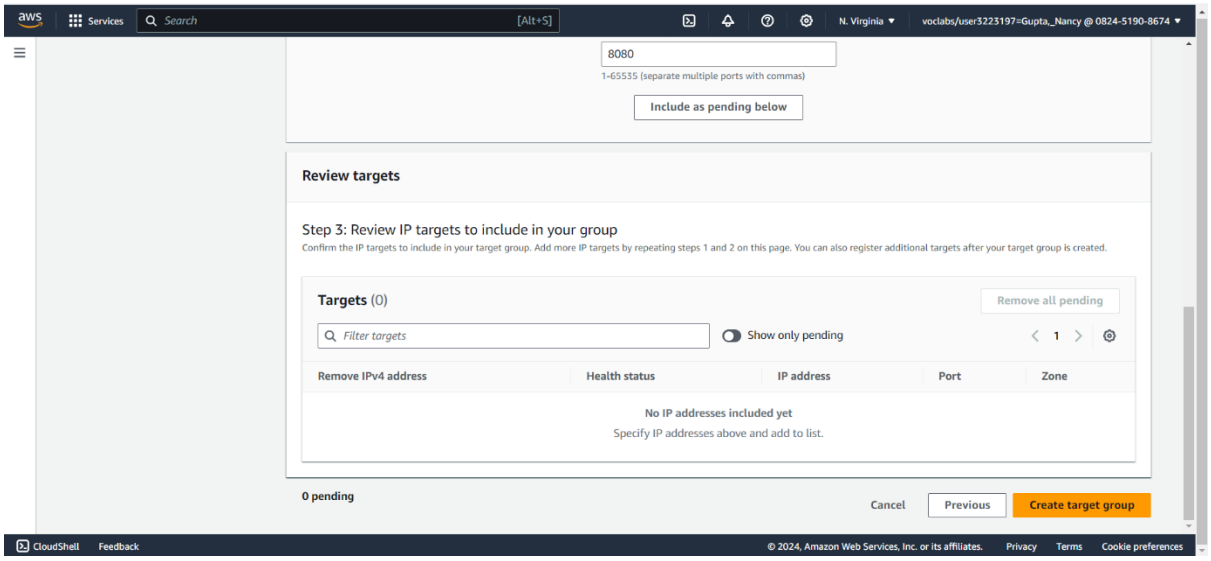

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
Application Load Balancer
Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.
Target group name
employee-tg-one
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
8080
1-65535
IP address type
Only targets with the indicated IP address type can be registered to this target group.
IPv4
IPv6
VPC
Select the VPC that hosts the load balancer. Only VPCs that support the IP address type selected above are available in this list. On the Register targets page, you can register IP addresses from this VPC, or from private IP addresses located outside of this load balancer's VPC (such as a peered VPC, EC2-Classic, or on-premises targets that are reachable over Direct Connect or VPN).
-
vpc-000e564836083dda8
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

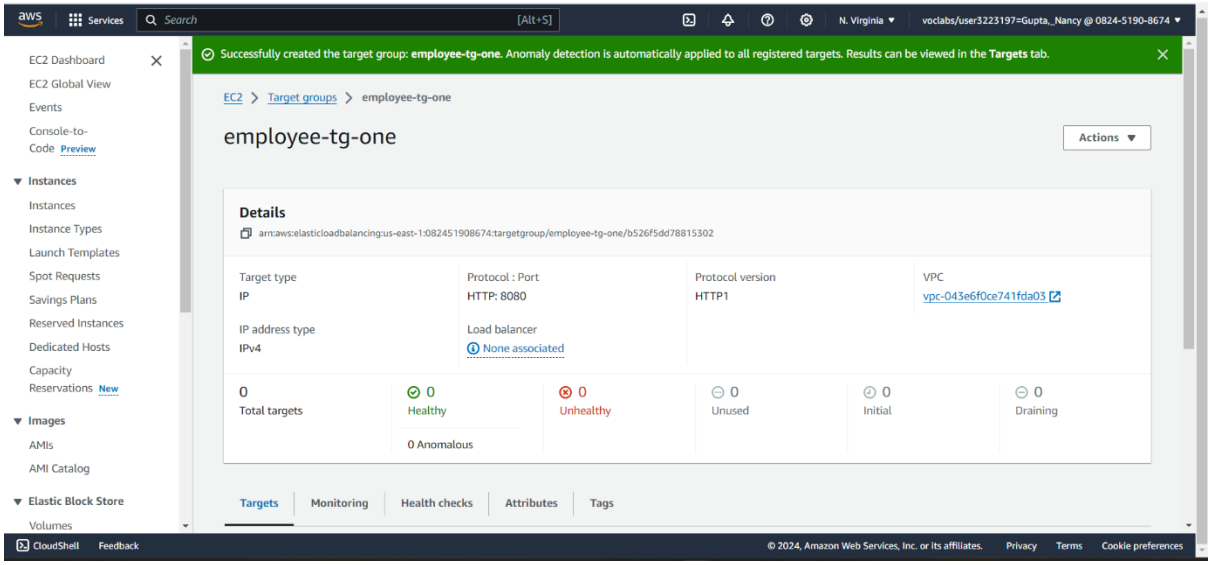

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
IP address type
Only targets with the indicated IP address type can be registered to this target group.
IPv4
IPv6
VPC
Select the VPC that hosts the load balancer. Only VPCs that support the IP address type selected above are available in this list. On the Register targets page, you can register IP addresses from this VPC, or from private IP addresses located outside of this load balancer's VPC (such as a peered VPC, EC2-Classic, or on-premises targets that are reachable over Direct Connect or VPN).
LabVPC
vpc-043e6f0ce741fda03
IPv4 VPC CIDR: 10.16.0.0/16
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.
Health checks
The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.
Health check protocol
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

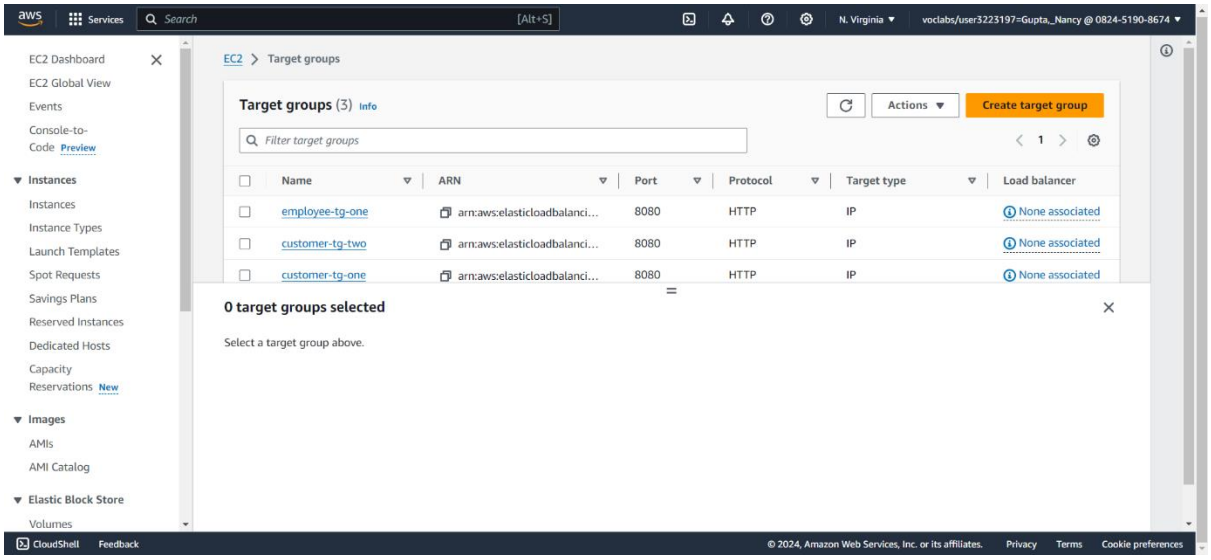

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
Send requests to targets using gRPC. Supported when the request protocol is gRPC.
Health checks
The associated load balancer periodically sends requests, per the settings below, to the registered targets to test 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.
/admin/suppliers
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.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
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.
/admin/suppliers
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

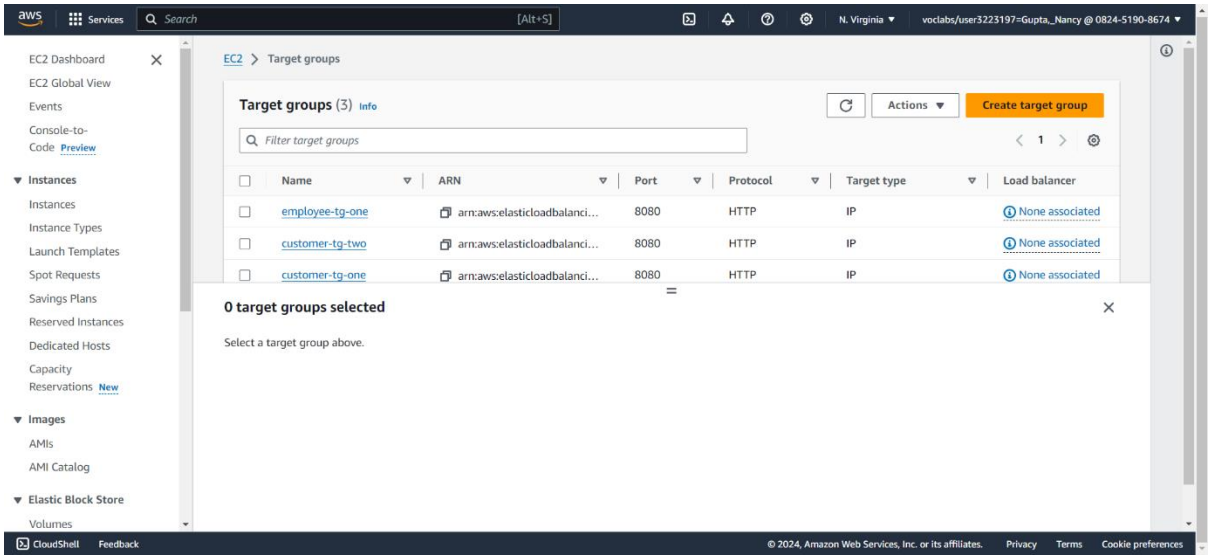

Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
EC2 > Target groups > Create target group
Step 1
Specify group details
Step 2
Register targets
Register targets
This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.
IP addresses
Step 1: Choose a network
You can add IP addresses from the VPC selected for your target group or from outside the VPC. Note that you can assemble a mix of targets from multiple network sources by returning to this step and choosing another network.
Network
LabVPC
vpc-043e6f0ce741fda03
IPv4 VPC CIDR: 10.16.0.0/16
Step 2: Specify IPs and define ports
You can manually enter IP addresses from the selected network.
Enter an IPv4 address from a VPC subnet.
10.16.0.
Remove
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

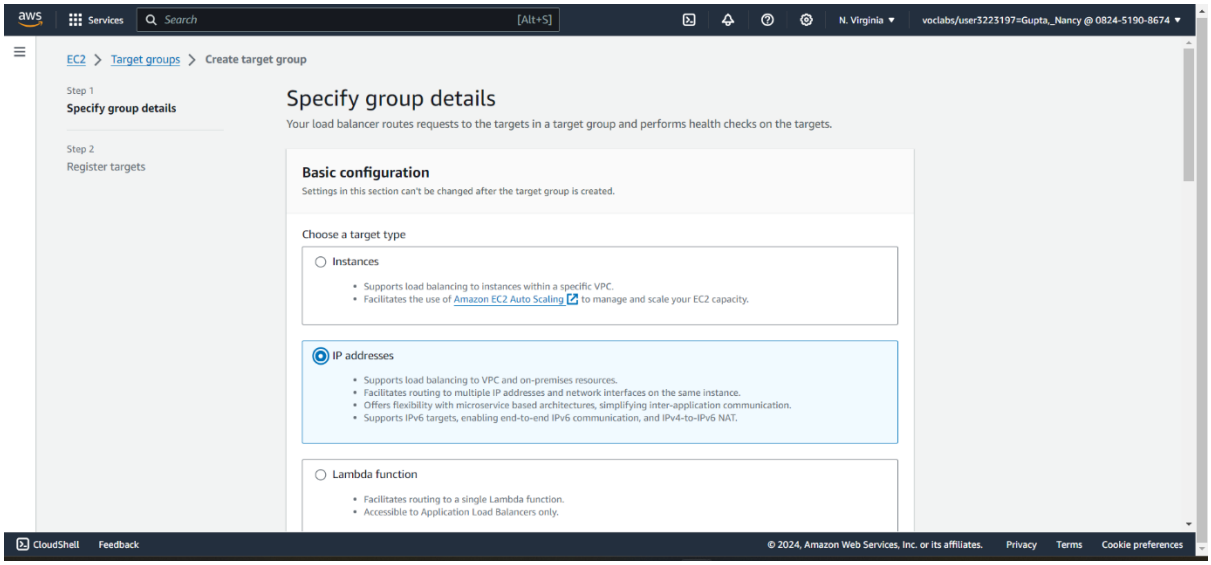

Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
8080
1-65535 (separate multiple ports with commas)
Include as pending below
Review targets
Step 3: Review IP targets to include in your group
Confirm the IP targets to include in your target group. Add more IP targets by repeating steps 1 and 2 on this page. You can also register additional targets after your target group is created.
Targets (0)
Remove all pending
Filter targets
Show only pending
Remove IPv4 address
Health status
IP address
Port
Zone
No IP addresses included yet
Specify IP addresses above and add to list.
0 pending
Cancel
Previous
Create target group
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

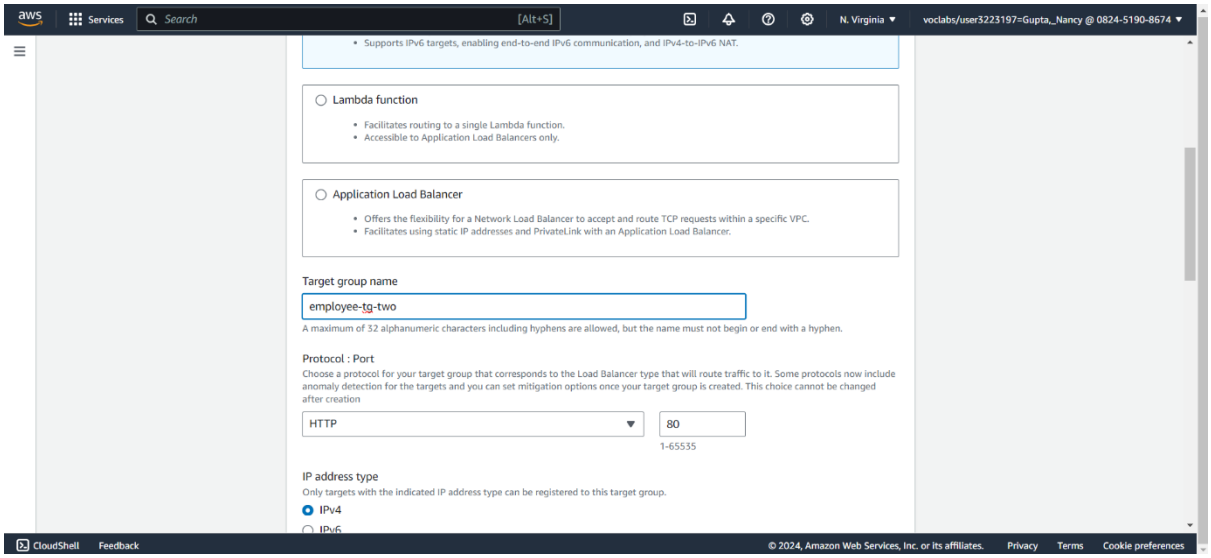

Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Successfully created the target group: employee-tg-one. Anomaly detection is automatically applied to all registered targets. Results can be viewed in the Targets tab.
EC2 > Target groups > employee-tg-one
employee-tg-one
Actions
Details
arn:aws:elasticloadbalancing:us-east-1:082451908674:targetgroup/employee-tg-one/b526f5dd78815302
Target type
IP
Protocol : Port
HTTP: 8080
Protocol version
HTTP1
VPC
vpc-043e6f0ce741fda03
IP address type
IPv4
Load balancer
None associated
0
Total targets
0
Healthy
0 Anomalous
0
Unhealthy
0
Unused
0
Initial
0
Draining
Targets
Monitoring
Health checks
Attributes
Tags
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

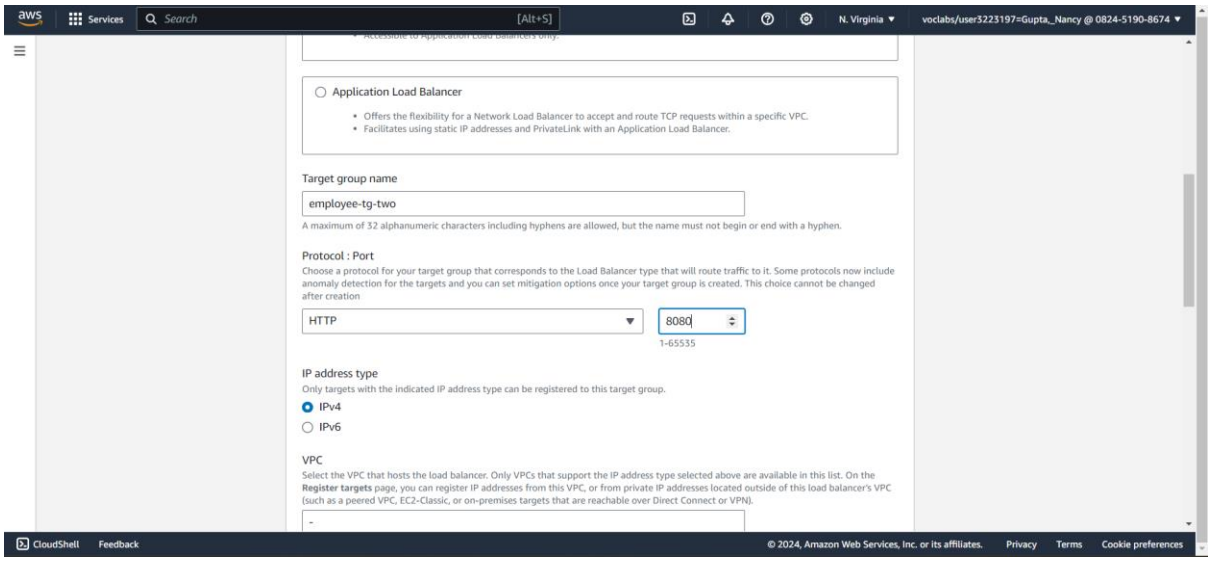


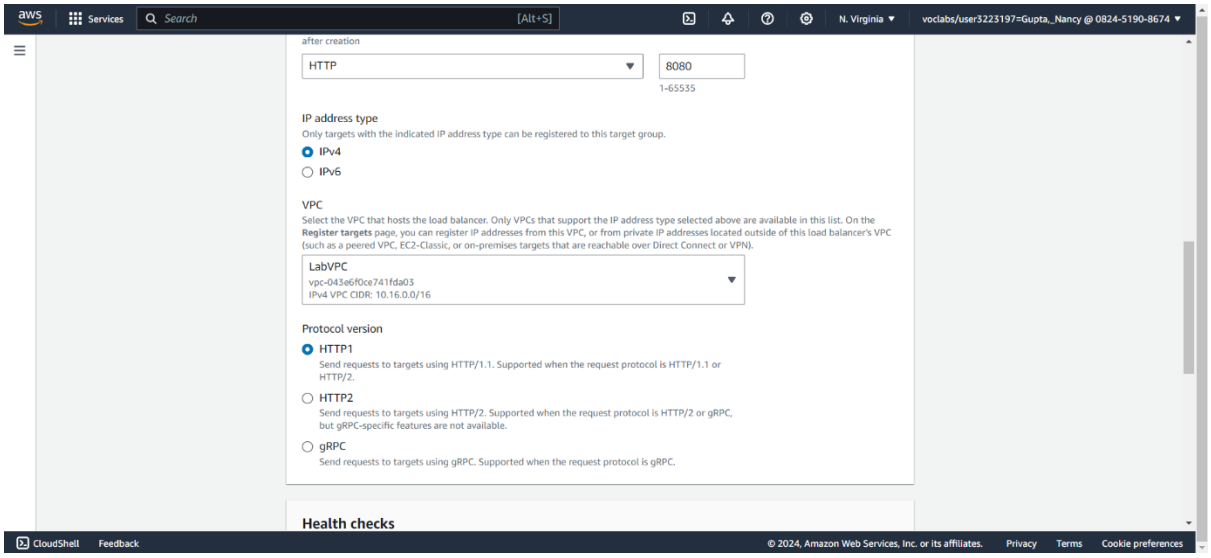
4. **Create a second target group for the *employee* microservice. Use the same settings as the other target groups with the following exceptions:**
    - **Target group name: Enter employee-tg-two**
    - **Health check path: Enter /admin/suppliers**

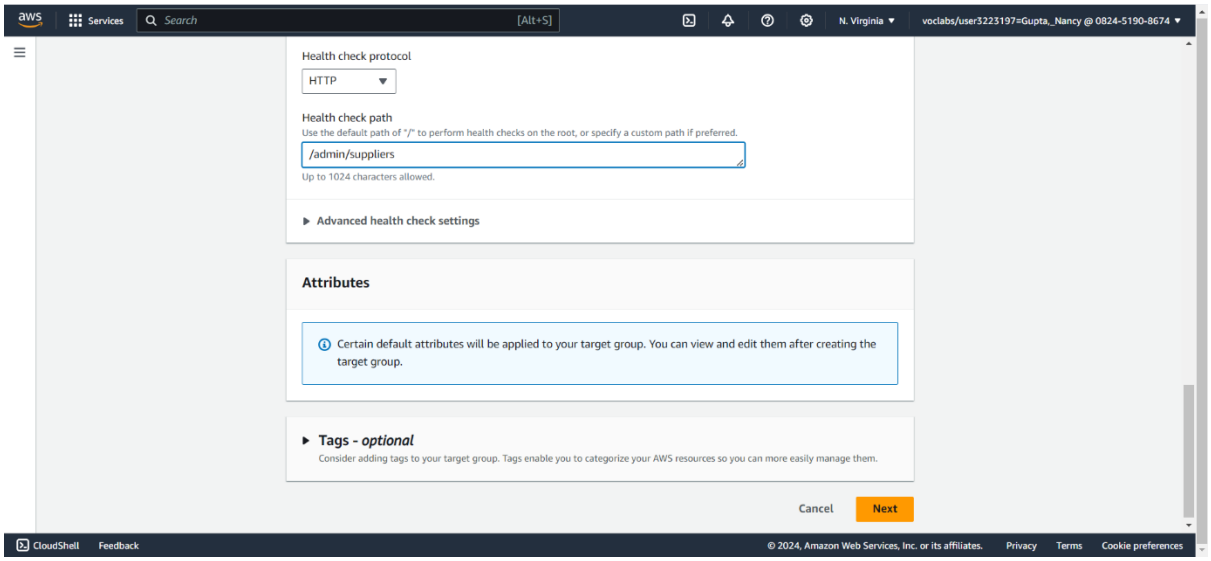


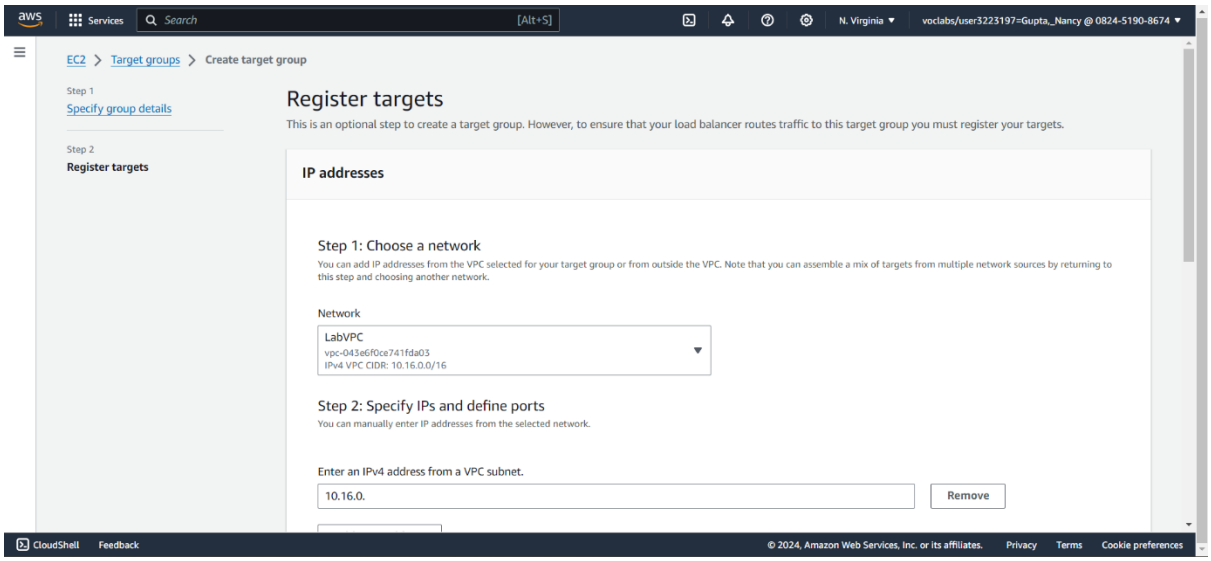

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
EC2 > Target groups > Create target group
Step 1
Specify group details
Step 2
Register targets
Specify group details
Your load balancer routes requests to the targets in a target group and performs health checks on the targets.
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.
Lambda function
Facilitates routing to a single Lambda function.
Accessible to Application Load Balancers only.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

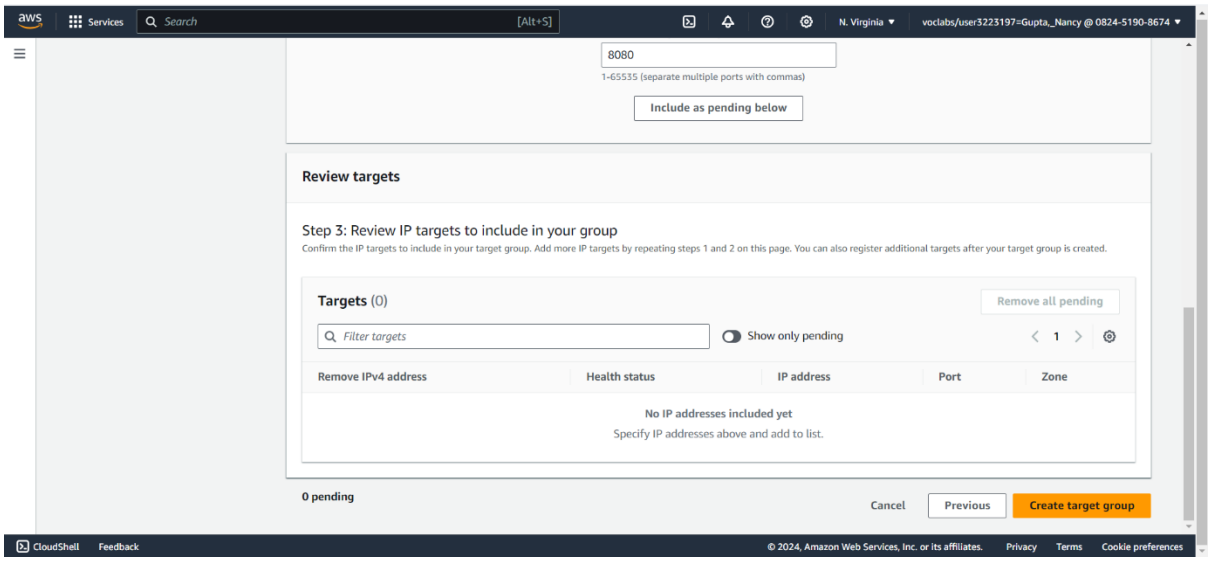

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.
Lambda function
Facilitates routing to a single Lambda function.
Accessible to Application Load Balancers only.
Application Load Balancer
Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.
Target group name
employee-tg-two
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
IPv6
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

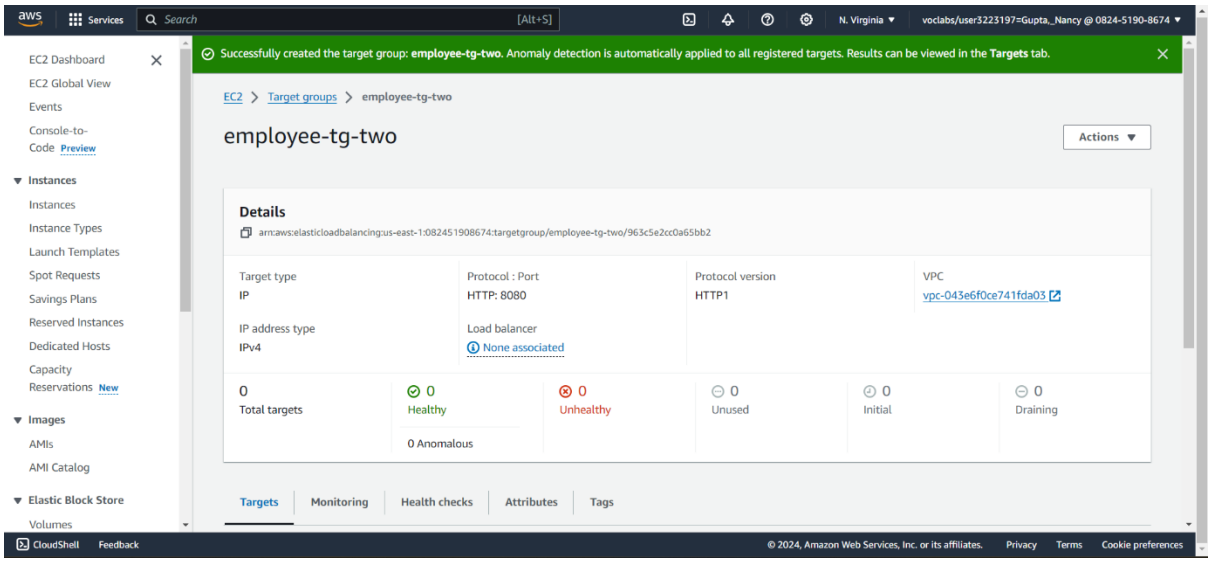

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
Application Load Balancer
Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.
Target group name
employee-tg-two
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
8080
1-65535
IP address type
Only targets with the indicated IP address type can be registered to this target group.
IPv4
IPv6
VPC
Select the VPC that hosts the load balancer. Only VPCs that support the IP address type selected above are available in this list. On the Register targets page, you can register IP addresses from this VPC, or from private IP addresses located outside of this load balancer's VPC (such as a peered VPC, EC2-Classic, or on-premises targets that are reachable over Direct Connect or VPN).
-
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
after creation
HTTP
8080
1-65535
IP address type
Only targets with the indicated IP address type can be registered to this target group.
IPv4
IPv6
VPC
Select the VPC that hosts the load balancer. Only VPCs that support the IP address type selected above are available in this list. On the Register targets page, you can register IP addresses from this VPC, or from private IP addresses located outside of this load balancer's VPC (such as a peered VPC, EC2-Classic, or on-premises targets that are reachable over Direct Connect or VPN).
LabVPC
vpc-043e6f0ce741fda03
IPv4 VPC CIDR: 10.16.0.0/16
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.
Health checks
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

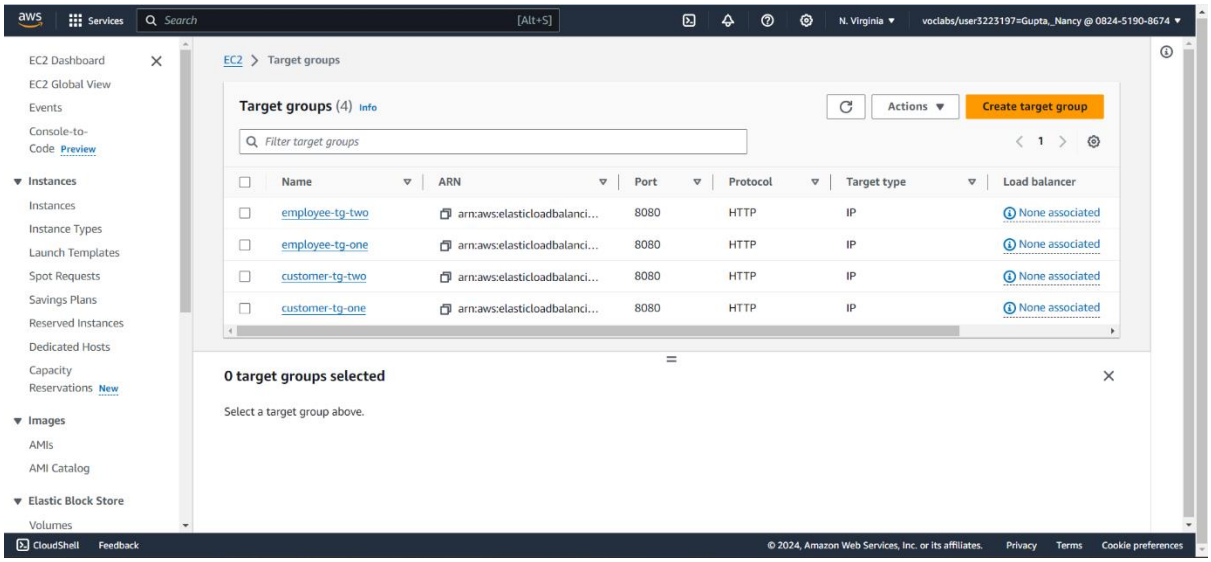

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
Health check protocol
HTTP
Health check path
Use the default path of "/" to perform health checks on the root, or specify a custom path if preferred.
/admin/suppliers
Up to 1024 characters allowed.
Advanced health 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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
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.
IP addresses
Step 1: Choose a network
You can add IP addresses from the VPC selected for your target group or from outside the VPC. Note that you can assemble a mix of targets from multiple network sources by returning to this step and choosing another network.
Network
LabVPC
vpc-043e6f0ce741fda03
IPv4 VPC CIDR: 10.16.0.0/16
Step 2: Specify IPs and define ports
You can manually enter IP addresses from the selected network.
Enter an IPv4 address from a VPC subnet.
10.16.0.
Remove
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



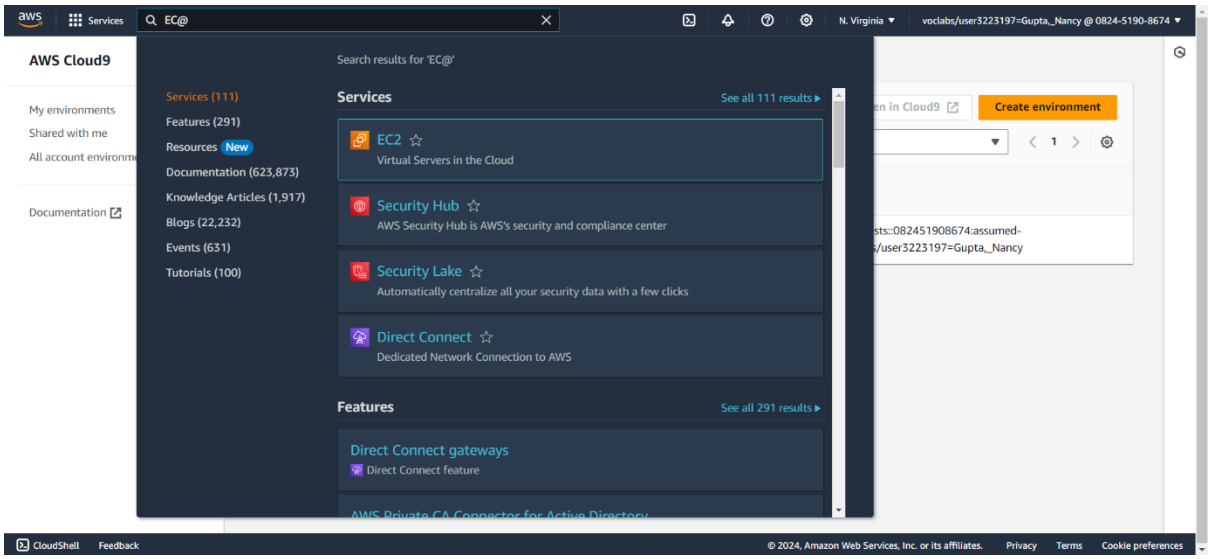


Important: Carefully confirm the name and port number of each target group. The following image provides an example:

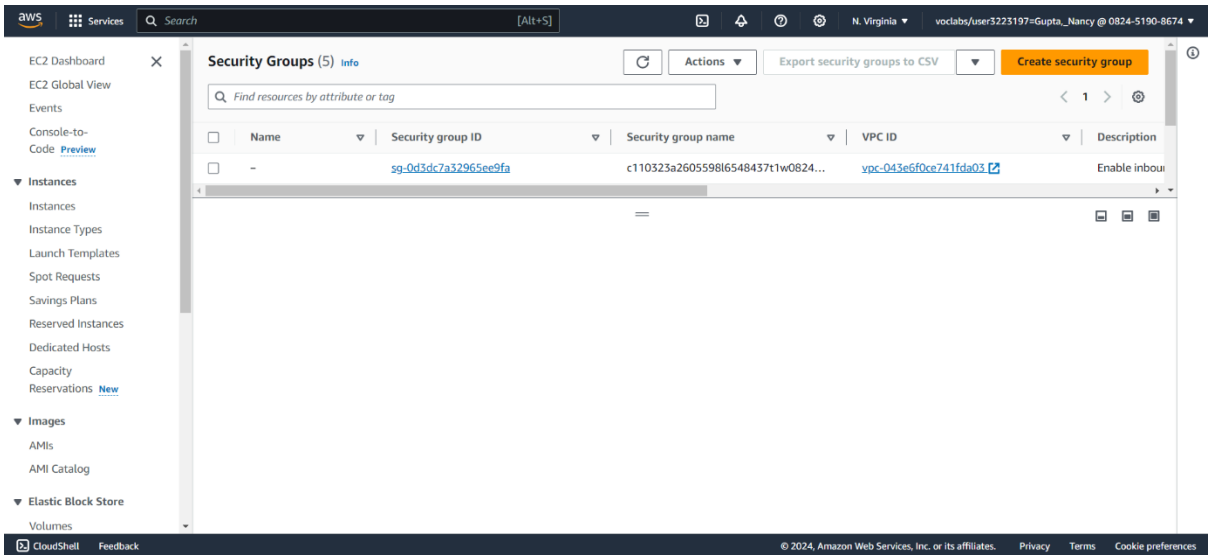


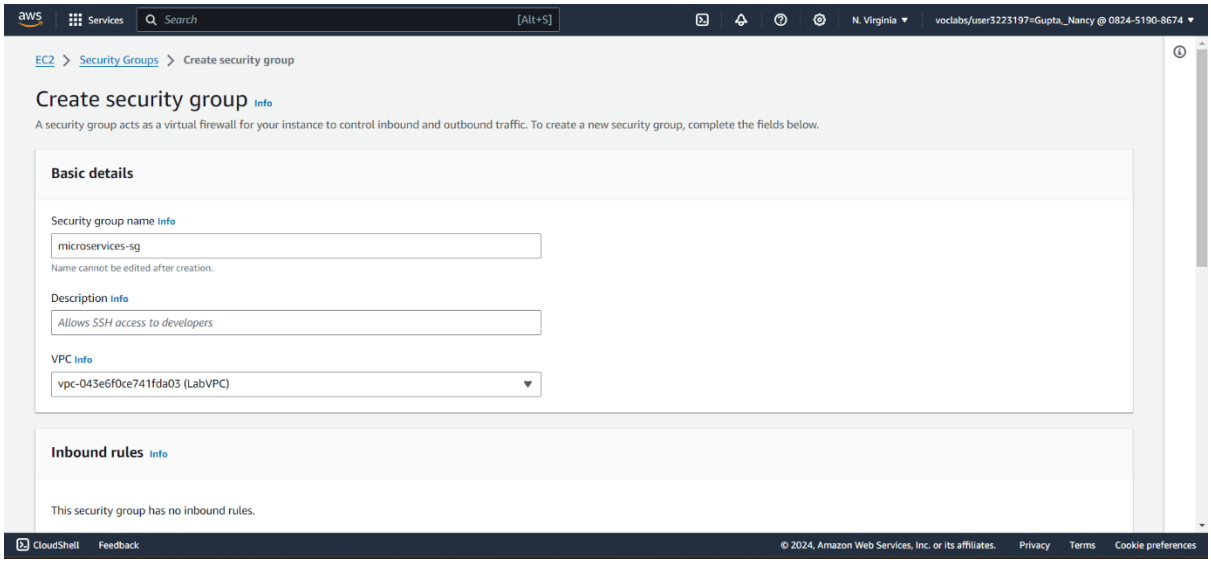
Task 6.2: Create a security group and an Application Load Balancer, and configure rules to route traffic

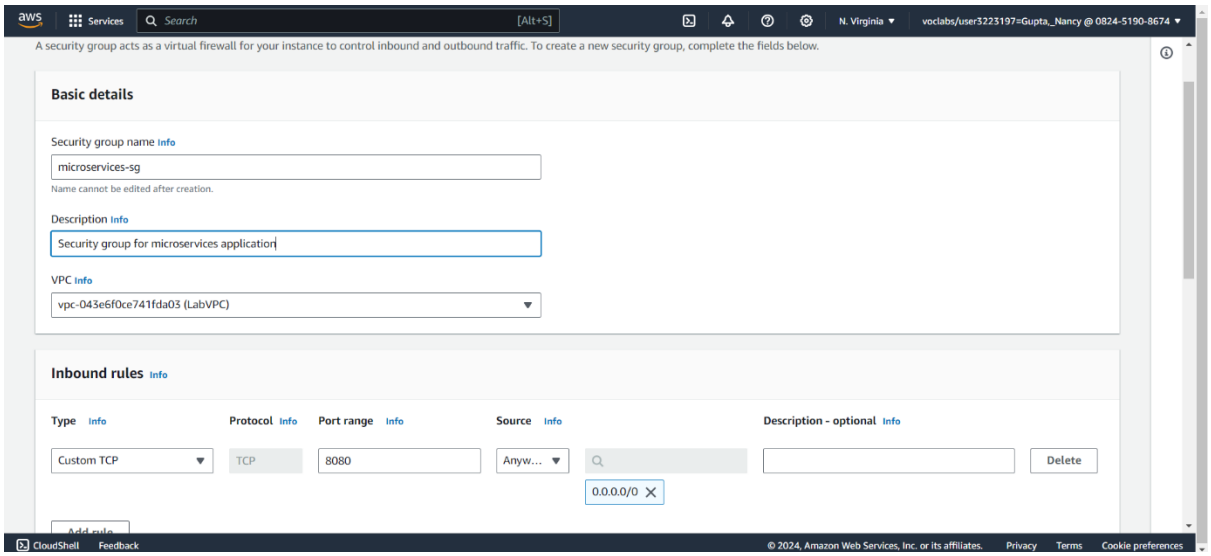
In this task, you will create an Application Load Balancer. You will also define two listeners for the load balancer: one on port 80 and another on port 8080. For each listener, you will then define path-based routing rules so that traffic is routed to the correct target group depending on the URL that a user attempts to load.

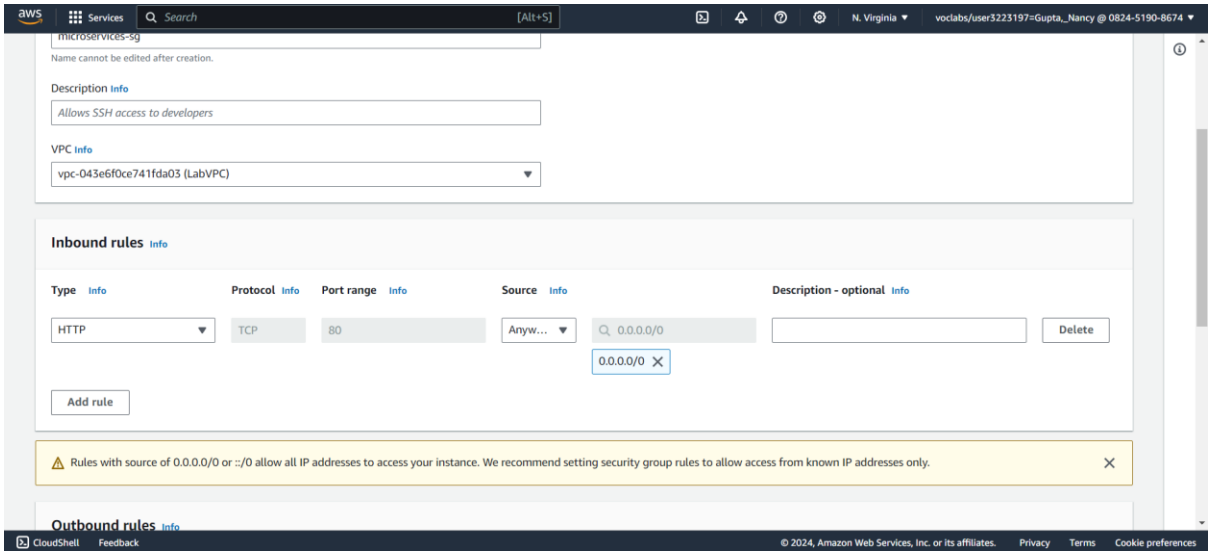


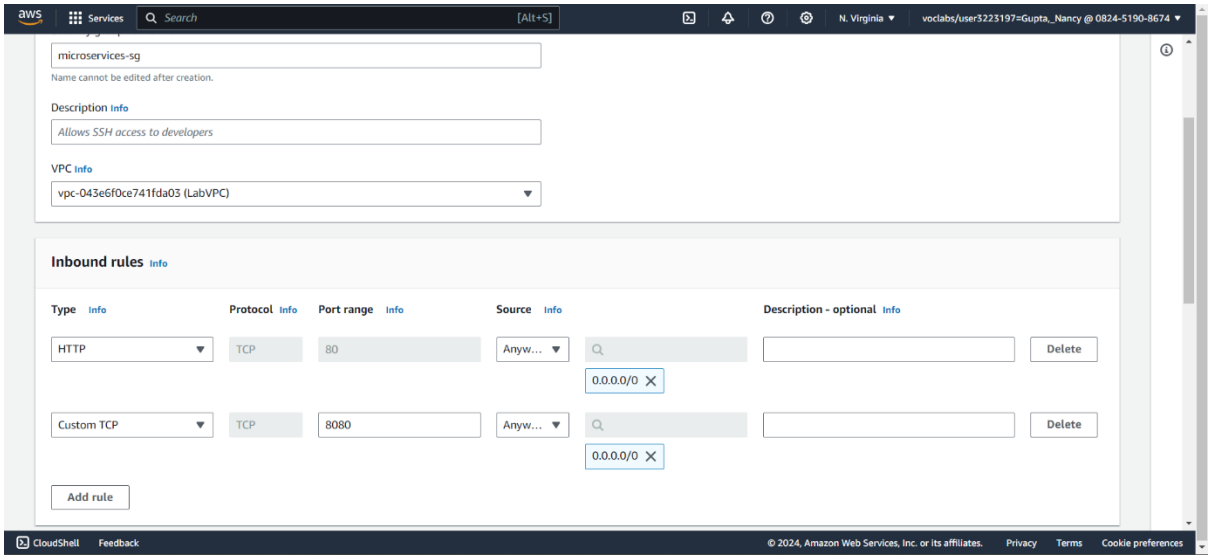
1. **Create a new EC2 security group named microservices-sg to use in *LabVPC*. Add inbound rules that allow TCP traffic from any IPv4 address on ports 80 and 8080.**

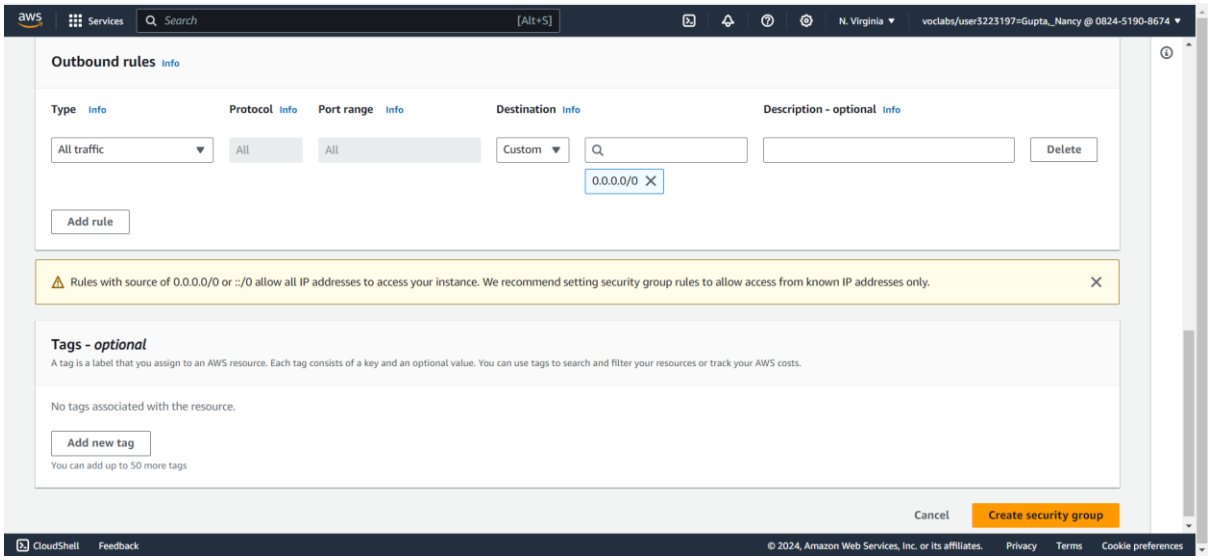


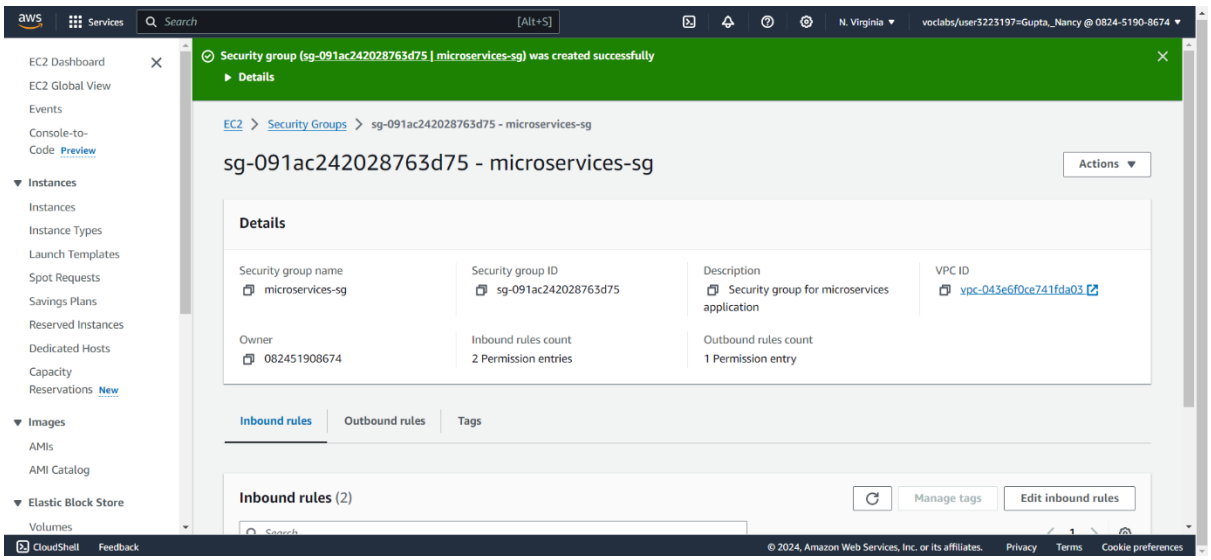

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
EC2 > Security Groups > Create security group
Create security group Info
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.
Basic details
Security group name Info
microservices-sg
Name cannot be edited after creation.
Description Info
Allows SSH access to developers
VPC Info
vpc-043e6f0ce741fda03 (LabVPC)
Inbound rules Info
This security group has no inbound rules.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

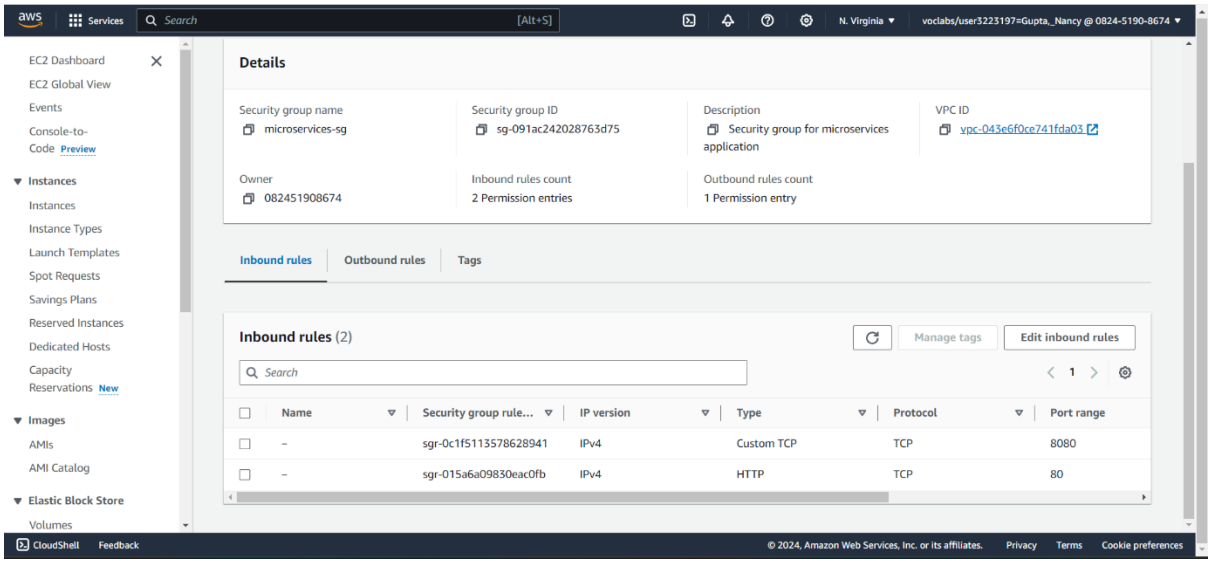

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.
Basic details
Security group name Info
microservices-sg
Name cannot be edited after creation.
Description Info
Security group for microservices application
VPC Info
vpc-043e6f0ce741fda03 (LabVPC)
Inbound rules Info
Type Info
Protocol Info
Port range Info
Source Info
Description - optional Info
Custom TCP
TCP
8080
Anyw...
0.0.0.0/0
Delete
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

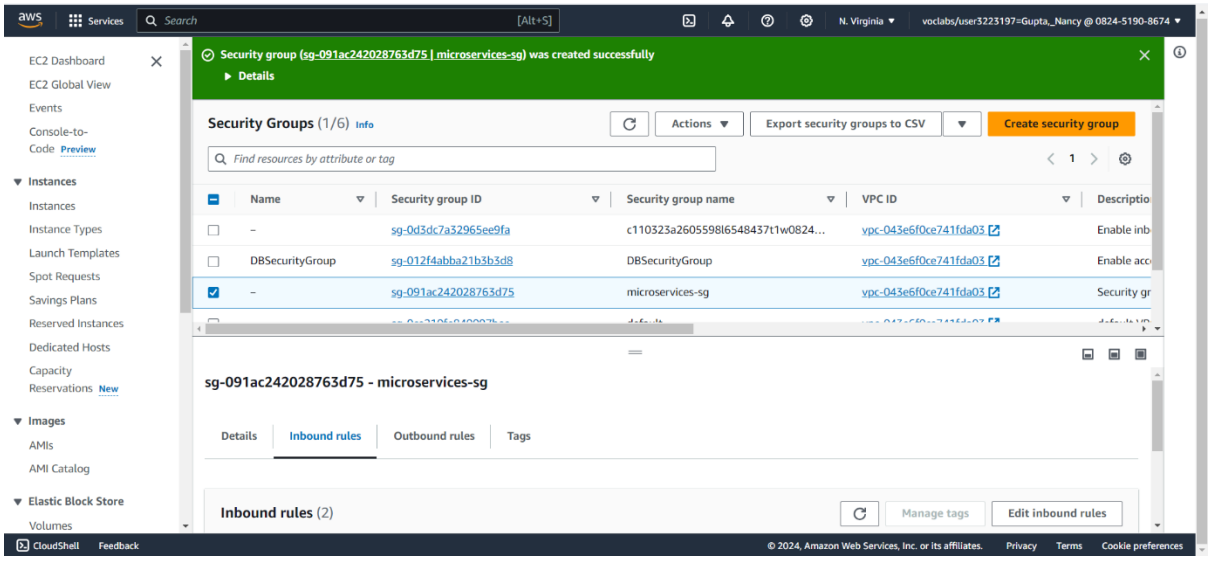

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
Name cannot be edited after creation.
Description Info
Allows SSH access to developers
VPC Info
vpc-043e6f0ce741fda03 (LabVPC)
Inbound rules Info
Type Info
Protocol Info
Port range Info
Source Info
Description - optional Info
HTTP
TCP
80
Anyw...
0.0.0.0/0
0.0.0.0/0
Delete
Add rule
Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Outbound rules Info
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


microservices-sg
Name cannot be edited after creation.
Description Info
Allows SSH access to developers
VPC Info
vpc-043e6f0ce741fda03 (LabVPC)
Inbound rules Info
Type Info
Protocol Info
Port range Info
Source Info
Description - optional Info
HTTP
TCP
80
Anyw…
0.0.0.0/0
Delete
Custom TCP
TCP
8080
Anyw…
0.0.0.0/0
Delete
Add rule
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

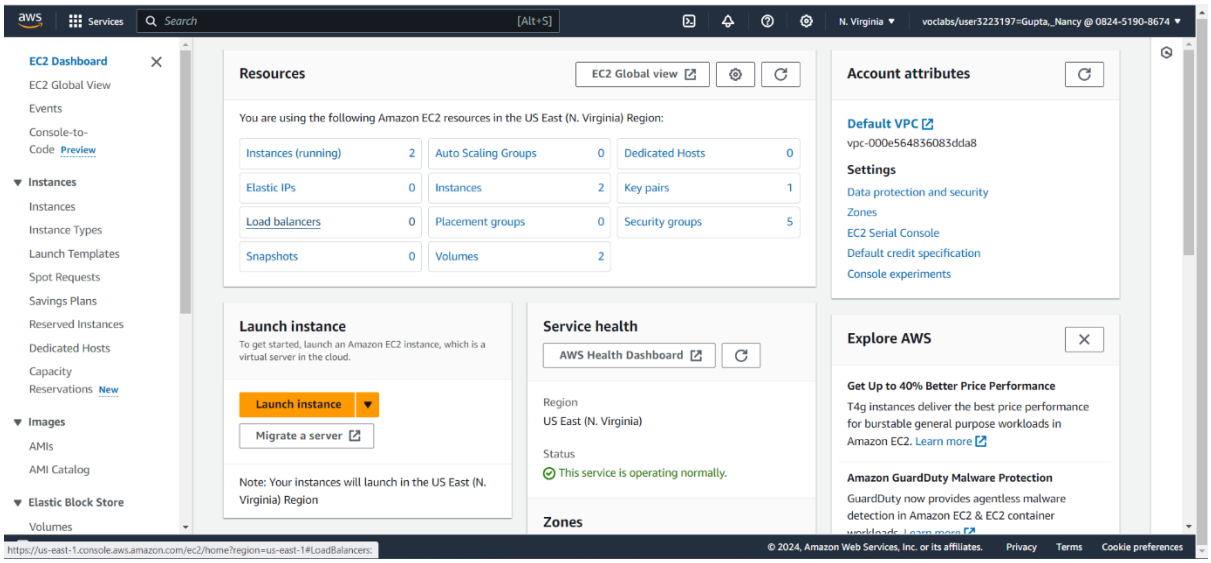

Outbound rules Info
Type Info
Protocol Info
Port range Info
Destination Info
Description - optional Info
All traffic
All
All
Custom
0.0.0.0/0
Delete
Add rule
Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Tags - optional
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 or track your AWS costs.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags
Cancel
Create security group
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

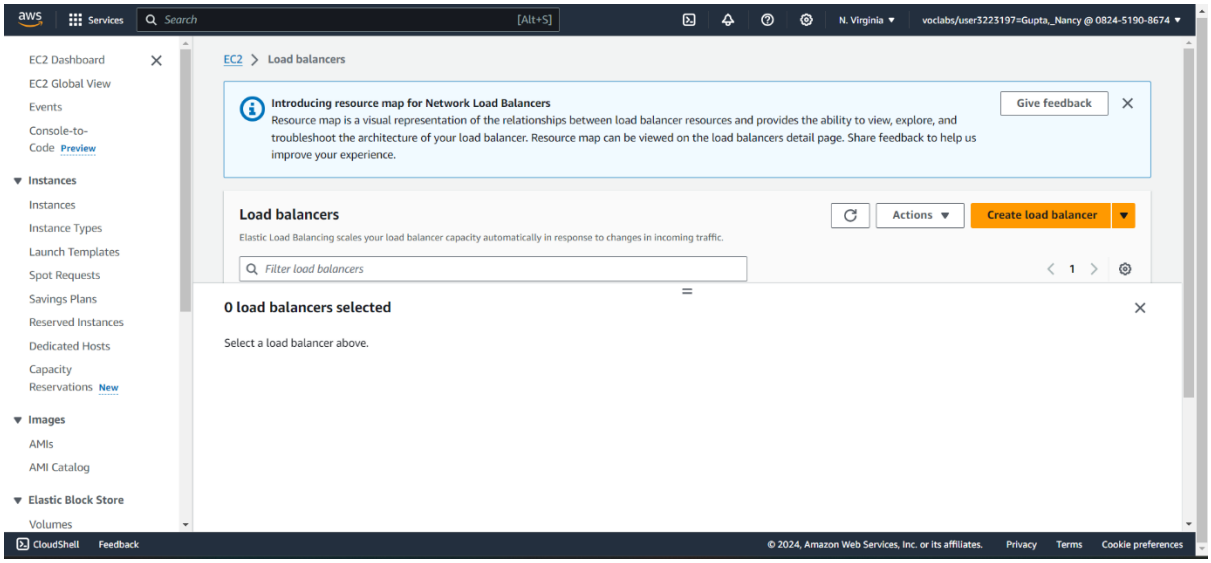

Security group (sg-091ac242028763d75 | microservices-sg) was created successfully
Details
EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
EC2 > Security Groups > sg-091ac242028763d75 - microservices-sg
sg-091ac242028763d75 - microservices-sg
Actions
Details
Security group name
microservices-sg
Security group ID
sg-091ac242028763d75
Description
Security group for microservices application
VPC ID
vpc-043e6f0ce741fda03
Owner
082451908674
Inbound rules count
2 Permission entries
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Tags
Inbound rules (2)
Manage tags
Edit inbound rules
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

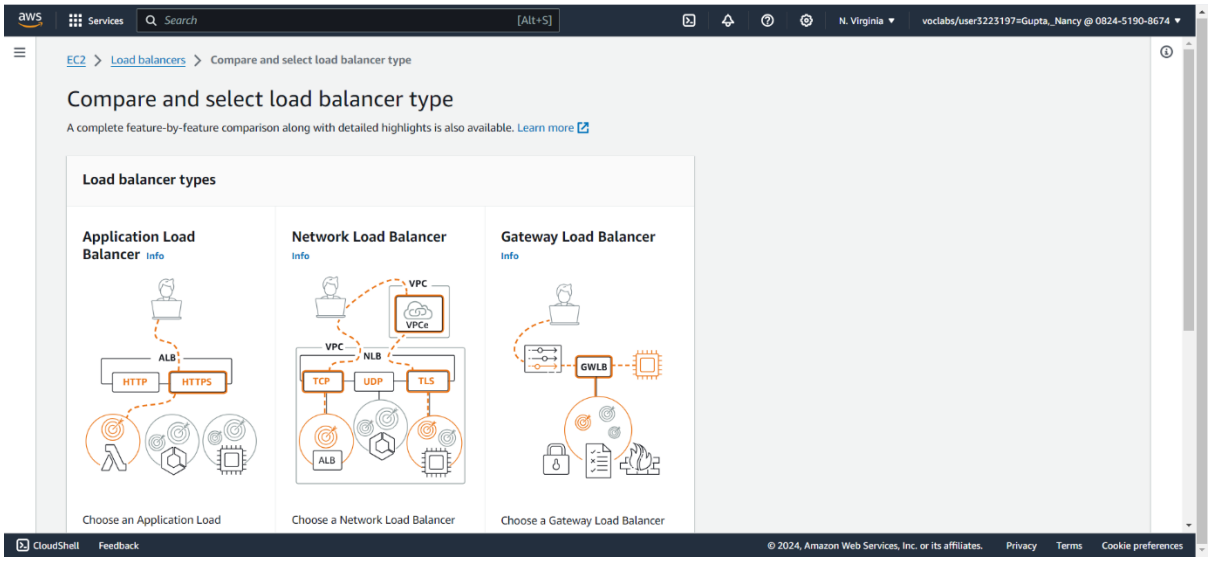


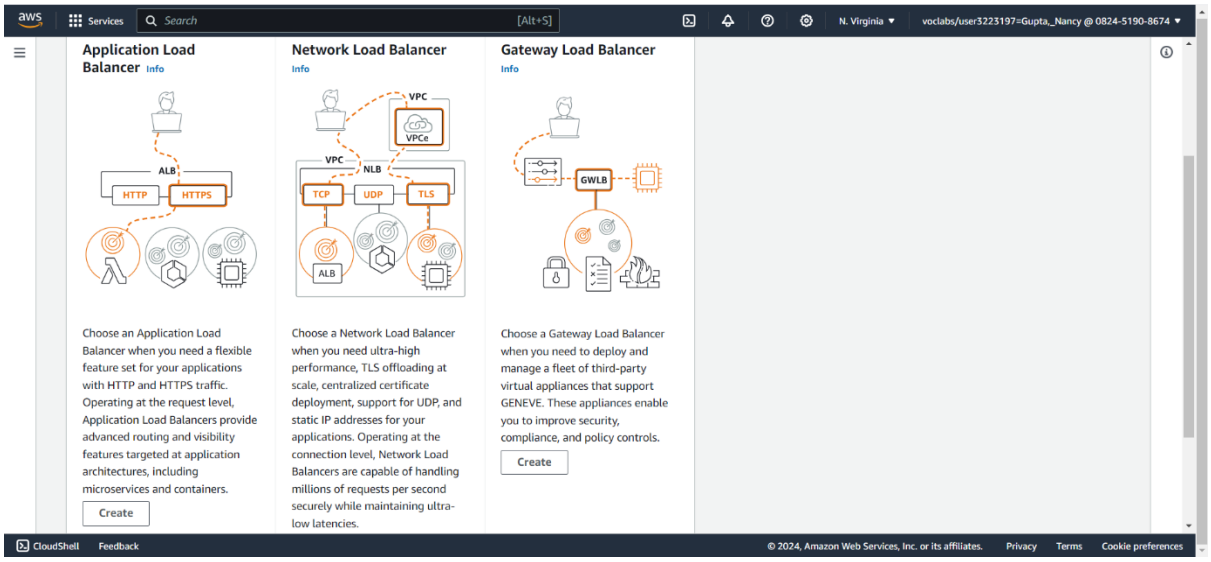


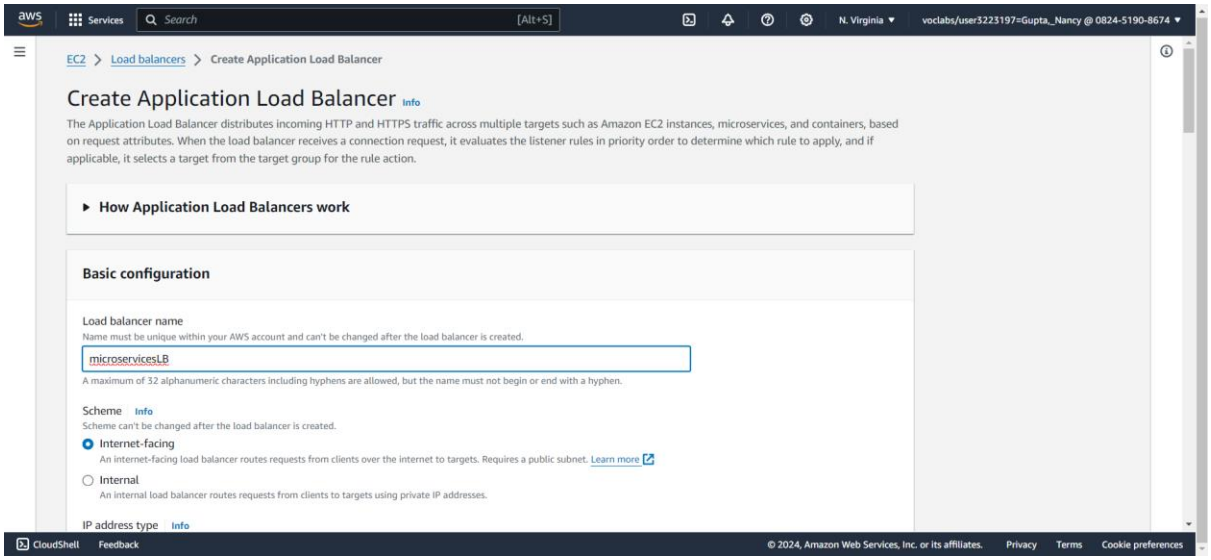
2. In the Amazon EC2 console, create an Application Load Balancer named microservicesLB.



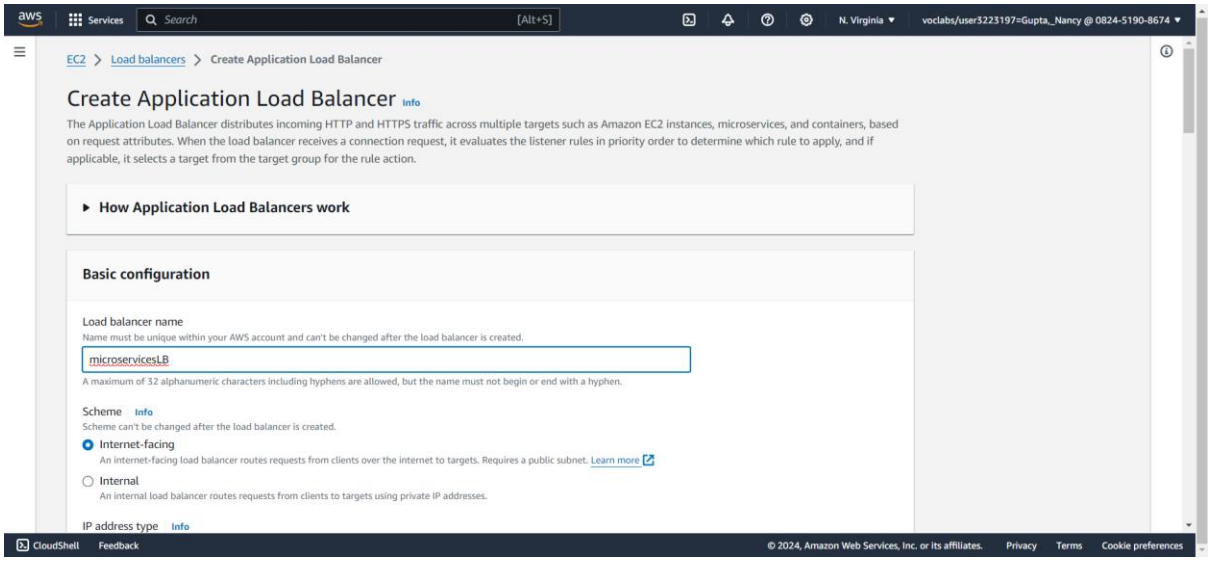

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
EC2 > Load balancers
Introducing resource map for Network Load Balancers
Resource map is a visual representation of the relationships between load balancer resources and provides the ability to view, explore, and troubleshoot the architecture of your load balancer. Resource map can be viewed on the load balancers detail page. Share feedback to help us improve your experience.
Give feedback
Load balancers
Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.
Actions
Create load balancer
Filter load balancers
1
0 load balancers selected
Select a load balancer above.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
EC2 > Load balancers > Compare and select load balancer type
Compare and select load balancer type
A complete feature-by-feature comparison along with detailed highlights is also available. Learn more
Load balancer types
Application Load Balancer Info
Network Load Balancer Info
Gateway Load Balancer Info
VPC
VPCe
ALB
HTTP
HTTPS
NLB
TCP
UDP
TLS
GWLB
Choose an Application Load
Choose a Network Load Balancer
Choose a Gateway Load Balancer
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

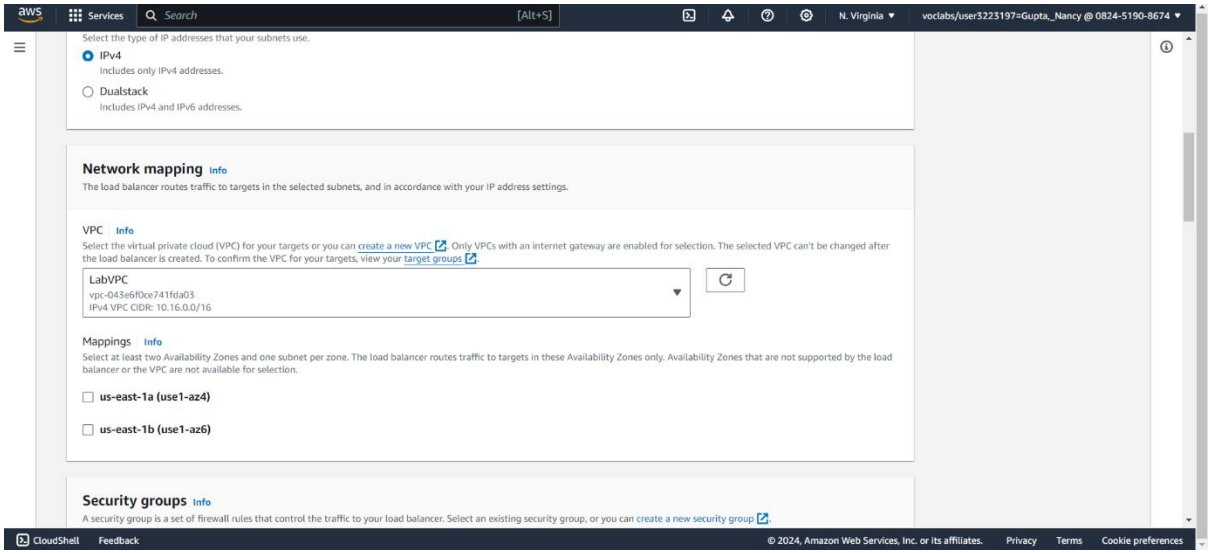

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
Application Load Balancer Info
Network Load Balancer Info
Gateway Load Balancer Info
VPC
VPCe
ALB
HTTP
HTTPS
NLB
TCP
UDP
TLS
GWLB
Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.
Create
Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.
Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.
Create
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

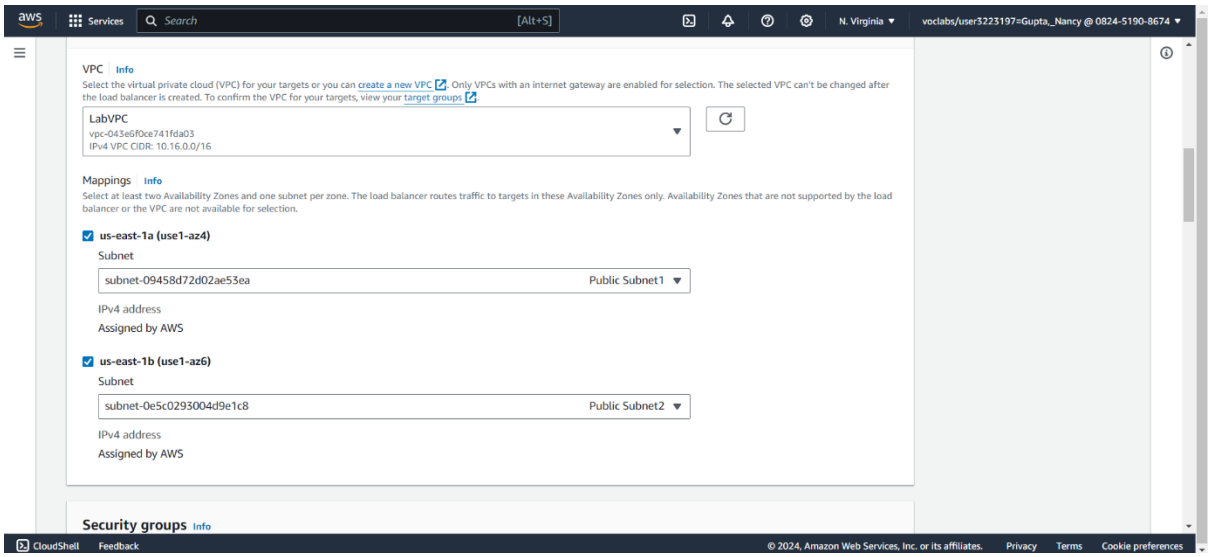


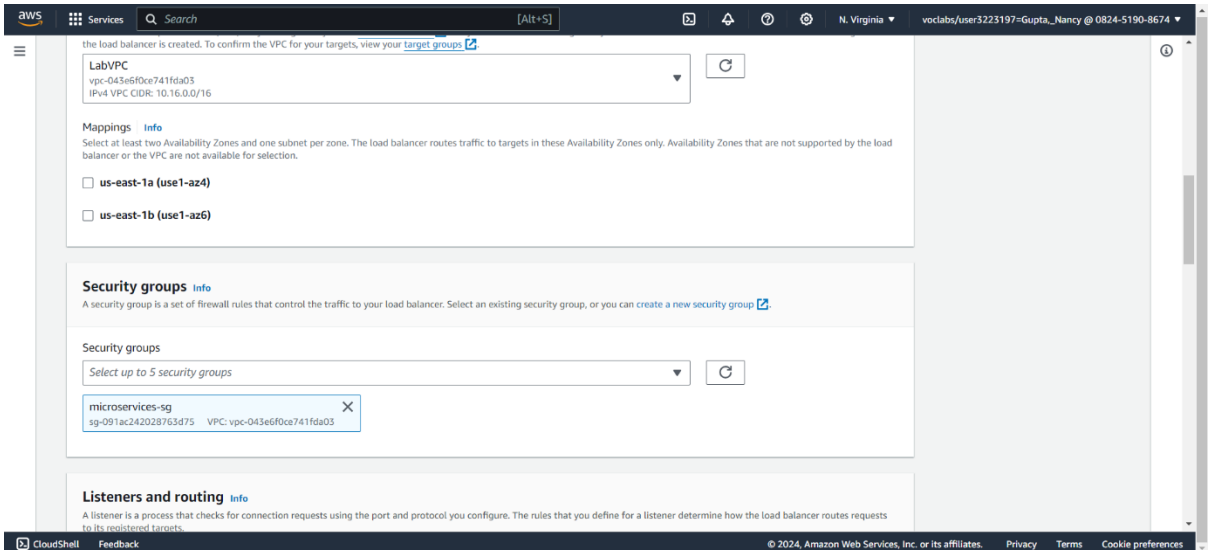
- **Make it internet facing for IPv4 addresses.**



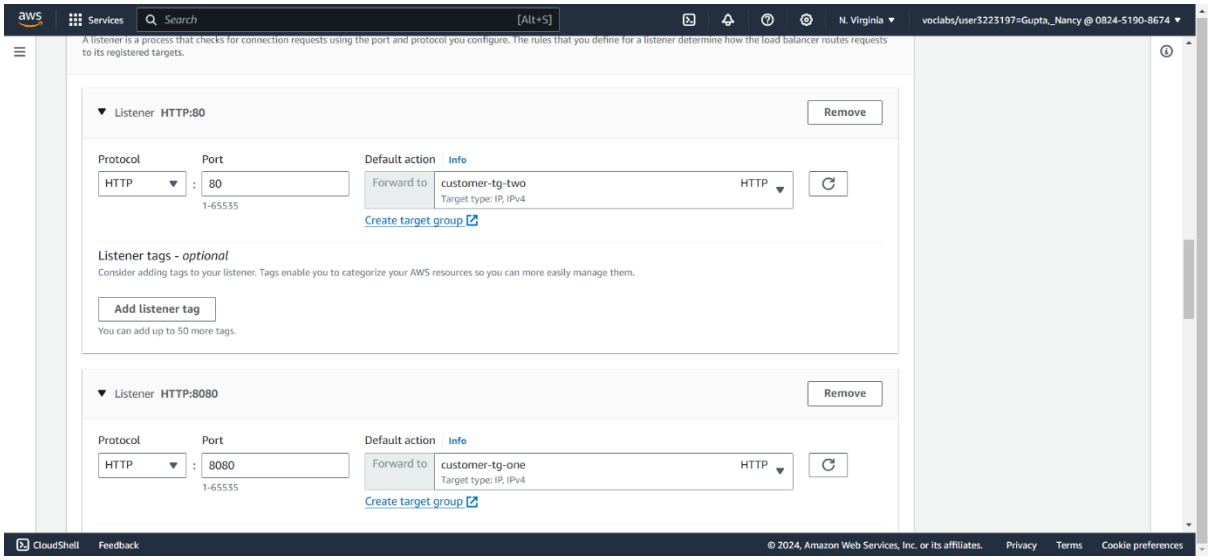
- **Use *LabVPC*, *Public Subnet1*, *Public Subnet2*, and the *microservices-sg* security group.**

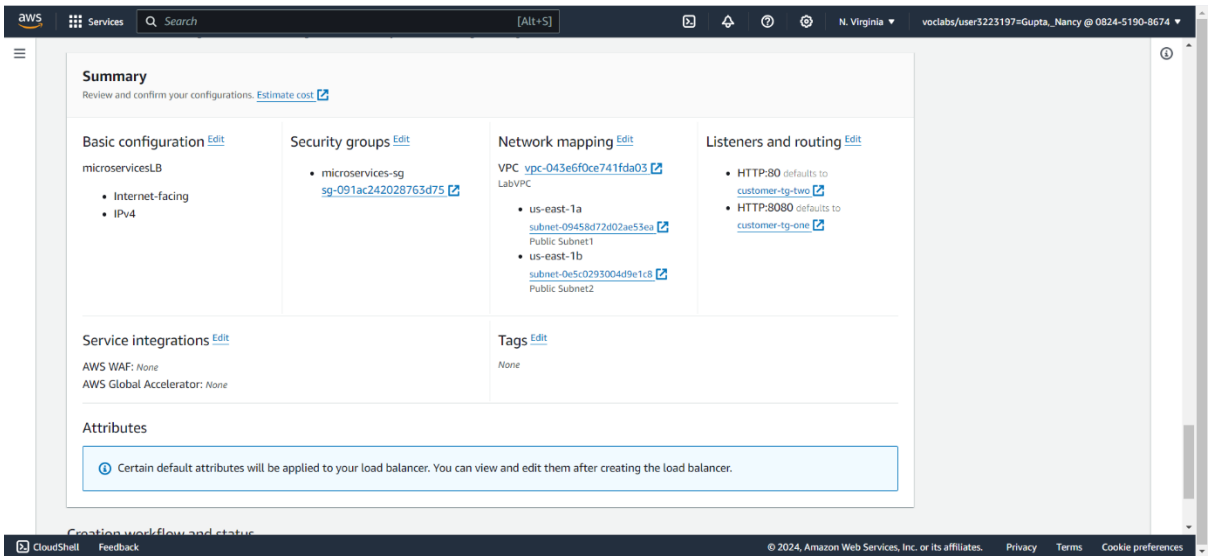


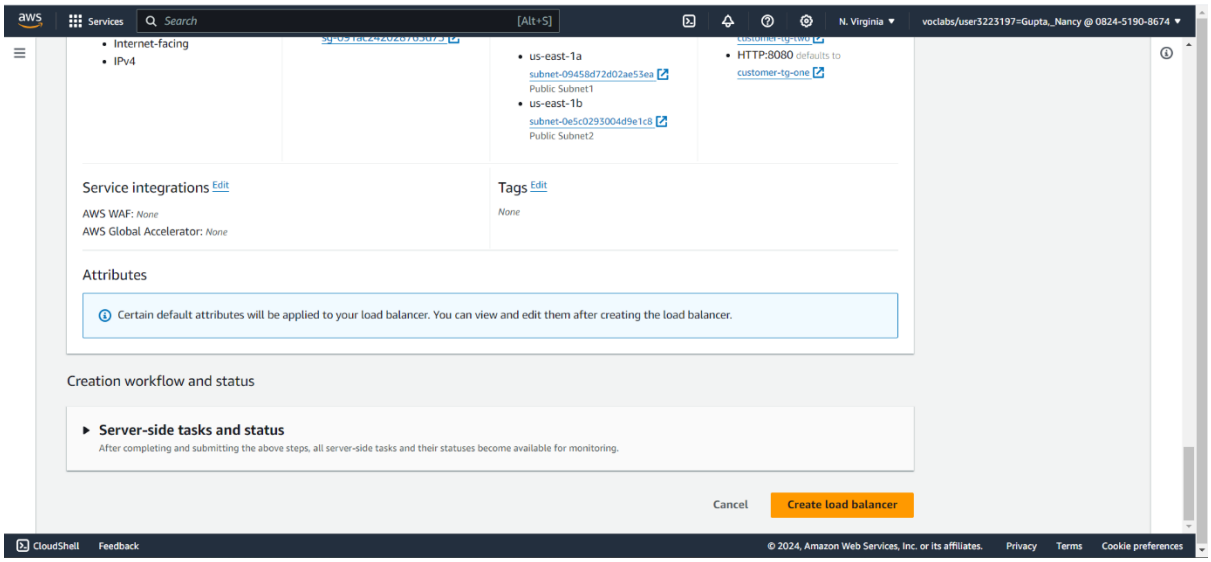


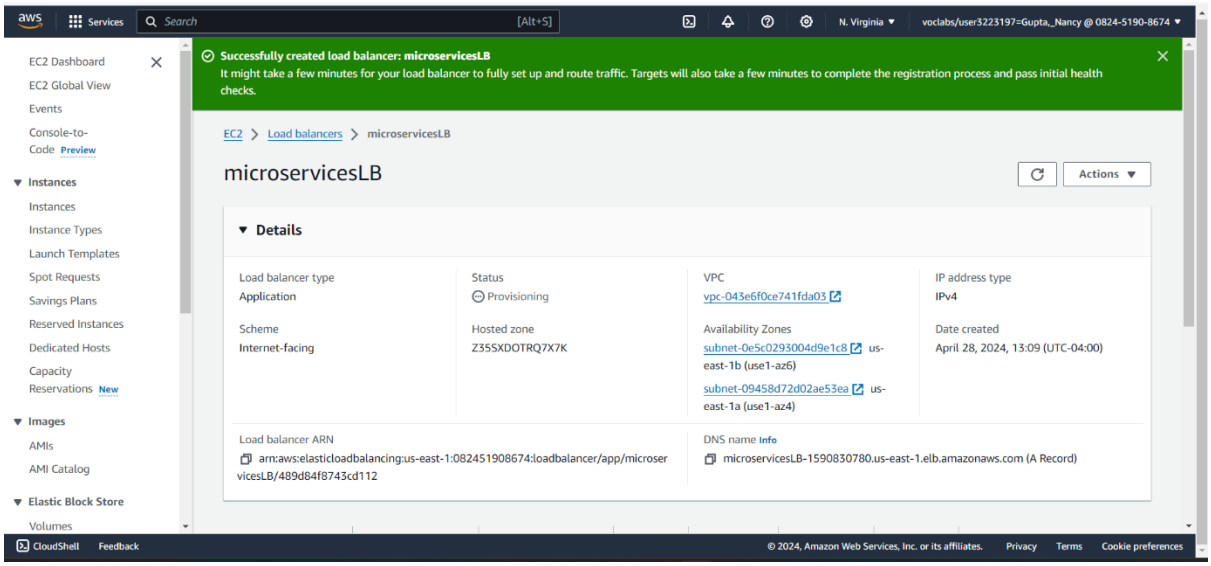


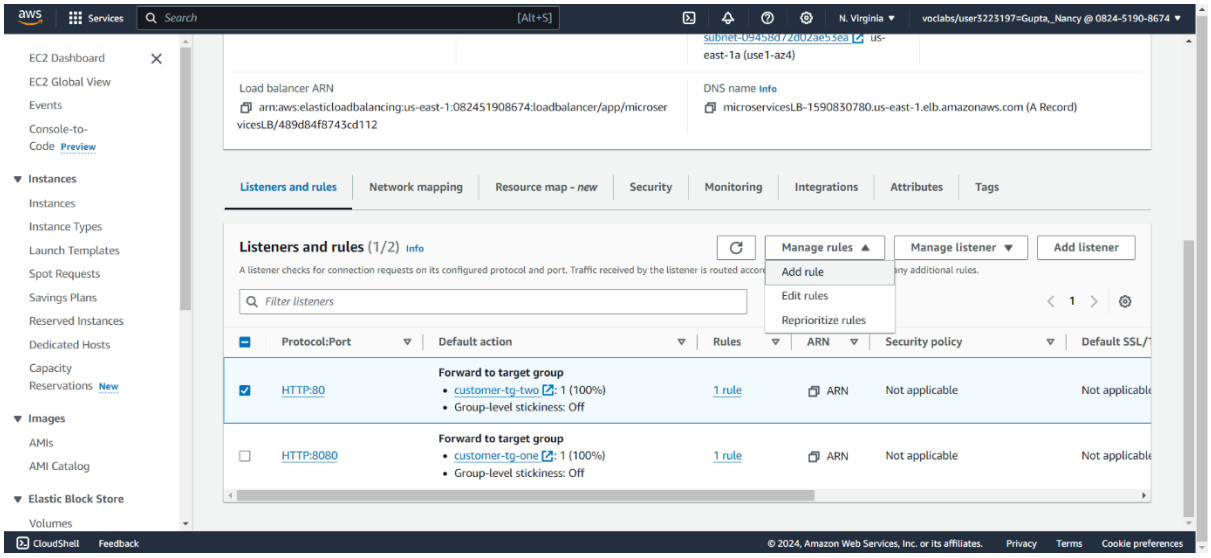
- **Configure two listeners on it. The first should listen on *HTTP:80* and forward traffic to *customer-tg-two* by default. The second should listen on *HTTP:8080* and forward traffic to *customer-tg-one* by default.**


Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
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
Default action
Info
HTTP
80
1-65535
Forward to
customer-tg-two
HTTP
Target type: IP, IPv4
Create target group
Listener tags - optional
Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.
Add listener tag
You can add up to 50 more tags.
Listener HTTP:8080
Remove
Protocol
Port
Default action
Info
HTTP
8080
1-65535
Forward to
customer-tg-one
HTTP
Target type: IP, IPv4
Create target group
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
Summary
Review and confirm your configurations. Estimate cost
Basic configuration Edit
microservicesLB
Internet-facing
IPv4
Security groups Edit
microservices-sg
sg-091ac242028763d75
Network mapping Edit
VPC vpc-043e6f0ce741fda03
LabVPC
us-east-1a
subnet-09458d72d02ae53ea
Public Subnet1
us-east-1b
subnet-0e5c0293004d9e1c8
Public Subnet2
Listeners and routing Edit
HTTP:80 defaults to
customer-tg-two
HTTP:8080 defaults to
customer-tg-one
Service integrations Edit
AWS WAF: None
AWS Global Accelerator: None
Tags Edit
None
Attributes
Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
Internet-facing
IPv4
us-east-1a
subnet-09458d72d02ae53ea
Public Subnet1
us-east-1b
subnet-0e5c0293004d9e1c8
Public Subnet2
HTTP:8080 defaults to
customer-tg-one
Service integrations Edit
AWS WAF: None
AWS Global Accelerator: None
Tags Edit
None
Attributes
Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.
Creation workflow and status
Server-side tasks and status
After completing and submitting the above steps, all server-side tasks and their statuses become available for monitoring.
Cancel
Create load balancer
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

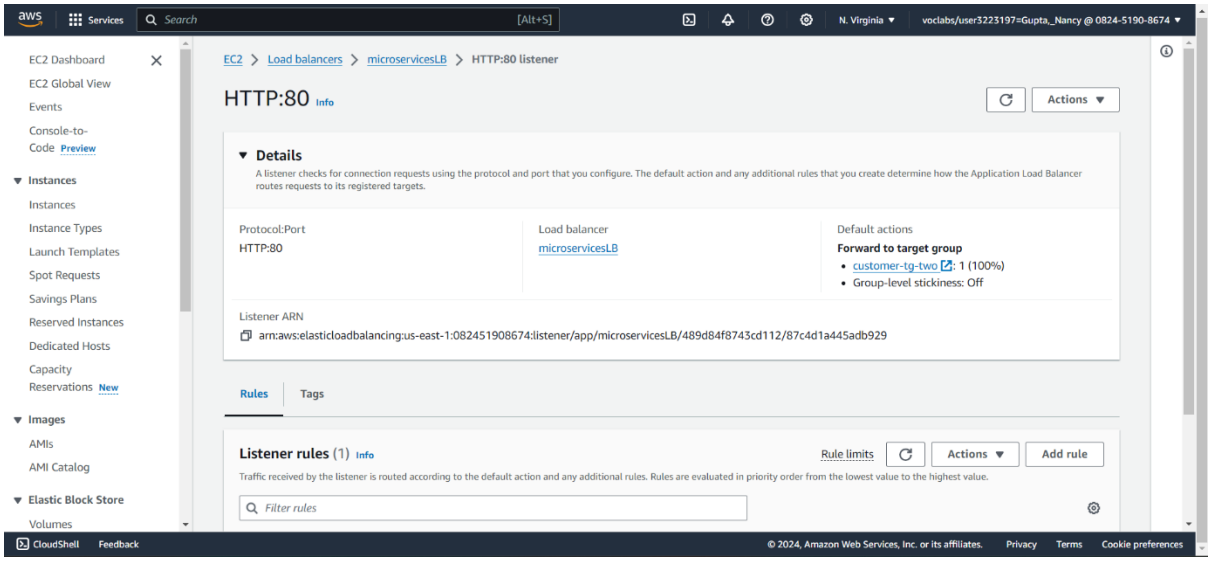


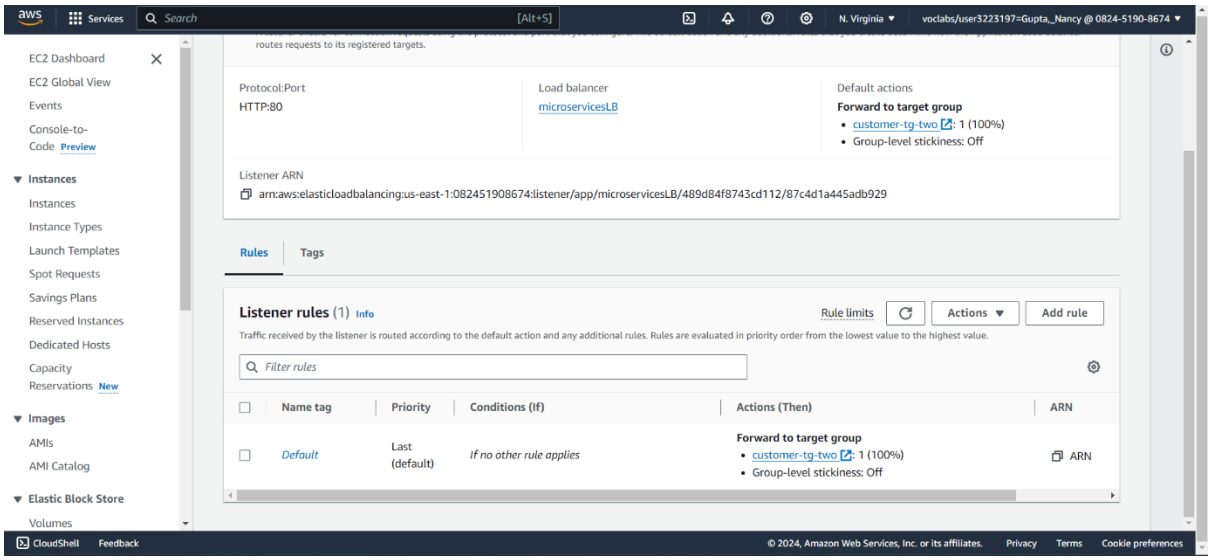


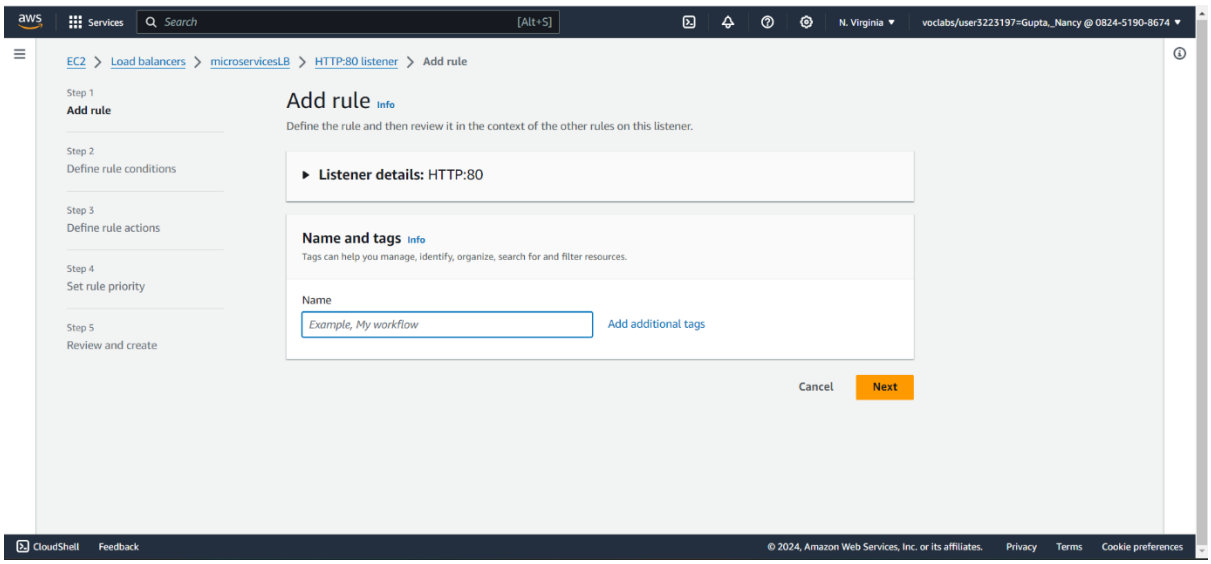
3. **Add a second rule for the *HTTP:80* listener. Define the following logic for this new rule:**
    - **IF Path is /admin/***
    - **THEN Forward to... the employee-tg-two target group.**

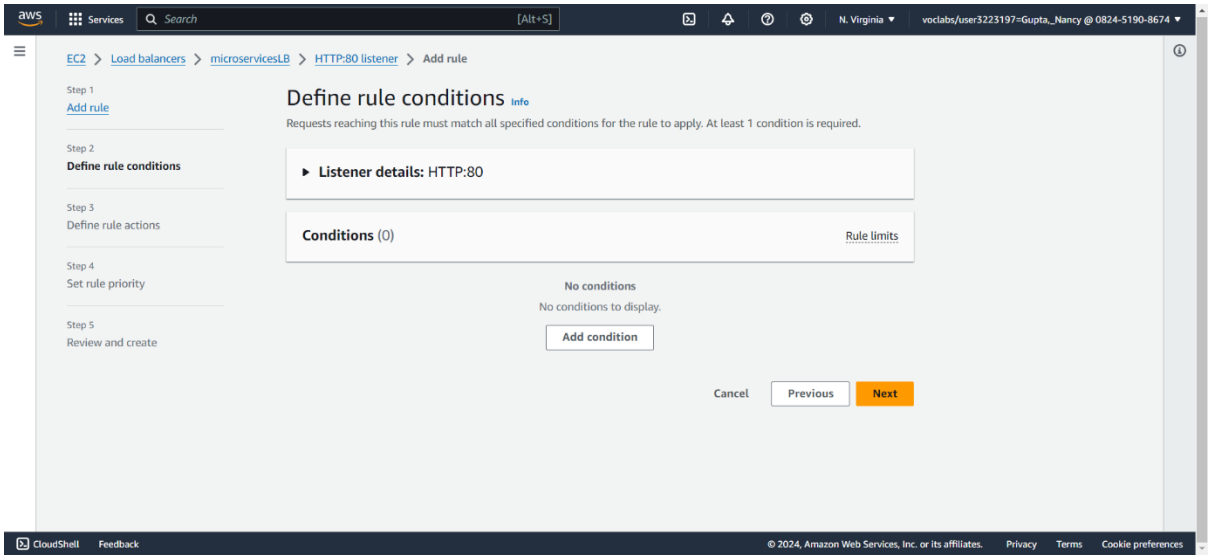
The settings should be the same as shown in the following image:

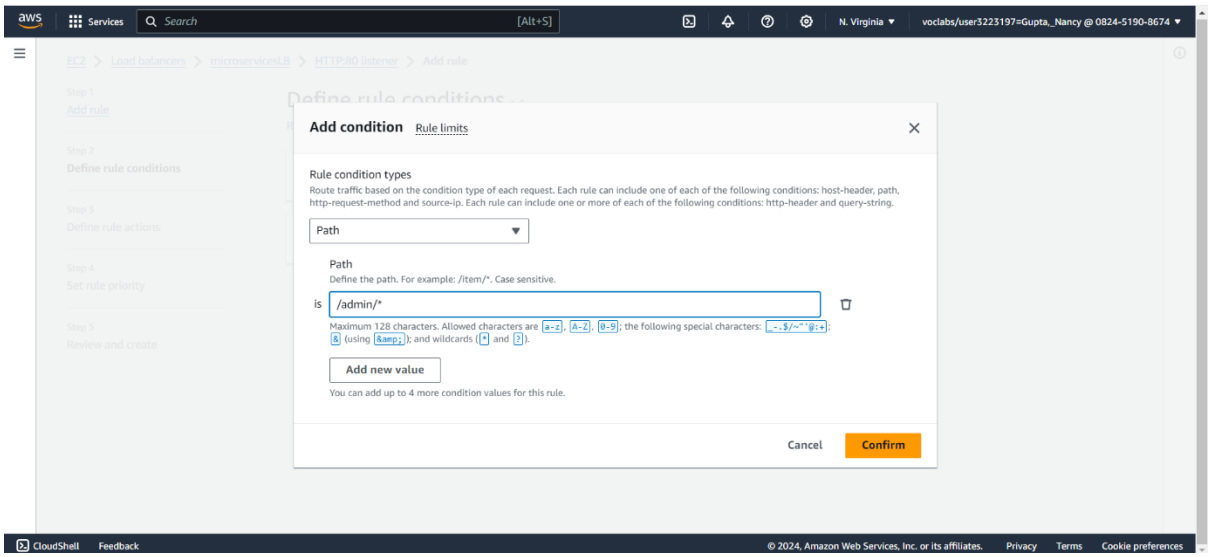
Name tag	Priority	Conditions (If)	Actions (Then)
-	1	**Path Pattern** is /admin/*	**Forward to target group** • employee-tg-two: 1 (100%) • Group-level stickiness: Off
Default	Last (default)	*If no other rule applies*	**Forward to target group** • customer-tg-two: 1 (100%) • Group-level stickiness: Off

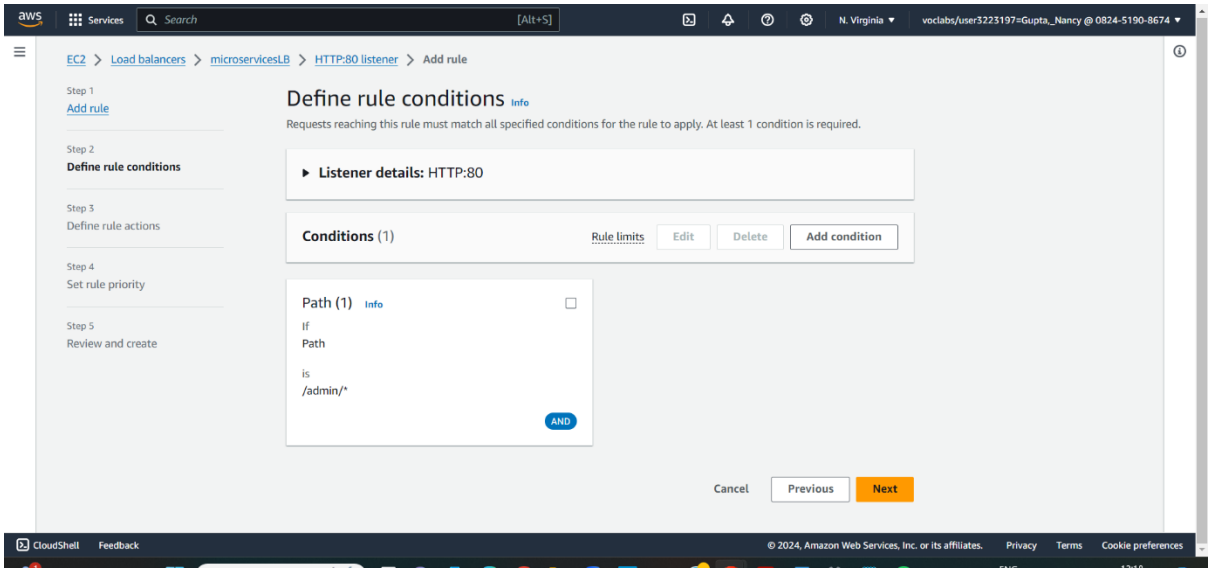

Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
EC2 > Load balancers > microservicesLB > HTTP:80 listener
HTTP:80 Info
Actions
Details
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.
Protocol:Port
HTTP:80
Load balancer
microservicesLB
Default actions
Forward to target group
customer-tg-two: 1 (100%)
Group-level stickiness: Off
Listener ARN
arn:aws:elasticloadbalancing:us-east-1:082451908674:listener/app/microservicesLB/489d84f8743cd112/87c4d1a445adb929
Rules
Tags
Listener rules (1) Info
Rule limits
Actions
Add rule
Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest value.
Filter rules
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

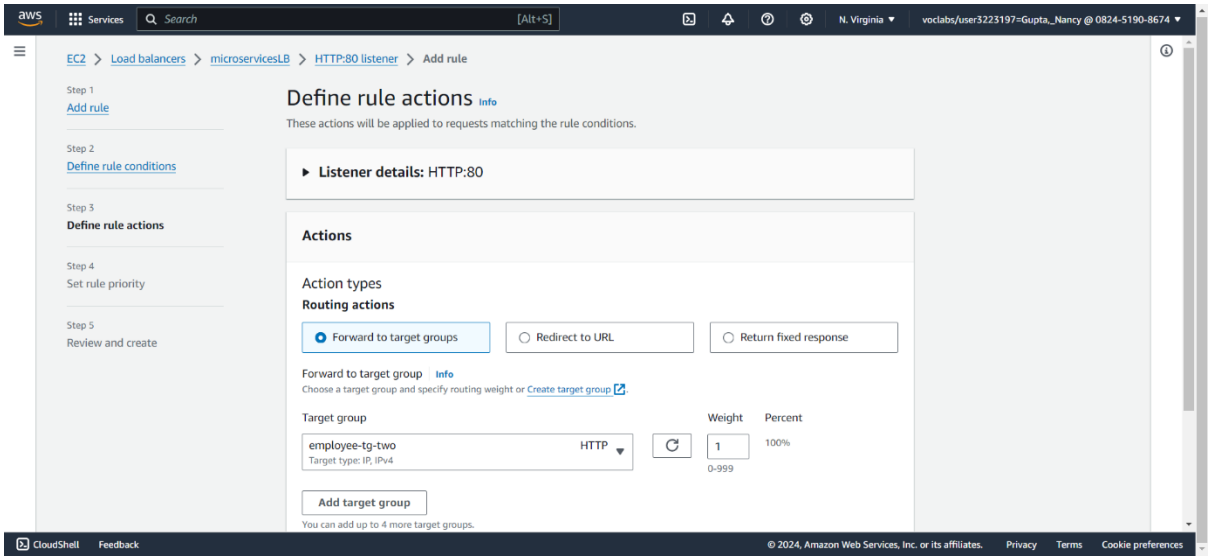

Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
routes requests to its registered targets.
Protocol:Port
HTTP:80
Load balancer
microservicesLB
Default actions
Forward to target group
customer-tg-two: 1 (100%)
Group-level stickiness: Off
Listener ARN
arn:aws:elasticloadbalancing:us-east-1:082451908674:listener/app/microservicesLB/489d84f8743cd112/87c4d1a445adb929
Rules
Tags
Listener rules (1) Info
Rule limits
Actions
Add rule
Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest value.
Filter rules
Name tag
Priority
Conditions (If)
Actions (Then)
ARN
Default
Last (default)
If no other rule applies
Forward to target group
customer-tg-two: 1 (100%)
Group-level stickiness: Off
ARN
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

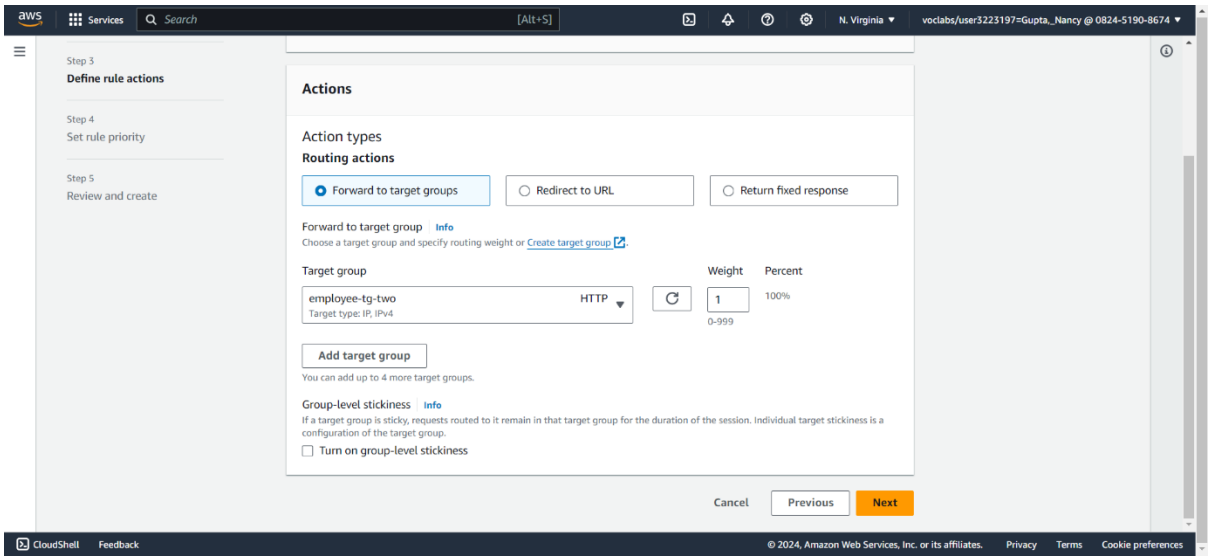

Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
EC2 > Load balancers > microservicesLB > HTTP:80 listener > Add rule
Step 1
Add rule
Step 2
Define rule conditions
Step 3
Define rule actions
Step 4
Set rule priority
Step 5
Review and create
Add rule Info
Define the rule and then review it in the context of the other rules on this listener.
Listener details: HTTP:80
Name and tags Info
Tags can help you manage, identify, organize, search for and filter resources.
Name
Example, My workflow
Add additional tags
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

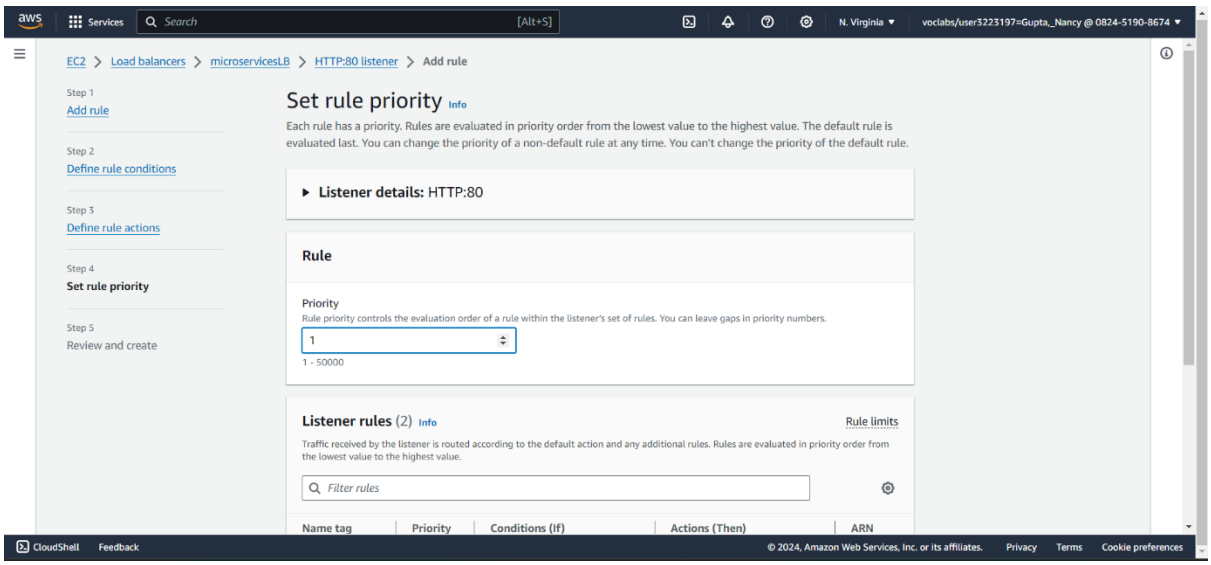

Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
EC2 > Load balancers > microservicesLB > HTTP:80 listener > Add rule
Step 1
Add rule
Step 2
Define rule conditions
Step 3
Define rule actions
Step 4
Set rule priority
Step 5
Review and create
Define rule conditions Info
Requests reaching this rule must match all specified conditions for the rule to apply. At least 1 condition is required.
Listener details: HTTP:80
Conditions (0)
Rule limits
No conditions
No conditions to display.
Add condition
Cancel
Previous
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

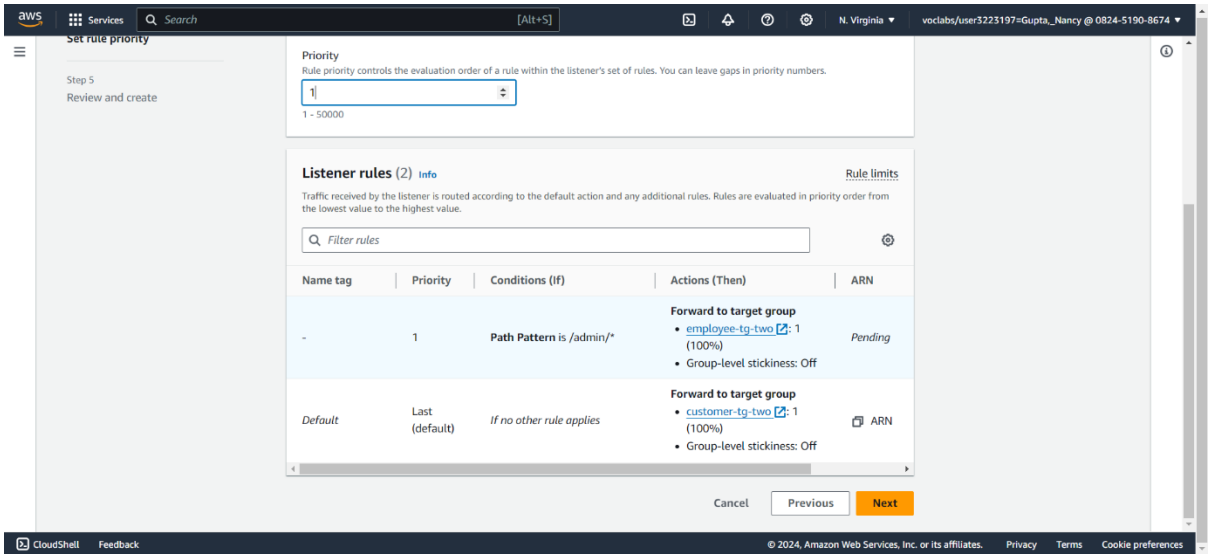

Add condition
Rule limits
Rule condition types
Route traffic based on the condition type of each request. Each rule can include one of each of the following conditions: host-header, path, http-request-method and source-ip. Each rule can include one or more of each of the following conditions: http-header and query-string.
Path
Path
Define the path. For example: /item/*. Case sensitive.
is
/admin/*
Maximum 128 characters. Allowed characters are a-z, A-Z, 0-9; the following special characters: _-.$/~"':+; & (using &); and wildcards (* and ?).
Add new value
You can add up to 4 more condition values for this rule.
Cancel
Confirm

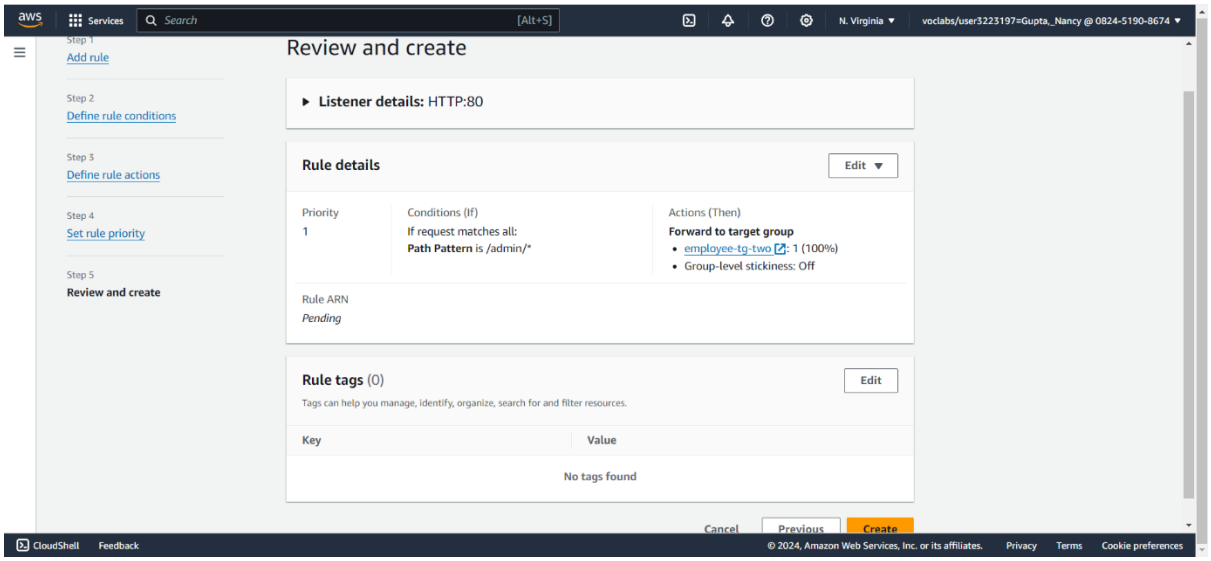

Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
EC2 > Load balancers > microservicesLB > HTTP:80 listener > Add rule
Step 1
Add rule
Step 2
Define rule conditions
Step 3
Define rule actions
Step 4
Set rule priority
Step 5
Review and create
Define rule conditions Info
Requests reaching this rule must match all specified conditions for the rule to apply. At least 1 condition is required.
Listener details: HTTP:80
Conditions (1)
Rule limits
Edit
Delete
Add condition
Path (1) Info
If
Path
is
/admin/*
AND
Cancel
Previous
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

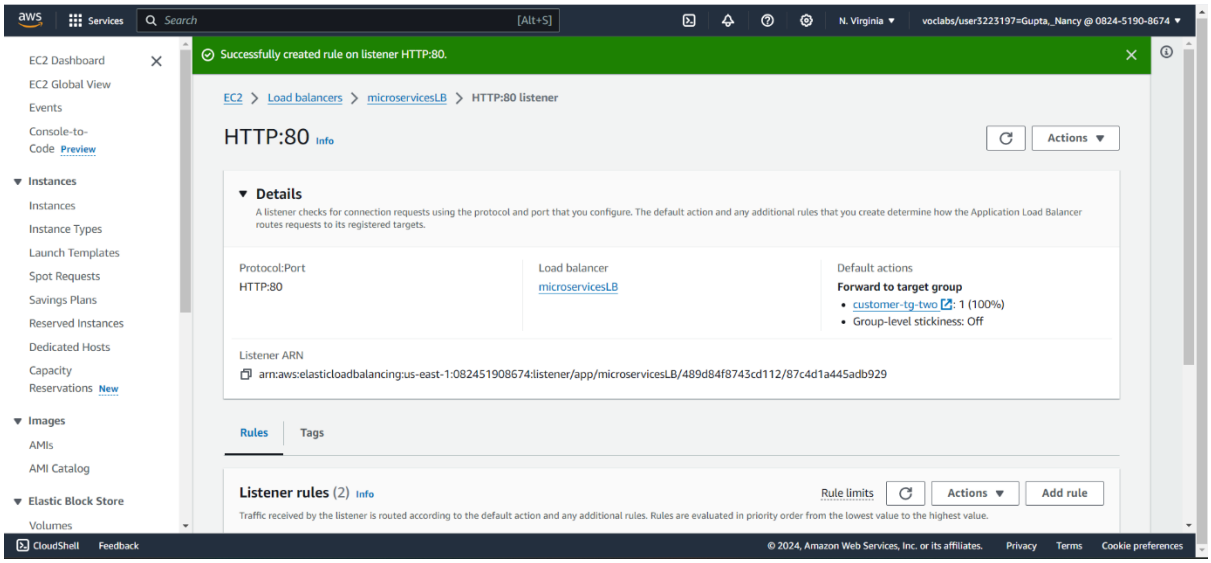

Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
EC2 > Load balancers > microservicesLB > HTTP:80 listener > Add rule
Step 1
Add rule
Step 2
Define rule conditions
Step 3
Define rule actions
Step 4
Set rule priority
Step 5
Review and create
Define rule actions Info
These actions will be applied to requests matching the rule conditions.
Listener details: HTTP:80
Actions
Action types
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
employee-tg-two
Target type: IP, IPv4
HTTP
1
100%
0-999
Add target group
You can add up to 4 more target groups.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

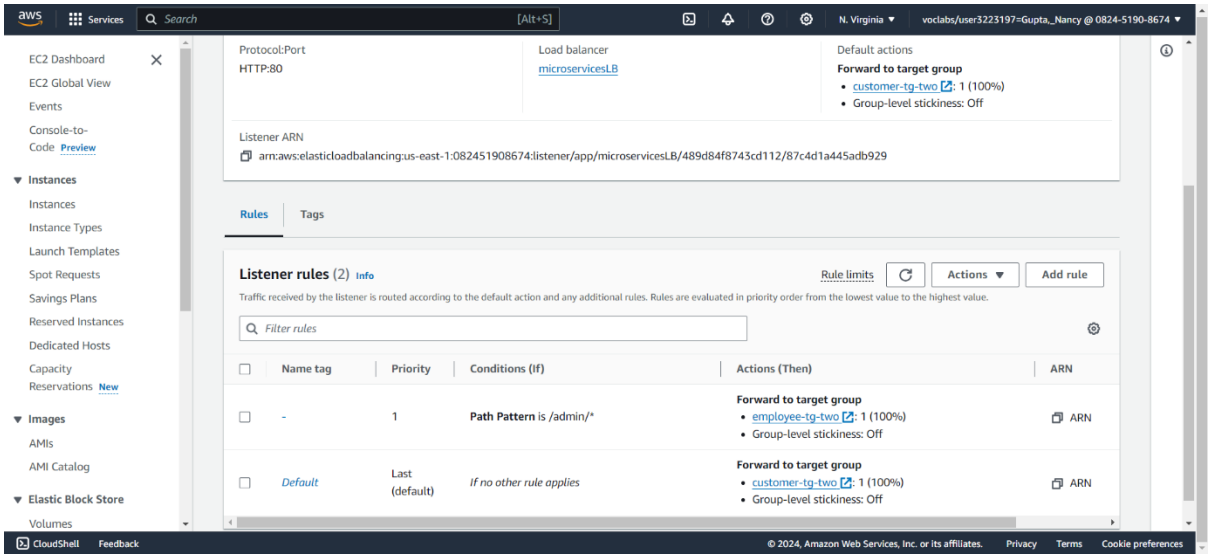

Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
Step 3
Define rule actions
Step 4
Set rule priority
Step 5
Review and create
Actions
Action types
Routing actions
Forward to target groups
Redirect to URL
Return fixed response
Forward to target group Info
Choose a target group and specify routing weight or Create target group.
Target group
Weight
Percent
employee-tg-two
Target type: IP, IPv4
HTTP
1
100%
0-999
Add target group
You can add up to 4 more target groups.
Group-level stickiness Info
If a target group is sticky, requests routed to it remain in that target group for the duration of the session. Individual target stickiness is a configuration of the target group.
Turn on group-level stickiness
Cancel
Previous
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
EC2 > Load balancers > microservicesLB > HTTP:80 listener > Add rule
Step 1
Add rule
Step 2
Define rule conditions
Step 3
Define rule actions
Step 4
Set rule priority
Step 5
Review and create
Set rule priority Info
Each rule has a priority. Rules are evaluated in priority order from the lowest value to the highest value. The default rule is evaluated last. You can change the priority of a non-default rule at any time. You can't change the priority of the default rule.
Listener details: HTTP:80
Rule
Priority
Rule priority controls the evaluation order of a rule within the listener's set of rules. You can leave gaps in priority numbers.
1
1 - 50000
Listener rules (2) Info
Rule limits
Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest value.
Filter rules
Name tag
Priority
Conditions (If)
Actions (Then)
ARN
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Set rule priority
Step 5
Review and create
Priority
Rule priority controls the evaluation order of a rule within the listener's set of rules. You can leave gaps in priority numbers.
1
1 - 50000
Listener rules (2) Info
Rule limits
Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest value.
Filter rules
Name tag
Priority
Conditions (If)
Actions (Then)
ARN
-
1
Path Pattern is /admin/*
Forward to target group
employee-tg-two: 1 (100%)
Group-level stickiness: Off
Pending
Default
Last (default)
If no other rule applies
Forward to target group
customer-tg-two: 1 (100%)
Group-level stickiness: Off
ARN
Cancel
Previous
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

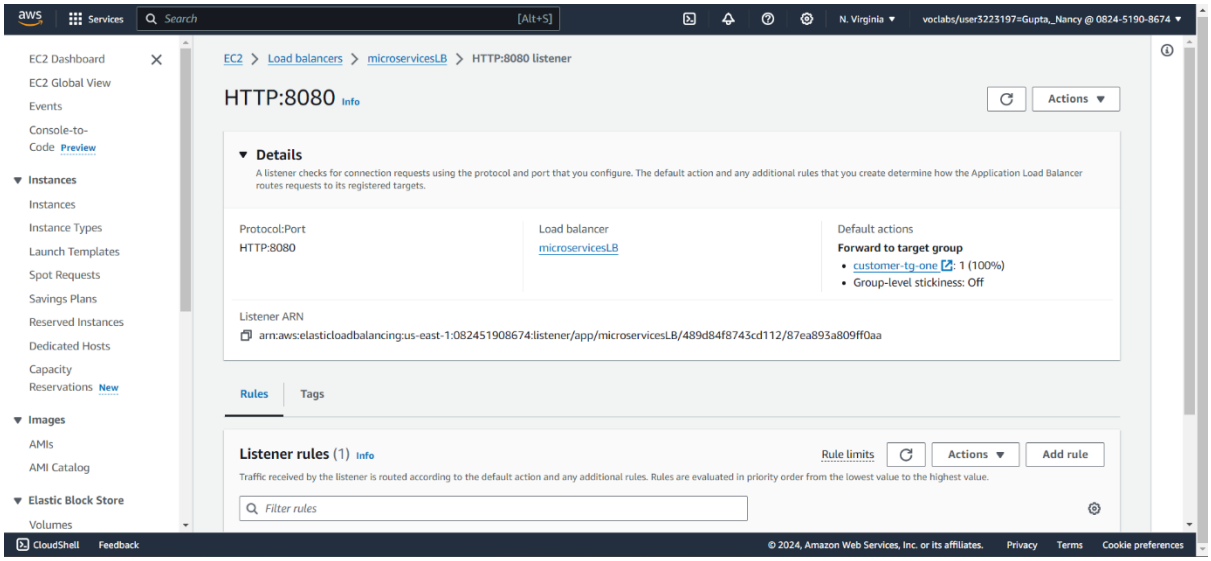

Step 1
Add rule
Step 2
Define rule conditions
Step 3
Define rule actions
Step 4
Set rule priority
Step 5
Review and create
Review and create
Listener details: HTTP:80
Rule details
Edit
Priority
1
Conditions (If)
If request matches all:
Path Pattern is /admin/*
Actions (Then)
Forward to target group
employee-tg-two: 1 (100%)
Group-level stickiness: Off
Rule ARN
Pending
Rule tags (0)
Edit
Tags can help you manage, identify, organize, search for and filter resources.
Key
Value
No tags found
Cancel
Previous
Create
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

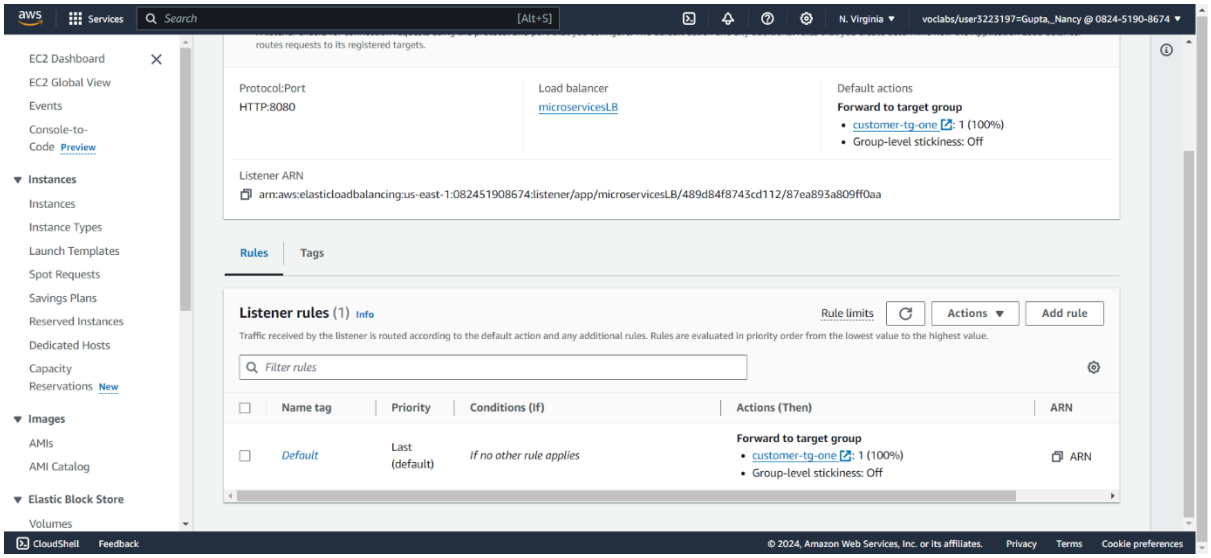

EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Successfully created rule on listener HTTP:80.
EC2 > Load balancers > microservicesLB > HTTP:80 listener
HTTP:80 Info
Actions
Details
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.
Protocol:Port
HTTP:80
Load balancer
microservicesLB
Default actions
Forward to target group
customer-tg-two: 1 (100%)
Group-level stickiness: Off
Listener ARN
arn:aws:elasticloadbalancing:us-east-1:082451908674:listener/app/microservicesLB/489d84f8743cd112/87c4d1a445adb929
Rules
Tags
Listener rules (2) Info
Rule limits
Actions
Add rule
Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest value.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

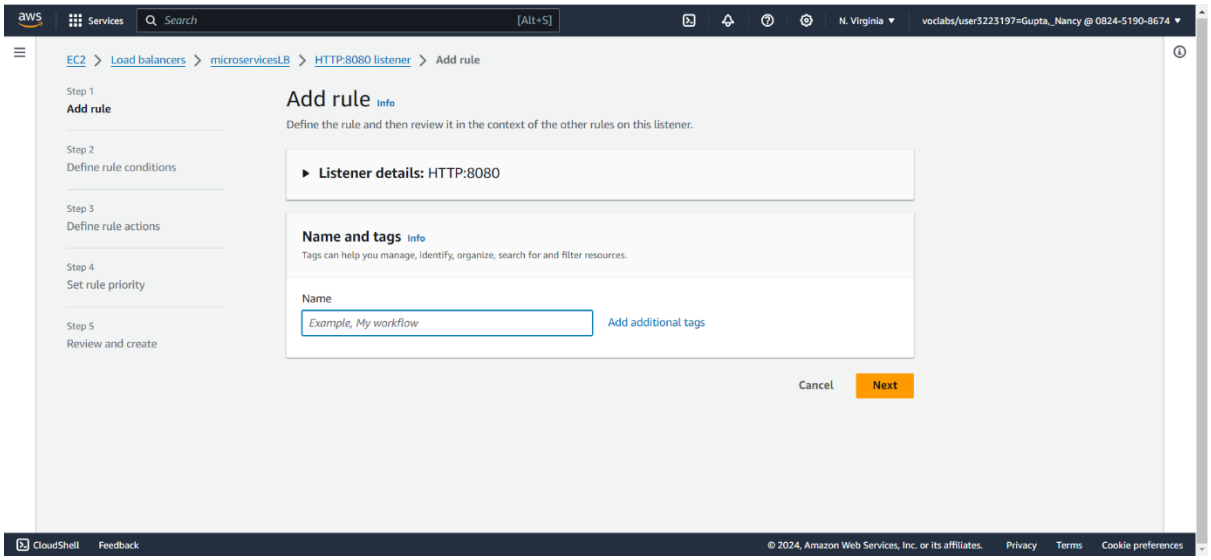


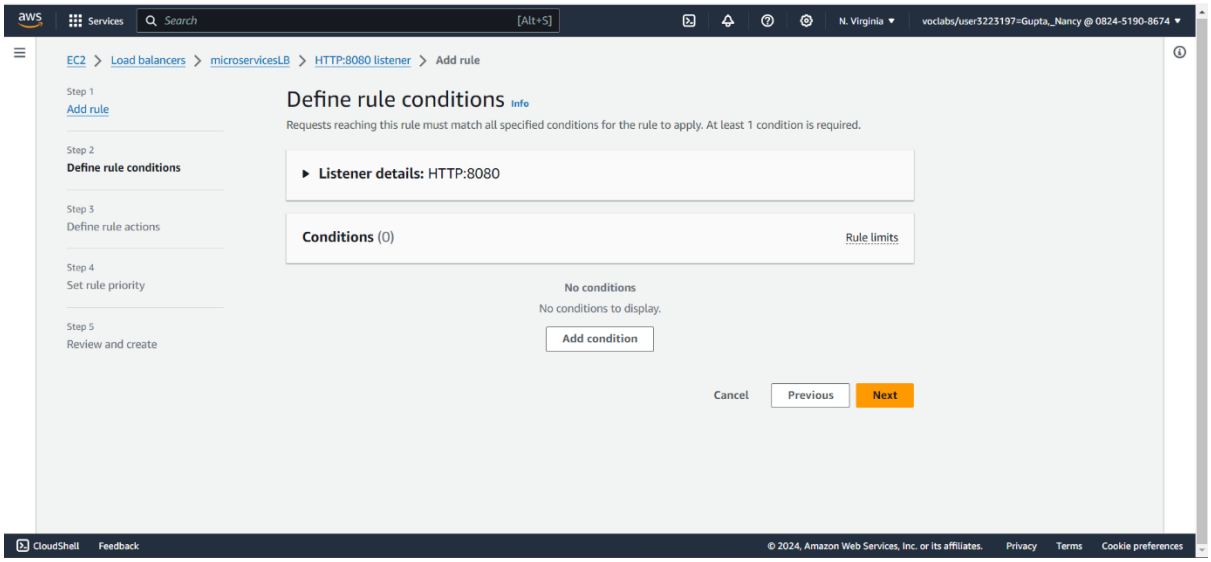
4. **Add a second rule for the *HTTP:8080* listener. Define the following logic for this new rule:**
    - **IF Path is /admin/***
    - **THEN Forward to the employee-tg-one target group.**

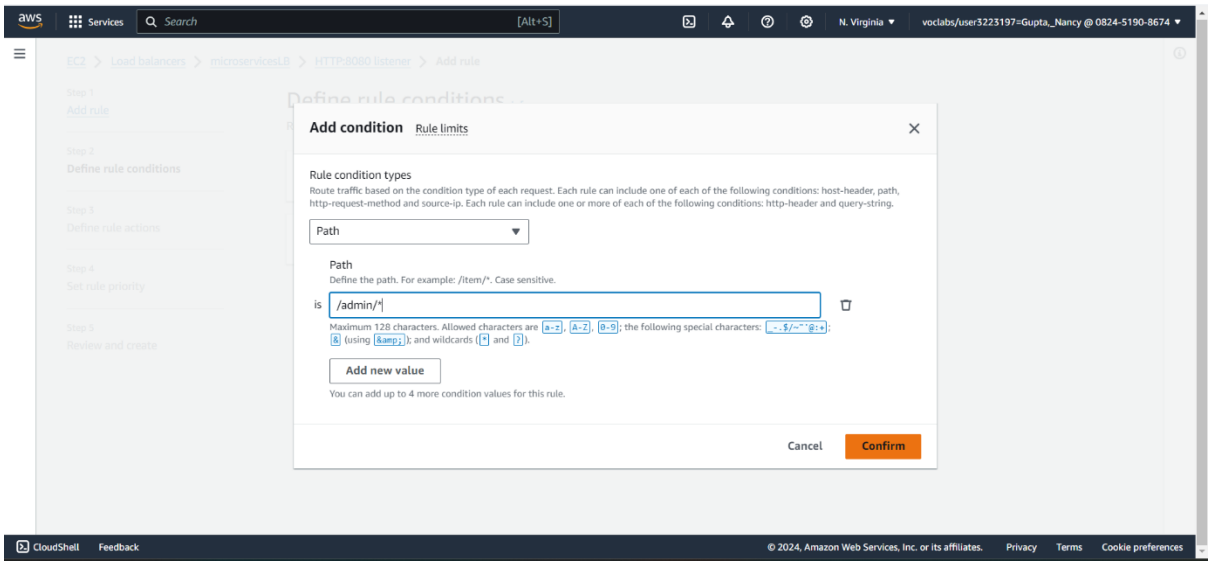
The settings should be the same as shown in the following image:

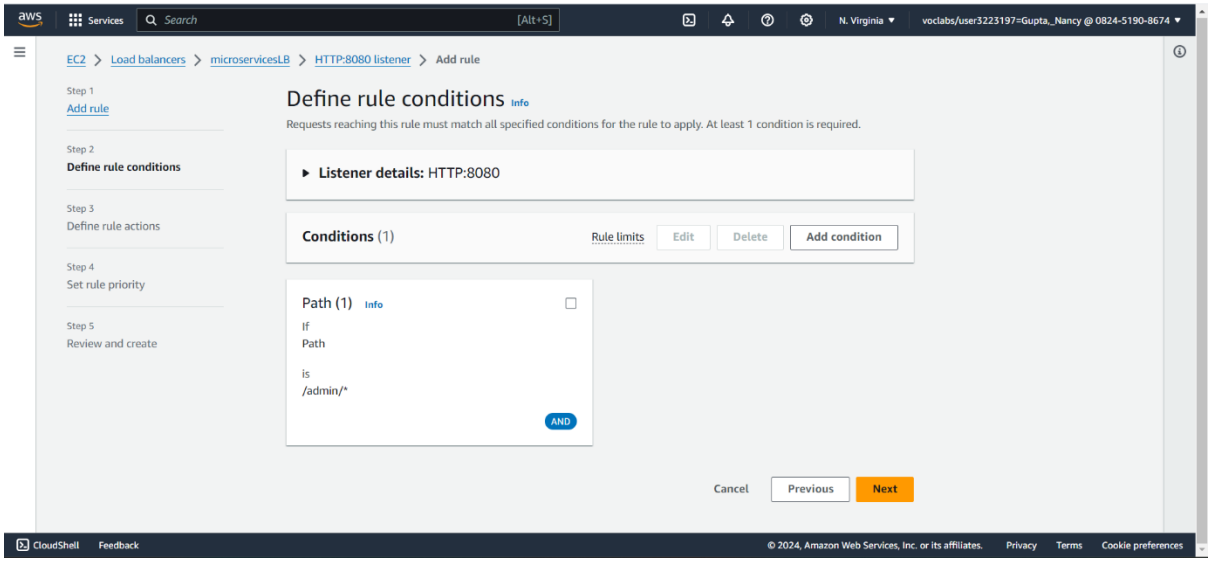


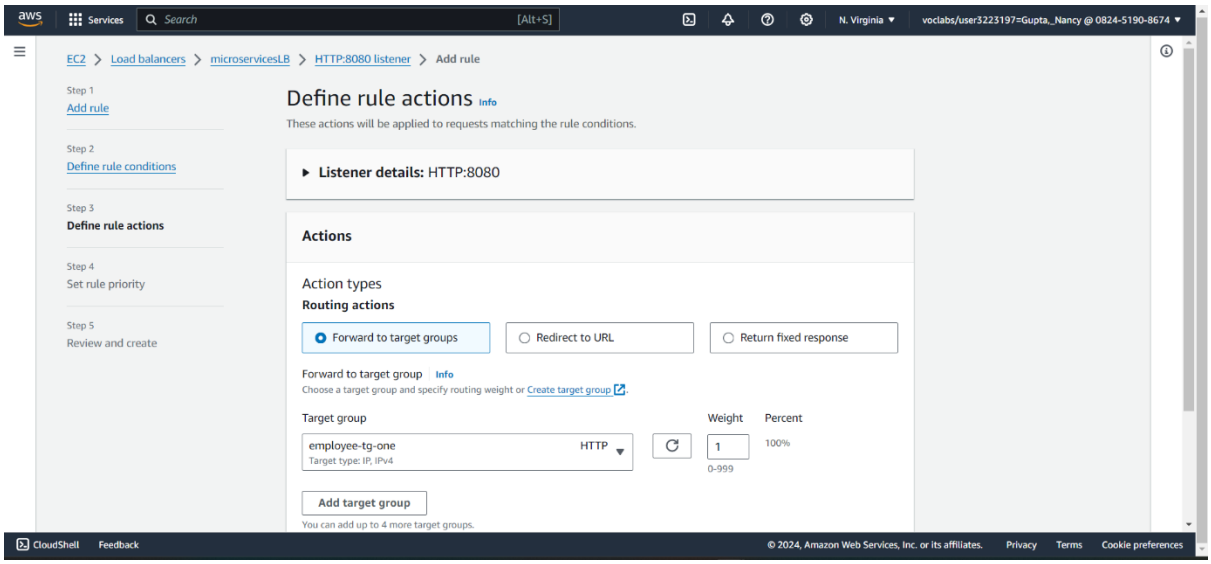

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
routes requests to its registered targets.
Protocol:Port
HTTP:8080
Load balancer
microservicesLB
Default actions
Forward to target group
customer-tg-one: 1 (100%)
Group-level stickiness: Off
Listener ARN
arn:aws:elasticloadbalancing:us-east-1:082451908674:listener/app/microservicesLB/489d84f8743cd112/87ea893a809ff0aa
Rules
Tags
Listener rules (1) Info
Rule limits
Actions
Add rule
Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest value.
Filter rules
Name tag
Priority
Conditions (If)
Actions (Then)
ARN
Default
Last (default)
If no other rule applies
Forward to target group
customer-tg-one: 1 (100%)
Group-level stickiness: Off
ARN
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

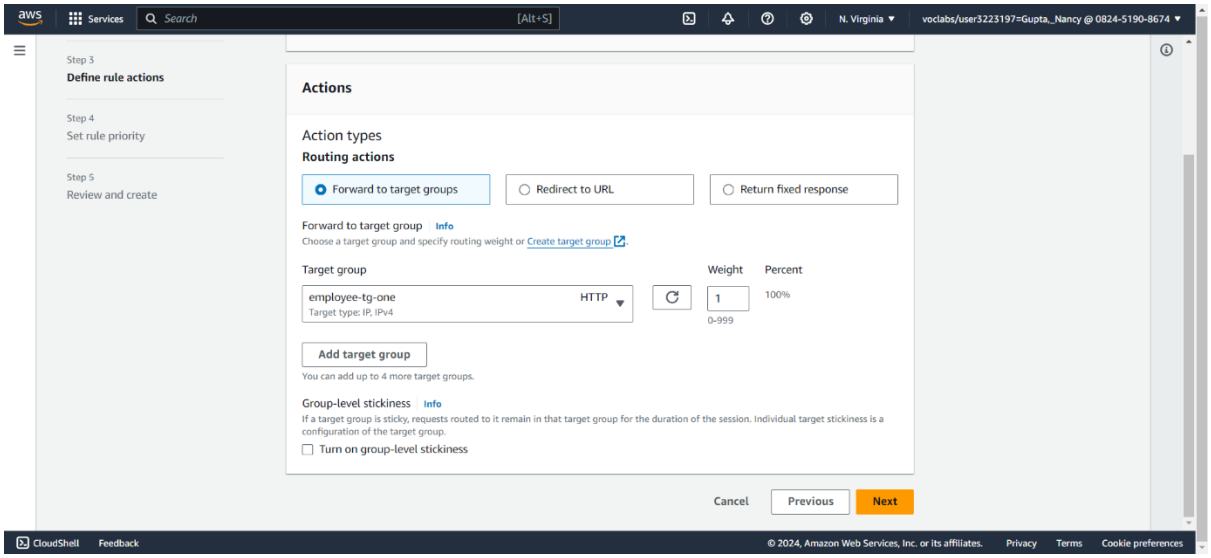

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
EC2 > Load balancers > microservicesLB > HTTP:8080 listener > Add rule
Step 1
Add rule
Step 2
Define rule conditions
Step 3
Define rule actions
Step 4
Set rule priority
Step 5
Review and create
Add rule Info
Define the rule and then review it in the context of the other rules on this listener.
Listener details: HTTP:8080
Name and tags Info
Tags can help you manage, identify, organize, search for and filter resources.
Name
Example, My workflow
Add additional tags
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

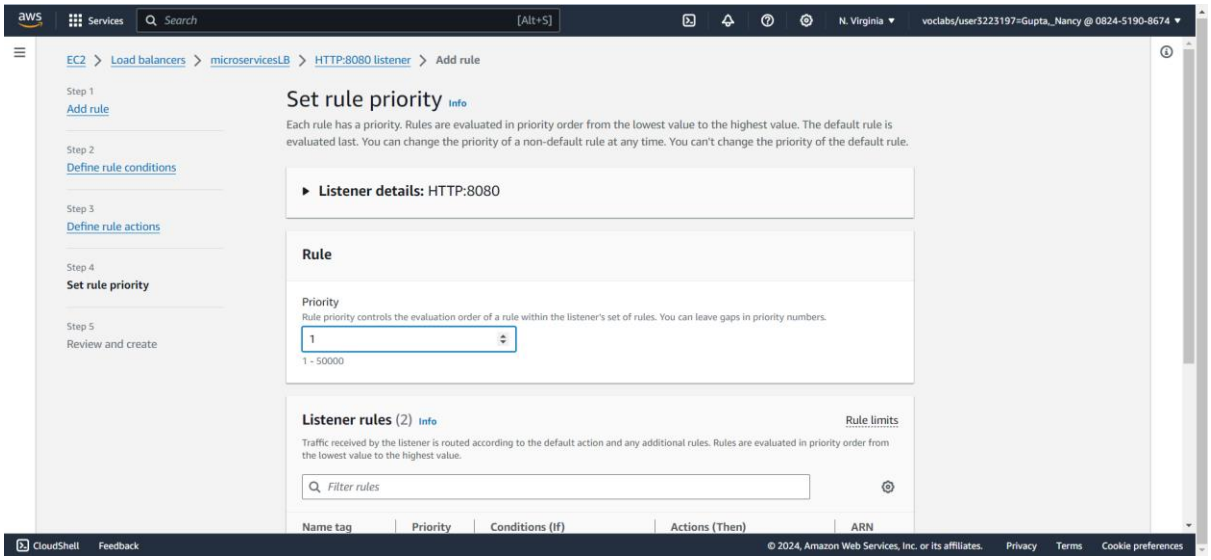

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
EC2 > Load balancers > microservicesLB > HTTP:8080 listener > Add rule
Step 1
Add rule
Step 2
Define rule conditions
Step 3
Define rule actions
Step 4
Set rule priority
Step 5
Review and create
Define rule conditions Info
Requests reaching this rule must match all specified conditions for the rule to apply. At least 1 condition is required.
Listener details: HTTP:8080
Conditions (0)
Rule limits
No conditions
No conditions to display.
Add condition
Cancel
Previous
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

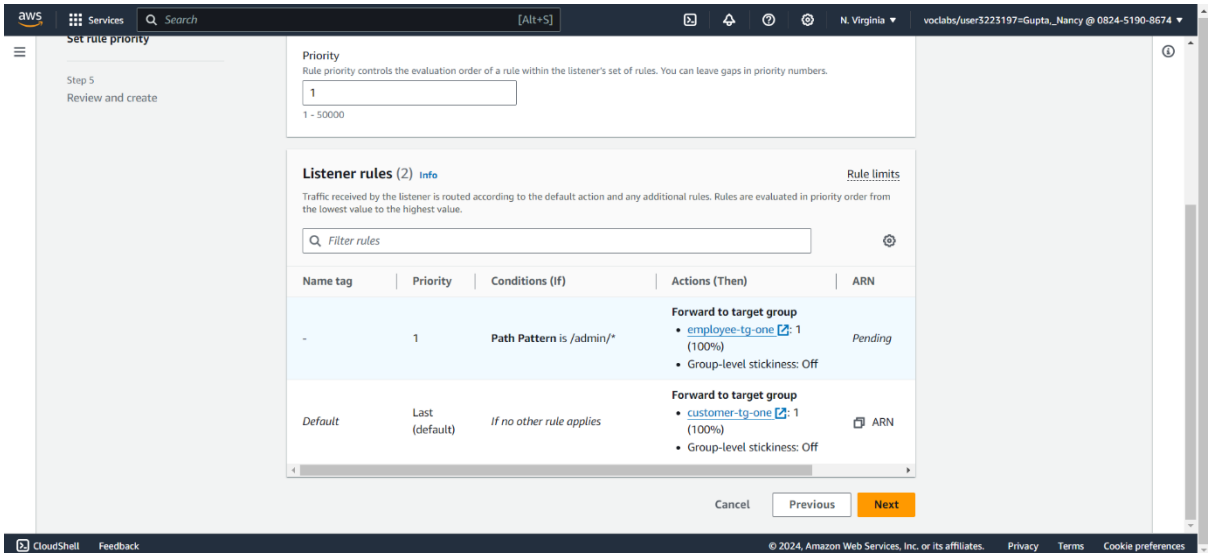

Add condition
Rule limits
Rule condition types
Route traffic based on the condition type of each request. Each rule can include one of each of the following conditions: host-header, path, http-request-method and source-ip. Each rule can include one or more of each of the following conditions: http-header and query-string.
Path
Path
Define the path. For example: /item/*. Case sensitive.
is
/admin/*
Maximum 128 characters. Allowed characters are a-z, A-Z, 0-9; the following special characters: _ - . $ / ~ " ' @ : +; & (using &); and wildcards (* and ?).
Add new value
You can add up to 4 more condition values for this rule.
Cancel
Confirm

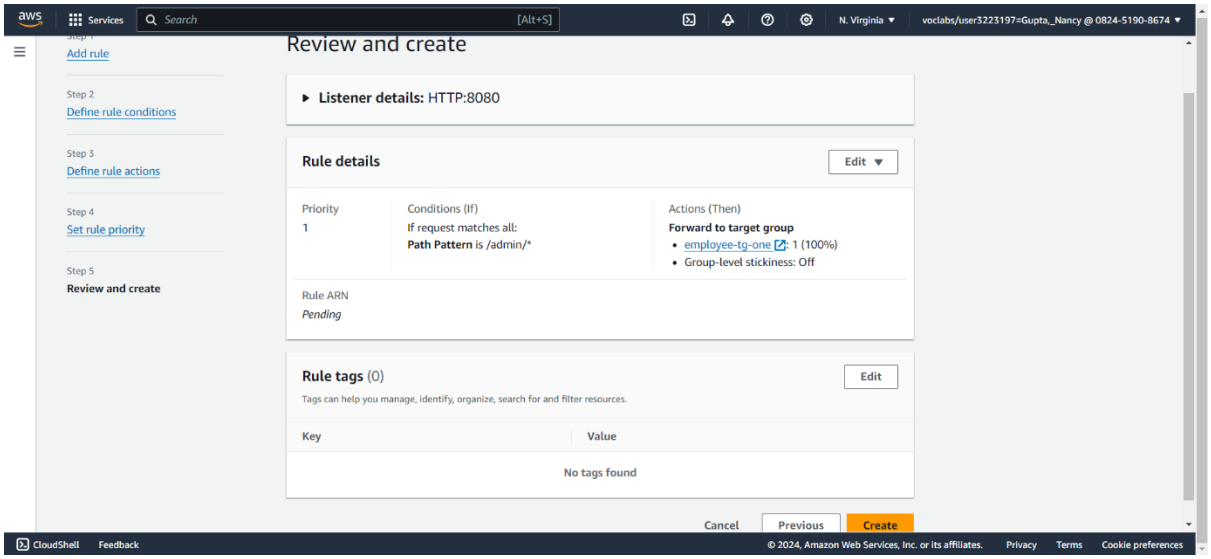

EC2 > Load balancers > microservicesLB > HTTP:8080 listener > Add rule
Step 1
Add rule
Step 2
Define rule conditions
Step 3
Define rule actions
Step 4
Set rule priority
Step 5
Review and create
Define rule conditions Info
Requests reaching this rule must match all specified conditions for the rule to apply. At least 1 condition is required.
Listener details: HTTP:8080
Conditions (1)
Rule limits
Edit
Delete
Add condition
Path (1) Info
If
Path
is
/admin/*
AND
Cancel
Previous
Next

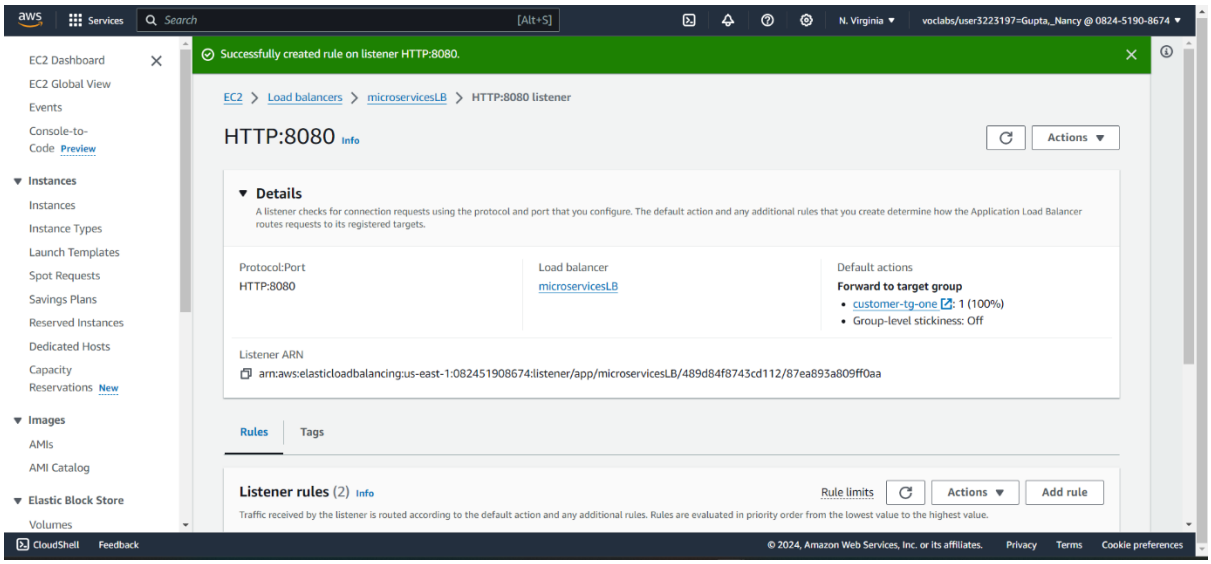

EC2 > Load balancers > microservicesLB > HTTP:8080 listener > Add rule
Step 1
Add rule
Step 2
Define rule conditions
Step 3
Define rule actions
Step 4
Set rule priority
Step 5
Review and create
Define rule actions Info
These actions will be applied to requests matching the rule conditions.
Listener details: HTTP:8080
Actions
Action types
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
employee-tg-one
Target type: IP, IPv4
HTTP
1
100%
0-999
Add target group
You can add up to 4 more target groups.

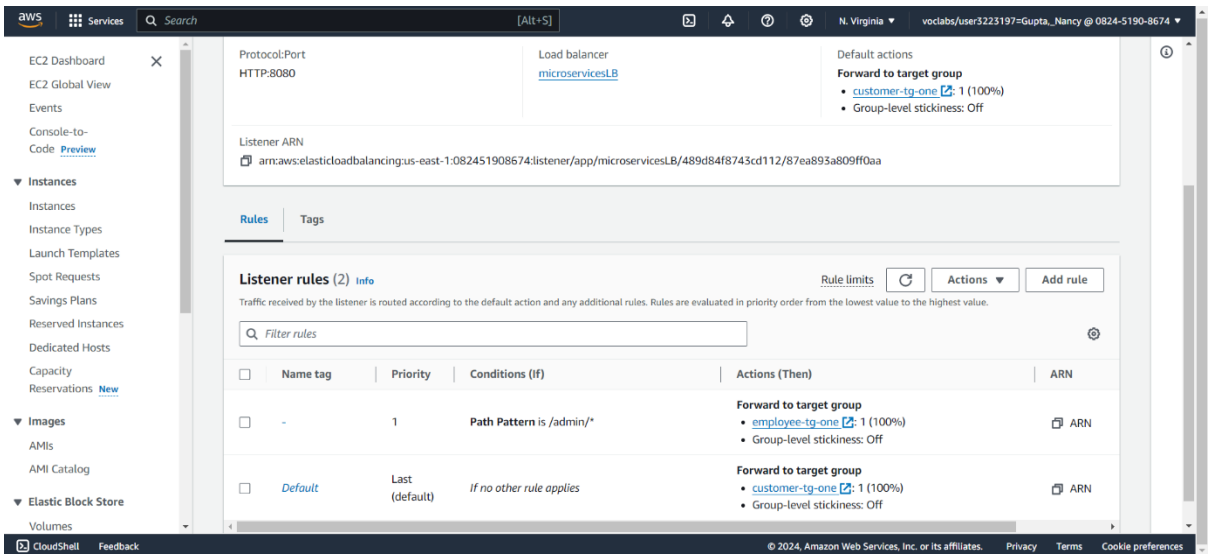

Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
Step 3
Define rule actions
Step 4
Set rule priority
Step 5
Review and create
Actions
Action types
Routing actions
Forward to target groups
Redirect to URL
Return fixed response
Forward to target group Info
Choose a target group and specify routing weight or Create target group.
Target group
Weight
Percent
employee-tg-one
HTTP
Target type: IP, IPv4
1
100%
0-999
Add target group
You can add up to 4 more target groups.
Group-level stickiness Info
If a target group is sticky, requests routed to it remain in that target group for the duration of the session. Individual target stickiness is a configuration of the target group.
Turn on group-level stickiness
Cancel
Previous
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

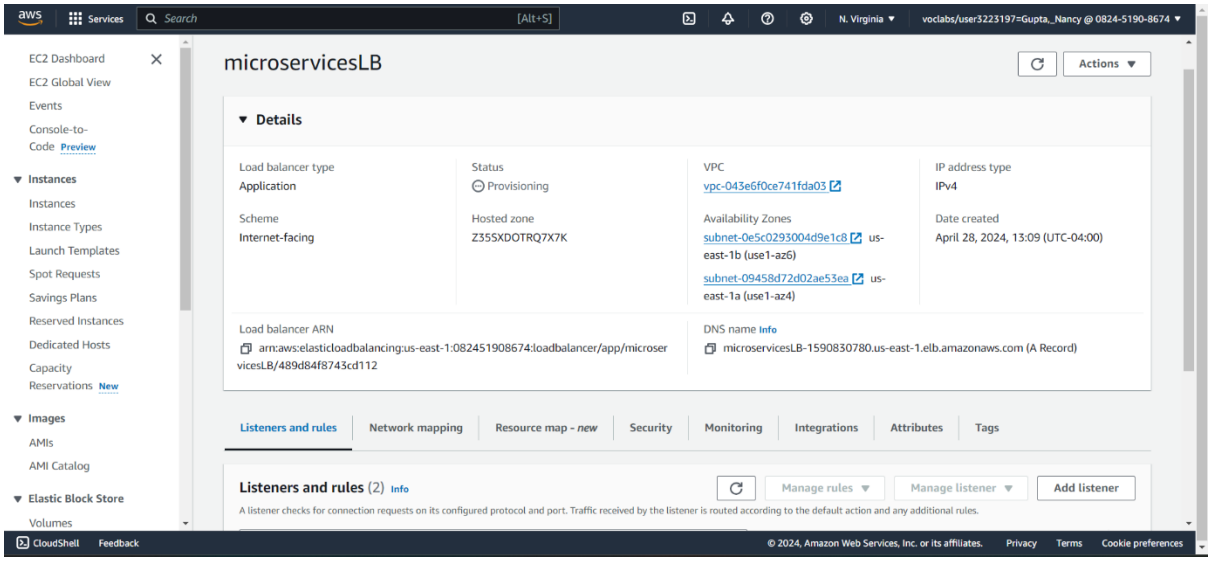

Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
EC2
Load balancers
microservicesLB
HTTP:8080 listener
Add rule
Step 1
Add rule
Step 2
Define rule conditions
Step 3
Define rule actions
Step 4
Set rule priority
Step 5
Review and create
Set rule priority Info
Each rule has a priority. Rules are evaluated in priority order from the lowest value to the highest value. The default rule is evaluated last. You can change the priority of a non-default rule at any time. You can't change the priority of the default rule.
Listener details: HTTP:8080
Rule
Priority
Rule priority controls the evaluation order of a rule within the listener's set of rules. You can leave gaps in priority numbers.
1
1 - 50000
Listener rules (2) Info
Rule limits
Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest value.
Filter rules
Name tag
Priority
Conditions (If)
Actions (Then)
ARN
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

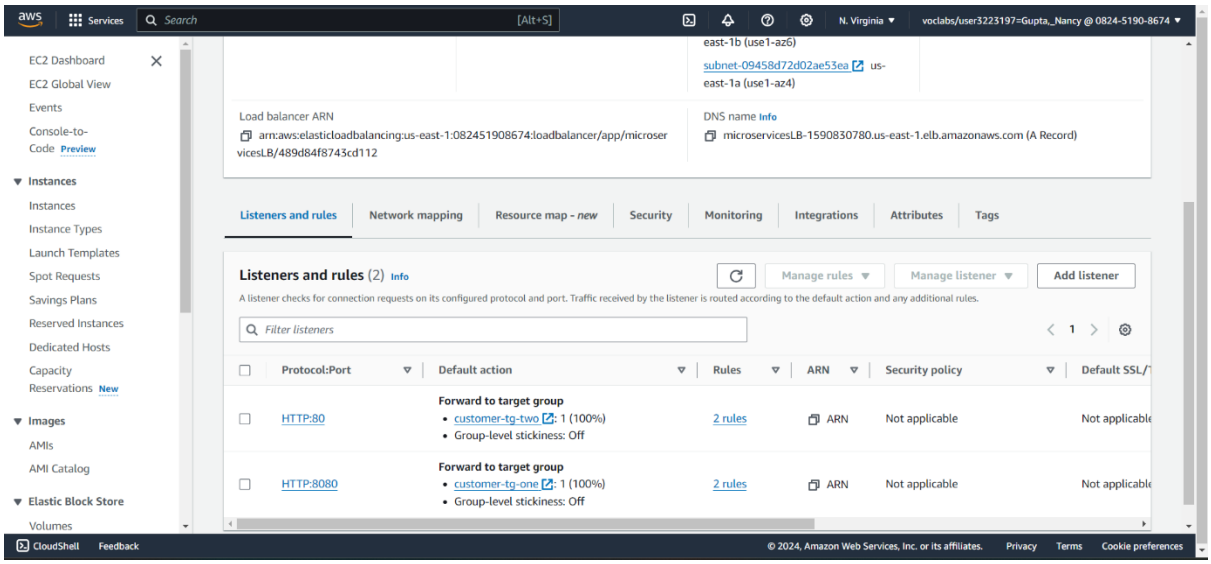

Services
Search
[Alt+S]
N. Virginia
voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
Set rule priority
Step 5
Review and create
Priority
Rule priority controls the evaluation order of a rule within the listener's set of rules. You can leave gaps in priority numbers.
1
1 - 50000
Listener rules (2) Info
Rule limits
Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest value.
Filter rules
Name tag
Priority
Conditions (If)
Actions (Then)
ARN
-
1
Path Pattern is /admin/*
Forward to target group
employee-tg-one: 1 (100%)
Group-level stickiness: Off
Pending
Default
Last (default)
If no other rule applies
Forward to target group
customer-tg-one: 1 (100%)
Group-level stickiness: Off
ARN
Cancel
Previous
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Add rule
Step 2
Define rule conditions
Step 3
Define rule actions
Step 4
Set rule priority
Step 5
Review and create
Review and create
Listener details: HTTP:8080
Rule details
Edit
Priority
1
Conditions (If)
If request matches all:
Path Pattern is /admin/*
Actions (Then)
Forward to target group
employee-tg-one: 1 (100%)
Group-level stickiness: Off
Rule ARN
Pending
Rule tags (0)
Edit
Tags can help you manage, identify, organize, search for and filter resources.
Key
Value
No tags found
Cancel
Previous
Create


Successfully created rule on listener HTTP:8080.
EC2 > Load balancers > microservicesLB > HTTP:8080 listener
HTTP:8080 Info
Actions
Details
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.
Protocol:Port
HTTP:8080
Load balancer
microservicesLB
Default actions
Forward to target group
customer-tg-one: 1 (100%)
Group-level stickiness: Off
Listener ARN
arn:aws:elasticloadbalancing:us-east-1:082451908674:listener/app/microservicesLB/489d84f8743cd112/87ea893a809ff0aa
Rules
Tags
Listener rules (2) Info
Rule limits
Actions
Add rule
Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest value.


Protocol:Port
HTTP:8080
Load balancer
microservicesLB
Default actions
Forward to target group
customer-tg-one: 1 (100%)
Group-level stickiness: Off
Listener ARN
arn:aws:elasticloadbalancing:us-east-1:082451908674:listener/app/microservicesLB/489d84f8743cd112/87ea893a809ff0aa
Rules
Tags
Listener rules (2) Info
Rule limits
Actions
Add rule
Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest value.
Filter rules
Name tag
Priority
Conditions (If)
Actions (Then)
ARN
-
1
Path Pattern is /admin/*
Forward to target group
employee-tg-one: 1 (100%)
Group-level stickiness: Off
ARN
Default
Last (default)
If no other rule applies
Forward to target group
customer-tg-one: 1 (100%)
Group-level stickiness: Off
ARN



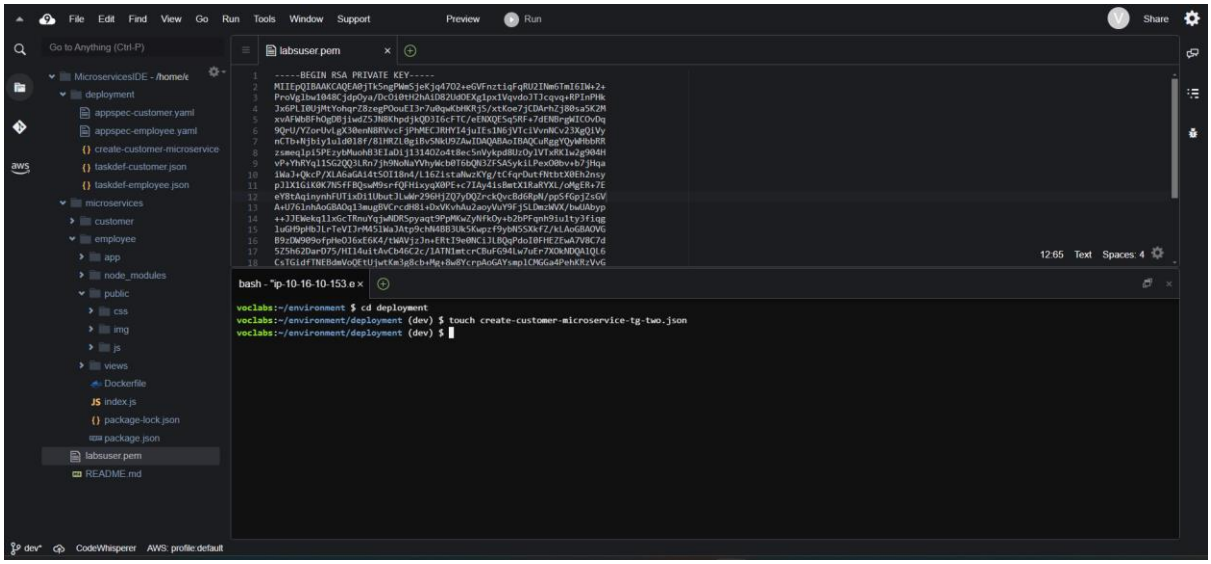


Phase 7: Creating two Amazon ECS services

In this phase, you will create a service in Amazon ECS for each microservice. Although you could deploy both microservices to a single ECS service, for this project, it will be easier to manage the microservices independently if each is deployed to its own ECS service.

Task 7.1: Create the ECS service for the *customer* microservice

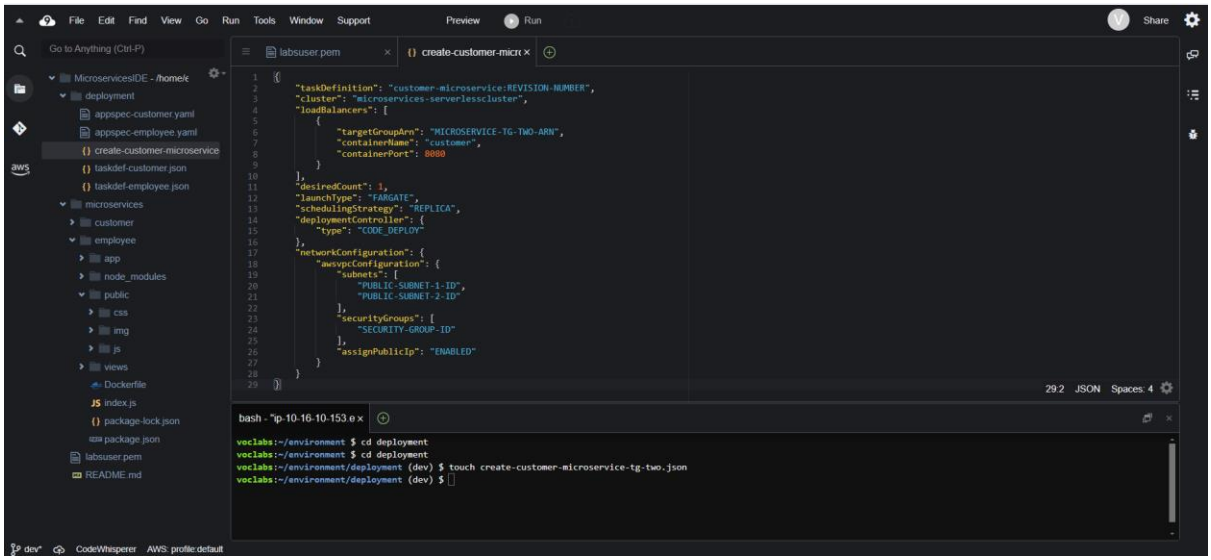
1. **In AWS Cloud9, create a new file named create-customer-microservice-tg-two.json in the deployment directory.**



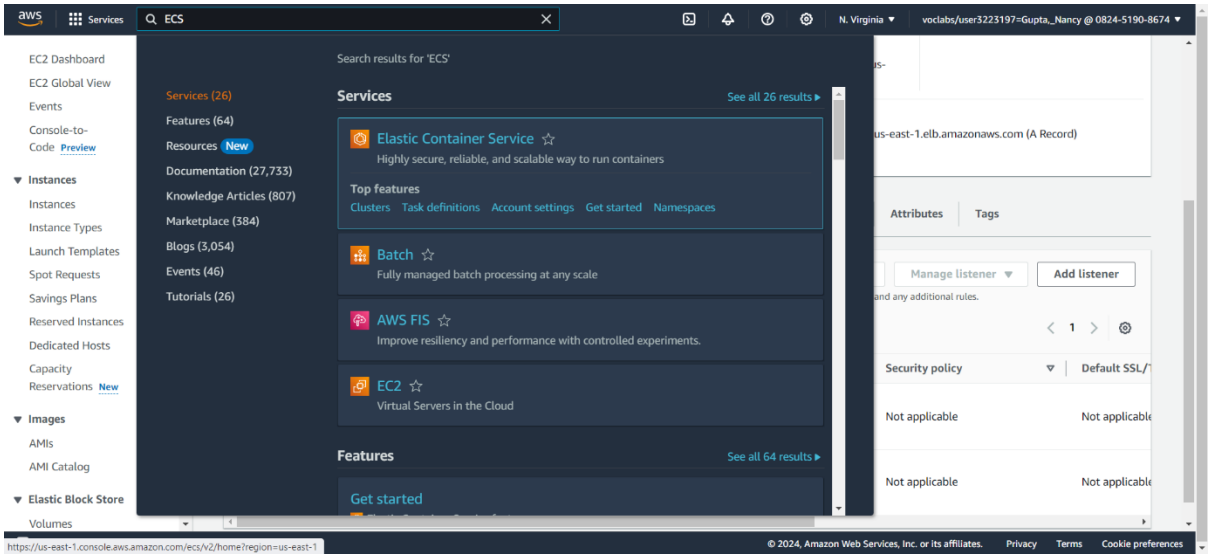
2. Paste the following JSON code into the file:

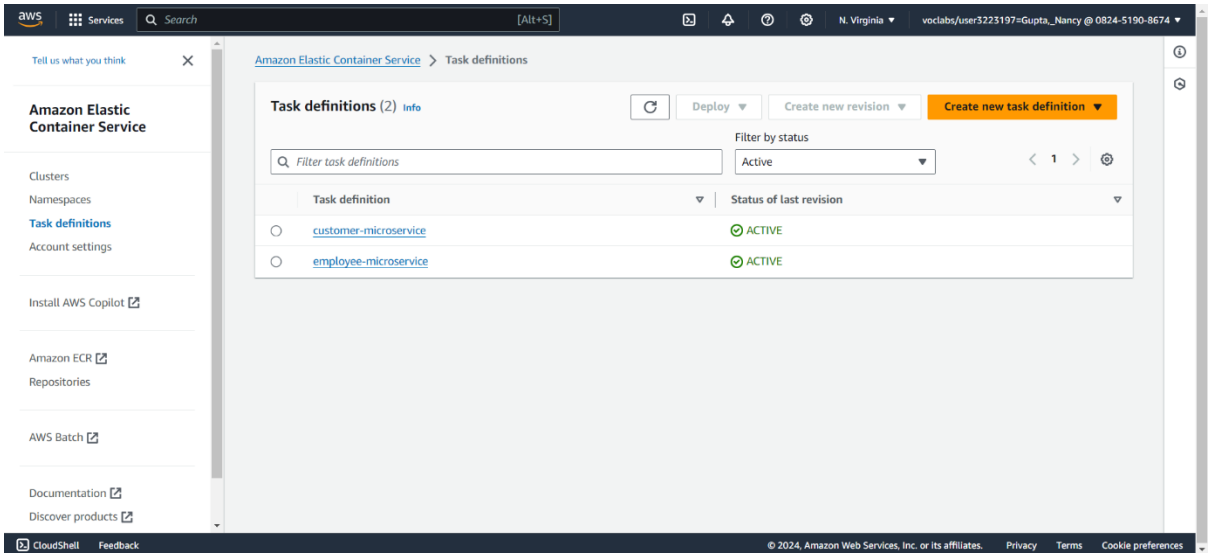
```
{
  "taskDefinition": "customer-microservice:REVISION-NUMBER",
  "cluster": "microservices-serverlesscluster",
  "loadBalancers": [
    {
      "targetGroupArn": "MICROSERVICE-TG-TWO-ARN",
      "containerName": "customer",
      "containerPort": 8080
    }
  ],
  "desiredCount": 1,
  "launchType": "FARGATE",
  "schedulingStrategy": "REPLICA",
  "deploymentController": {
    "type": "CODE_DEPLOY"
  },
  "networkConfiguration": {
    "awsvpcConfiguration": {
      "subnets": [
        "PUBLIC-SUBNET-1-ID",
```

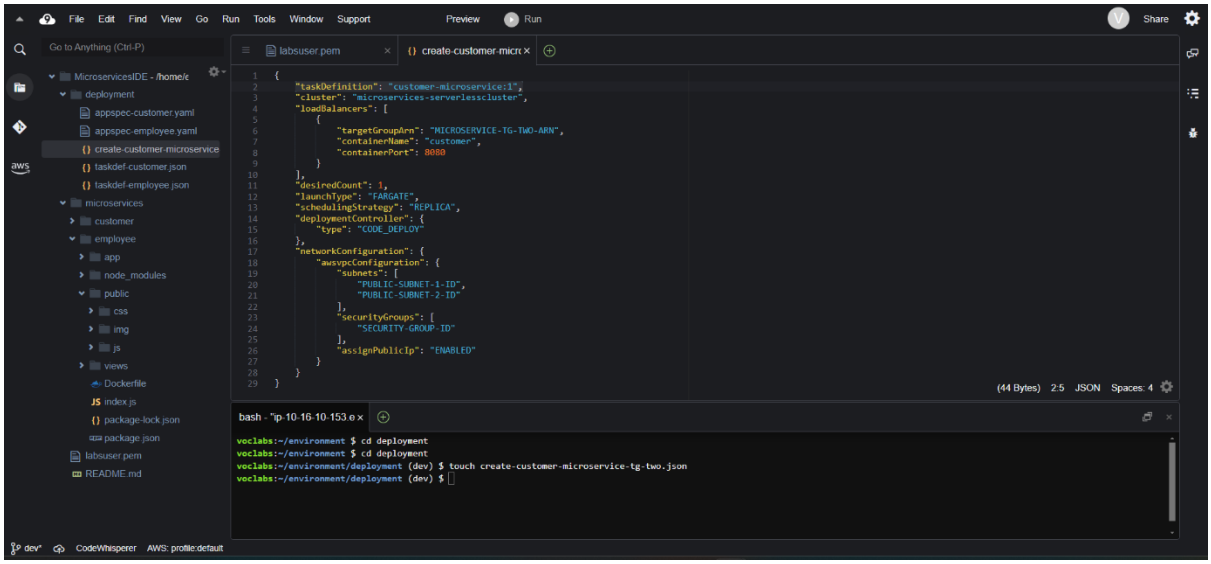
```
            "PUBLIC-SUBNET-2-ID"
        ],
        "securityGroups": [
            "SECURITY-GROUP-ID"
        ],
        "assignPublicIp": "ENABLED"
    }
  }
}
```



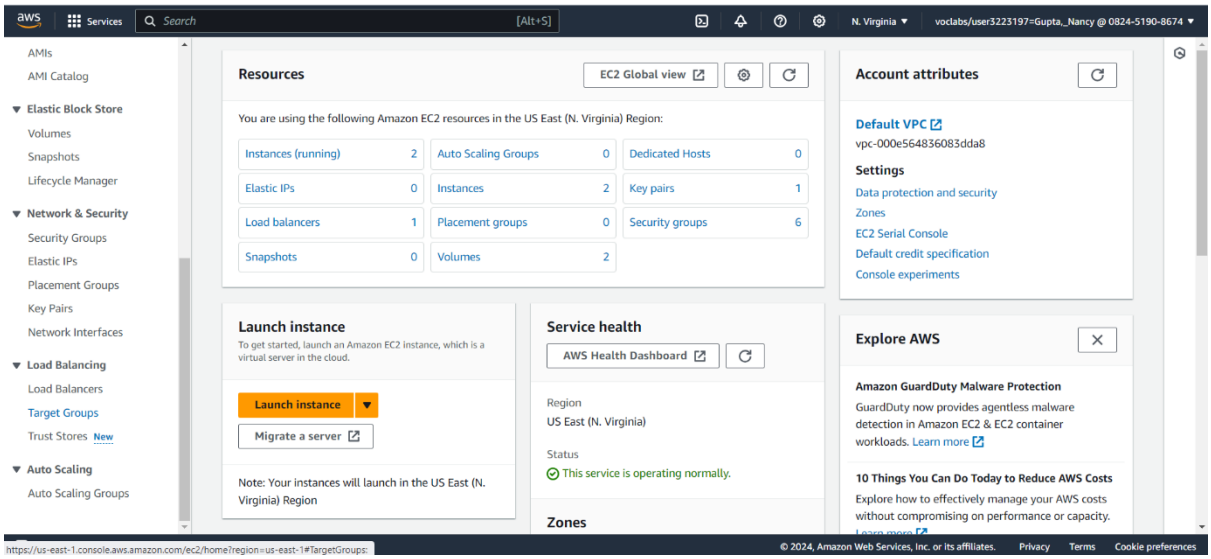
3. **Edit the create-customer-microservice-tg-two.json file:**
    - **Replace REVISION-NUMBER with the number of the latest revision of the *customer-microservice* task definition that is registered with Amazon ECS.**
        - **If this is the first time that you are completing this step, the revision number should be 1.**
        - **If you are repeating this step, find the latest revision number in the Amazon ECS console by choosing Task definitions, and then choosing customer-microservice.**

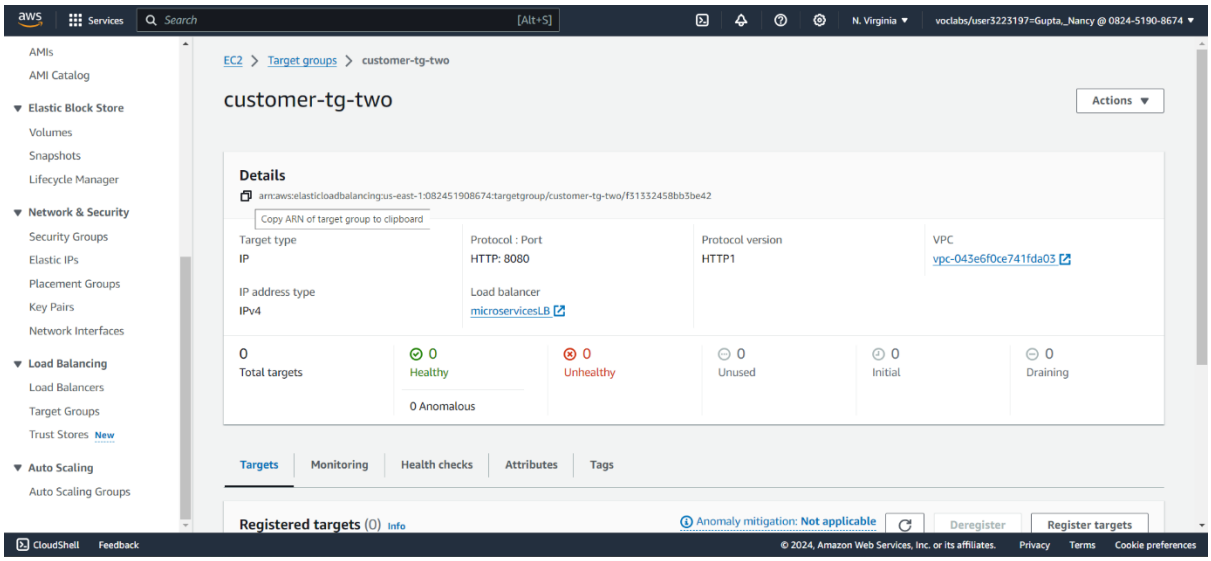


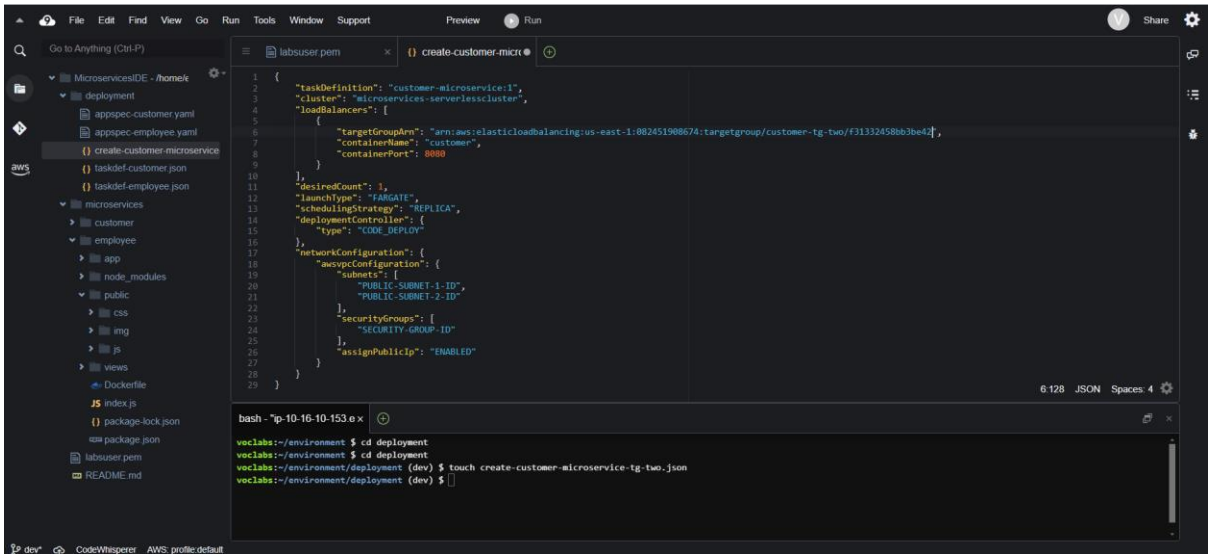




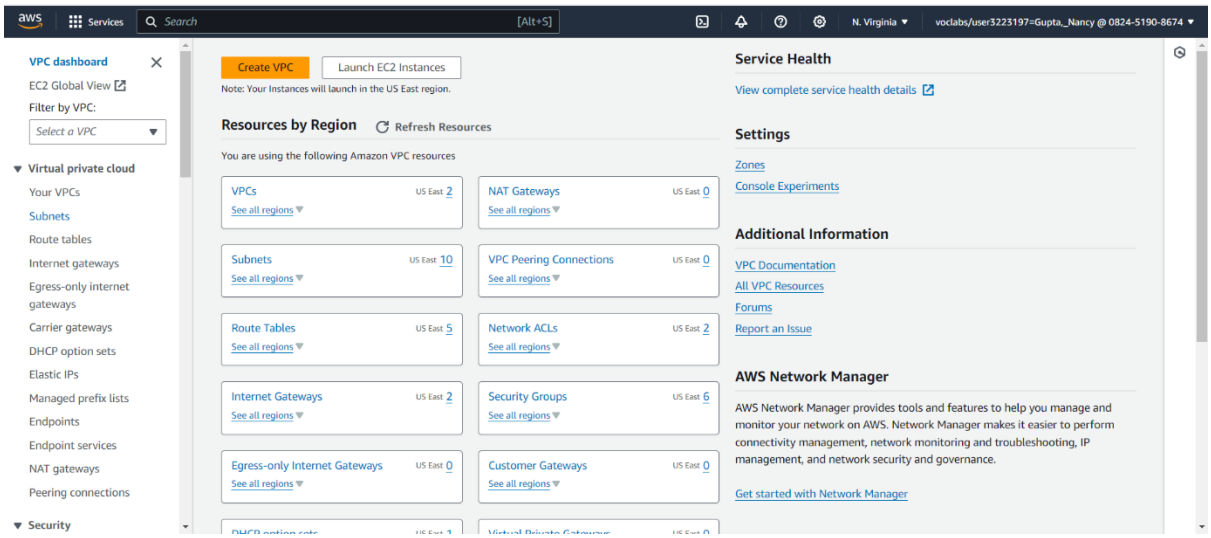
- **Replace MICROSERVICE-TG-TWO-ARN with the actual ARN of the *customer-tg-two* target group.**

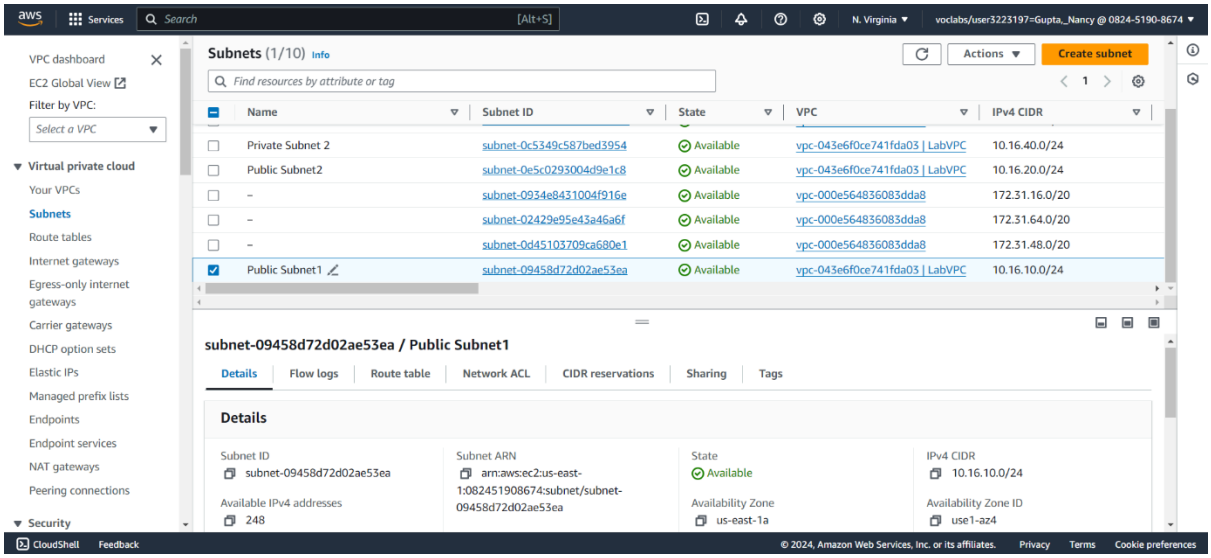


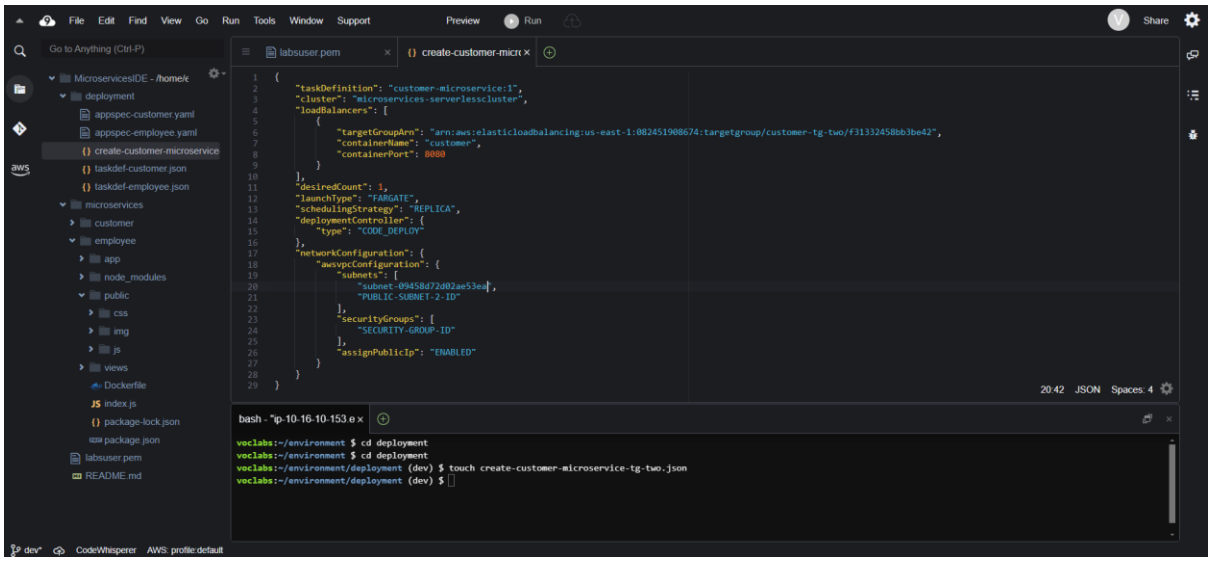




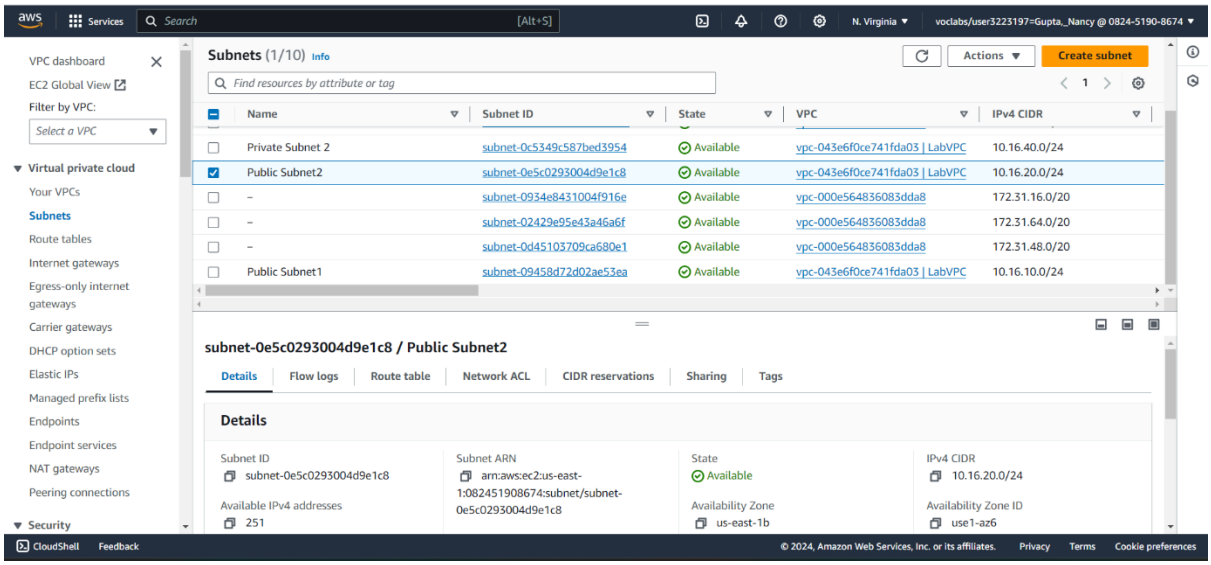
- **Replace PUBLIC-SUBNET-1-ID with the actual subnet ID of *Public Subnet1*.**

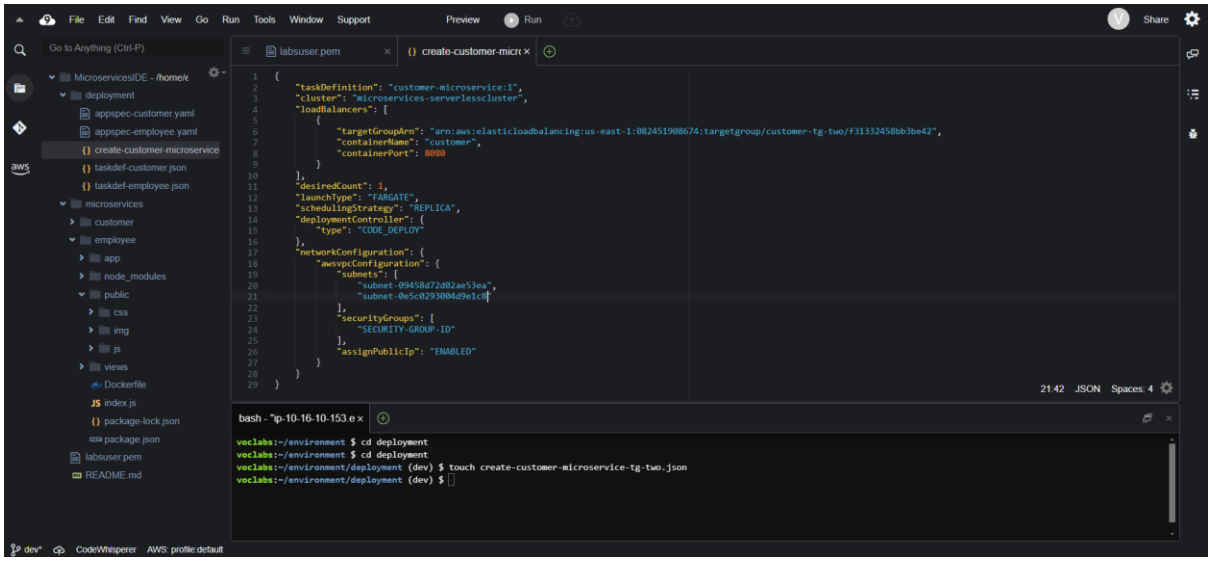




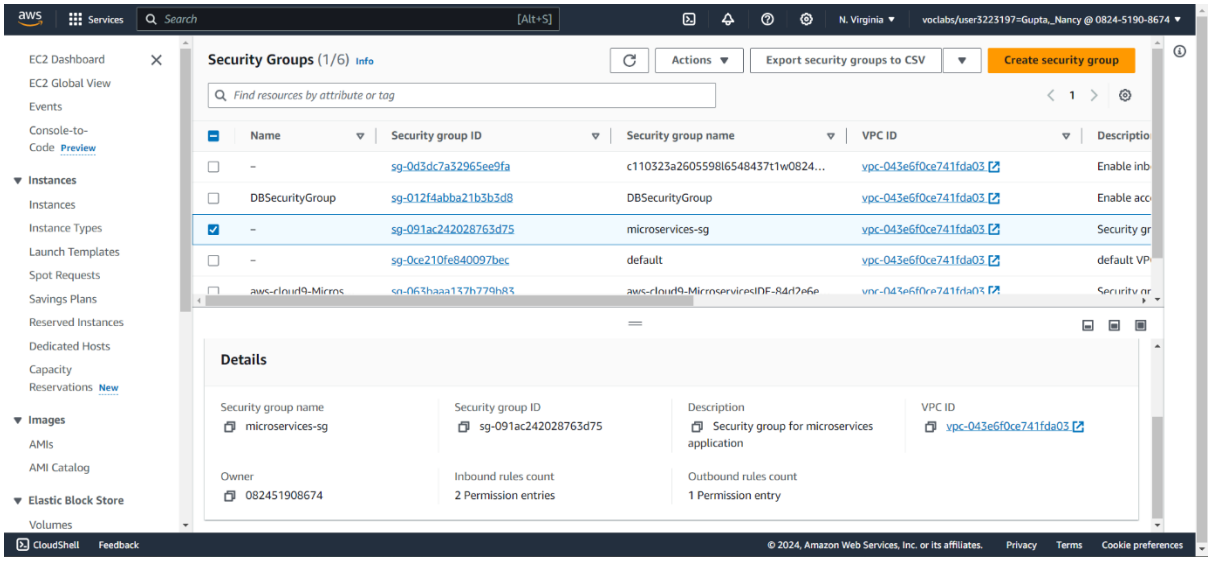


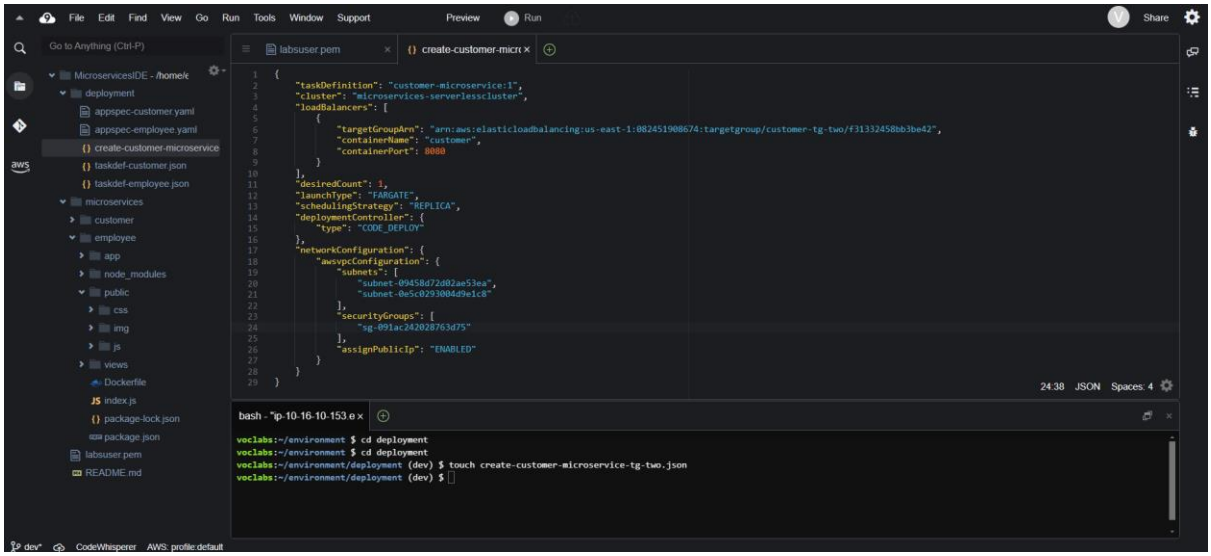
- **Replace PUBLIC-SUBNET-2-ID with the actual subnet ID of *Public Subnet2*.**





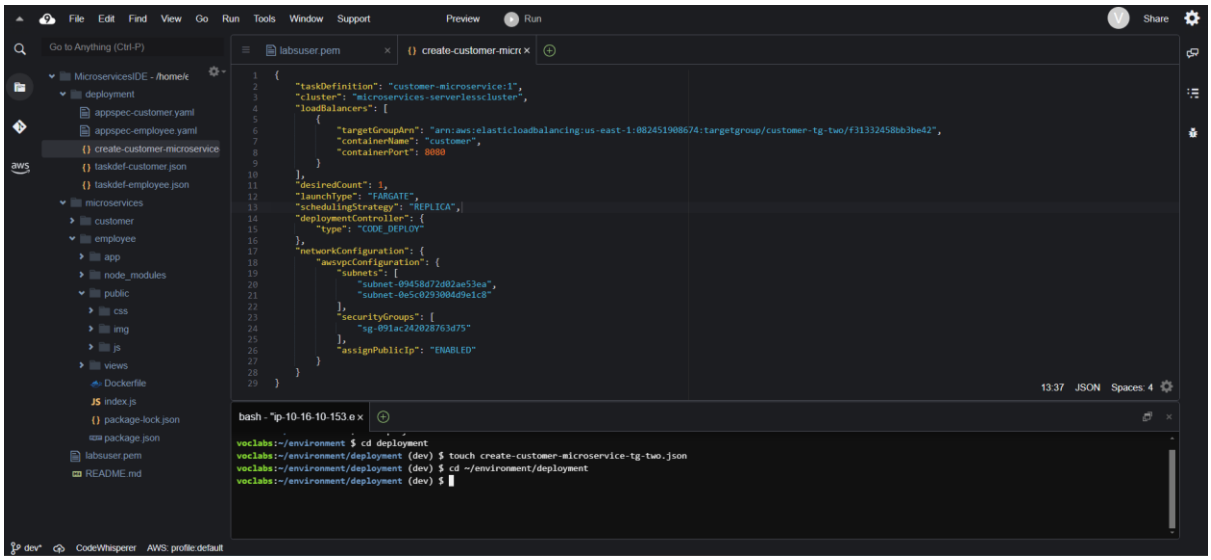
- **Replace SECURITY-GROUP-ID with the actual security group ID of *microservices-sg*.**
- **Save the changes.**





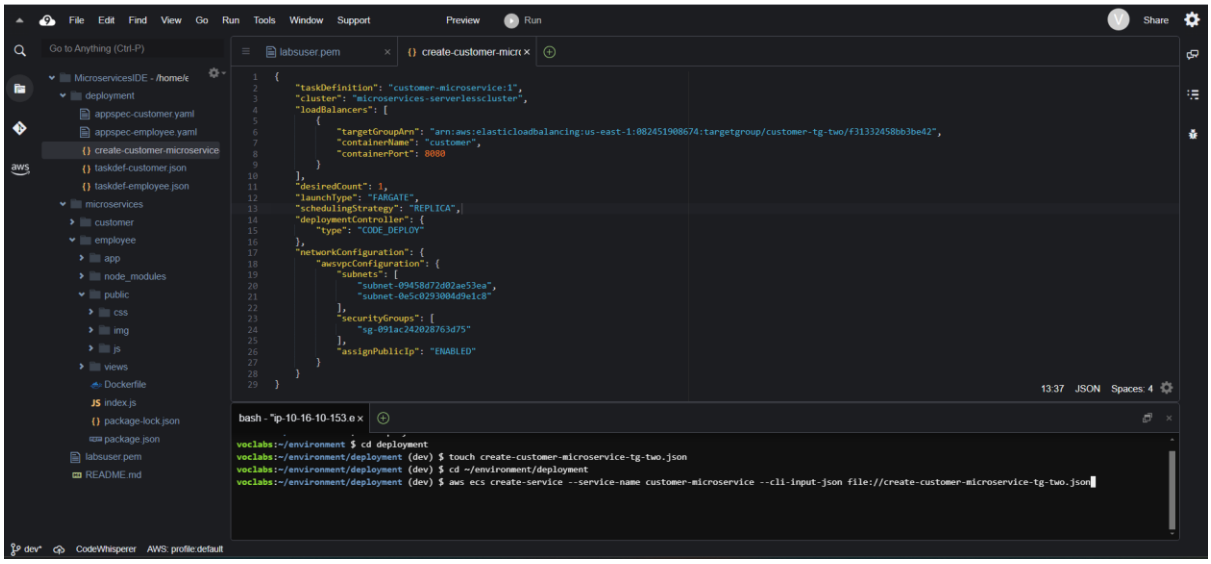
4. **To create the Amazon ECS service for the *customer* microservice, run the following commands:**

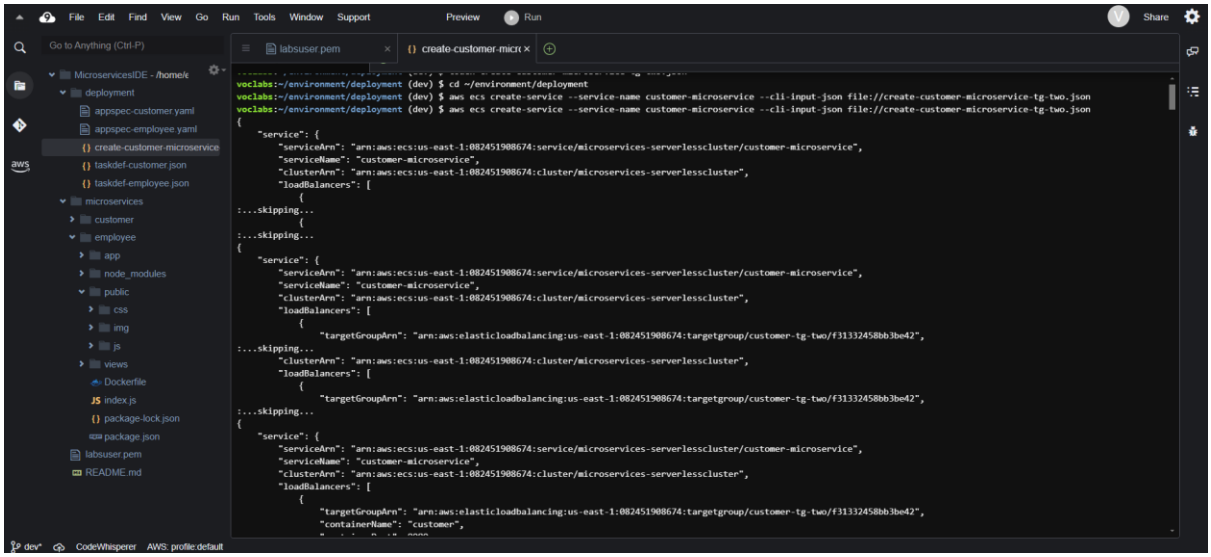
cd ~/environment/deployment

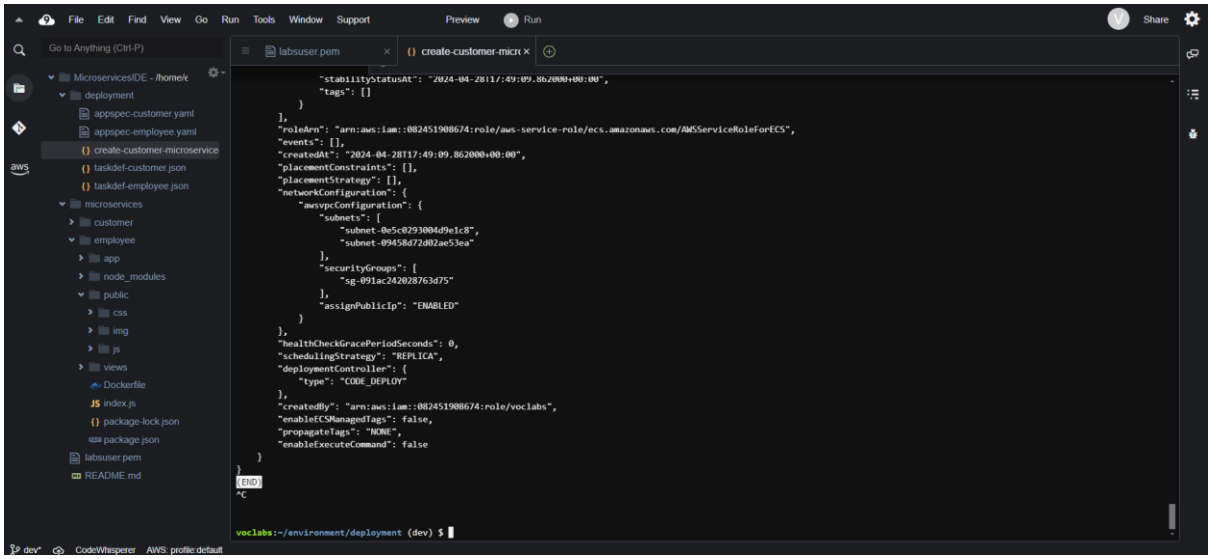


aws ecs create-service --service-name customer-microservice --cli-input-json file://create-customer-microservice-tg-two.json

Troubleshooting tip: If you are repeating this step and previously created the ECS service, you might receive an error about the creation of the service not being idempotent. To resolve this error, force delete the service from the Amazon ECS console, wait for it to drain, and then run the commands again.

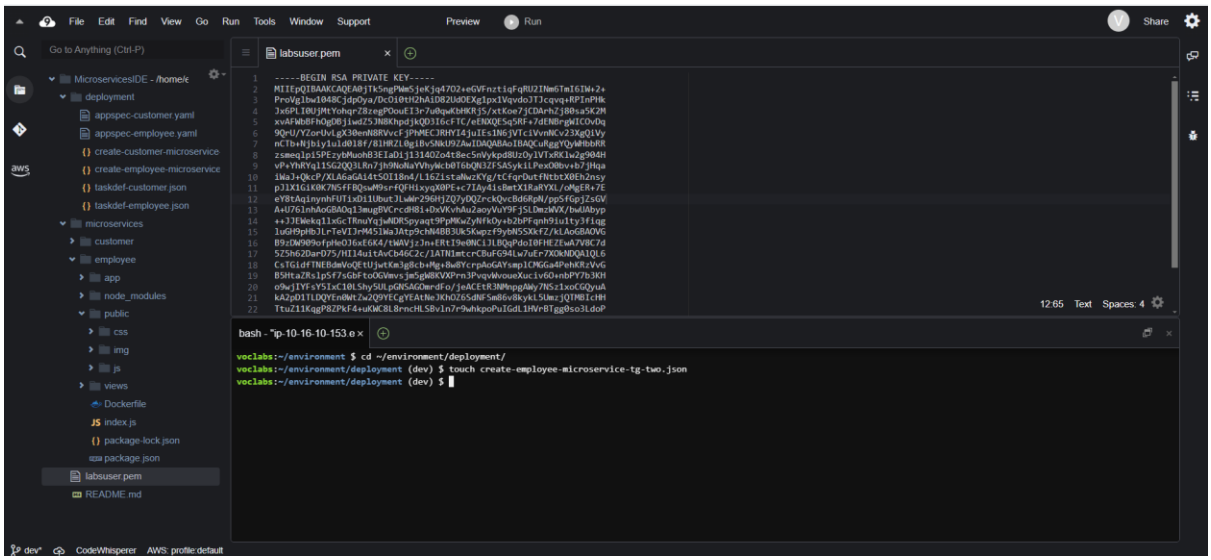




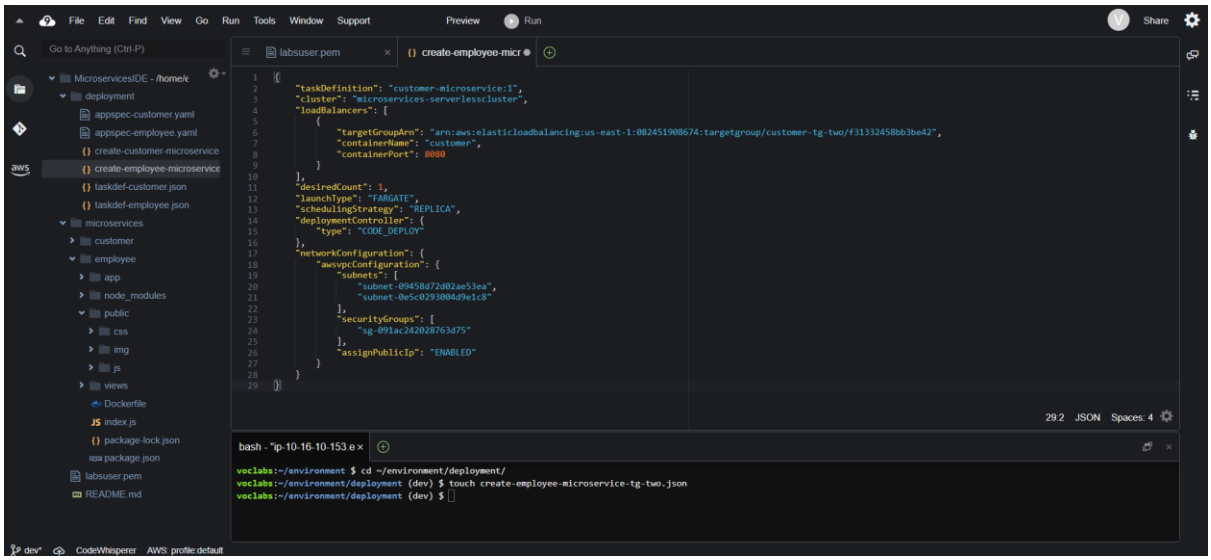


Task 7.2: Create the Amazon ECS service for the *employee* microservice

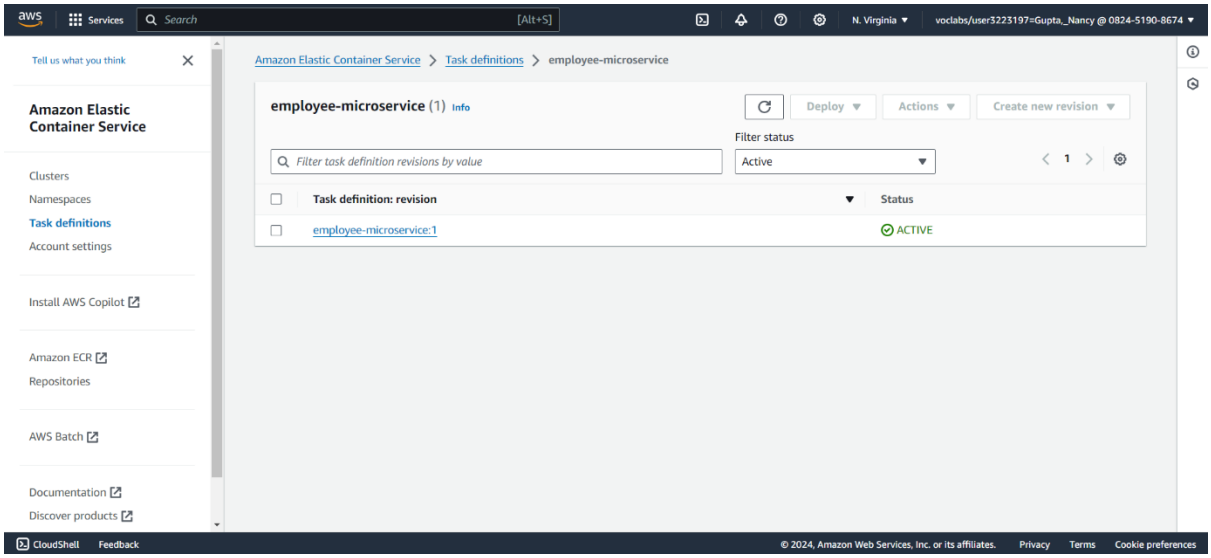
1. **Create an Amazon ECS service for the *employee* microservice.**

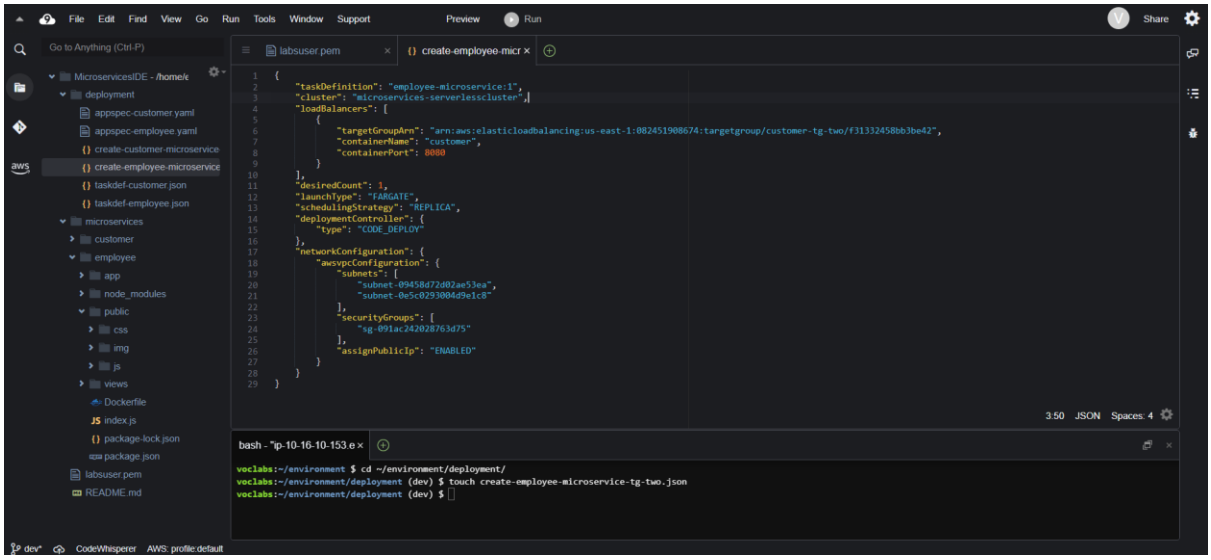


- **Copy the JSON file that you created for the *customer* microservice, and name it create-employee-microservice-tg-two.json. Save it in the same directory.**



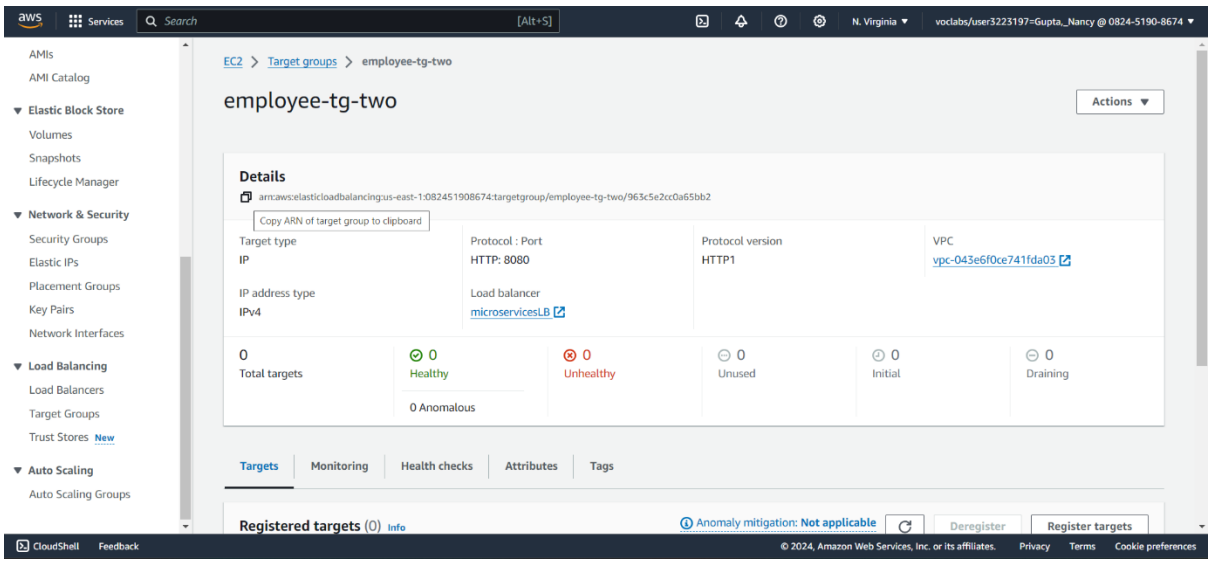
- **Modify the create-employee-microservice-tg-two.json file:**
  - **On line 2, change customer-microservice to employee-microservice and also update the revision number.**

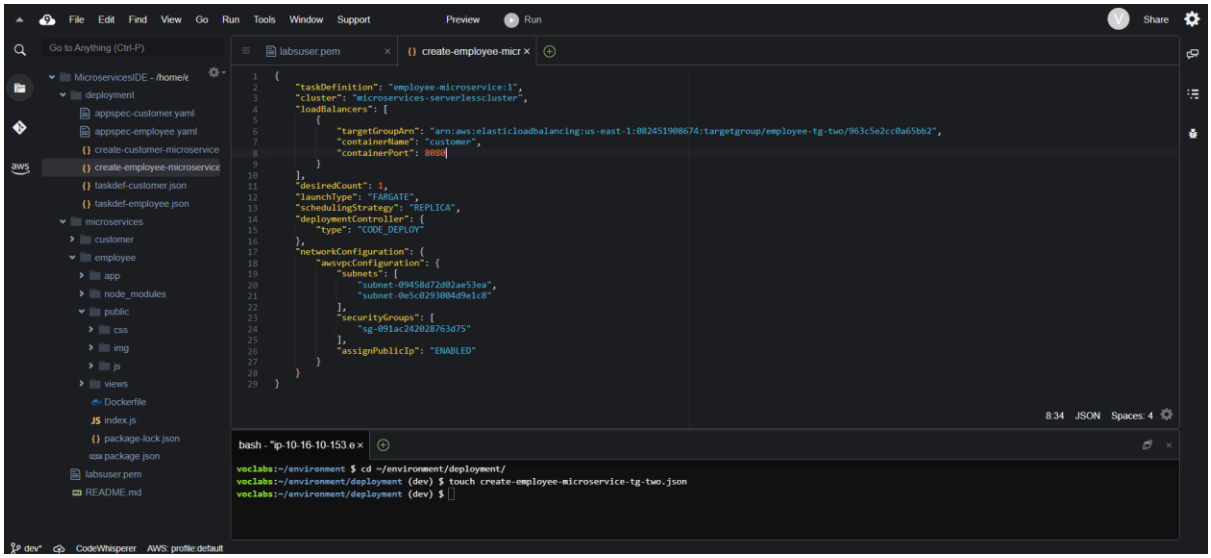




- **On line 6, enter the ARN of the employee-tg-two target group.**

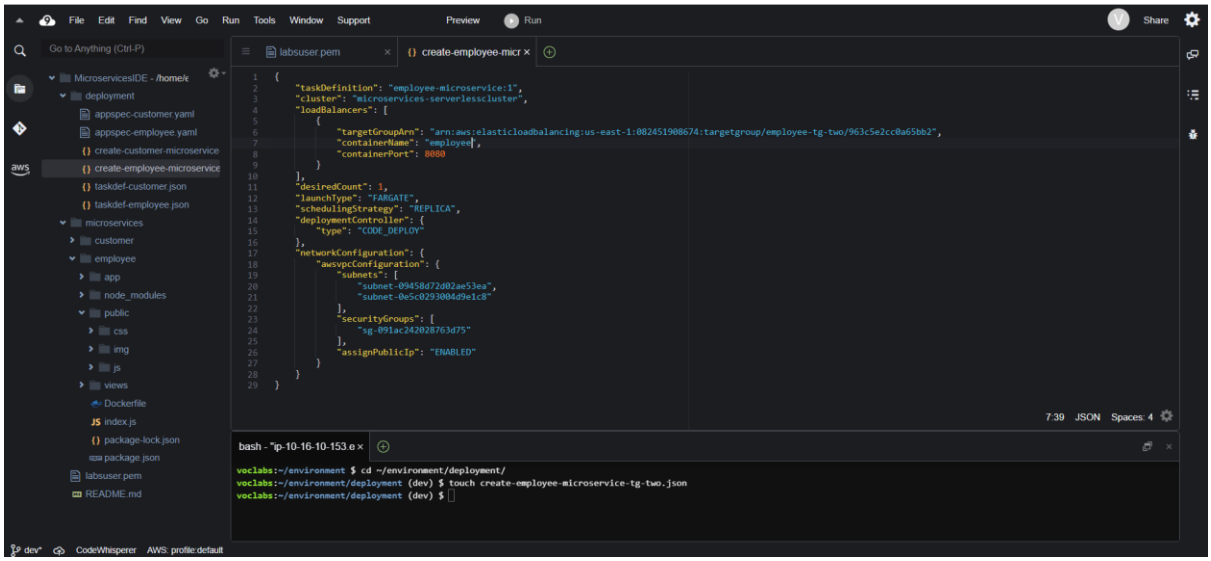
Tip: Don't just change customer to employee on this line. The ARN is unique in other ways.





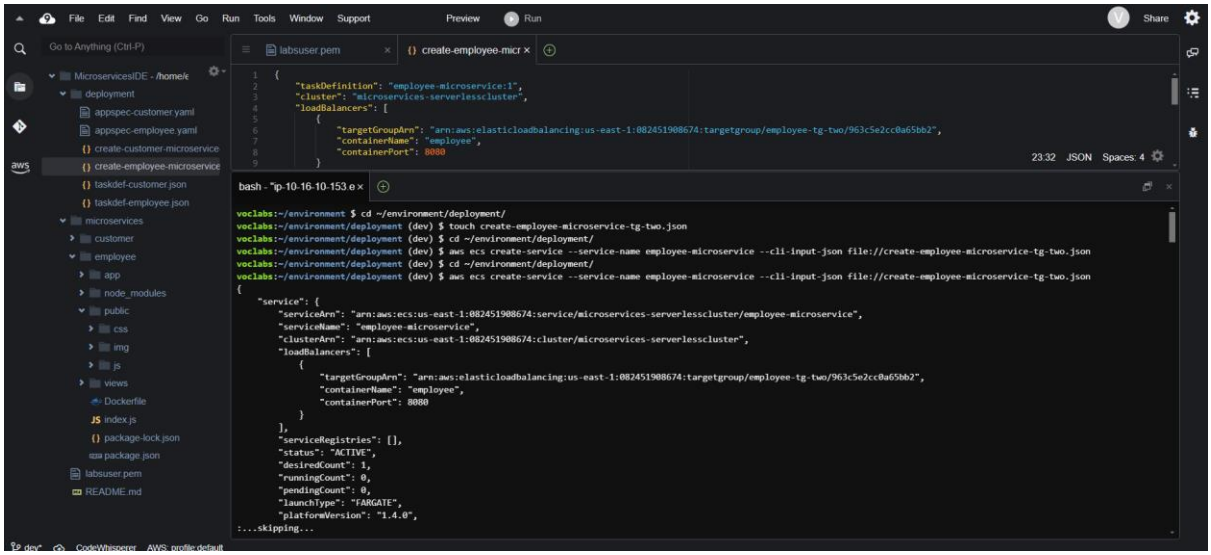
- **On line 7, change customer to employee**

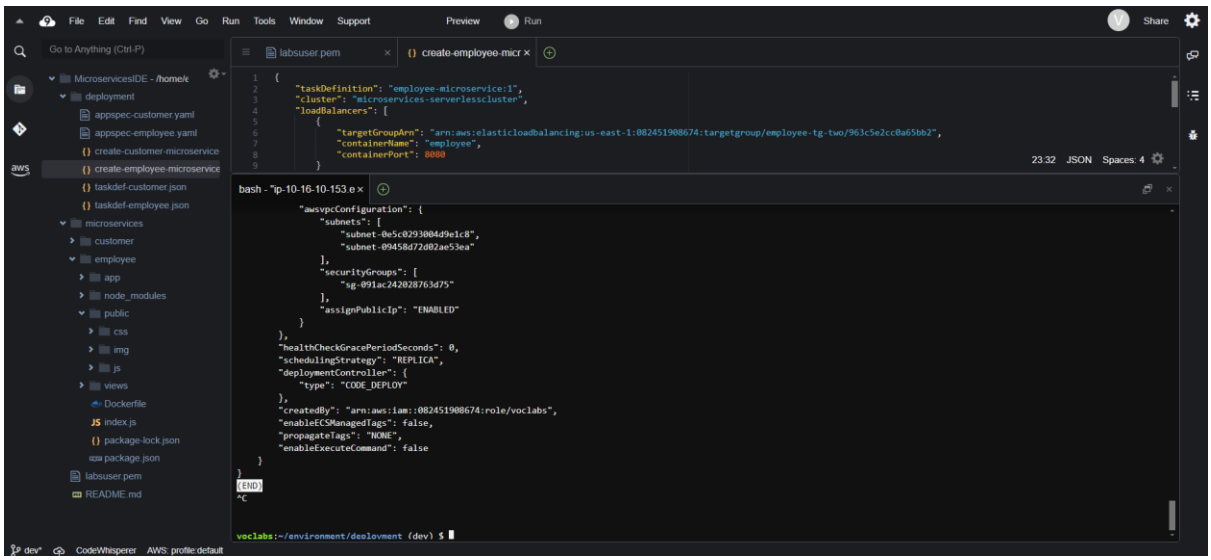
- **Save the changes.**

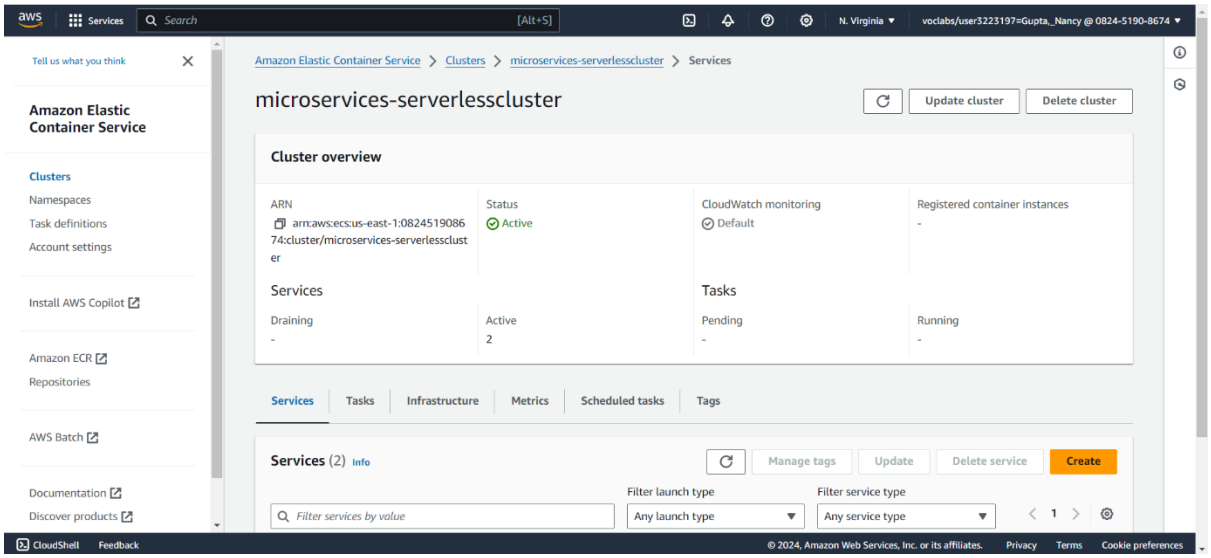


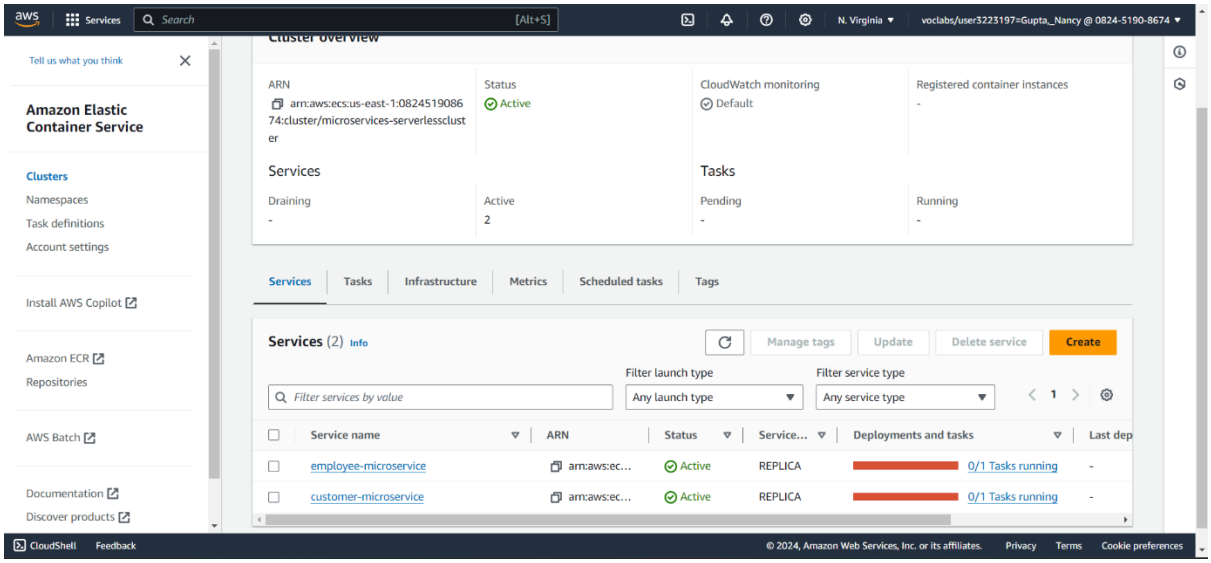
2. **Run the appropriate AWS CLI command to create the service in Amazon ECS.**

Note: If you go to the Amazon ECS console and look at the services in the cluster, you might see *0/1 Task running*, as shown in the following image. This is expected for now because you haven't launched task sets for these services yet.


File Edit Find View Go Run Tools Window Support Preview Run Share
Go to Anything (Ctrl-P)
labsuser.pem
create-employee-micr
MicroservicesIDE - /home/e
deployment
appspec-customer.yaml
appspec-employee.yaml
create-customer-microservice
create-employee-microservice
taskdef-customer.json
taskdef-employee.json
microservices
customer
employee
app
node_modules
public
css
img
js
views
Dockerfile
index.js
package-lock.json
package.json
labsuser.pem
README.md
{
"taskDefinition": "employee-microservice:1",
"cluster": "microservices-serverlesscluster",
"loadBalancers": [
{
"targetGroupArn": "arn:aws:elasticloadbalancing:us-east-1:082451908674:targetgroup/employee-tg-two/963c5e2cc0a65bb2",
"containerName": "employee",
"containerPort": 8080
}
23:32 JSON Spaces: 4
bash - "ip-10-16-10-153.e
voclabs:~/environment $ cd ~/environment/deployment/
voclabs:~/environment/deployment (dev) $ touch create-employee-microservice-tg-two.json
voclabs:~/environment/deployment (dev) $ cd ~/environment/deployment/
voclabs:~/environment/deployment (dev) $ aws ecs create-service --service-name employee-microservice --cli-input-json file://create-employee-microservice-tg-two.json
voclabs:~/environment/deployment (dev) $ cd ~/environment/deployment/
voclabs:~/environment/deployment (dev) $ aws ecs create-service --service-name employee-microservice --cli-input-json file://create-employee-microservice-tg-two.json
{
"service": {
"serviceArn": "arn:aws:ecs:us-east-1:082451908674:service/microservices-serverlesscluster/employee-microservice",
"serviceName": "employee-microservice",
"clusterArn": "arn:aws:ecs:us-east-1:082451908674:cluster/microservices-serverlesscluster",
"loadBalancers": [
{
"targetGroupArn": "arn:aws:elasticloadbalancing:us-east-1:082451908674:targetgroup/employee-tg-two/963c5e2cc0a65bb2",
"containerName": "employee",
"containerPort": 8080
}
],
"serviceRegistries": [],
"status": "ACTIVE",
"desiredCount": 1,
"runningCount": 0,
"pendingCount": 0,
"launchType": "FARGATE",
"platformVersion": "1.4.0",
:...skipping...
dev* CodeWhisperer AWS: profile:default


File Edit Find View Go Run Tools Window Support Preview Run Share
Go to Anything (Ctrl-P)
labsuser.pem
create-employee-micr
MicroservicesIDE - /home/e
deployment
appspec-customer.yaml
appspec-employee.yaml
create-customer-microservice
create-employee-microservice
taskdef-customer.json
taskdef-employee.json
microservices
customer
employee
app
node_modules
public
css
img
js
views
Dockerfile
index.js
package-lock.json
package.json
labsuser.pem
README.md
{
"taskDefinition": "employee-microservice:1",
"cluster": "microservices-serverlesscluster",
"loadBalancers": [
{
"targetGroupArn": "arn:aws:elasticloadbalancing:us-east-1:082451908674:targetgroup/employee-tg-two/963c5e2cc0a65bb2",
"containerName": "employee",
"containerPort": 8080
}
23:32 JSON Spaces: 4
bash - "ip-10-16-10-153.e
"awsvpcConfiguration": {
"subnets": [
"subnet-0e5c0293004d9e1c8",
"subnet-09458d72d02ae53ea"
],
"securityGroups": [
"sg-091ac242028763d75"
],
"assignPublicIp": "ENABLED"
}
},
"healthCheckGracePeriodSeconds": 0,
"schedulingStrategy": "REPLICA",
"deploymentController": {
"type": "CODE_DEPLOY"
},
"createdBy": "arn:aws:iam::082451908674:role/voclabs",
"enableECSManagedTags": false,
"propagateTags": "NONE",
"enableExecuteCommand": false
}
}
(END)
^C
voclabs:~/environment/deployment (dev) $
dev* CodeWhisperer AWS: profile:default


aws Services Search [Alt+S] N. Virginia voclabs/user3223197=Gupta,_Nancy @ 0824-5190-8674
Tell us what you think
Amazon Elastic Container Service
Clusters
Namespaces
Task definitions
Account settings
Install AWS Copilot
Amazon ECR
Repositories
AWS Batch
Documentation
Discover products
Amazon Elastic Container Service > Clusters > microservices-serverlesscluster > Services
microservices-serverlesscluster
Update cluster
Delete cluster
Cluster overview
ARN
arn:aws:ecs:us-east-1:082451908674:cluster/microservices-serverlesscluster
Status
Active
CloudWatch monitoring
Default
Registered container instances
-
Services
Draining
-
Active
2
Tasks
Pending
-
Running
-
Services
Tasks
Infrastructure
Metrics
Scheduled tasks
Tags
Services (2) Info
Manage tags
Update
Delete service
Create
Filter services by value
Filter launch type
Any launch type
Filter service type
Any service type
1
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



Phase 8: Configuring CodeDeploy and CodePipeline

Now that you have defined the Application Load Balancer, target groups, and the Amazon ECS services that comprise the infrastructure that you will deploy your microservices to, the next step is to define the CI/CD pipeline to deploy the application.

The following diagram illustrates the role of the pipeline in the solution that you are building.

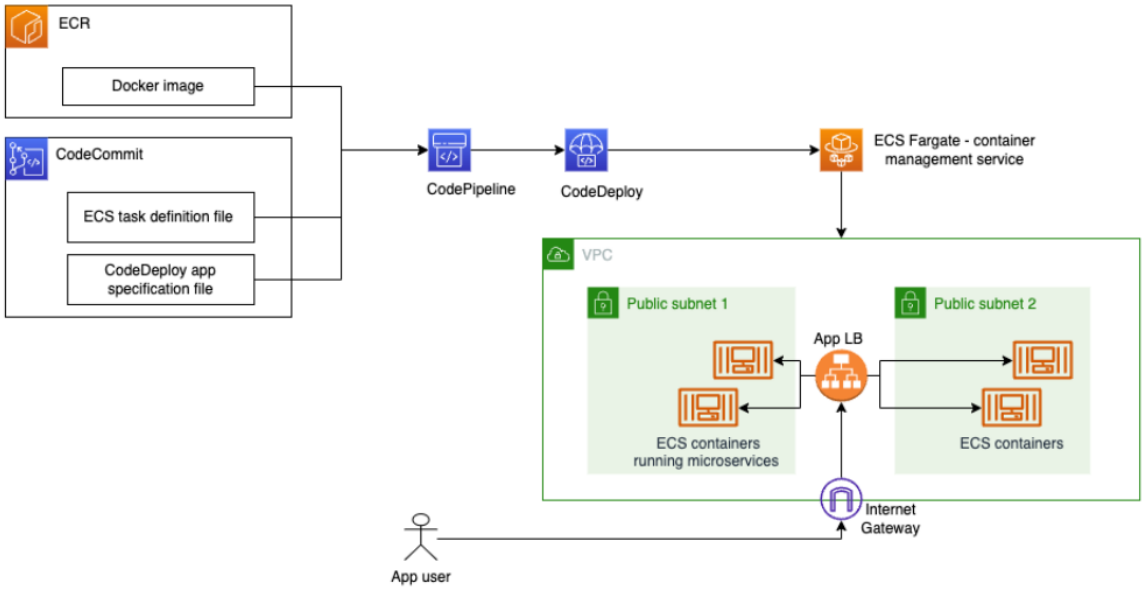


Diagram description: The pipeline will be invoked by updates to CodeCommit, where you have stored the ECS task definition files and the CodeDeploy AppSpec files. The pipeline can also be invoked by updates to one of the Docker image files that you have stored in Amazon ECR. When invoked, the pipeline will call the CodeDeploy service to deploy the updates. CodeDeploy will take the necessary actions to deploy the updates to the green environment. Assuming that no errors occur, the new task set will replace the existing task set.

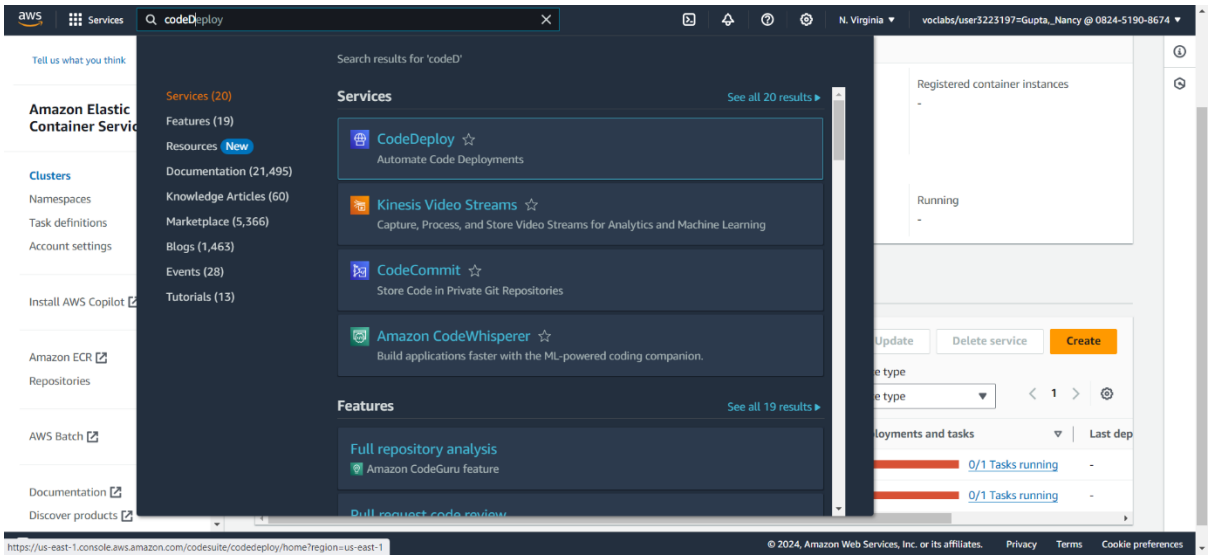
Task 8.1: Create a CodeDeploy application and deployment groups

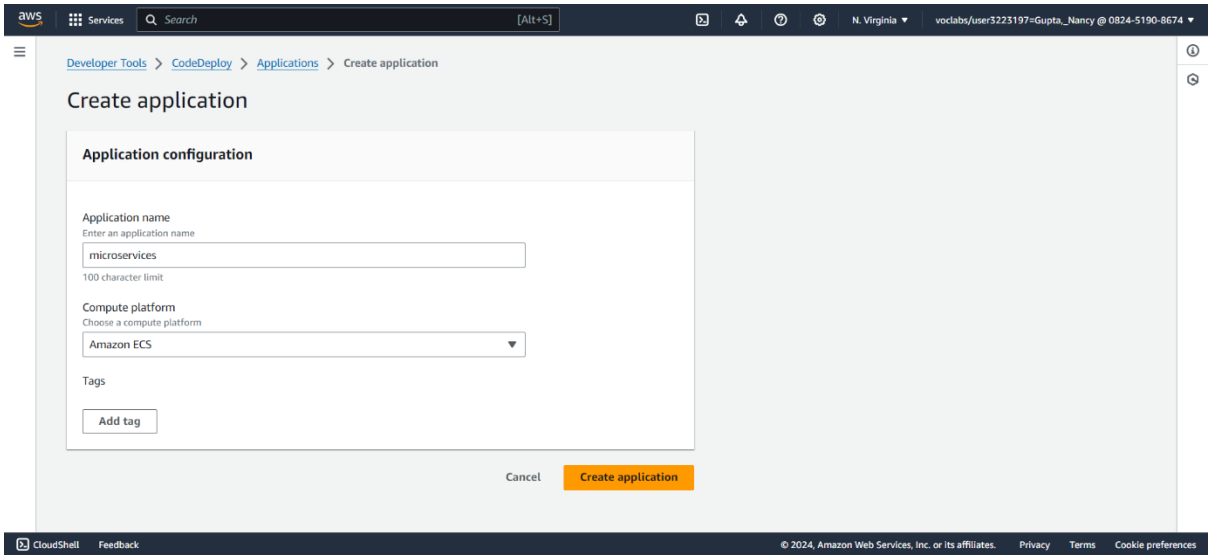
A CodeDeploy application is a collection of deployment groups and revisions. A deployment group specifies an Amazon ECS service, load balancer, optional test listener, and two target groups. A group specifies when to reroute traffic to the replacement task set, and when to terminate the original task set and Amazon ECS application after a successful deployment.

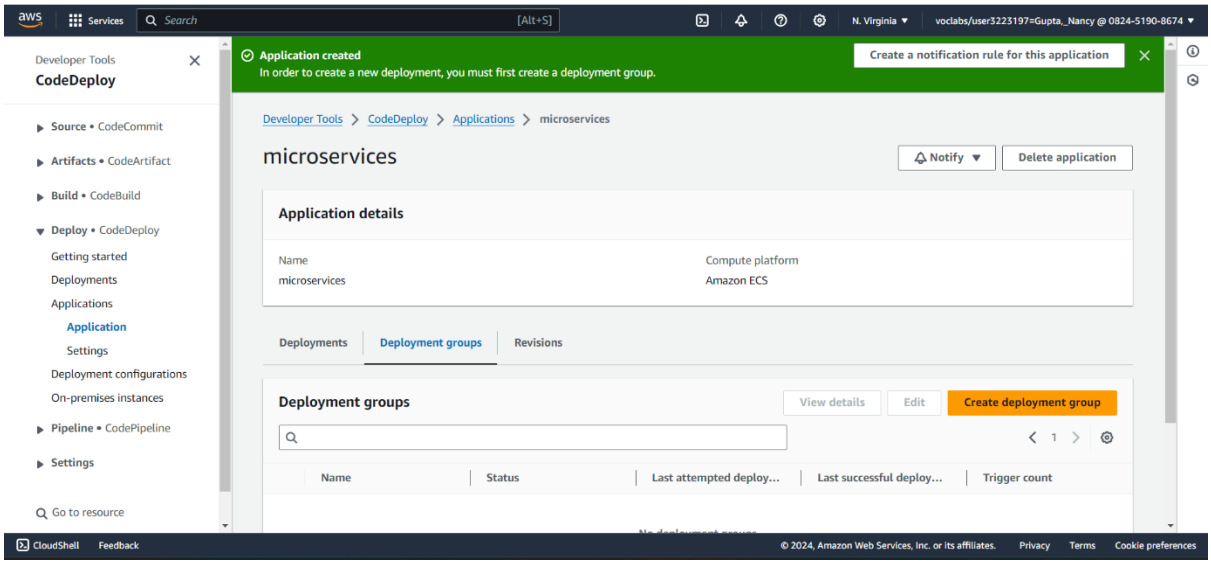
1. Use the CodeDeploy console to create a CodeDeploy application with the name microservices that uses Amazon ECS as the compute platform.

Tip: See [Create an Application for an Amazon ECS Service Deployment (Console)] in the *AWS CodeDeploy User Guide*.

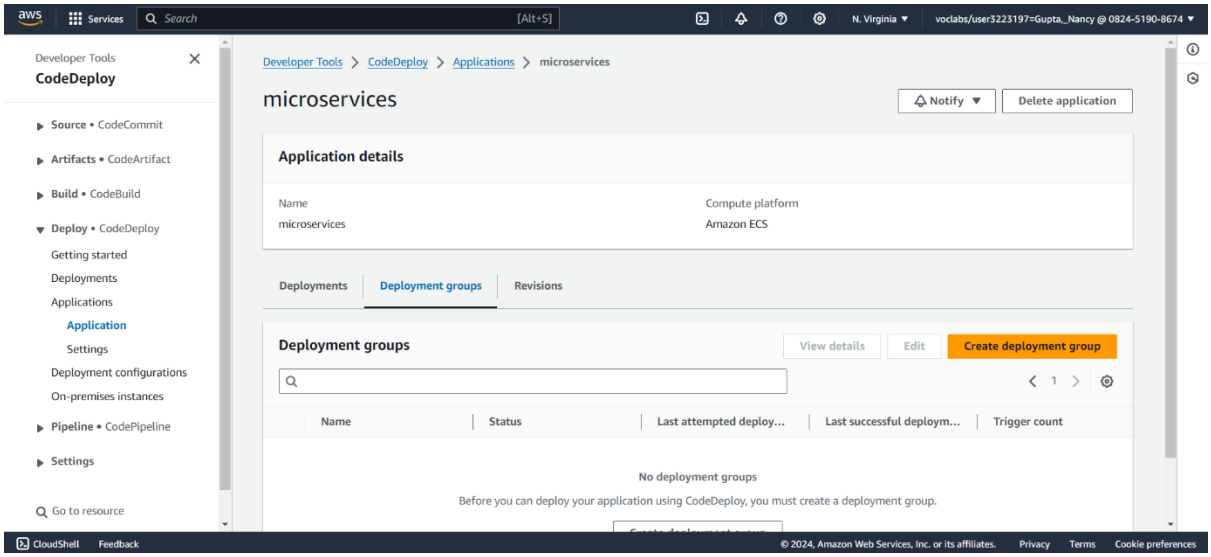
Important: *DON'T* create a deployment group yet. You will do that in the next step.



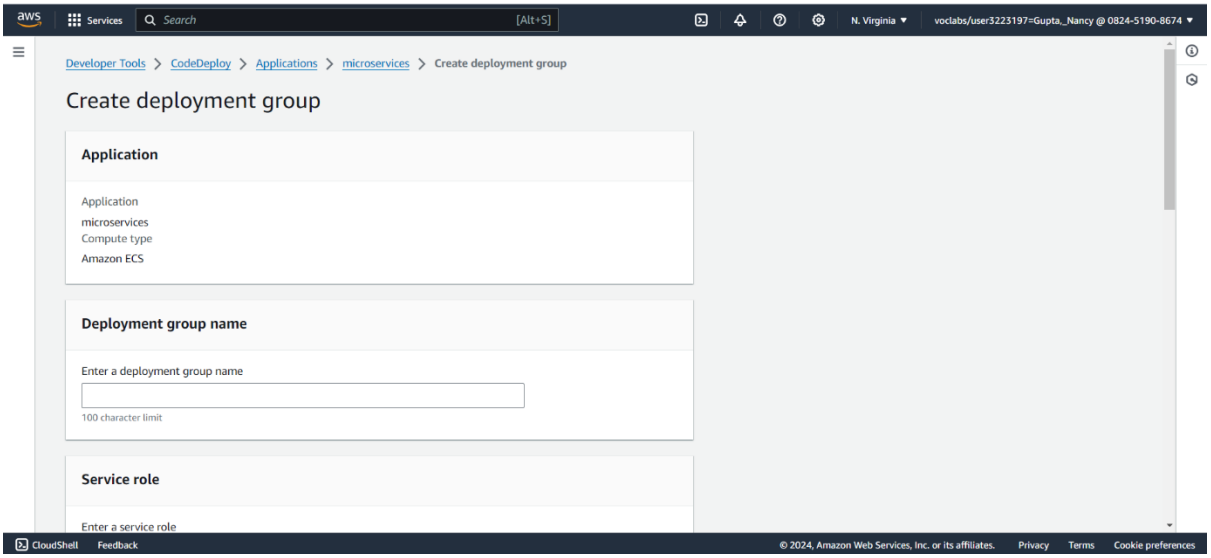




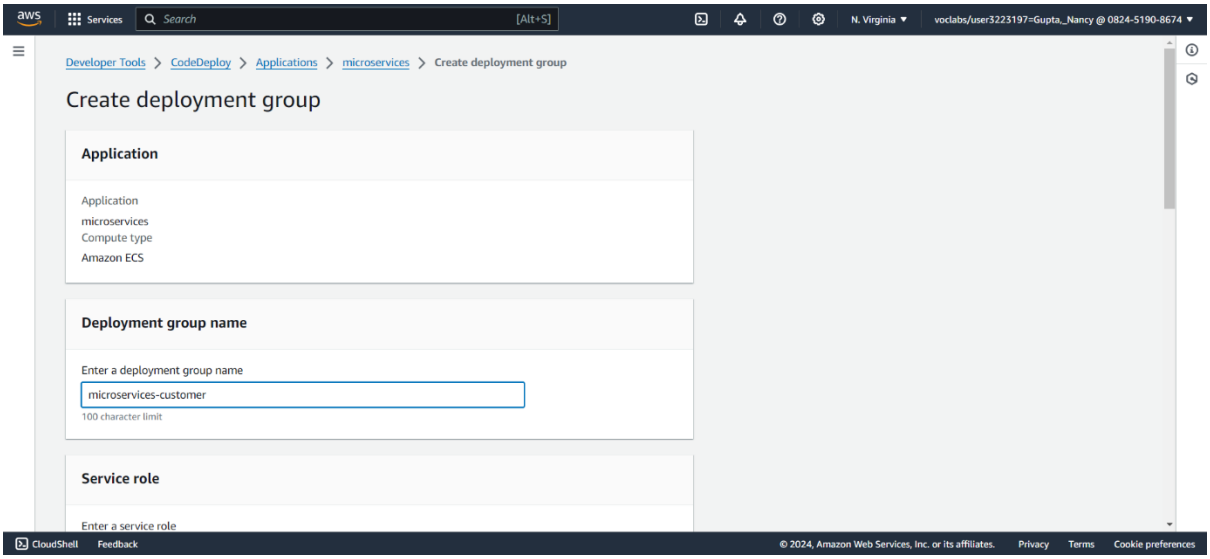
2. Create a CodeDeploy deployment group for the *customer* microservice.
    - On the *microservices* application detail page, choose the **Deployment groups** tab.



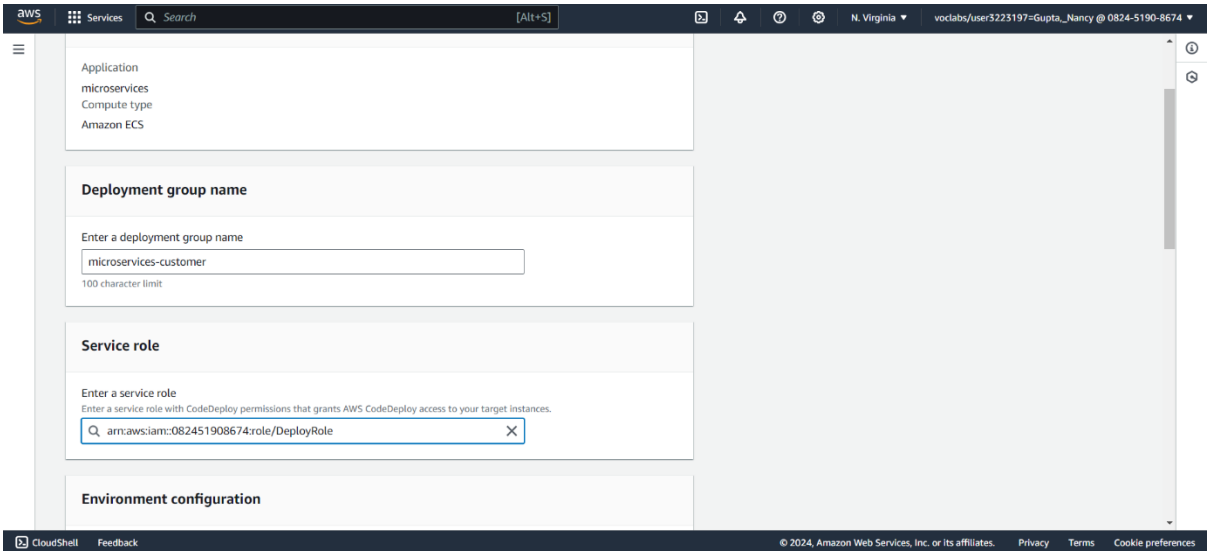
- Choose **Create deployment group** and configure the following:



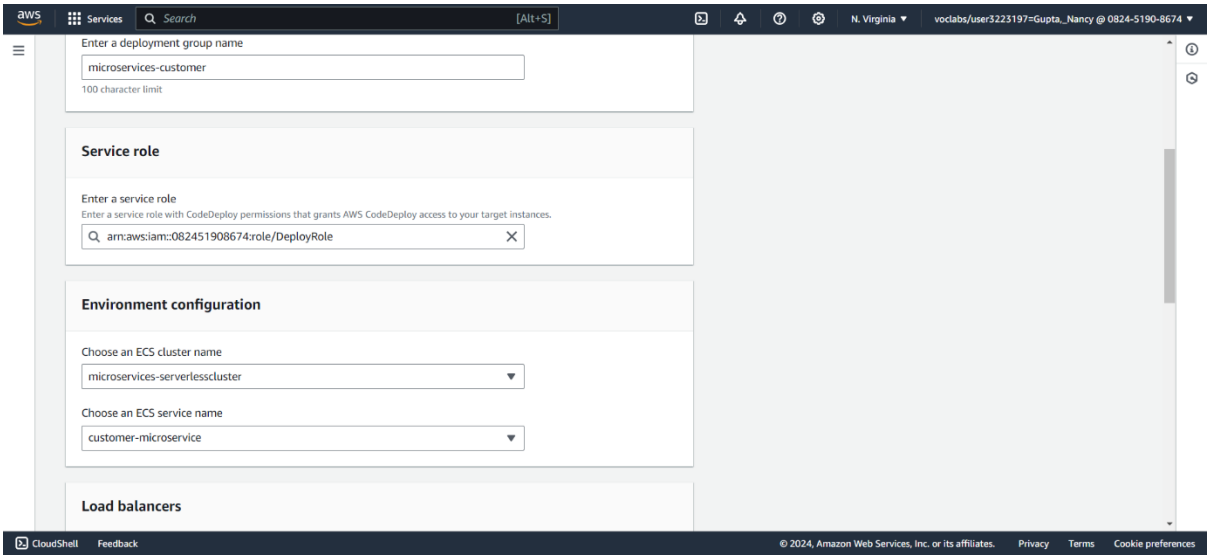
  - **Deployment group name:** Enter microservices-customer



  - **Service role:** Place your cursor in the search box, and choose the ARN for **DeployRole**.



- In the **Environment configuration** section:
  - **ECS cluster name:** Choose **microservices-serverlesscluster**.
  - **ECS service name:** Choose **customer-microservice**.



- In the **Load balancers** section:
  - **Load balancer:** Choose **microservicesLB**.
  - **Production listener port:** Choose **HTTP:80**.
  - **Test listener port:** Choose **HTTP:8080**.
  - **Target group 1 name:** Choose **customer-tg-two**.
  - **Target group 2 name:** Choose **customer-tg-one**.