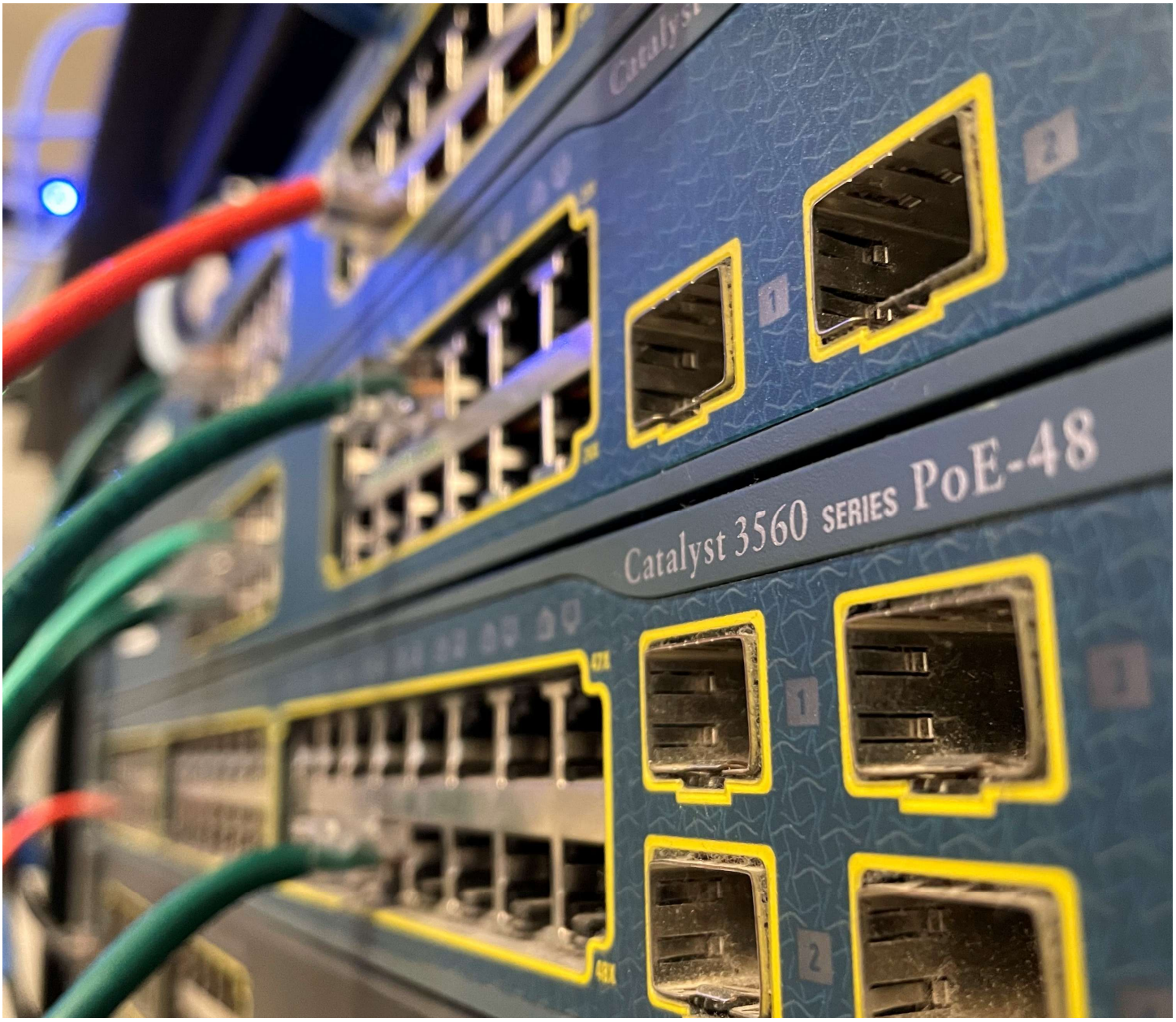


Portfolio – Newport Advanced Cisco Networking Academy – Newport Cybersecurity Academy

Colin J. Faletto

CISCO CERTIFIED CCNA

Networking Academy Verified CCNA: Introduction to Networks

Networking Academy Verified CCNA: Enterprise Networking, Security & Automation

Networking Academy Verified CCNA: Switching, Routing & Wireless Essentials

Networking Academy Verified Introduction to Cybersecurity

aws certified Cloud Practitioner FOUNDATIONAL

CompTIA Security+ CERTIFIED Plus Series

Table of Contents

Building Network Infrastructure/Donating IT Equipment in Antigua – Rotary Club of Antigua/BBRC/RCKD

Steve Lingenbrink, Colin J. Faletto, Jeffrey Cheung, Eric Xia

Bellevue School District · Cisco Networking Academy · Rotary Club of Kirkland Downtown · Bellevue Breakfast Rotary Club · Rotary Club of Antigua

Sites Visited

Clare Hall (Living Hope) Christian Union Church

Address: 45GC+HWX, Wireless Rd, Piggotts

Days Visited: 17-Feb

Completed Tasks:

- Donated Laptops

Equipment Used/Donated:

- 15 Laptops/chargers

Comments:
Our team was originally told to install new networking equipment in an external building, but this work had already been done by a third-party contractor.

Post-Millennial Academy

Address: 35QP+4PJ, All Saints Rd, Potters Village

Days Visited: 17-Feb

Completed Tasks:

- Donated Laptops
- Donated Projectors

Equipment Used/Donated:

- 44 Laptops/chargers
- 4 Projectors

Comments:

Big, well-funded private school (244 students); they need a lot of equipment but can likely afford to buy a lot of it themselves

Christ the King High School

Address: 45G8+2P6, Old Parham Rd, St John's

Days Visited: 17-Feb, 18-Feb

Other teams at school: Sara, Norm

Completed Tasks:

- Assisted Sara's team in mounting APs along back hallway
- Installed point-to-point to art room, connected to an AP mounted on the wall
- Assisted Norm's team in re-running cables to APs in back room

- Fixed AP/point-to-point in music room

Equipment Used/Donated (just our team):

- 1 Ubiquiti point-to-point set
- Cisco AP/mounting bracket
- 2 Ubiquiti Power Injectors
- 1 Cisco power injector
- 1 power strip

Comments:

Heavy collaboration with other teams, CTK is routinely a major project for the rotary club

New Bethel Seventh Day Adventist Academy

Address: 26R4+XGH, Liberta

Days Visited: 19-Feb, 20-Feb

Completed Tasks:

- Replaced old faulty switch (restored internet to computer lab)
- Installed new wall-mounted Cisco AP in computer lab
- Pulled old, broken cable
- Installed point-to-point from computer lab to external classroom, connected to wall-mounted AP

Equipment Used/Donated:

- 12 Laptops/chargers
- 1 Cisco PoE switch
- 2 Cisco APs
- 1 Cisco AP mounting bracket
- 1 Ubiquiti point-to-point set
- 2 Ubiquiti power injectors
- 1 Cisco power injector

Comments: Computer lab is very well-maintained; school was getting accredited within a few days so fixing their internet was well-appreciated

Liberta Primary School

Address: 26M5+RR8, Liberta

Days Visited: 19-Feb

Completed Tasks:

- Donated Laptops

Equipment Used/Donated:

- 24 Laptops/chargers

Comments: Very brief visit, our team was only there for ~10 minutes

Freeman's Village Primary School

Address: 26M5+RR8, Liberta

Days Visited: 20-Feb

Completed Tasks:

- Donated Laptops

Equipment Used/Donated:

- 24 Laptops/chargers

Comments: Another very brief visit

Sunshine Home

Address: 24J6+3FR, Urlings (On Valley Road, Across from Turners Beach, big painted mural out front)

Days Visited: 21-Feb, 25-Feb

Completed Tasks:

- Replaced old Linksys router with Cisco AP
- Ran new cable to computer lab
- Installed AP in computer lab
- Ran cable to dormitory building
- Installed AP in dormitory building

Equipment Used/Donated:

- 12 Laptops/chargers
- 3 Cisco APs
- 2 Cisco AP mounting brackets
- 3 Cisco power injectors

Comments:

Seemed like this was rotary's first time at this school, they didn't have any of our equipment

Boys' Training School / Denis Bowers Rehabilitation Center

Address: 37JP+97H, Willikies

Phone: 463-2029

Days Visited: 24-Feb

Other teams at school: Sara

Completed Tasks:

- Ran cable from fiber router in office to switch in break room
- Installed AP in break room
- Ran cable from switch to circular room, installed wall-mounted AP
- Ran cable from switch to middle of circular hallway, installed ceiling-mounted AP

Equipment used/donated:

- (Around) 24 laptops/chargers
- 3 Cisco APs
- 3 Cisco AP mounting brackets

Comments:

Rotary will assuredly be coming back to this school in the future, they still need internet in the external classroom, dining hall, guard room, and laundry room

Trinity Academy

Address: 34FP+943, Jennings, Saint Mary

Dates Visited: 25-Feb

Completed Tasks:

- Donated Projectors

Equipment Used/Donated:

- 2 Fudoni Projectors

Comments:

We walked into some sort of emergency situation; police were there, so we didn't stay long

Golden Grove Primary School

Address: 4545+P3H, Valley Rd, St John's

Dates Visited: 25-Feb

Other teams at school: Sara, Hansen

Completed Tasks:

- Installed new wall-mounted switch in classroom block, installed APs
- Installed point-to-point to switch in block of classrooms, installed 3 wall-mounted APs

Equipment Used/Donated:

- Refer to documentation from Sara's team/Hansen's team, our team only came in at the tail end of the project and was not here long enough to collect this information

Cover Image Attribution: Joe Mabel CC-BY-SA 4.0

AWS Academy Cloud Foundations: Configuring Elastic Block Store, Relational Database Service, and Elastic Cloud Compute Auto Scaling

Colin J. Faletto, CCNA

aws academy

Purpose

This write-up is intended to document and explain the fourth, fifth, and sixth in the AWS Academy Cloud Foundations course. These labs are intended to provide additional knowledge in the field of cloud computing, such as block-level file storage for virtual machines, basic relational database configuration, and automatic infrastructure scaling to meet user demand. These concepts are essential for new cloud engineers to provide parallels to more advanced facets of traditional IT. These labs also provide a strong foundation of knowledge for the AWS management console, as they all take place primarily inside this console.

Background

Amazon is a company based in Seattle that runs the biggest e-commerce platform in the world. They were started in 1994 by former CEO Jeff Bezos, and have grown from a small online bookstore to a giant online store offering a wide variety of products. Amazon also has a strong physical retail presence in the grocery space with their Amazon Fresh and Whole Foods chains, and has a strong online media presence through Twitch, Prime Video, and Amazon Music, which provide entertainment in the form of livestreams, movies and television shows, and music respectively. Amazon also has a popular line of e-readers and tablets with their Kindle brand and has a successful brand of artificial intelligence assistants with their Amazon Alexa A.I. and their Amazon Echo line of smart speakers.

Amazon Web Services, or AWS, is Amazon's cloud computing division. It was created in 2002 to provide simple web services to customers and expanded to cloud storage and computing in 2006. It is the leading cloud service provider and is popular for its pay-as-you-go service model. AWS provides services to everyone from small businesses to massive companies like Coca-Cola and Apple, and even provides web infrastructure to government branches. AWS takes the responsibility and cost of managing a data center out of the hands of businesses and maintains a massive global network of Amazon data centers that split customer traffic among them. AWS currently has 34 geographic regions, each of which have multiple availability zones which themselves contain multiple data centers. These data centers are in undisclosed locations for security reasons, though their general position is published. AWS offers services for virtual machines, cloud storage, database management, machine learning, IoT services, cloud networking, and much more.

Amazon Elastic Compute Cloud, or EC2, is an AWS service that allows customers to create virtual machines in the AWS cloud. These machines are very versatile, as they can be allocated as many or as few resources (CPU, RAM, GPU) as needed and can run nearly any operating system. By default, EC2 instances will run Amazon Linux, which is a version of Linux optimized for AWS servers. Amazon's e-commerce platform, its primary source of revenue, has been running on EC2 instances for over a decade. EC2 instances have a variety of different types, which are optimized for different purposes such as memory (R series, X series), compute (C series), and storage (H series, I series, D series).

Amazon Virtual Private Cloud, or VPC, is an AWS service that provides a virtual network inside the AWS cloud. This service allows AWS objects, such as EC2 instances, to communicate with each other. In a VPC, each EC2 machine is assigned a unique private IPv4 address, which is then connected via NAT to a public address on an internet gateway. Using this gateway, machines in the VPC can communicate with other AWS VPCs and other Internet-connected machines. Amazon VPC is provided at no additional charge to customers using EC2 instances.

Amazon Identity and Access Management, or IAM, is an AWS service that provides a layer of security to customers by limiting the resources different users can access. IAM follows the principle of least privilege, meaning that by default, all AWS controls are blocked for users unless they have been explicitly granted permissions. IAM represents a portion of the customer responsibilities in the AWS shared responsibility model, which is a model outlining that AWS is responsible for the physical security of data centers and networks while the customer is responsible for keeping their customer data and configurations safe. One of IAM's unique features is its role feature, which creates identities with elevated permissions that can be temporarily assigned to users. This feature works similarly to the "sudo" command in unix-based operating systems.

Amazon Elastic Block Store, or EBS, is an AWS service that allows virtual block-level storage to be attached to an EC2 instance. These drives can be formatted with any number of different file systems, such as ext3, ext4 (used with Linux), NTFS (used with Windows), and APFS (used with macOS). Depending on the partitioning scheme, EBS drives can be up to 16 tebibytes in size. EBS Volumes come as either solid-state or hard disk storage, with SSDs coming in high-performance IOPS and general-purpose GP variants, and HDDs coming in throughput-optimized (ST) and cold low-cost (SC) variants. EBS volumes are set up in a way that ensures redundancy, meaning that component failure in AWS data centers doesn't result in data loss for the customer.

A relational database is a type of database that stores information in terms of keys and values. A value is a specific data point that can be accessed by referencing its corresponding key. Relational databases can be divided further into any number of different tables. Amazon Relational Database Service, or RDS, is an AWS service that allows relational databases to be created and managed in the AWS cloud. RDS supports several database types, such as MySQL, Oracle Database, MariaDB, PostgreSQL, and Microsoft SQL Server. Amazon also offers their own database type, Aurora, which is compatible with MySQL and optimized for performance and availability. RDS databases can also be deployed across multiple availability zones, which can optionally create multiple instances of an RDS database in different locations.

AWS Elastic Load balancing, or ELB, is an AWS service that automatically balances traffic across multiple devices in the AWS cloud. It is often used in conjunction with EC2 instances. This service creates more consistency in how AWS resources are distributed, which ensures a more stable experience for end users.

AWS Auto Scaling is an AWS service that allows applications to automatically be created or deleted based on a variety of targets, such as CPU utilization or bandwidth. This service facilitates scalability of cloud computing services and adapts AWS

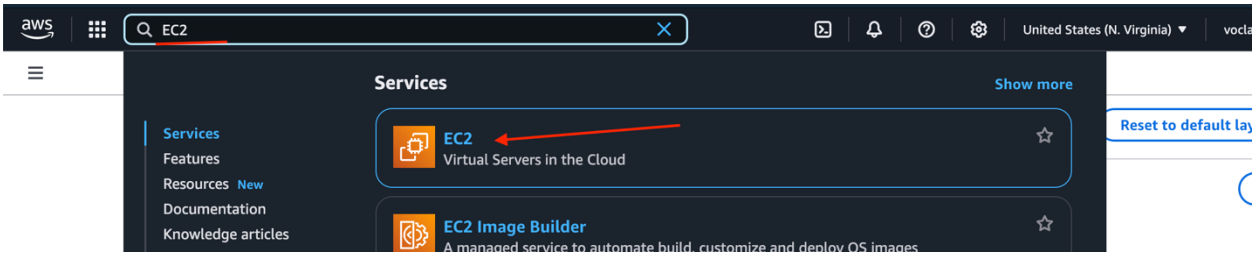
resources to better fit the needs of customers at any given time. This service is also economical for AWS users as it allows them to pay only for resources required for any given moment in time. Auto Scaling can automatically create and delete resources, EC2 instances, DynamoDB databases, and Aurora RDS databases.

Lab Summary

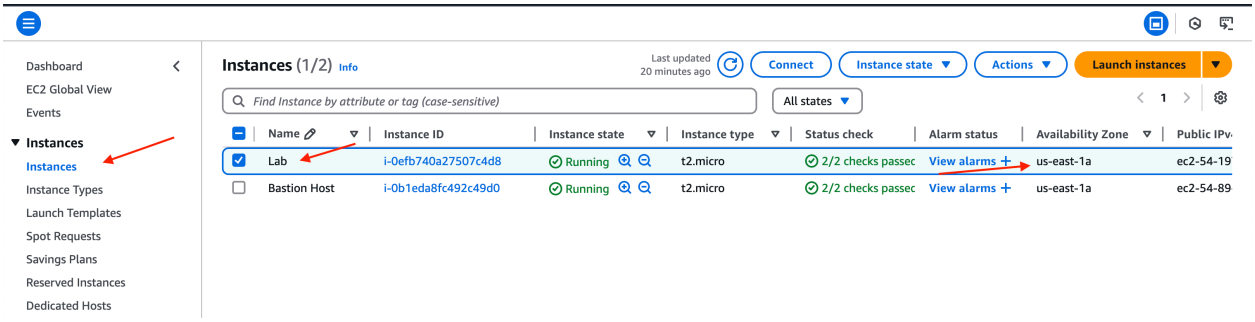
This write-up covers three different AWS labs. The first lab involves creating an EBS volume, attaching it to an EC2 instance, instantiating a new file system on the volume, then creating and restoring a snapshot of the volume. The second lab involves building and launching an RDS address book database, connecting it to a pre-existing web server, then manipulating the database with a web server GUI. The third lab involves creating a load balancer and auto scaling group based on an EC2 instance AMI, then testing the auto scaling feature by simulating excess CPU usage.

Lab Commands (EBS)

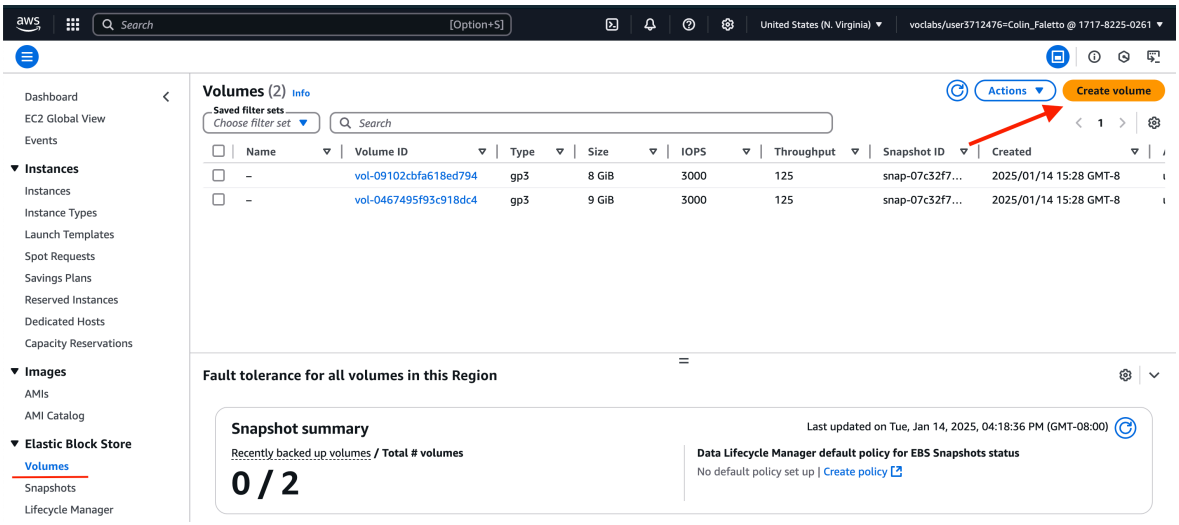
From the AWS search bar, type in and launch “EC2”.



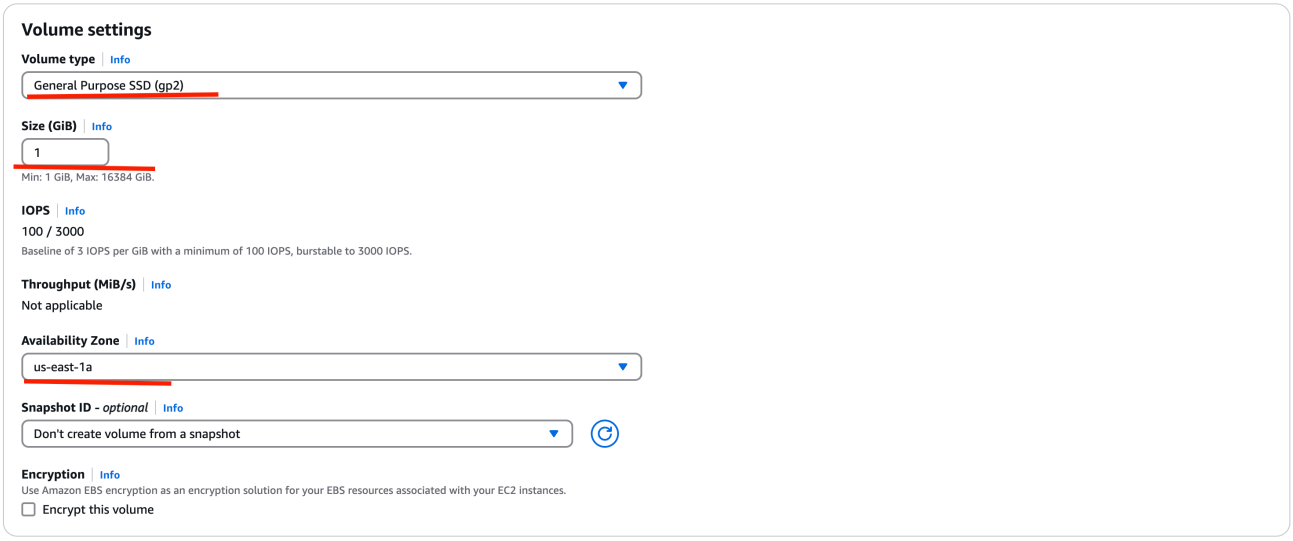
From the Instances tab, make sure that the EC2 instance named “Lab” has been created. Make sure to write down the EC2 instance’s availability zone, which is “us-east-1a” in this case.



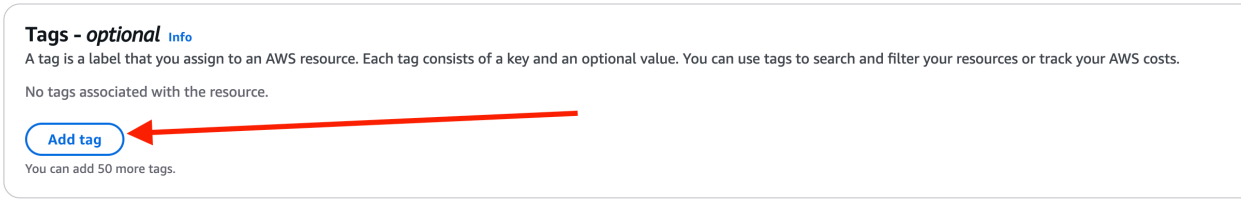
Go to the “Volumes” section and click “Create Volume”.



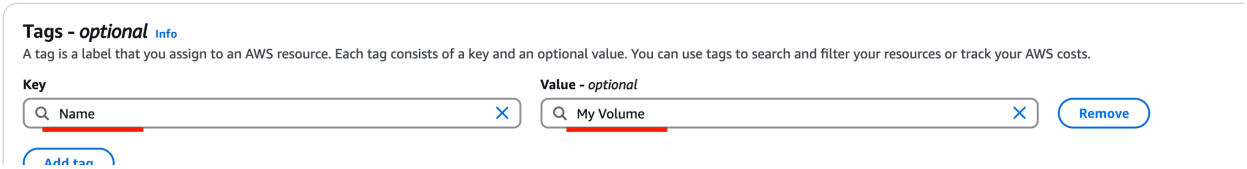
Set the volume type to “gp2”, the size to 1 gigabyte, and the availability zone to the same zone as the Lab instance.



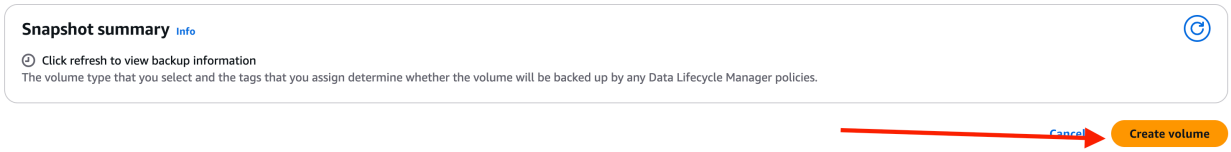
Under “Tags”, click “Add Tag”.



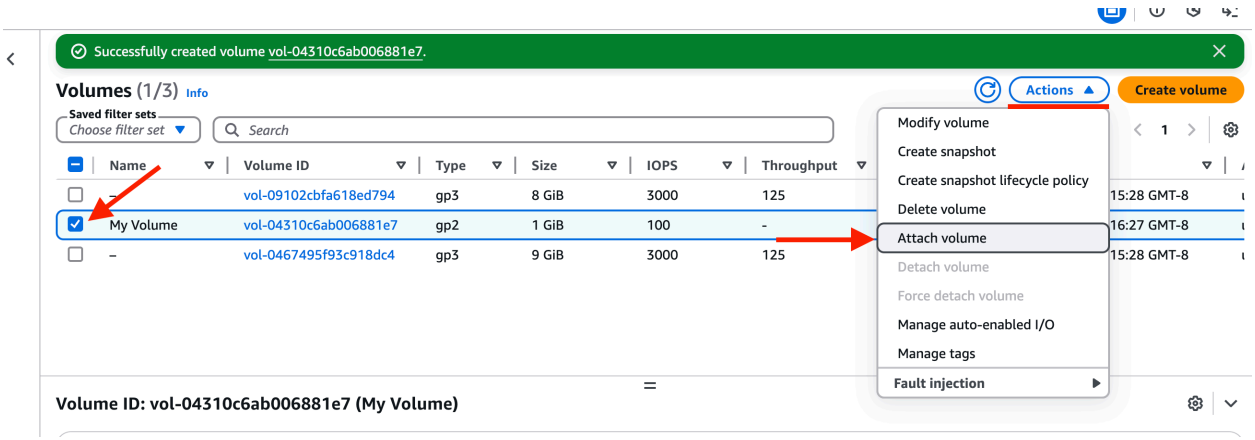
Set the key to “Name” and the value to “My Volume”.



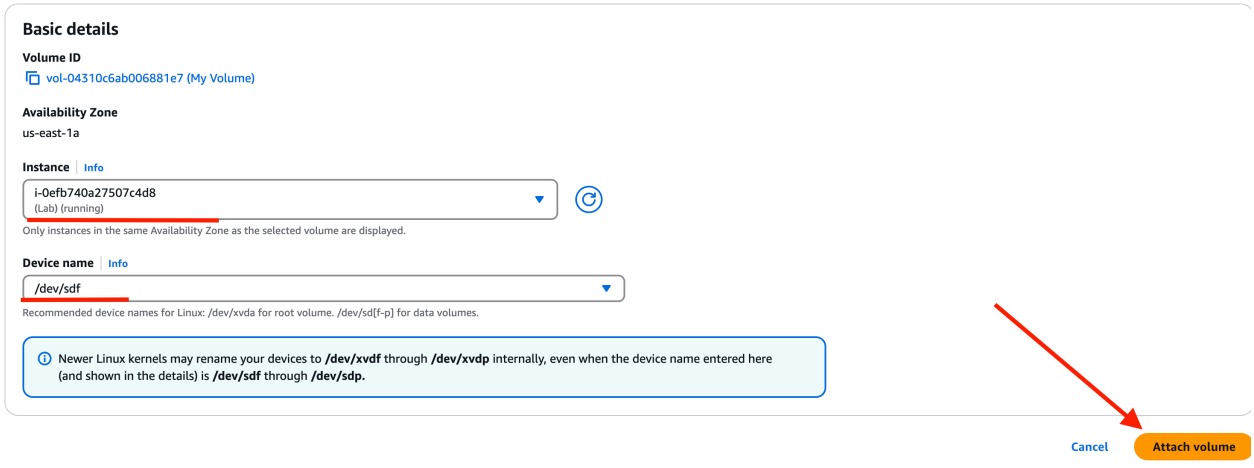
Click “Create Volume”.



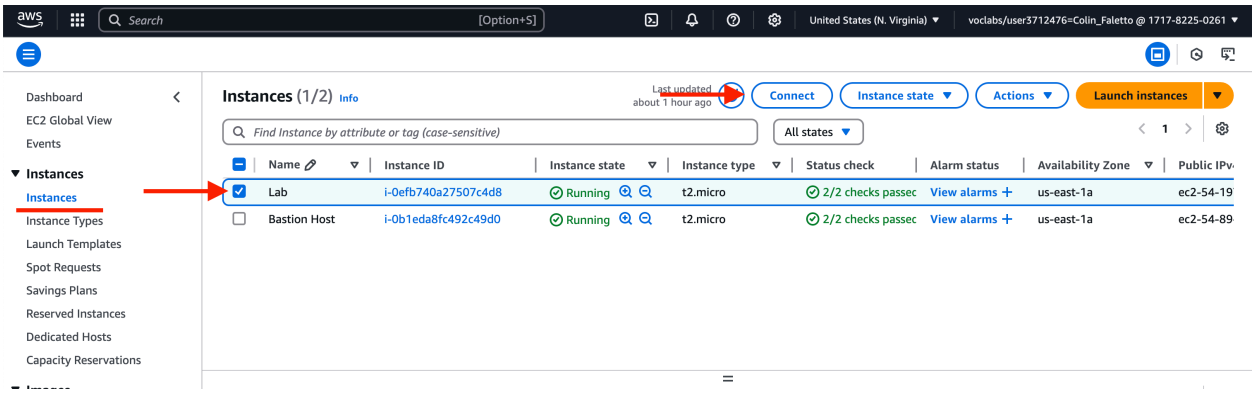
You should now be redirected to the Volumes page. Click the checkbox next to My Volume, then under Actions, click Attach Volume.



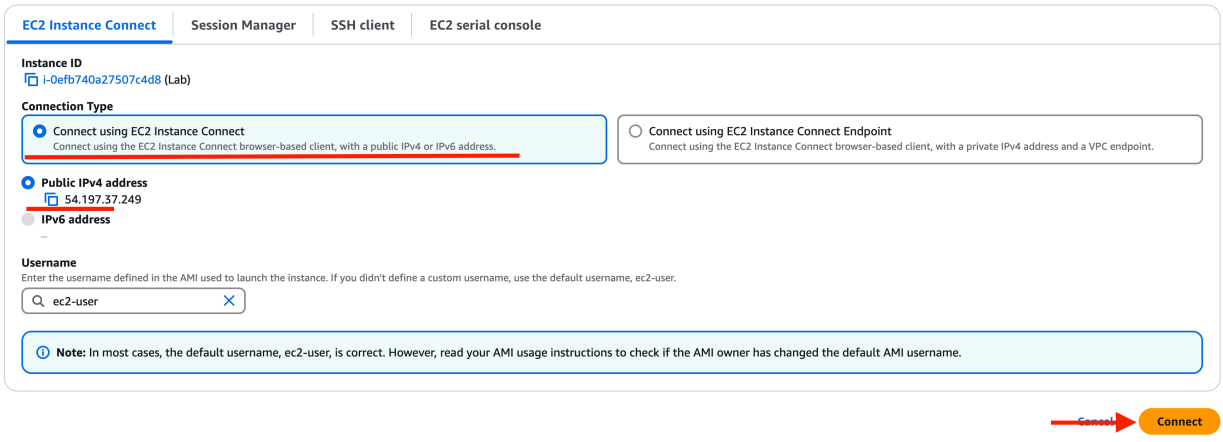
Set the instance to the Lab instance and the device name to /dev/sdf, then click Attach volume.



Go to the “Instances” section, click the checkbox next to “Lab”, and click “Connect”.



Select “EC2 instance connect”, select “Public IPv4 address”, then click “Connect”.



Run the command `df -h` to list the mounted volumes; you should see output like this:

```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-1-11-198 ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M     0  4.0M   0% /dev
tmpfs           475M     0  475M   0% /dev/shm
tmpfs           190M  452K  190M   1% /run
/dev/xvda1      8.0G  1.6G  6.4G  20% /
tmpfs           475M     0  475M   0% /tmp
/dev/xvda128     10M  1.3M  8.7M  13% /boot/efi
tmpfs            95M     0   95M   0% /run/user/1000
```

Run the command `sudo mkfs -t ext3 /dev/sdf` to create an ext3 file system on the volume you created.

```
[ec2-user@ip-10-1-11-198 ~]$ sudo mkfs -t ext3 /dev/sdf
mke2fs 1.46.5 (30-Dec-2021)
Creating filesystem with 262144 4k blocks and 65536 inodes
Filesystem UUID: d545580a-928e-4063-ad5d-bda7ee246ba3
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done
```

Run the command `sudo mkdir /mnt/data-store` to create a new folder at /mnt/data-store.

```
[ec2-user@ip-10-1-11-198 ~]$ sudo mkdir /mnt/data-store
```

Run the command `sudo mount /dev/sdf /mnt/data-store` to mount your volume at the created folder.

```
[ec2-user@ip-10-1-11-198 ~]$ sudo mount /dev/sdf /mnt/data-store
```

Run the command `echo "/dev/sdf  /mnt/data-store ext3 defaults,noatime 1 2" | sudo tee -a /etc/fstab` to add this mount binding to /etc/fstab, a file that automatically mounts volumes at startup.

```
[ec2-user@ip-10-1-11-198 ~]$ echo "/dev/sdf  /mnt/data-store ext3 defaults,noatime 1 2" | sudo tee -a /etc/fstab
```

Run the command `cat /etc/fstab` to confirm that the line was added.

```
[ec2-user@ip-10-1-11-198 ~]$ cat /etc/fstab
#
UUID=73e034f4-2887-4ec9-8b40-0d35c0091a37     /           xfs    defaults,noatime  1   1
UUID=9F37-3C35      /boot/efi       vfat    defaults,noatime,uid=0,gid=0,umask=0077,shortname=winnt,x-systemd.automount 0 2
/dev/sdf   /mnt/data-store ext3 defaults,noatime 1 2
```

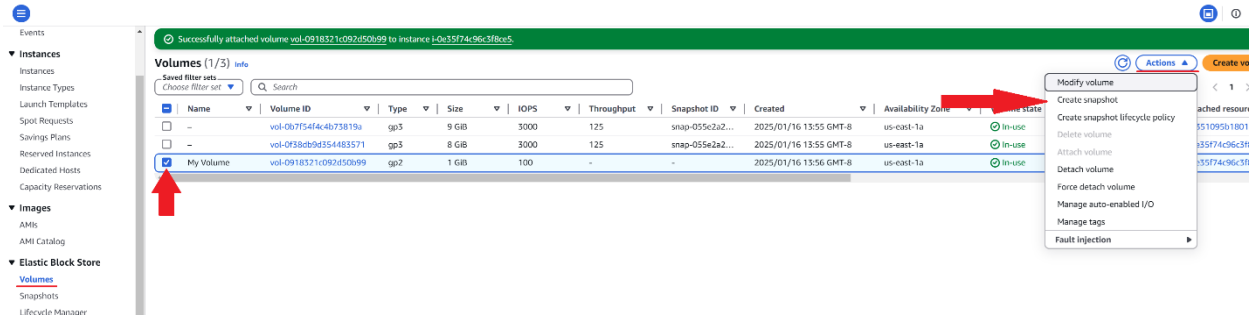
Run the command `sudo sh -c "echo some text has been written > /mnt/data-store/file.txt"` to create a file with the text “some text has been written” at the specified location.

```
[ec2-user@ip-10-1-11-50 ~]$ sudo sh -c "echo some text has been written > /mnt/data-store/file.txt"
```

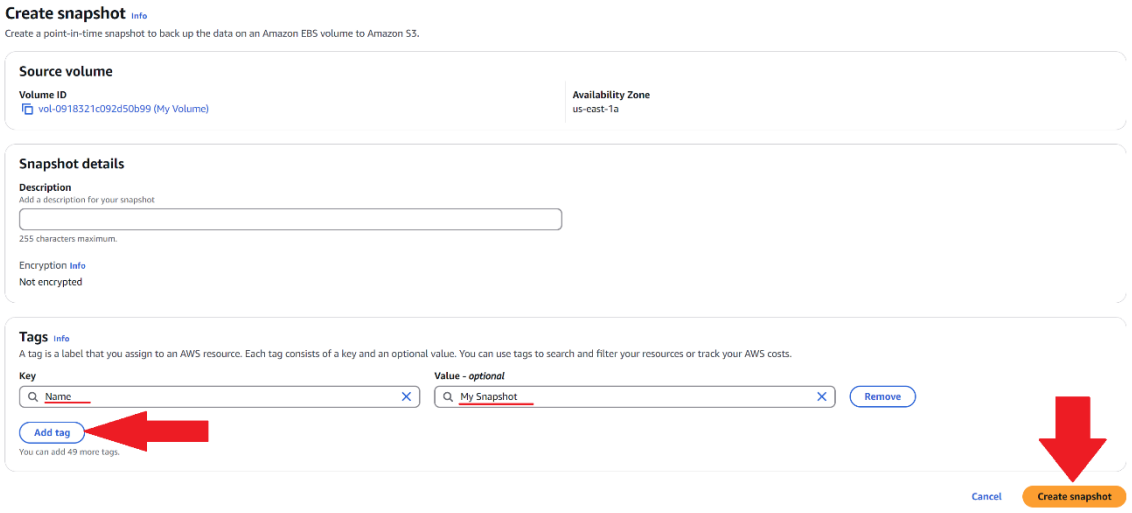
Run the command `cat /mnt/data-store/file.txt` to confirm that the file was written.

```
[ec2-user@ip-10-1-11-50 ~]$ cat /mnt/data-store/file.txt
some text has been written
```

Go back to the main AWS console tab. Under Volumes, check My Volume, then click Actions > Create Snapshot.



Under Tags, click Add Tag, set the key to Name, set the value to My Snapshot, then click Create Snapshot.



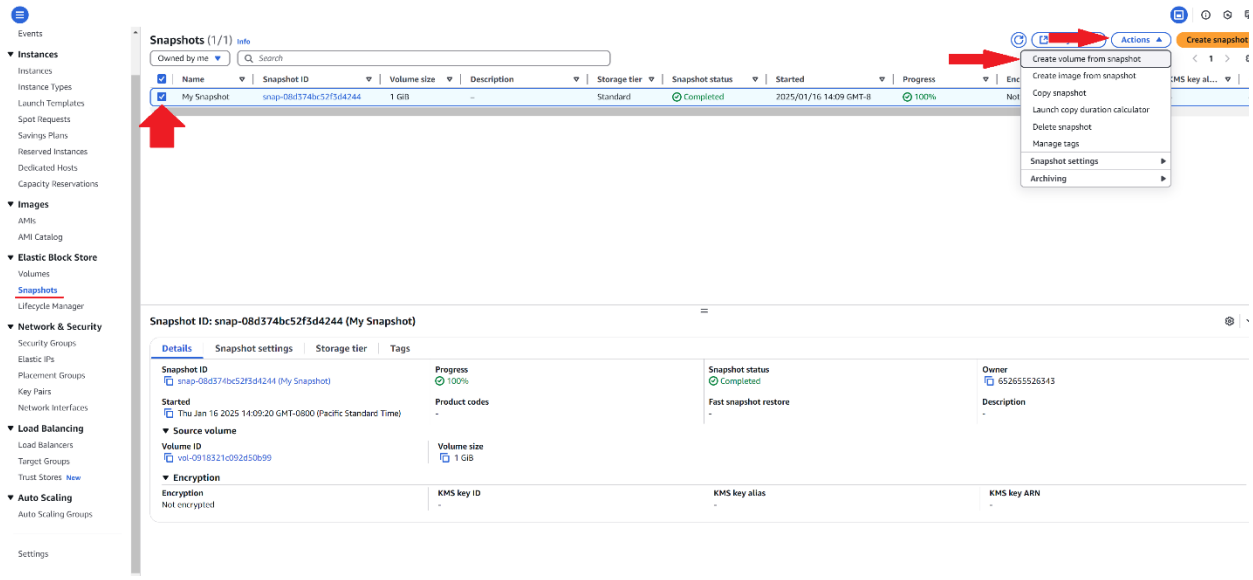
Switch back to the console and run the command `sudo rm /mnt/data-store/file.txt` to remove the file you created earlier.

```
[ec2-user@ip-10-1-11-50 ~]$ sudo rm /mnt/data-store/file.txt
```

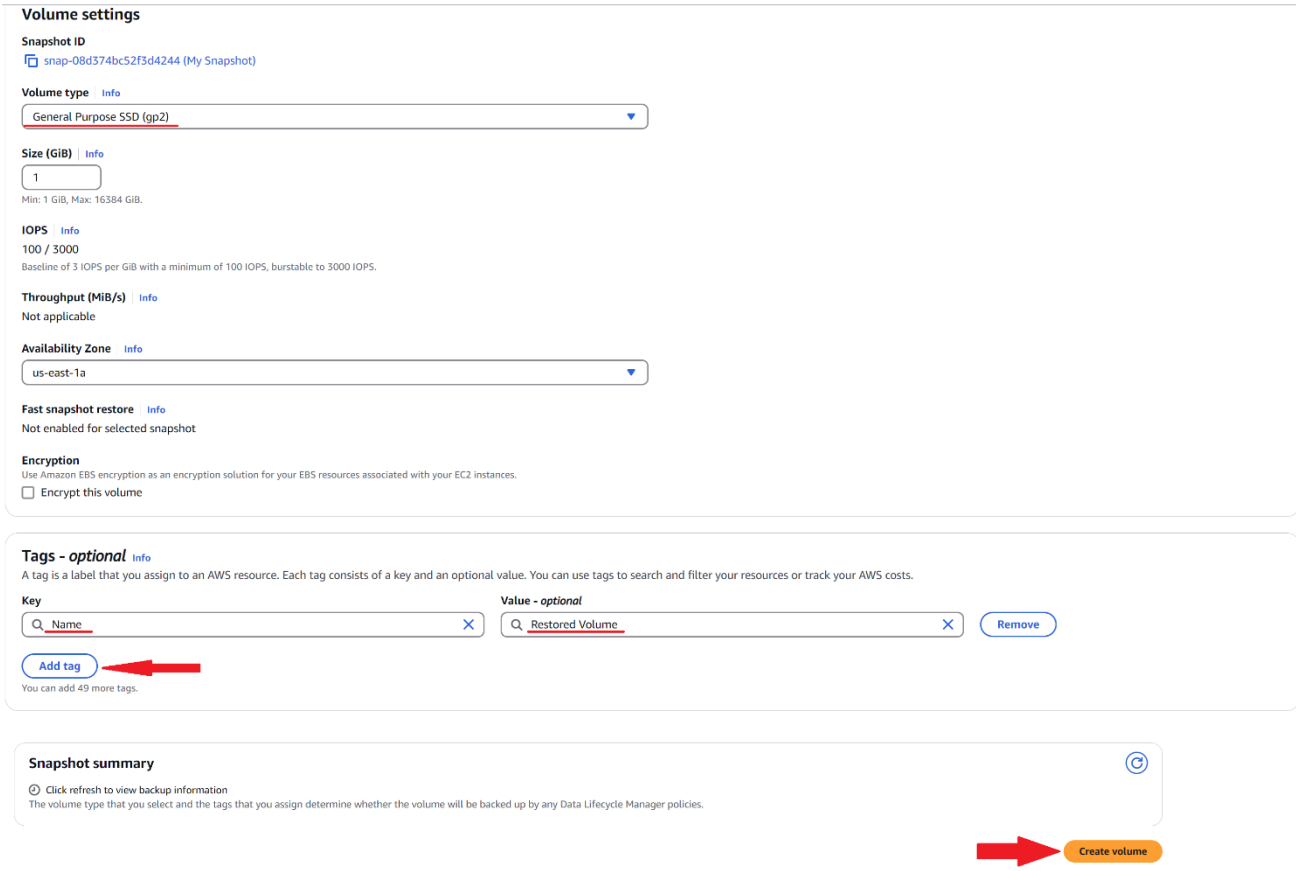
Run the command `ls /mnt/data-store` to confirm that the file has been deleted.

```
[ec2-user@ip-10-1-11-50 ~]$ ls /mnt/data-store
lost+found      no mention of file.txt
```

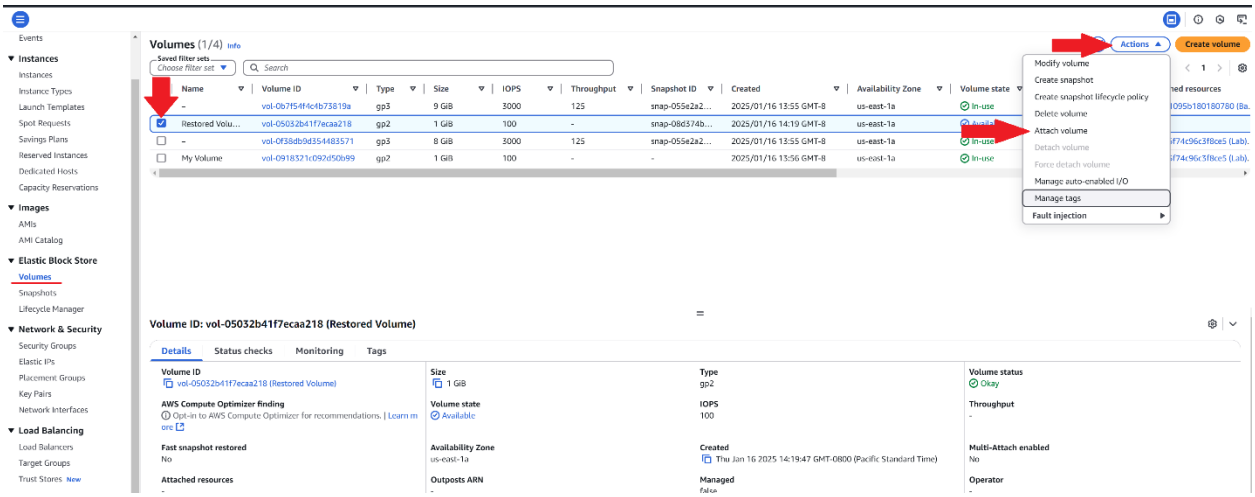
Back in the AWS console, go to Snapshots > Check My Snapshot > Actions > Create volume from snapshot.



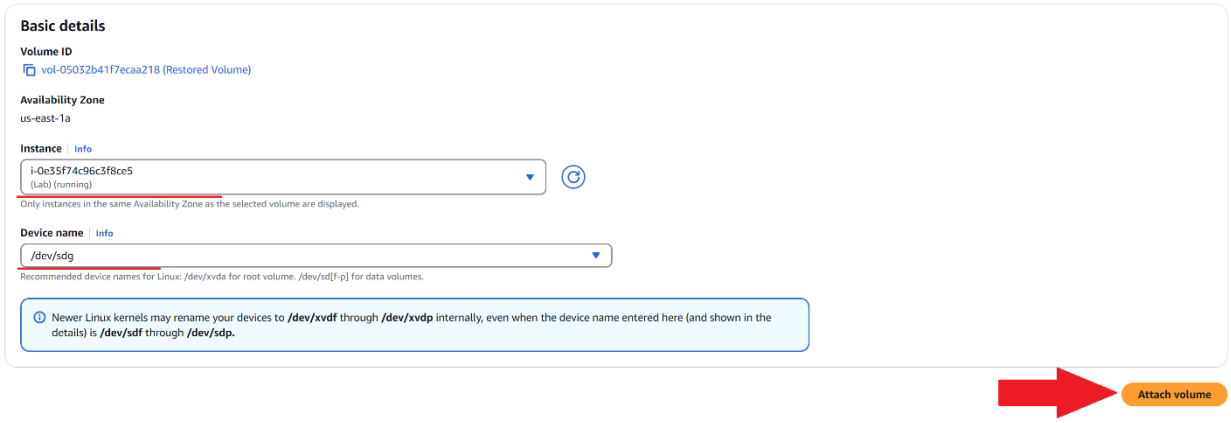
Set the volume type to gp2 (everything else should be correct by default), then click Add Tag, set the key to Name, set the value to Restored Volume, then click Create Volume.



Under Volumes, check Restored Volume, then click Actions > Attach Volume



Set the instance to Lab, the device name to /dev/sdg, then click Attach Volume.



Run the command `sudo mkdir /mnt/data-store2` to make a new folder for the restored drive.

```
[ec2-user@ip-10-1-11-50 ~]$ sudo mkdir /mnt/data-store2
```

Run the command `sudo mount /dev/sdg /mnt/data-store2` to mount the restored volume at the specified point.

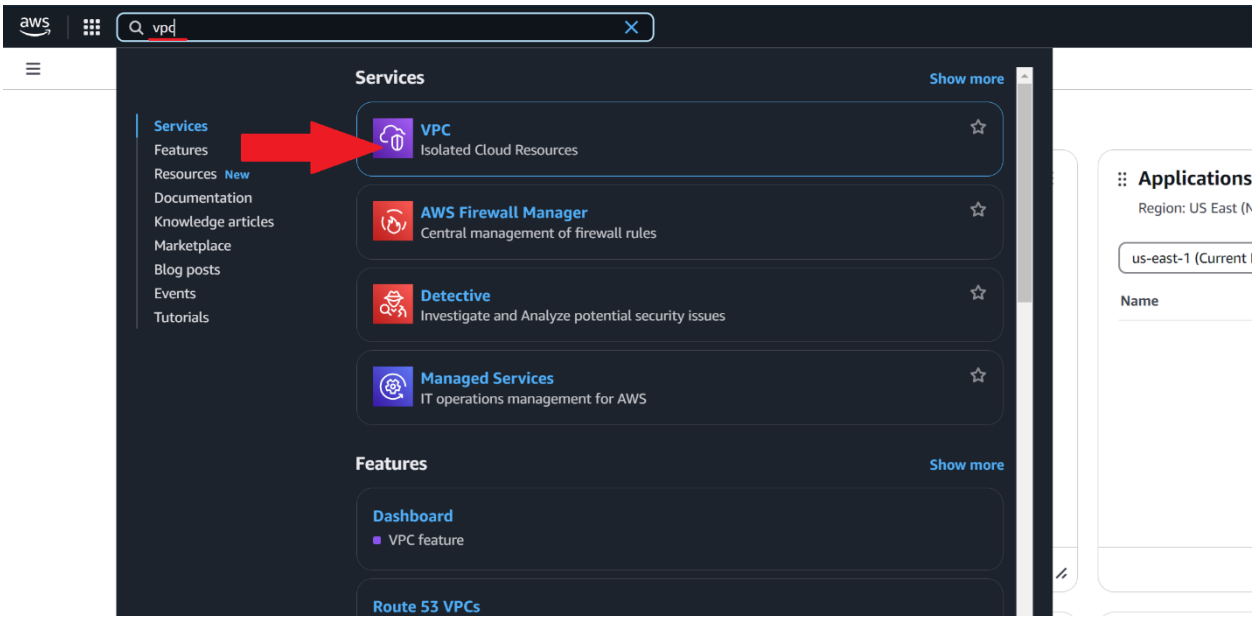
```
[ec2-user@ip-10-1-11-50 ~]$ sudo mount /dev/sdg /mnt/data-store2
```

Run the command `ls /mnt/data-store2/` and ensure that file.txt shows up.

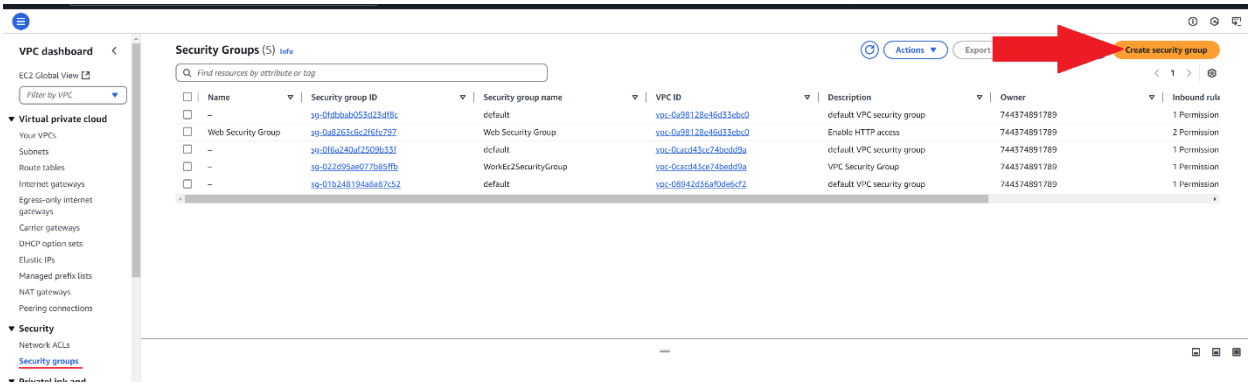
```
[ec2-user@ip-10-1-11-50 ~]$ ls /mnt/data-store2/
file.txt  lost+found
```

Lab Commands (RDS)

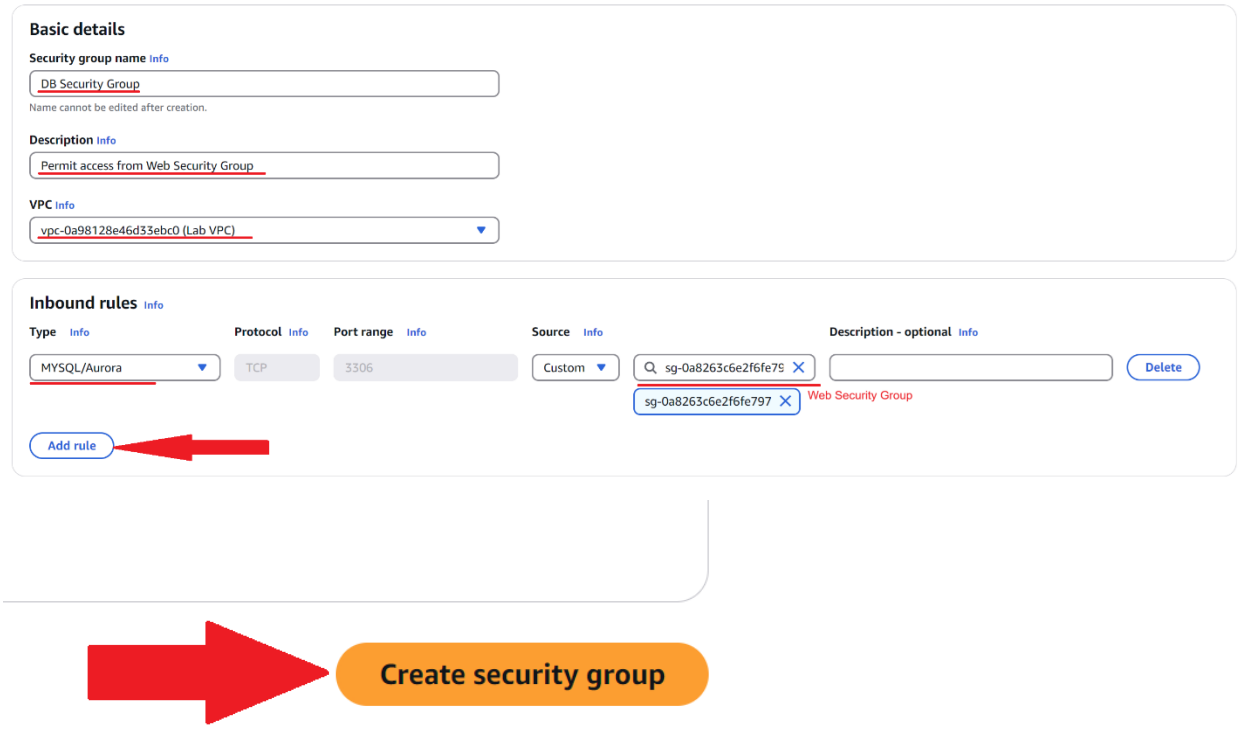
From the AWS console search bar, open VPC.



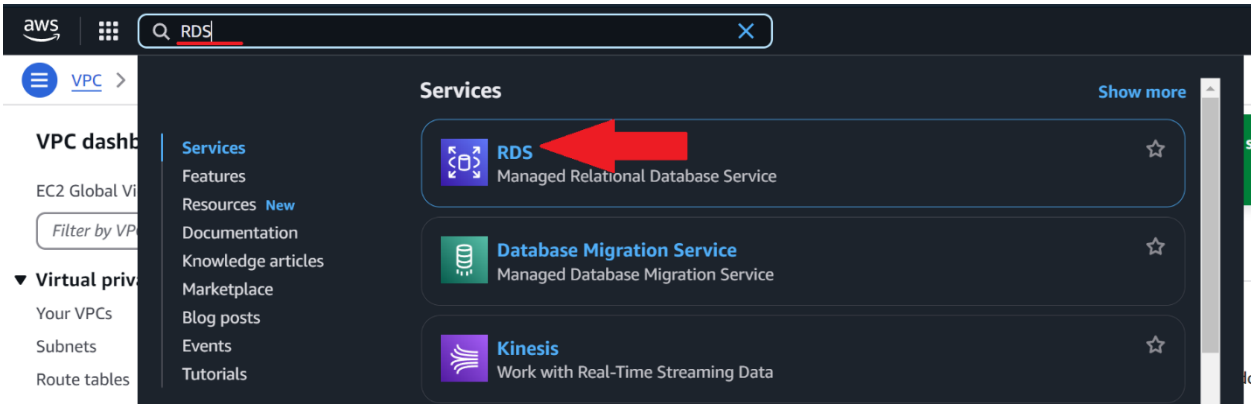
Under Security Groups, click Create Security Group.



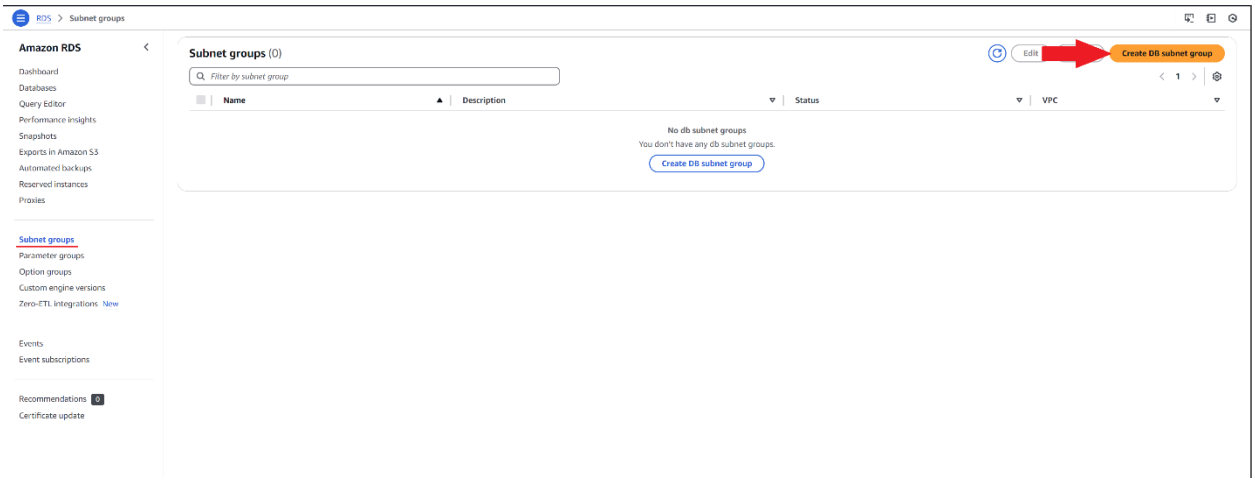
Set the name to DB Security Group, the description to Permit access from Web Security Group, and the VPC to Lab VPC. Under Inbound Rules, click Add Rule, set the type to MySQL/Aurora, and set the source to the Web Security Group. Click Create security group.



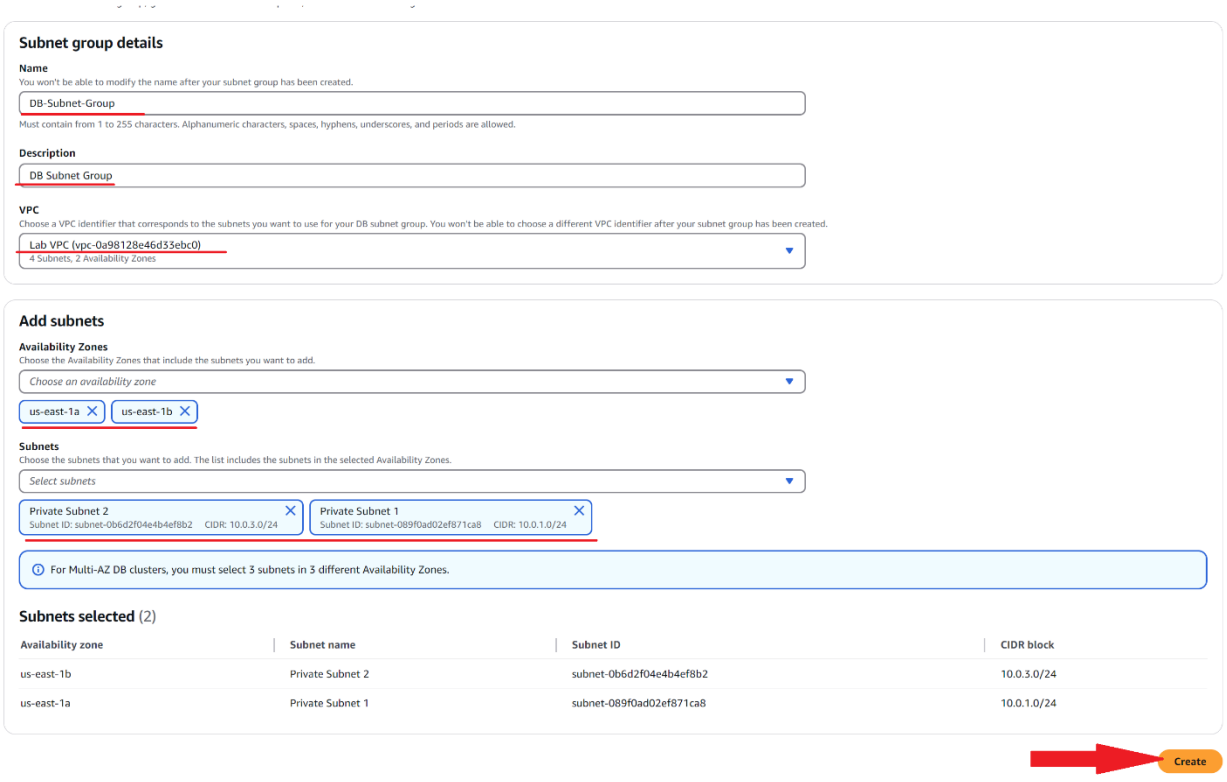
Go to RDS from the search bar.



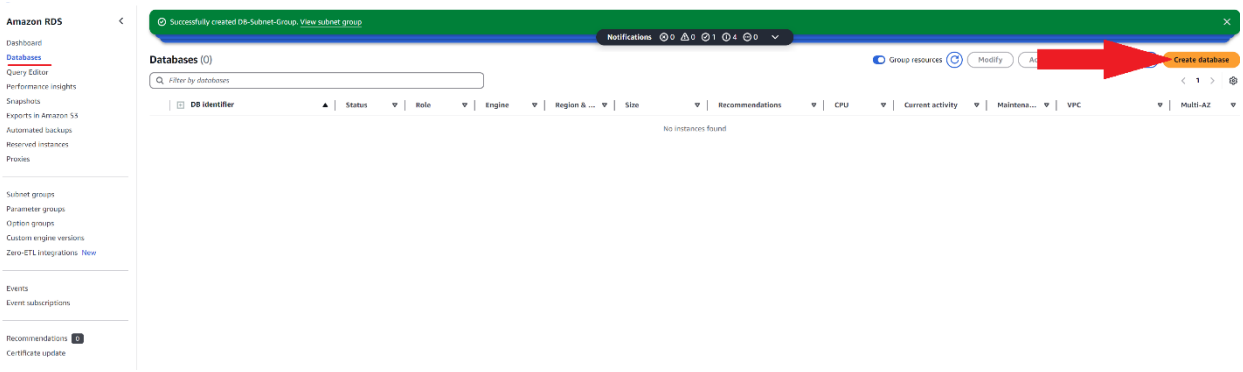
Go to Subnet groups > Create DB Subnet Group.



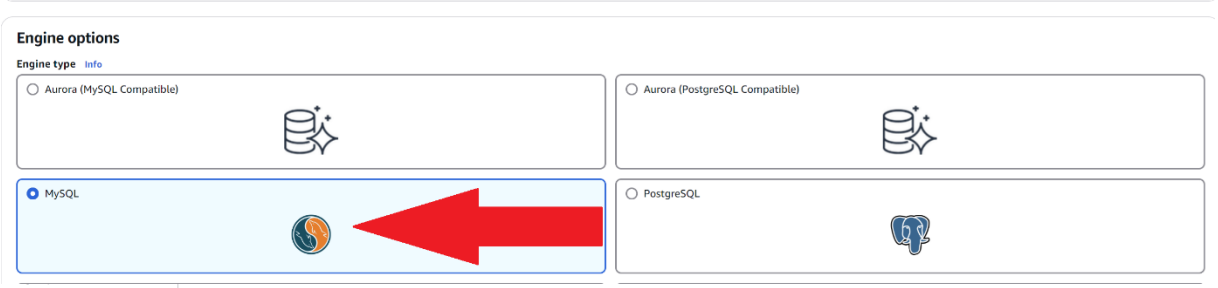
Set the name to DB-Subnet-Group, the description to DB Subnet Group, and the VPC to Lab VPC. Set the availability zones to us-east-1a and us-east-1b, and set the subnets to Private Subnet 1 and Private Subnet 2. Click Create.



Go to Databases > Create Database.

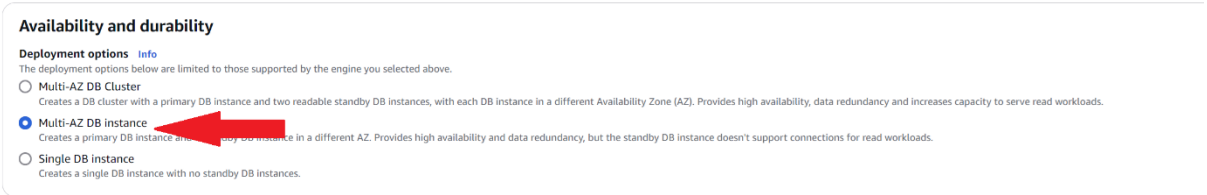


Set the engine type to MySQL.

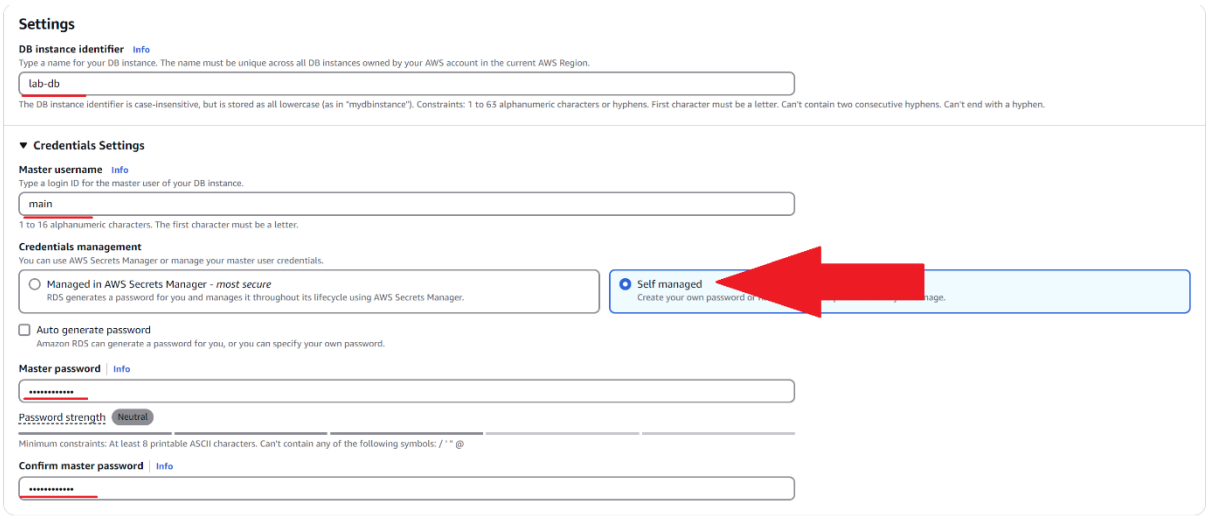


Set the template to Dev/Test.

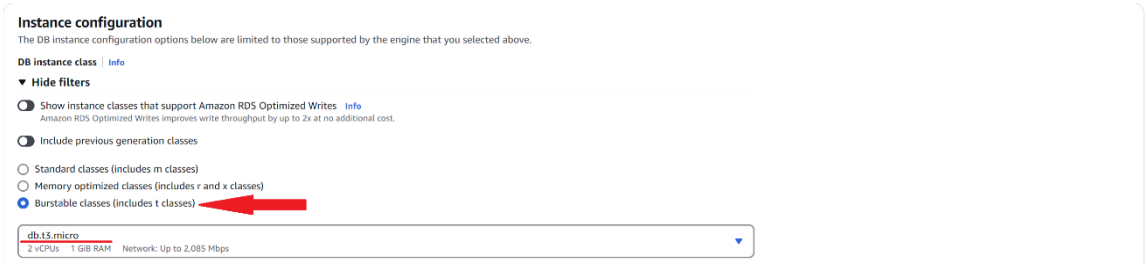
Set the deployment options to Multi-AZ DB instance.



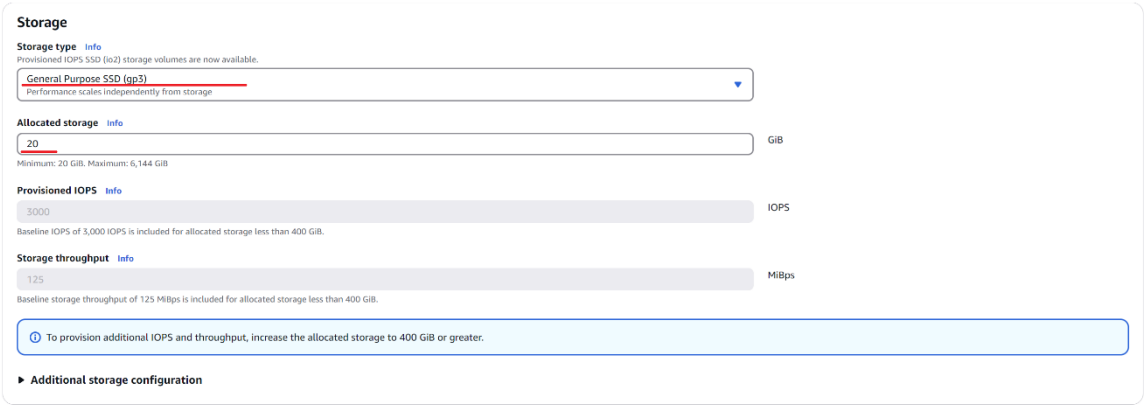
Set the DB instance identifier to lab-db, the master username to main, the credentials management to self-managed, and the master password to lab-password.



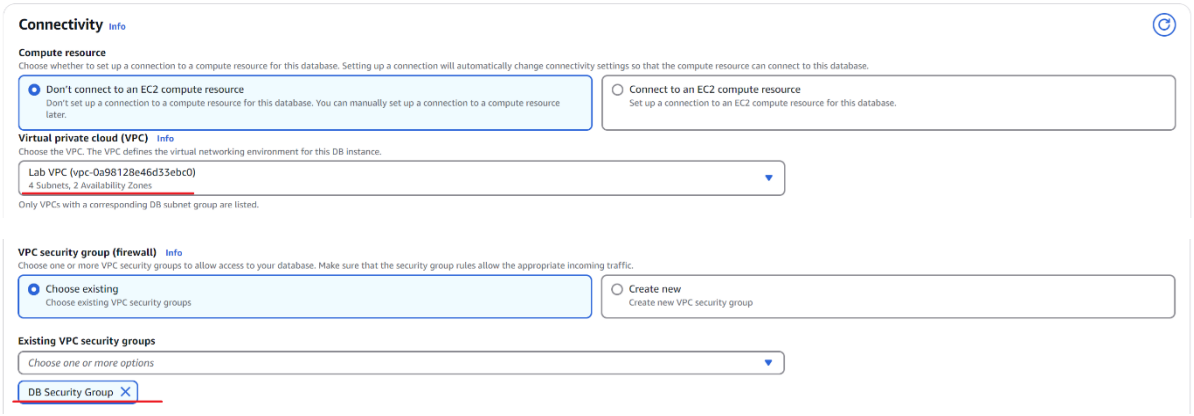
Under Instance configuration, set the instance class to Burstable classes, and select db.t3.micro.



Under storage, set the storage type to General Purpose SSD and the allocated storage to 20 GiB.

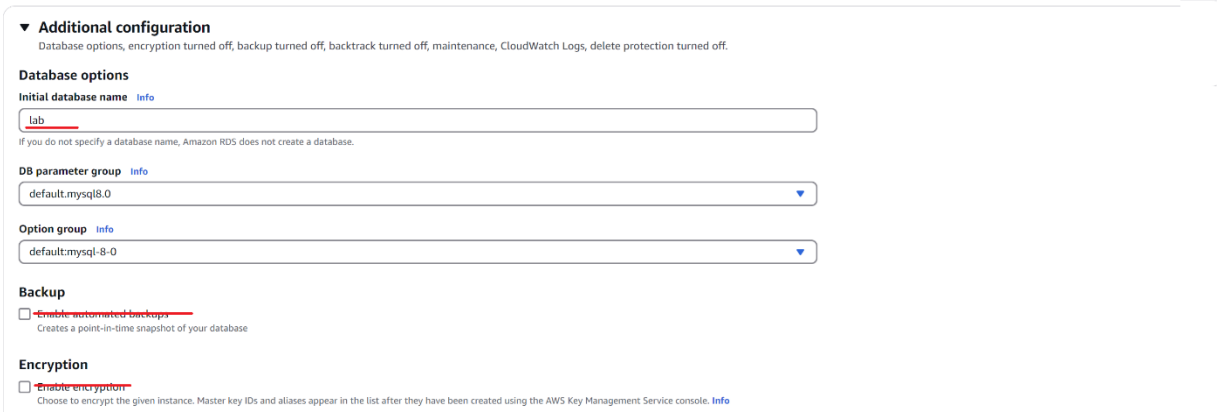


Under connectivity, set the VPC to Lab VPC and set the existing security groups to DB security group.

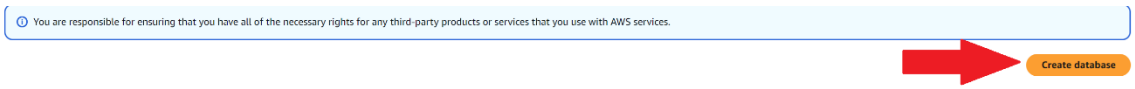


Under monitoring, disable Enhanced monitoring.

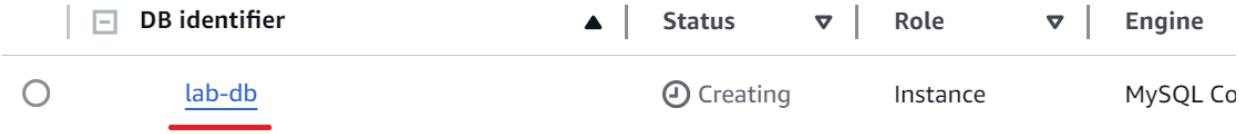
Under additional configuration, set the initial database name to lab, and disable automated backups and encryption.



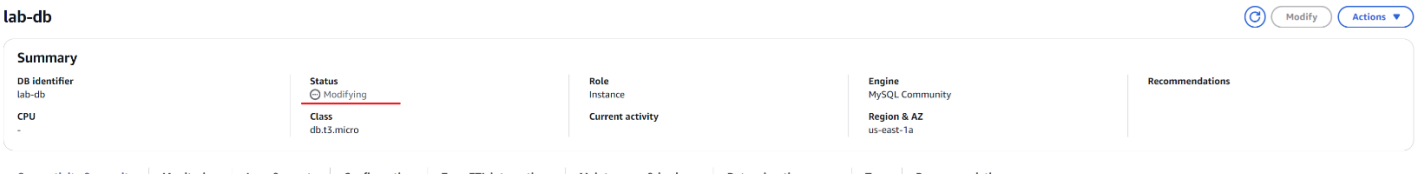
Click create database.



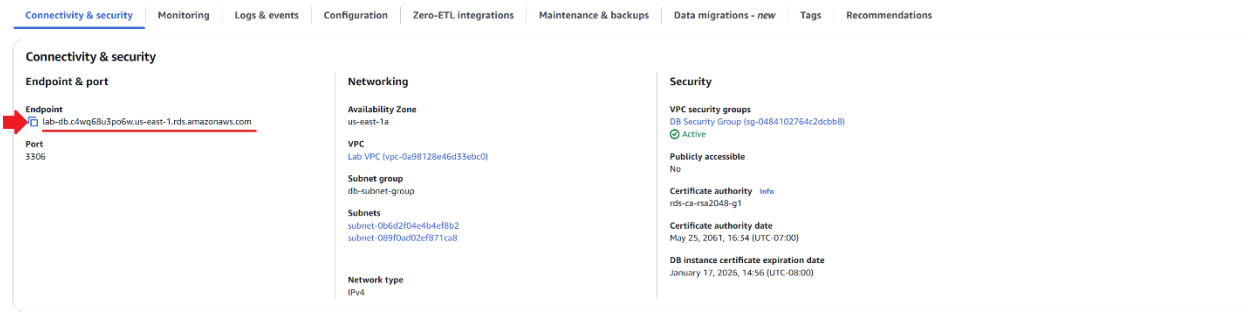
Click on lab-db.



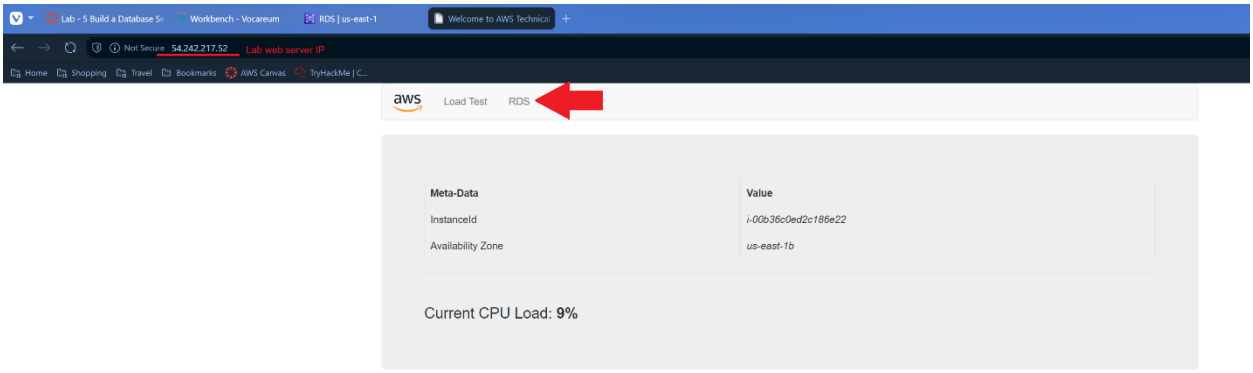
Wait until the status says Modifying or Available



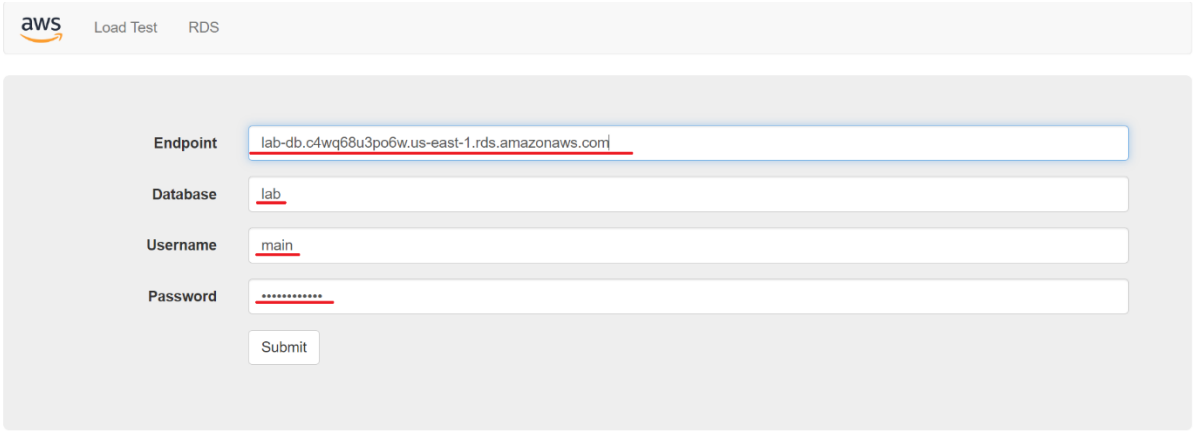
Scroll down to the Connectivity and security seciton and copy the Endpoint value.



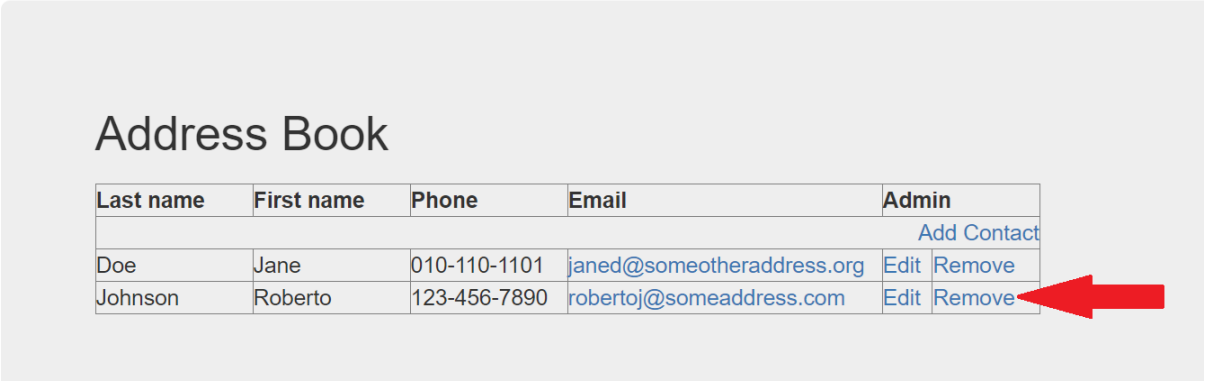
Connect to the Lab's web server IP, and click on RDS.



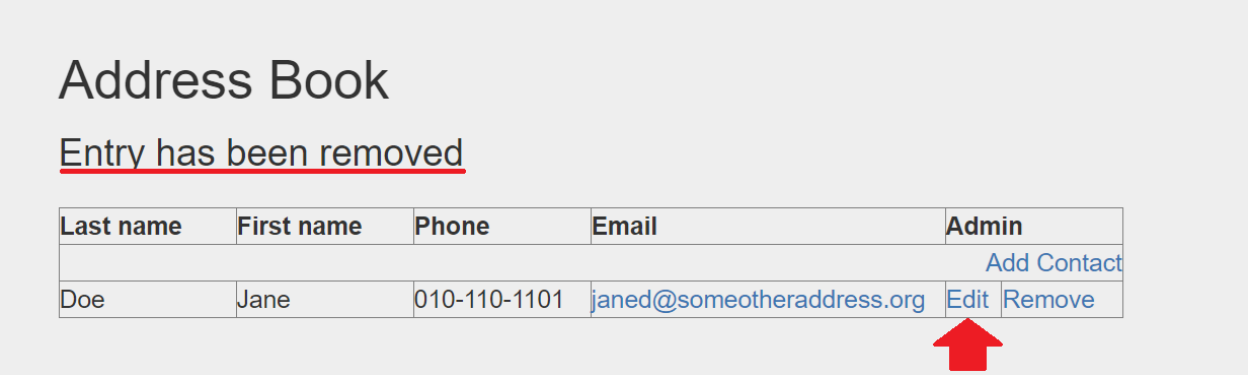
Paste the endpoint URL, and enter the database name, username, and password from earlier.



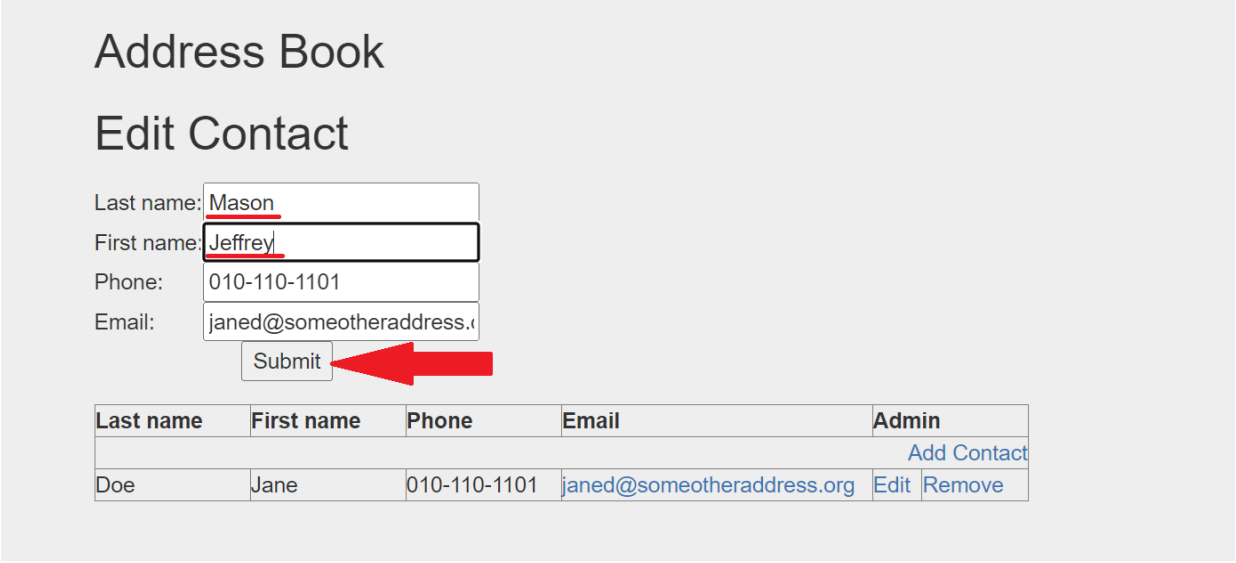
If done correctly, you should see an address book database. Click "Remove" to remove an entry.



You should see a message saying that the entry has been removed. Next, click the "Edit" button next to the remaining entry.

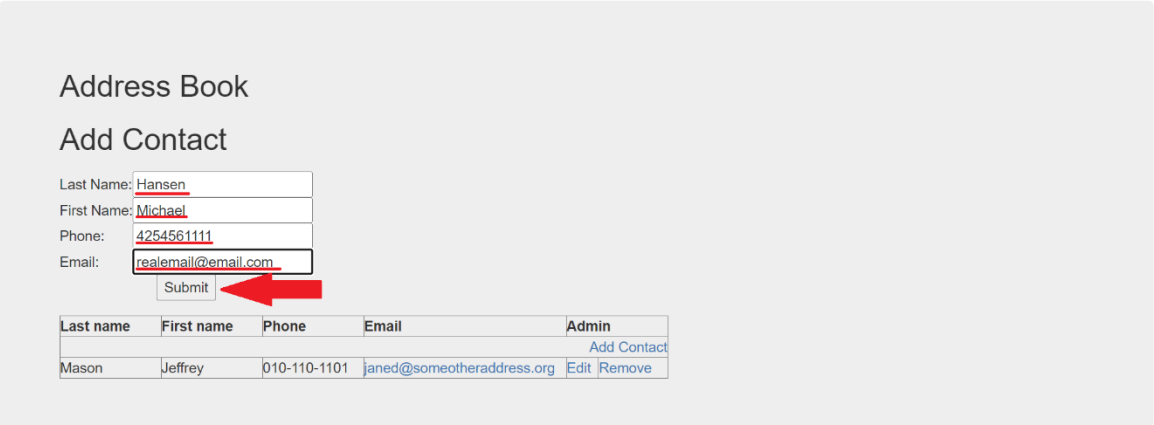


Change the details of the entry and click "Submit".



You should see a success message. Click "Add contact" to add a new contact.

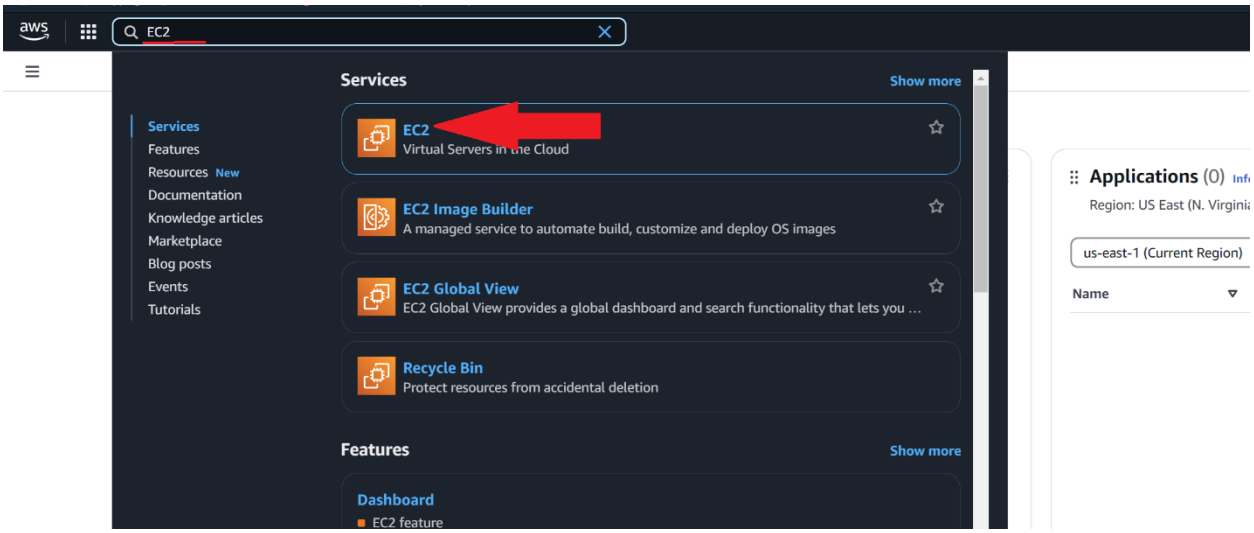
Add some information for the new contact and click “Submit”.



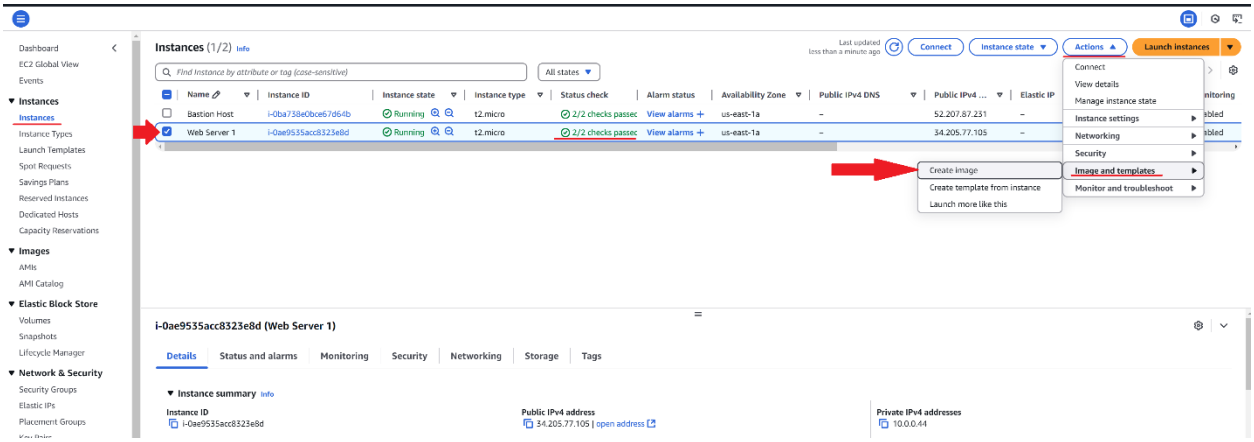
You should see both your newly created and newly modified entry in the address book.

Lab Commands (Auto Scaling)

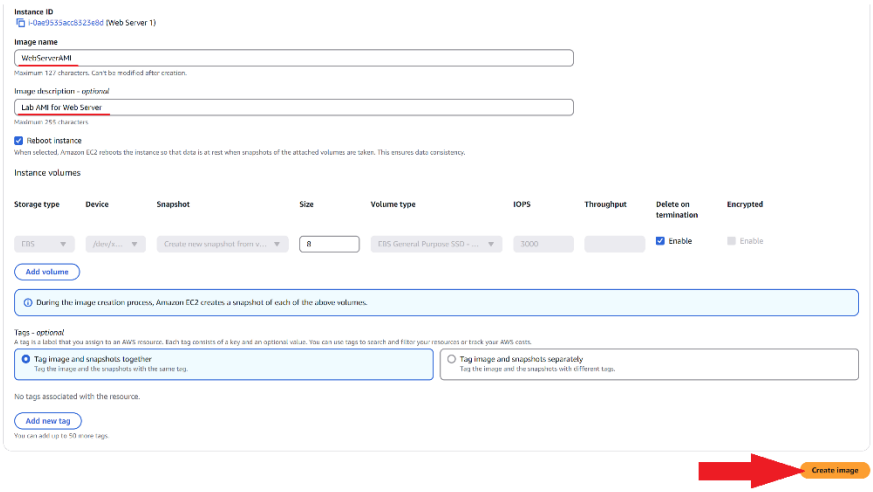
Go to the AWS management console and select “EC2”.



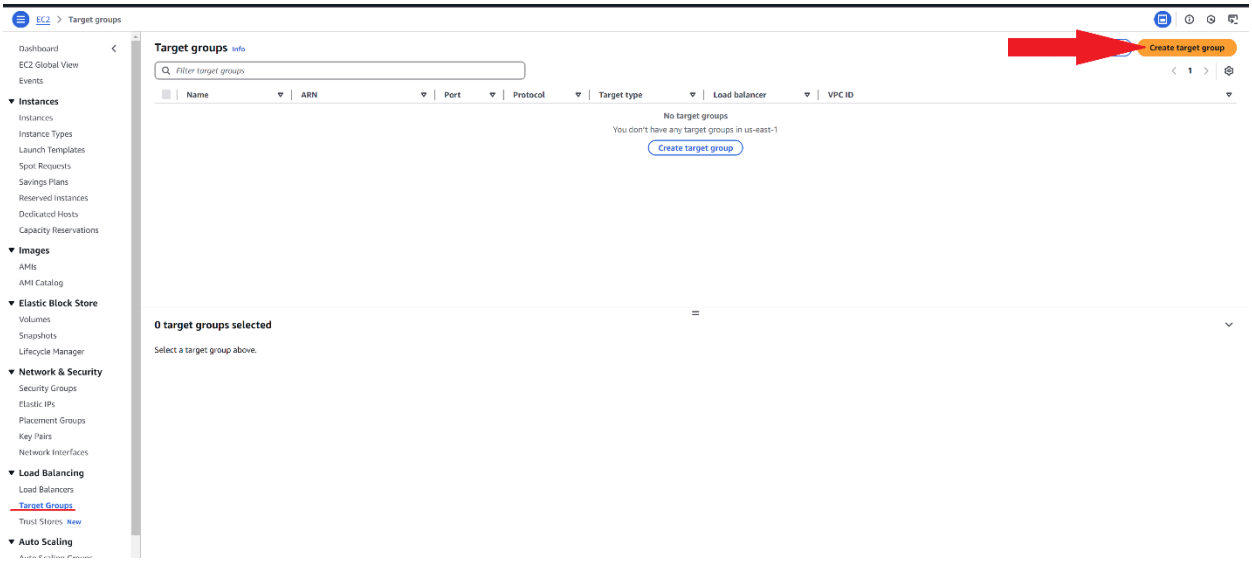
Go to Instances, ensure that Web Server 1's status is 2/2 checks passed, then click on the checkbox next to the web server and click Actions > Image and Templates > Create Image.



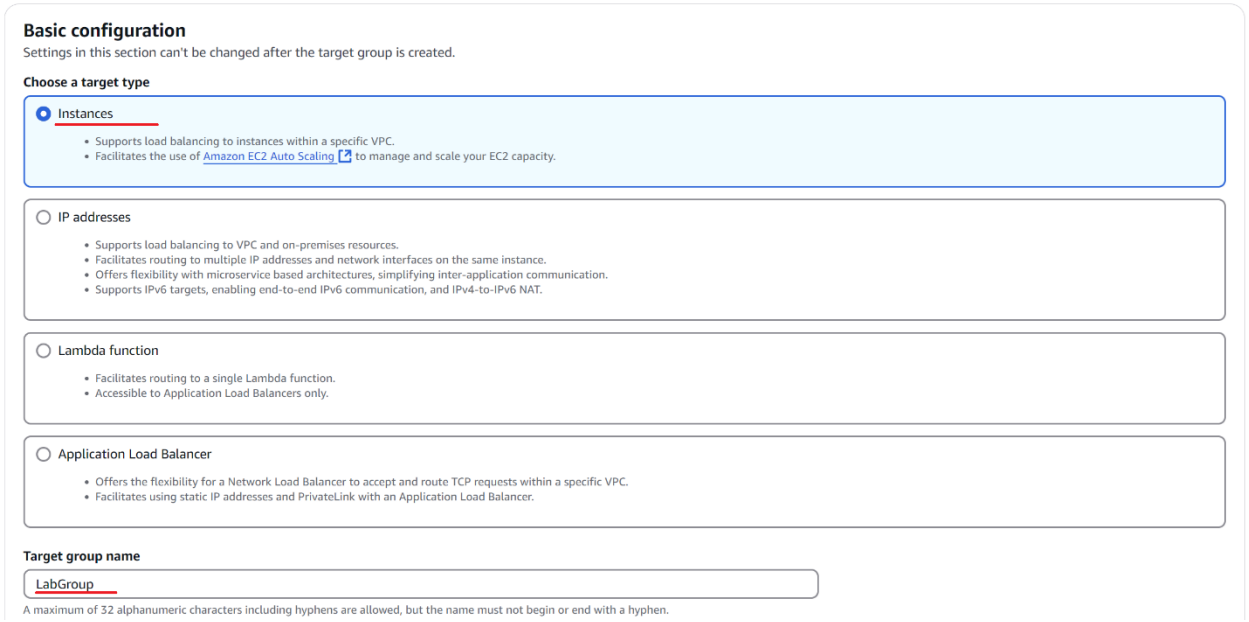
Set the image name to WebServerAMI and the image description to Lab AMI for Web Server, then click Create image.



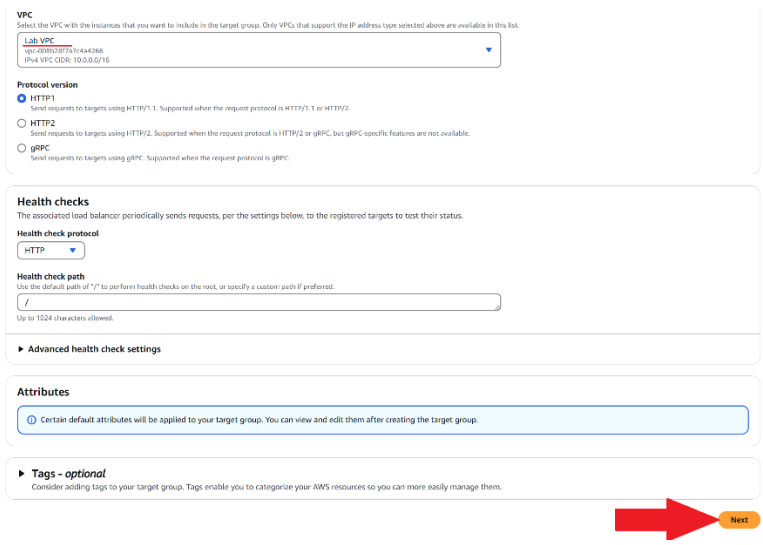
Go to Target Groups > Create target group.



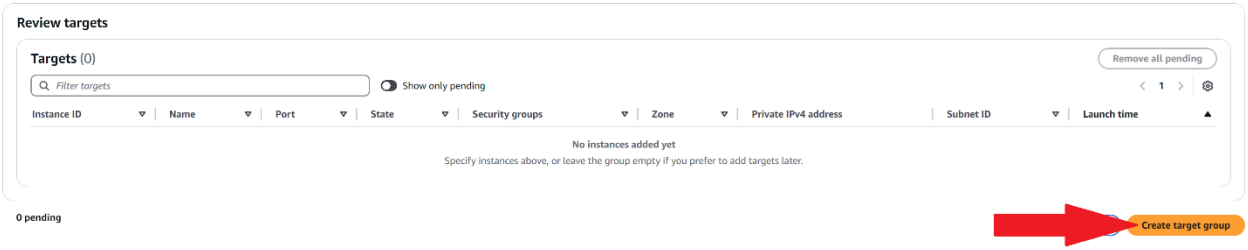
Set the target type to Instances and the target group name to LabGroup.



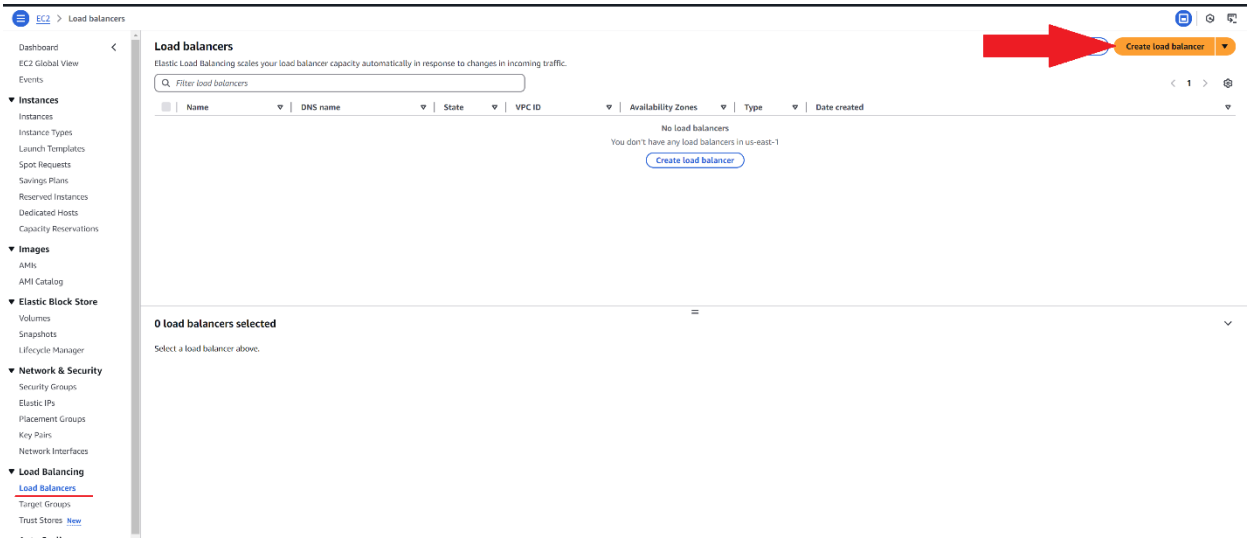
Set the VPC to Lab VPC, then click Next.



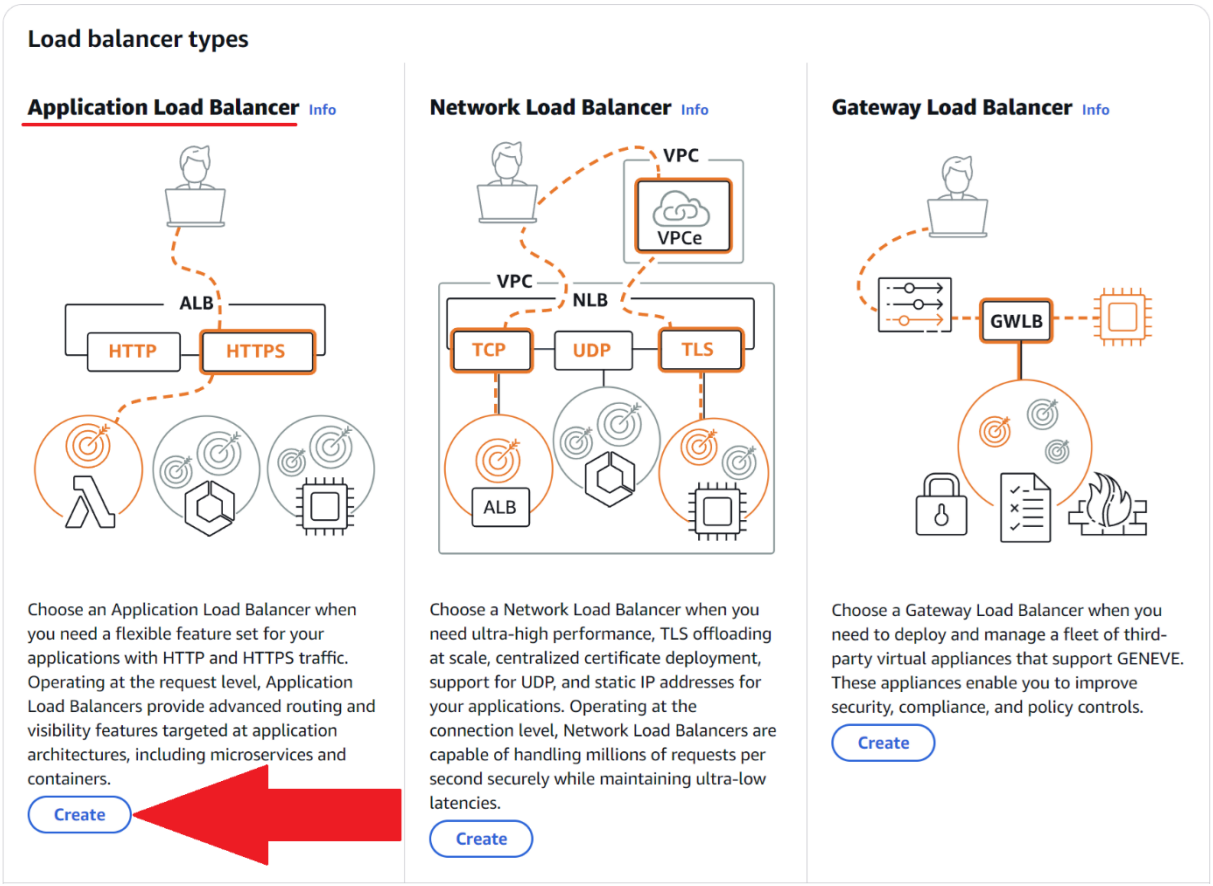
Click “Create target group”.



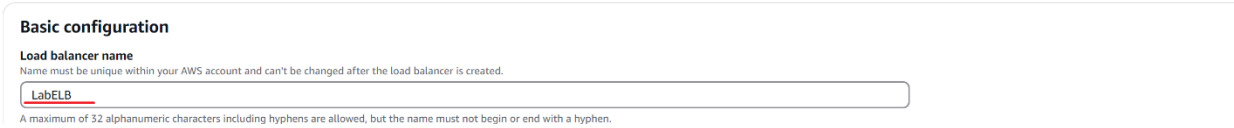
Go to Load Balancers > Create load balancer.



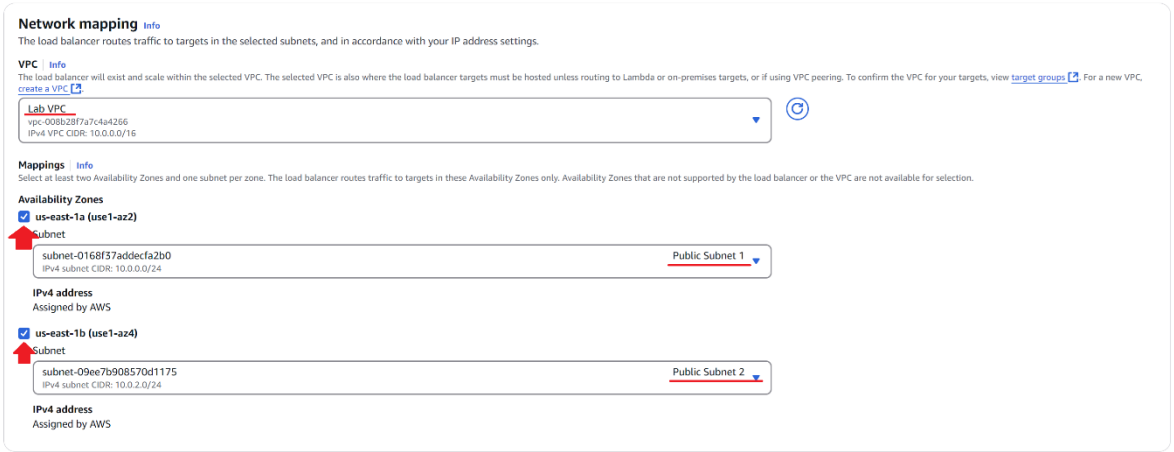
Under Application Load Balancer, click Create.



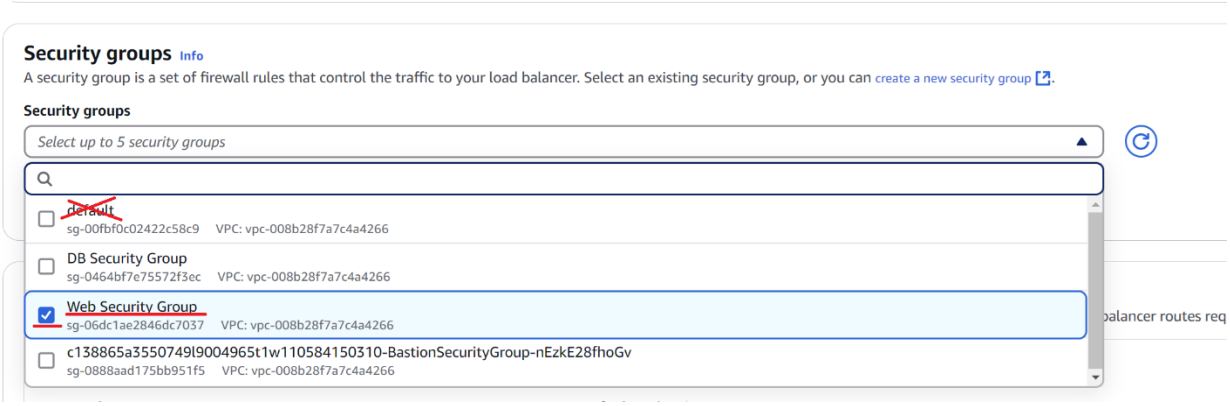
Under Basic configuration, set the load balancer name to LabELB.



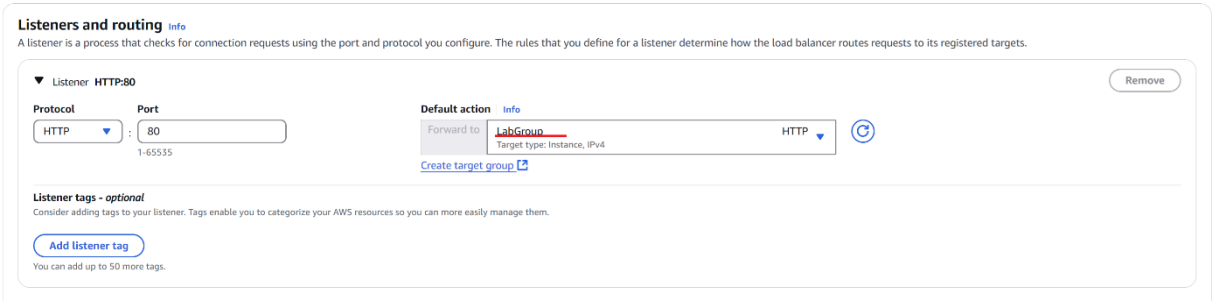
Under Network mapping, set the VPC to Lab VPC, check both availability zones, and set them to Public Subnets 1 and 2 respectively.



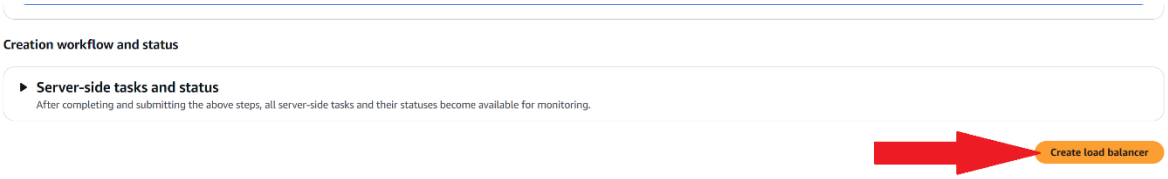
Under Security groups, select Web Security Group and unselect default.



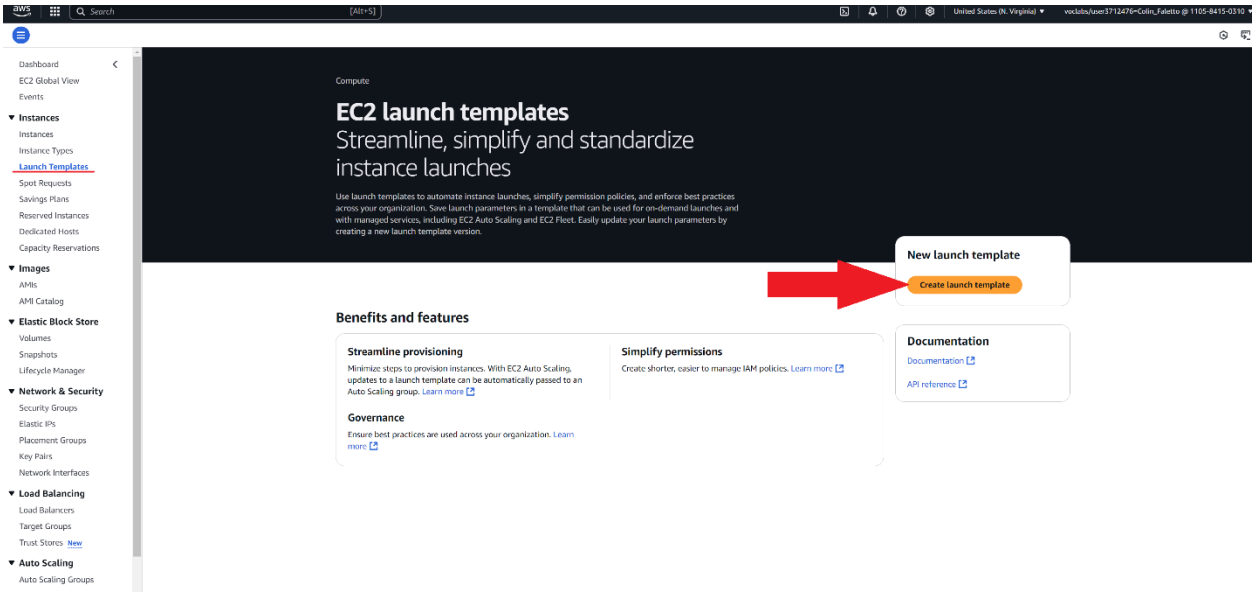
Under Listeners and routing, set the default action to LabGroup



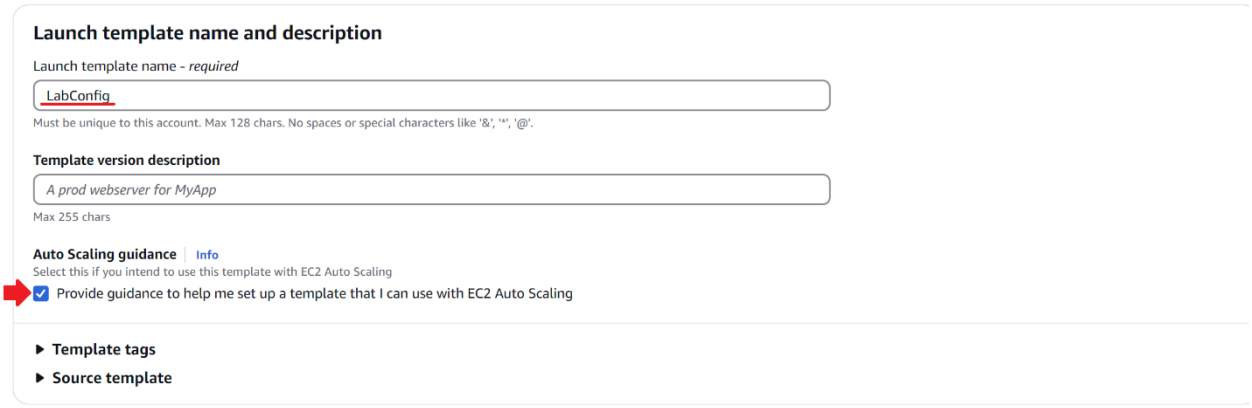
Click Create load balancer.



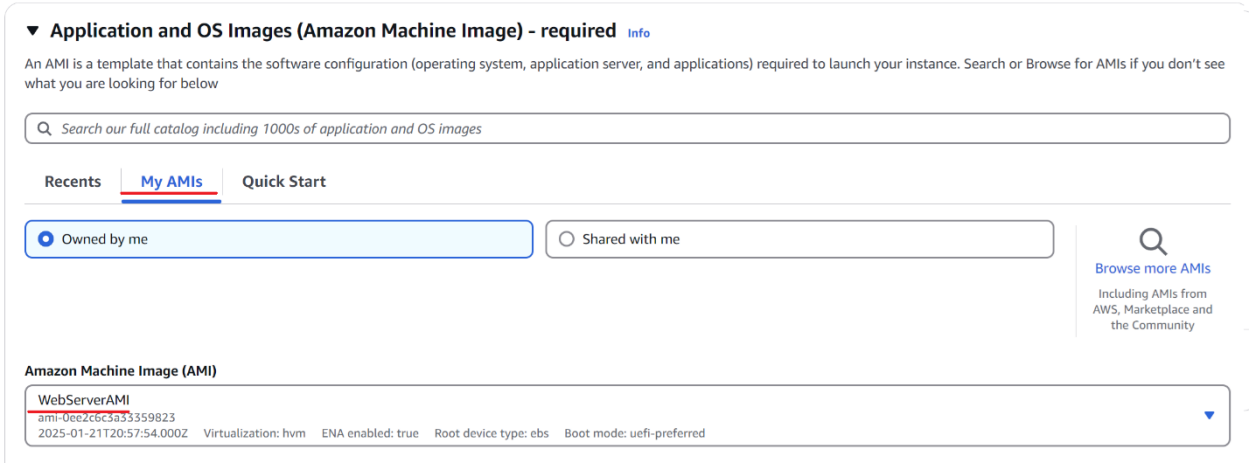
Go to Launch Templates > Create launch template.



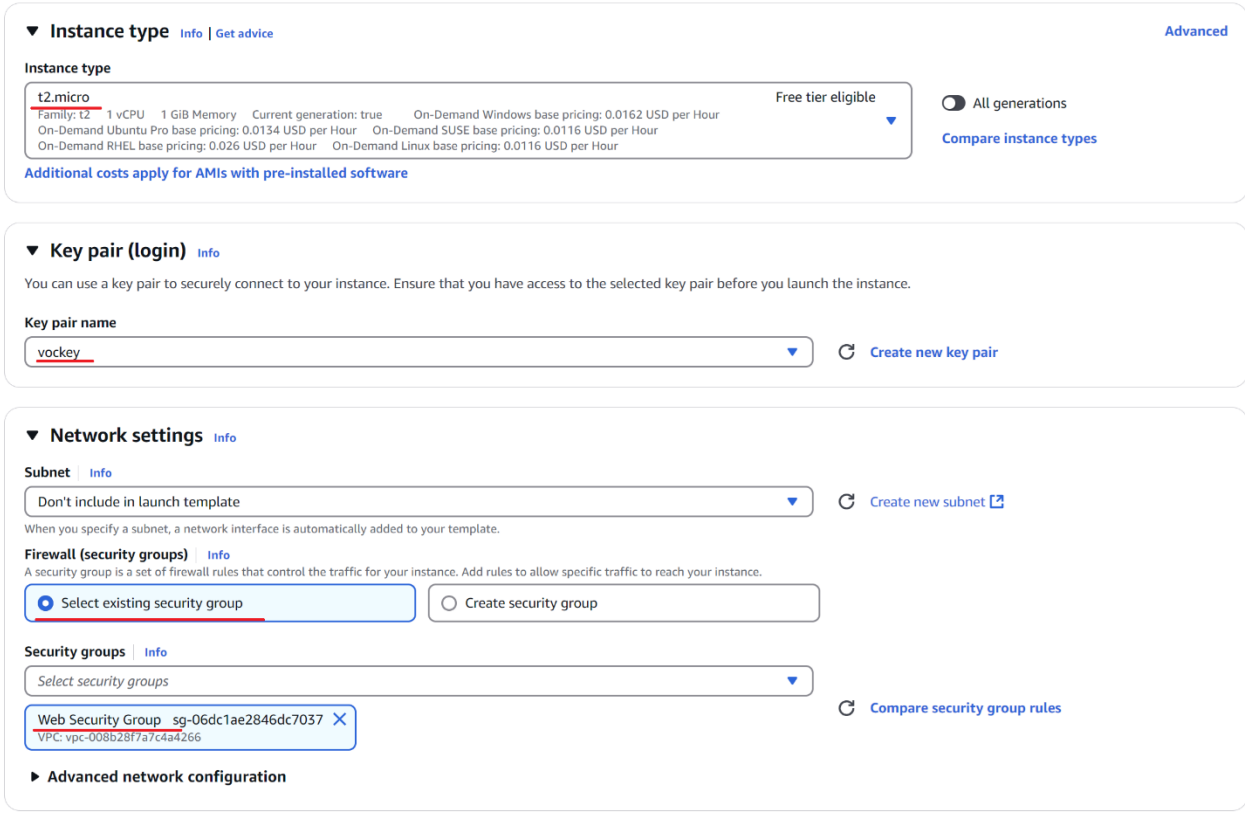
Set the launch template name to LabConfig and click the checkbox under Auto Scaling Guidance.



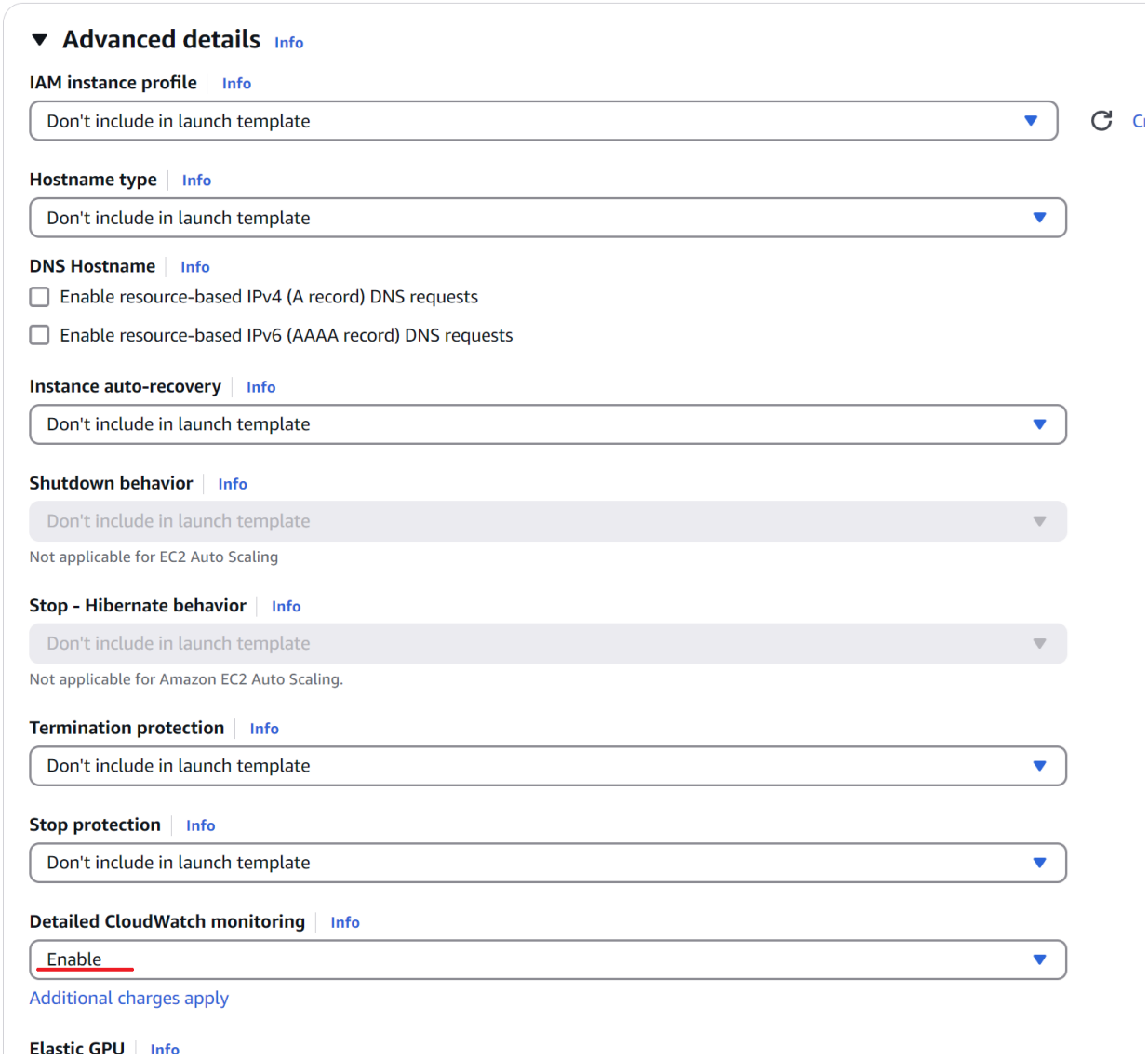
Under the Application and OS images section, click My AMIs and select the AMI you created earlier.



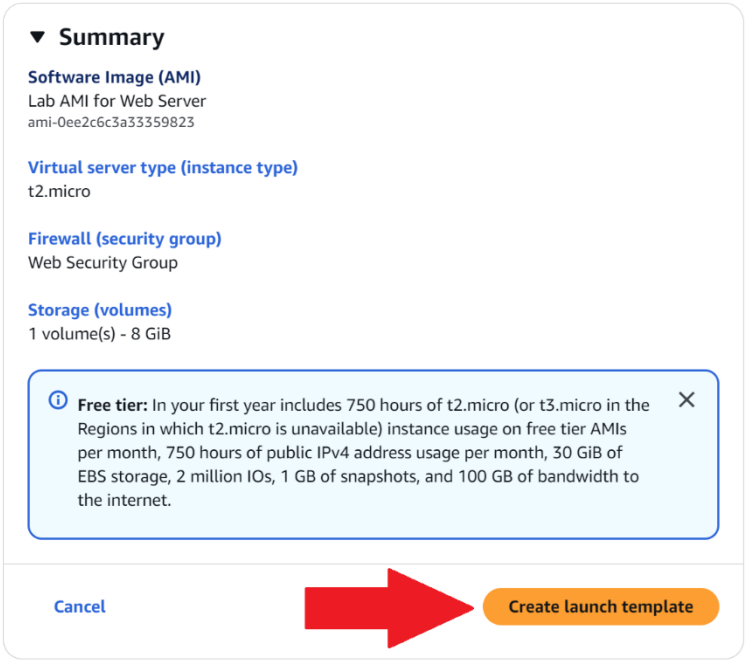
Set the instance type to t2.micro, the Key pair name to vockey, the Firewall (security groups) section to Select existing security group, and the Security groups dropdown to Web Security Group.



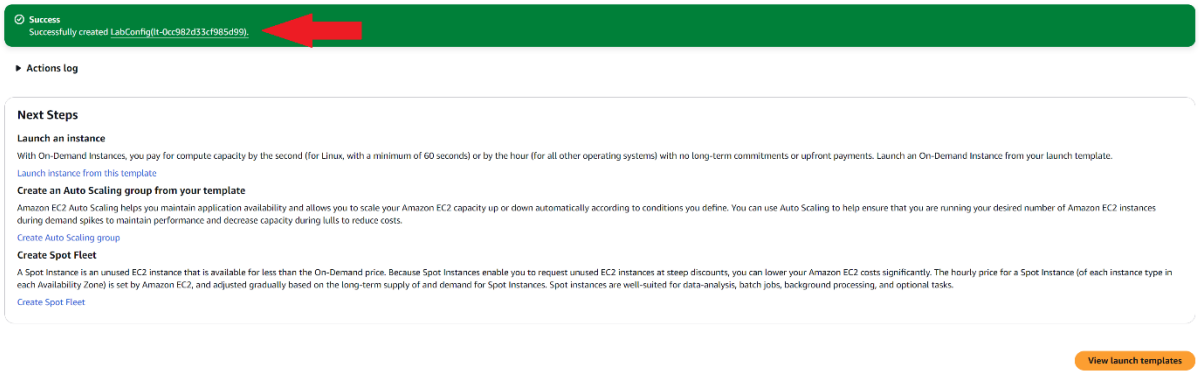
Under Advanced details, enable Detailed CloudWatch monitoring.



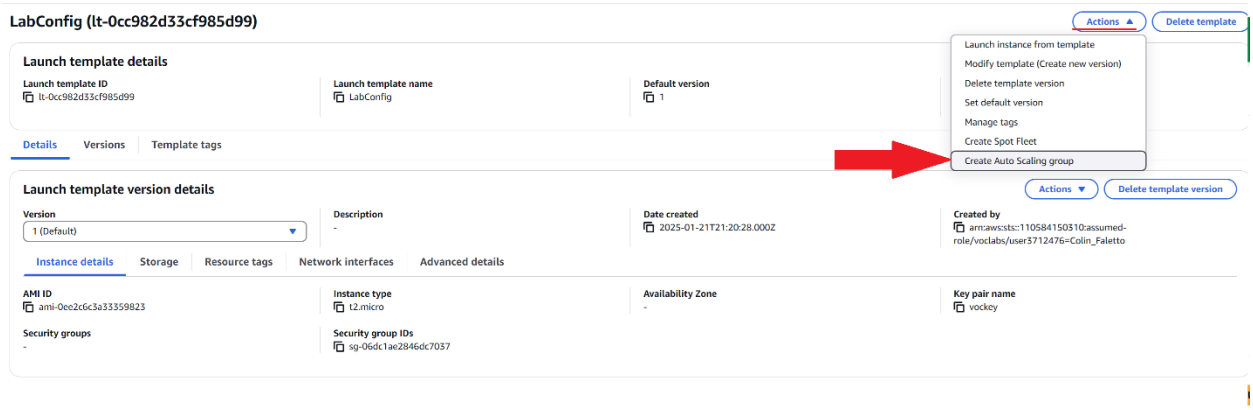
Under Summary, click Create launch template.



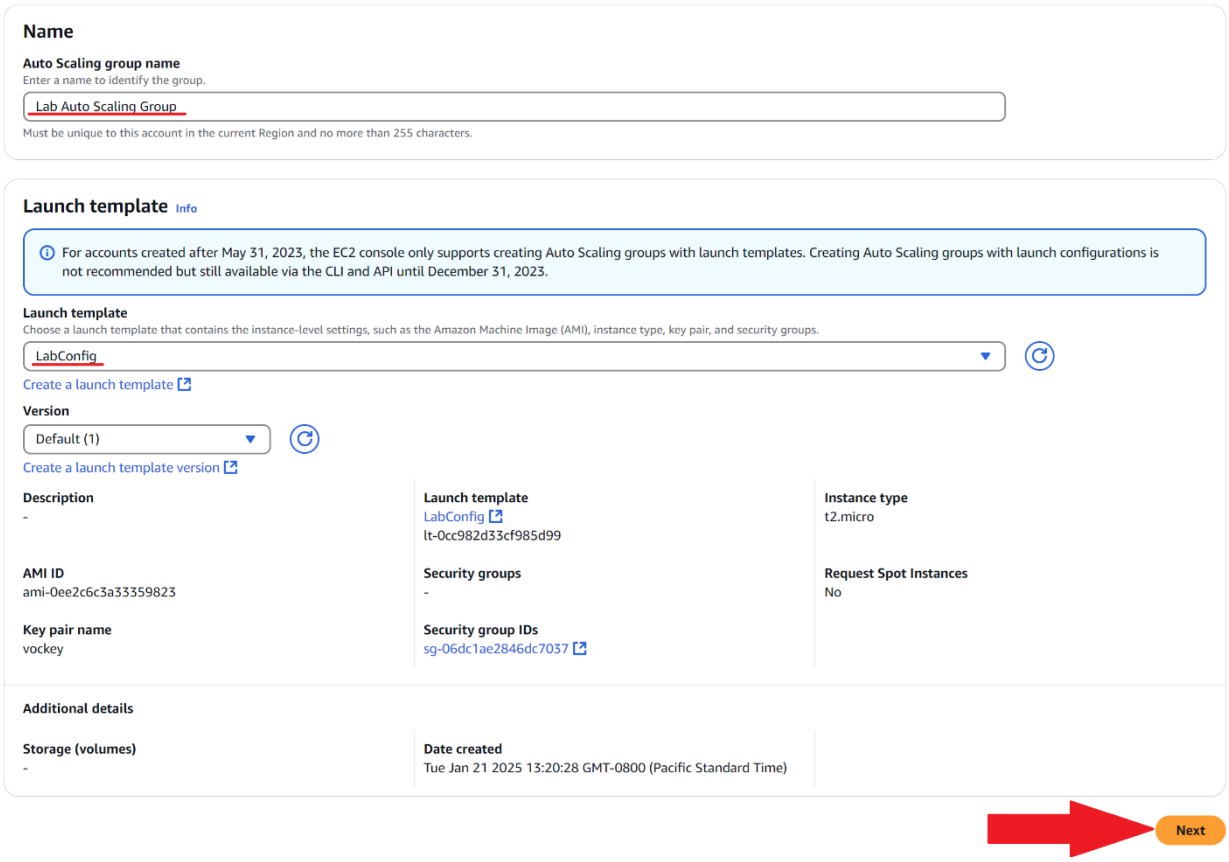
Click the hyperlink in the success dialog.



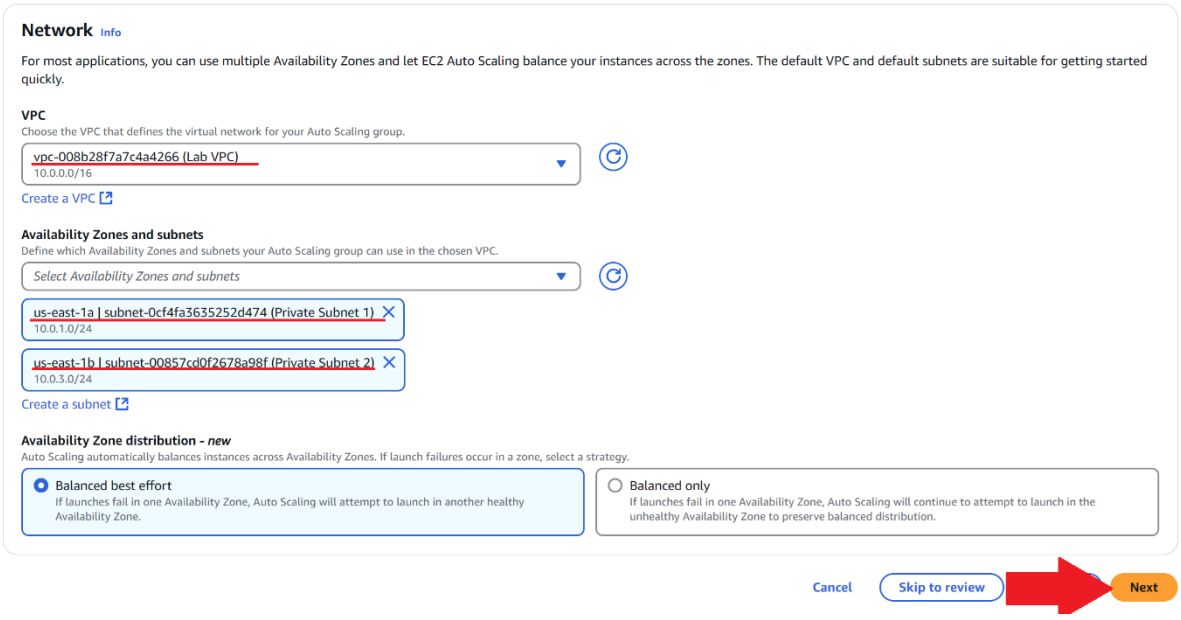
Click Actions > Create auto scaling group.



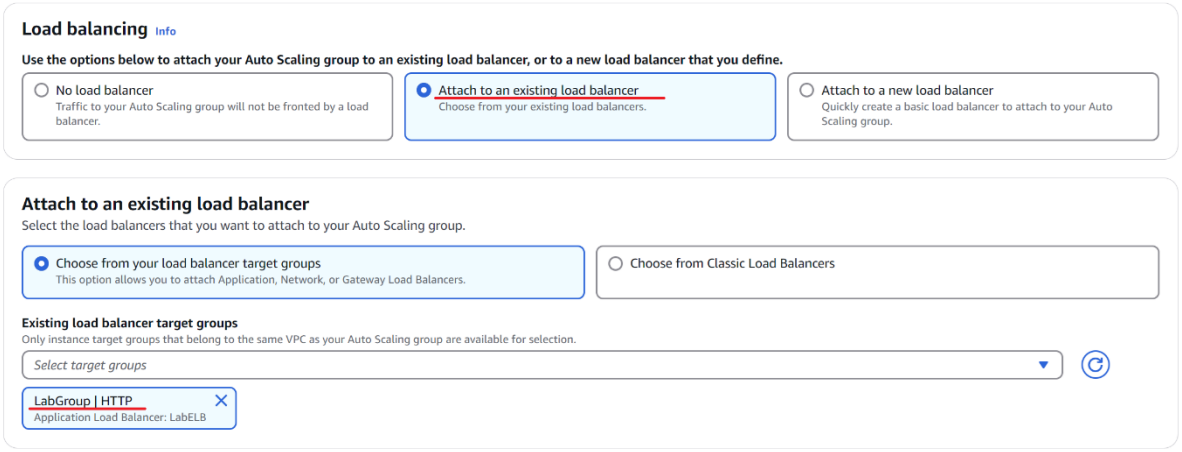
Set the name to Lab Auto Scaling Group, ensure that the Launch temlate is set to LabConfig, and click Next.



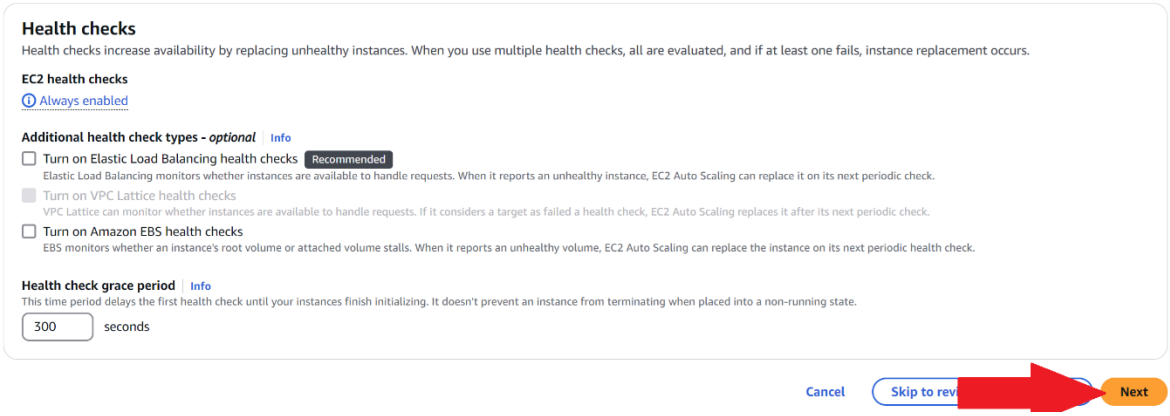
Set the VPC to Lab VPC, select both private subnets under Availability Zones and subnets, then click Next.



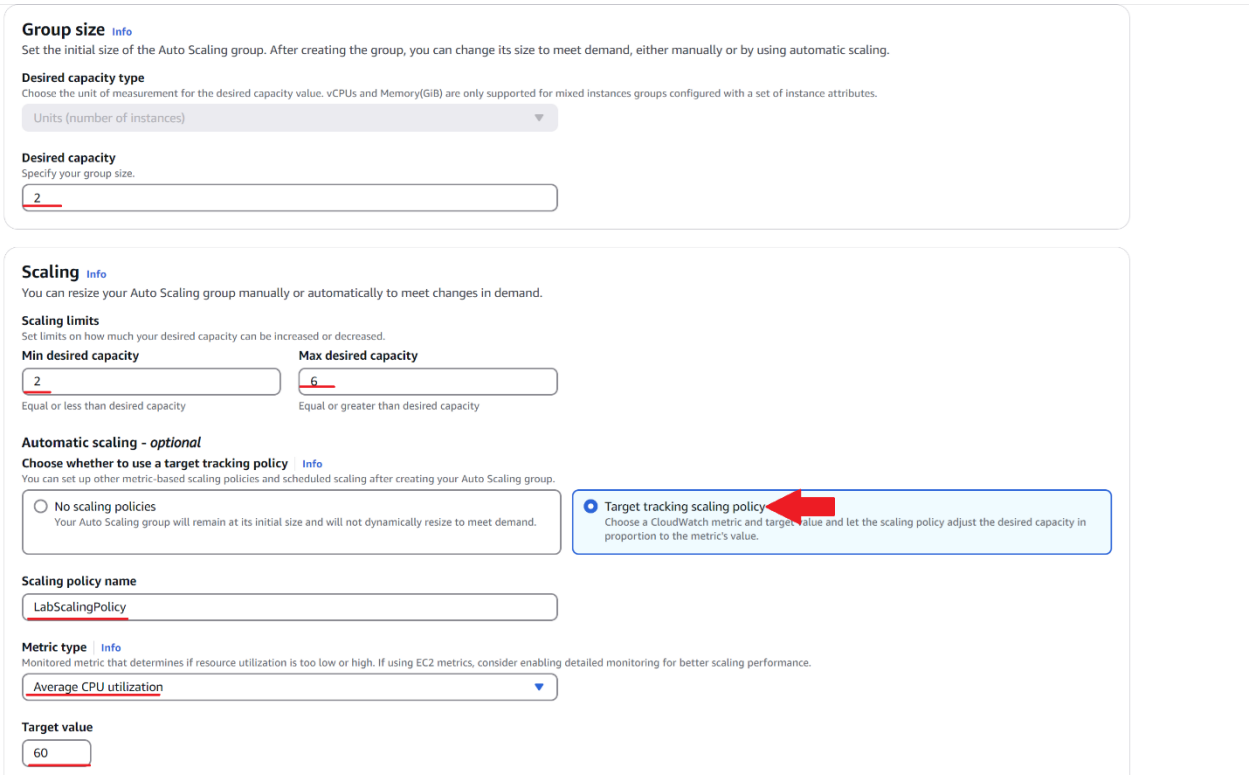
Under load balancing, select attach to an existing load balancer, and under existing load balancer target groups, select LabGroup



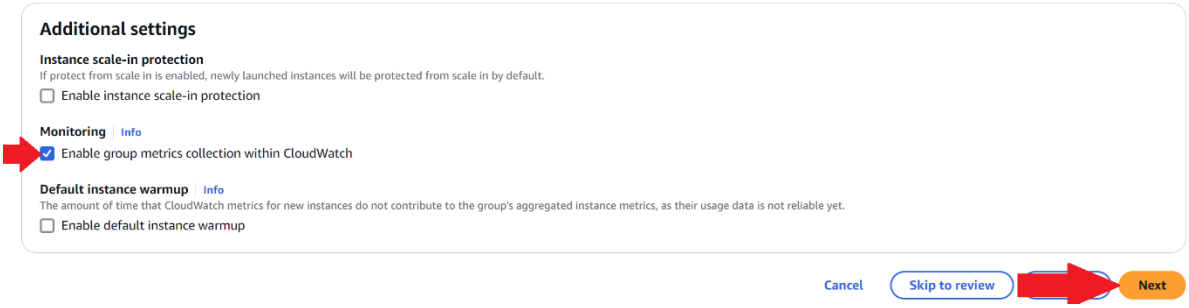
Click Next.



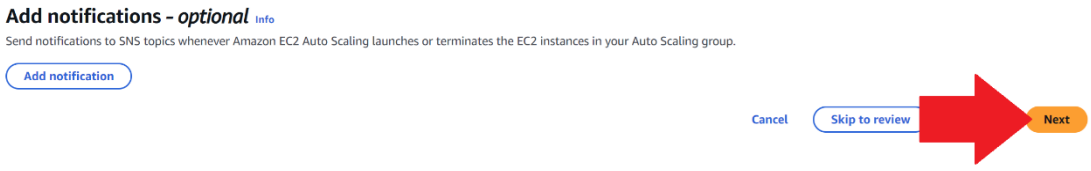
Set the the Desired capacity to 2, the minimum capacity to 2, and the maximum capacity to 6. Set the automatic scaling policy to target tracking scaling policy, set the name to LabScalingPolicy, the metric type to Average CPU utilization, and the target value to 60. This setting will automatically scale the number of EC2 instances to maintain an average of 60% CPU utilization across instances.



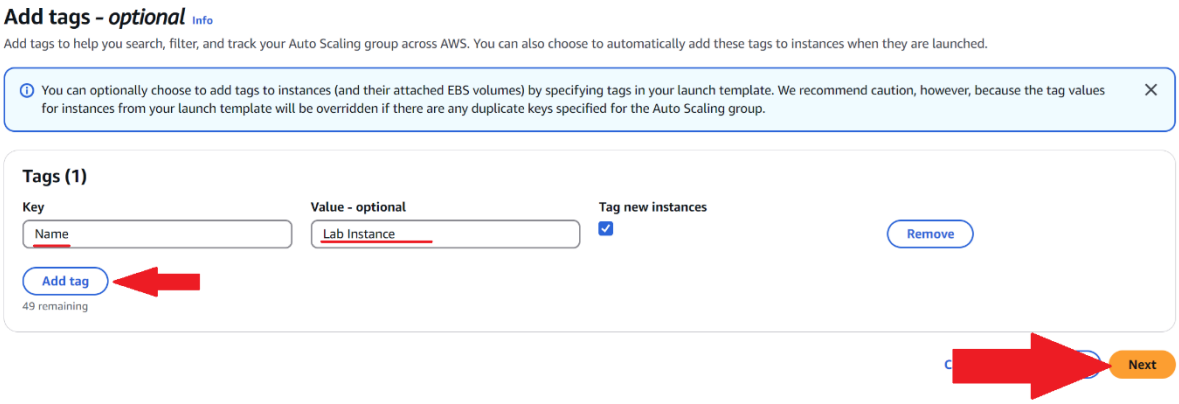
Under Additional settings, click Enable group metrics collection within CloudWatch, then click Next.



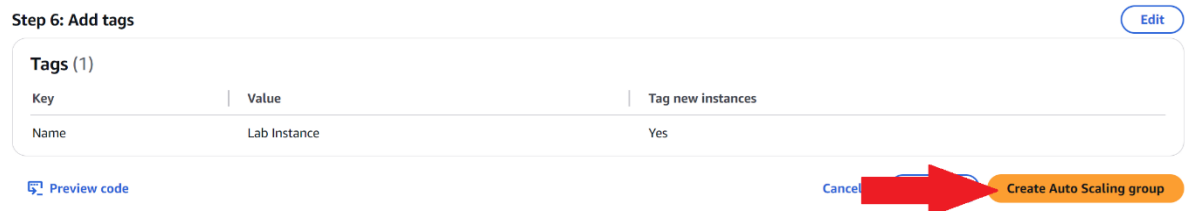
Under Add notifications, click Next.



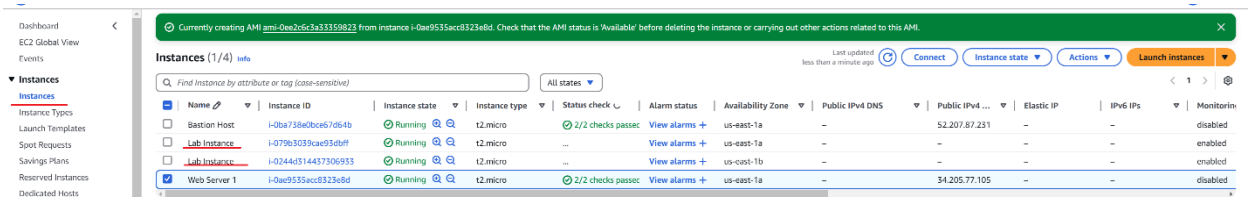
Under Add tags, click Add tag, set the key to Name, an



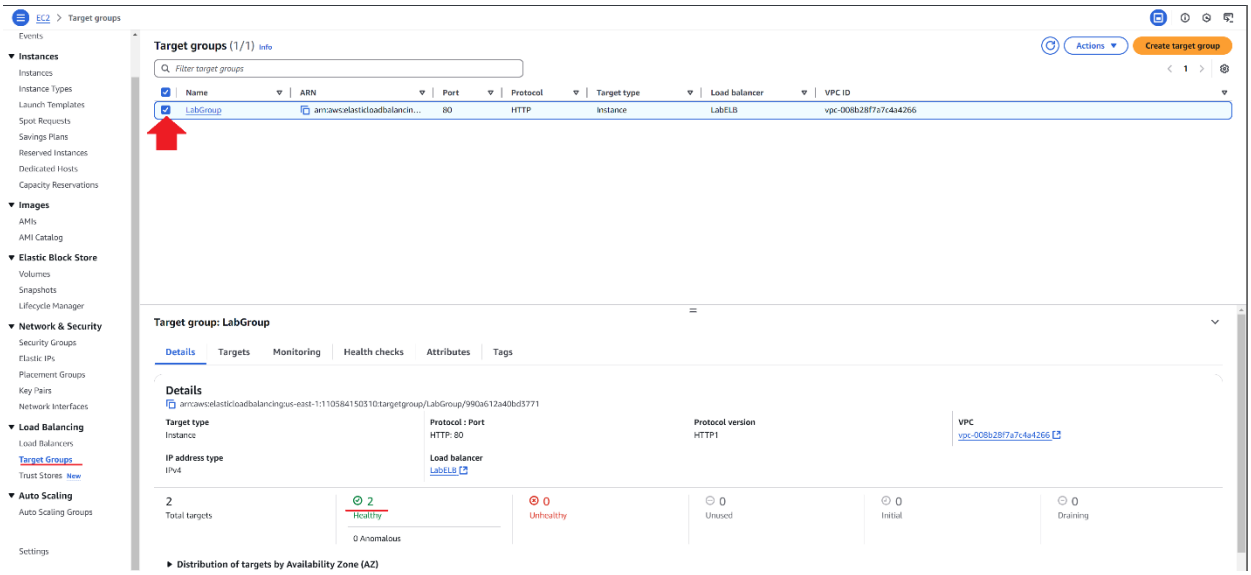
Click Create Auto Scaling Group.



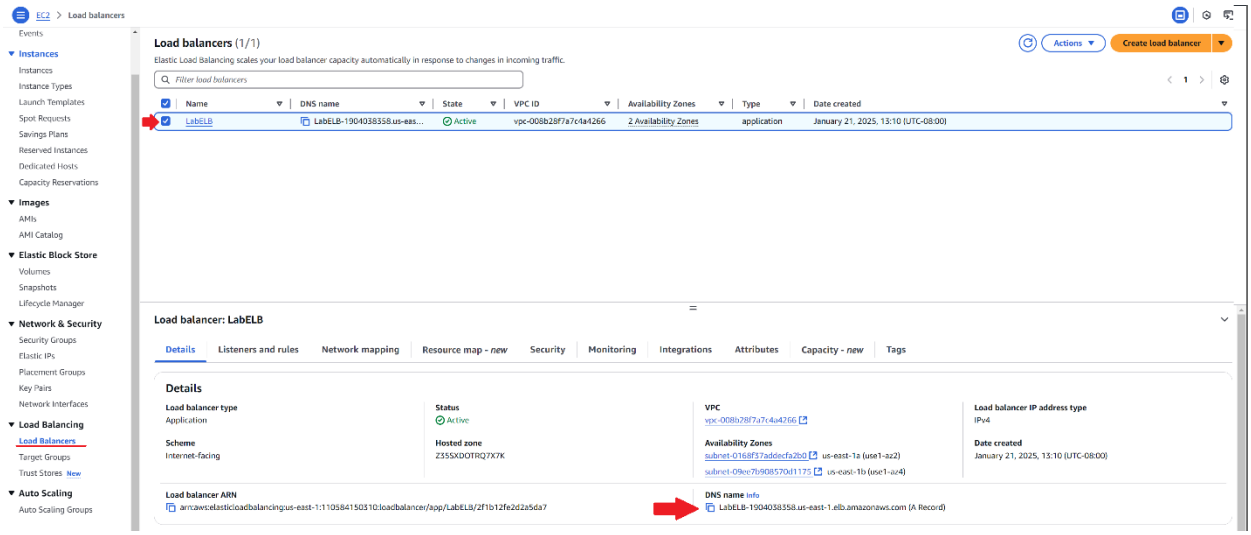
Click Instances and ensure that two copies of Lab Instance have been launched.



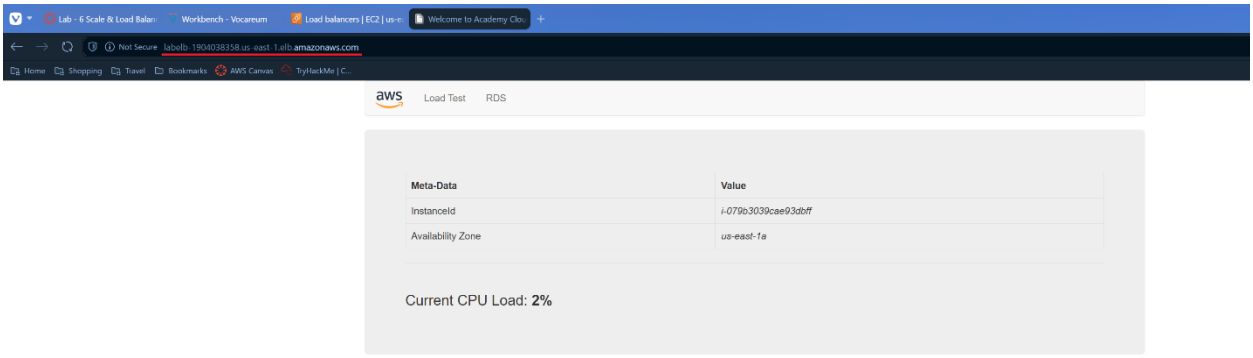
Go to Target Groups, check LabGroup, and ensure that both targets are healthy.



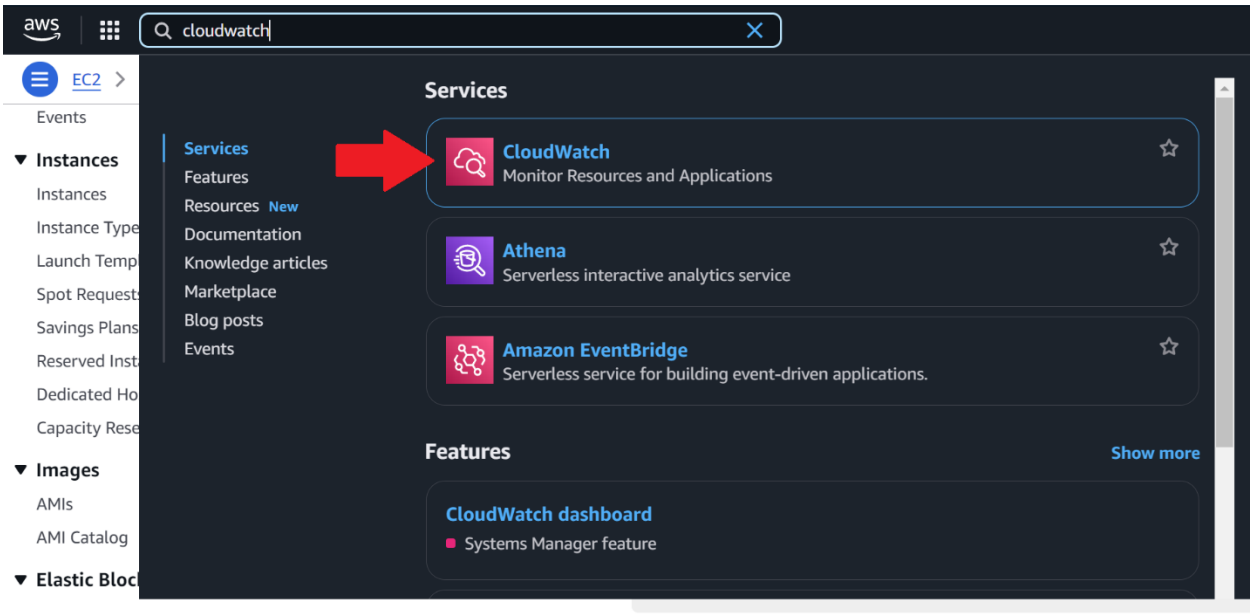
Go to Load balancers, select LabELB, then copy the DNS name.



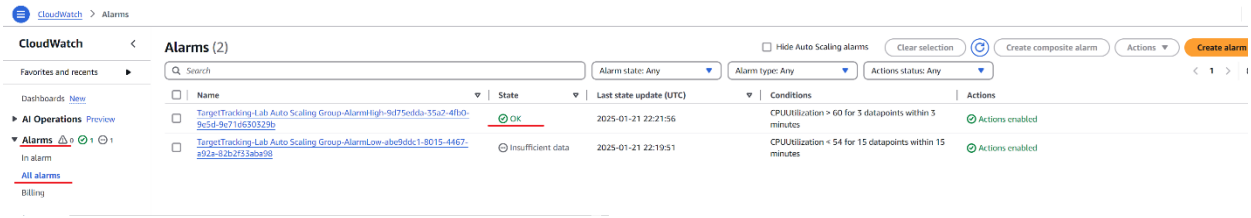
Open the DNS server in a new browser tab and ensure that you see the EC2 instance web server as shown below.



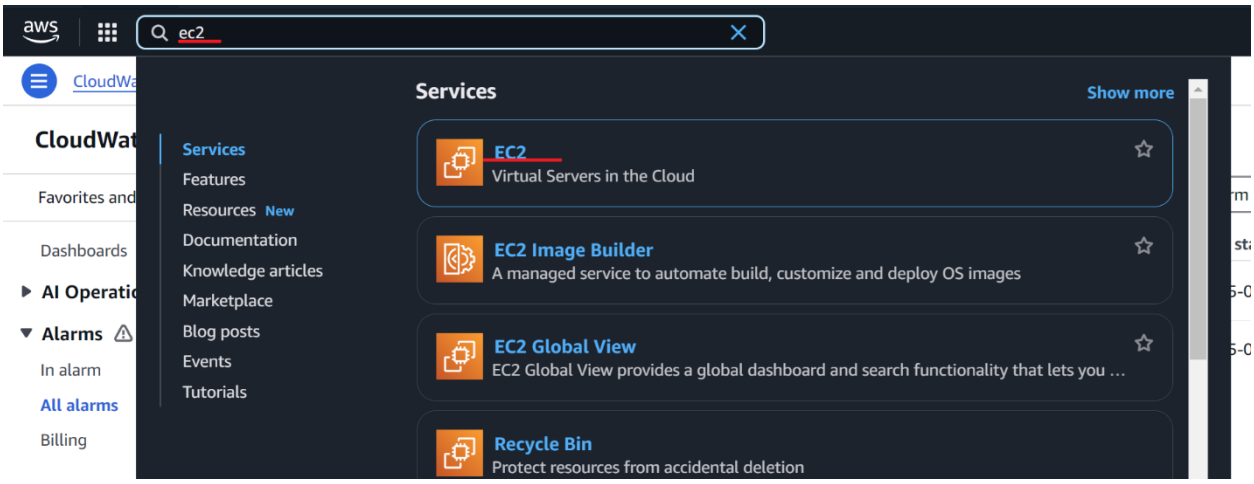
In the search bar, search for and open Cloudwatch.



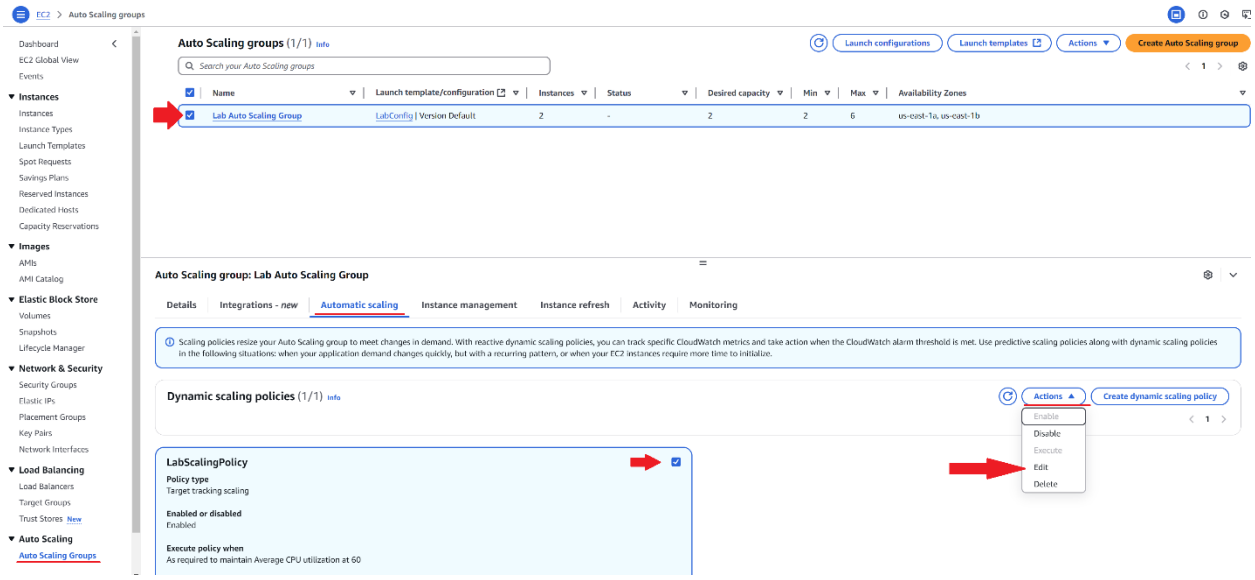
Click Alarms > All alarms, and ensure that the AlarmHigh alarm reports OK.



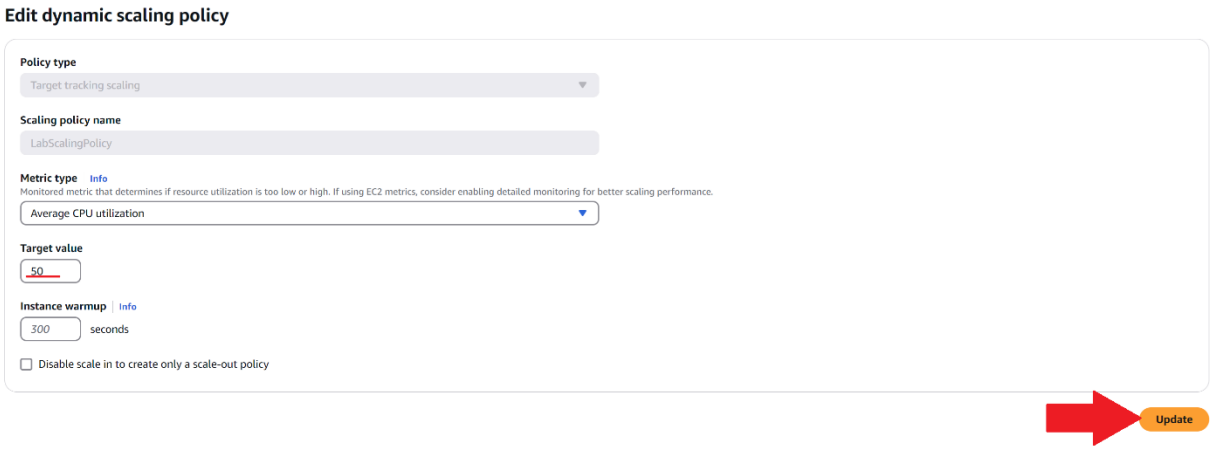
Go back to EC2 from the search bar.



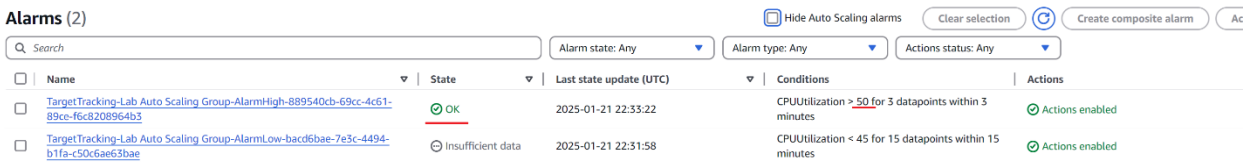
Select Auto Scaling groups, select Lab Auto Scaling group, click the Automatic Scaling tab, select LabScalingPolicy, then click Actions > Edit.



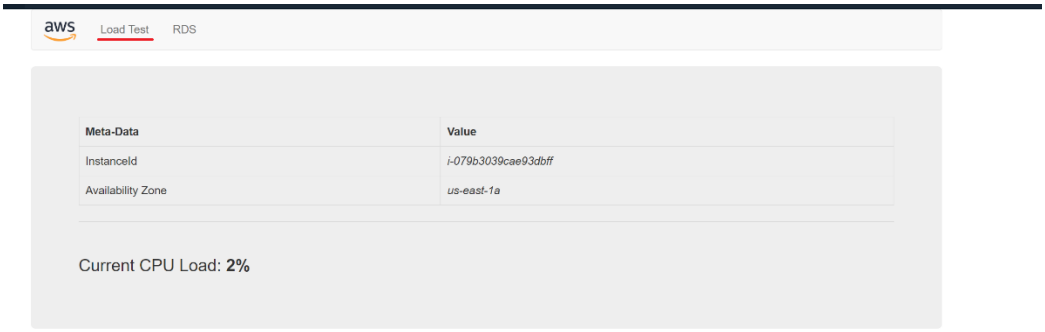
Set the target value to 50 and click Update.



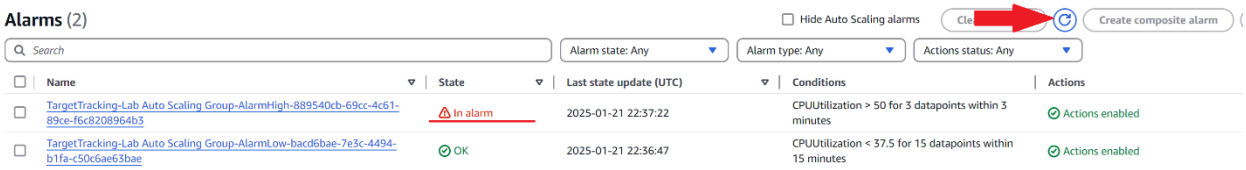
Return to Cloudwatch > Alarms > All alarms and ensure the updated AlarmHigh alarm still reports OK.



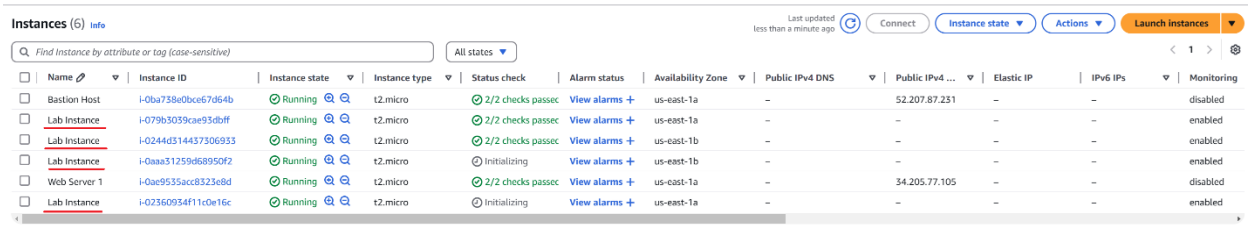
Return to the EC2 web server tab and click Load Test.



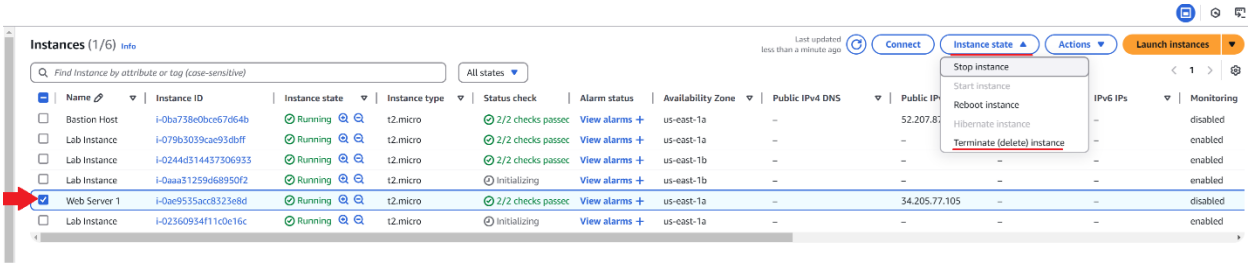
Return to the AWS console and continually press the refresh button on the alarms page. Eventually, the AlarmHigh will report that it is in alarm.



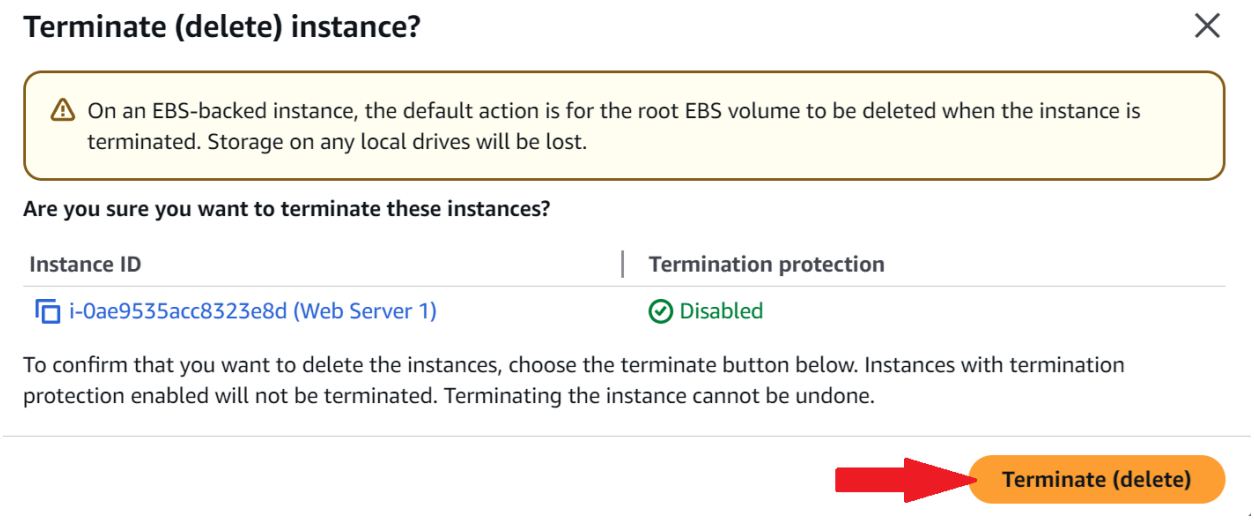
Return to EC2 > Instances. You should see that the Auto Scaling Group has automatically created more instances of the Lab Instance AMI.



Next, to clean up, select Web Server 1 and click Actions > Terminate (delete) instance.

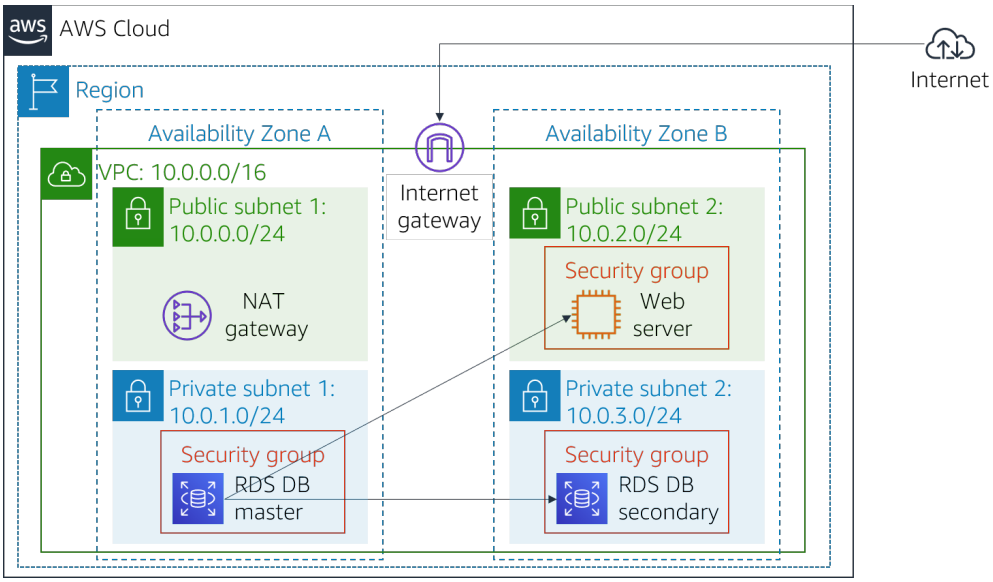


Click Terminate.

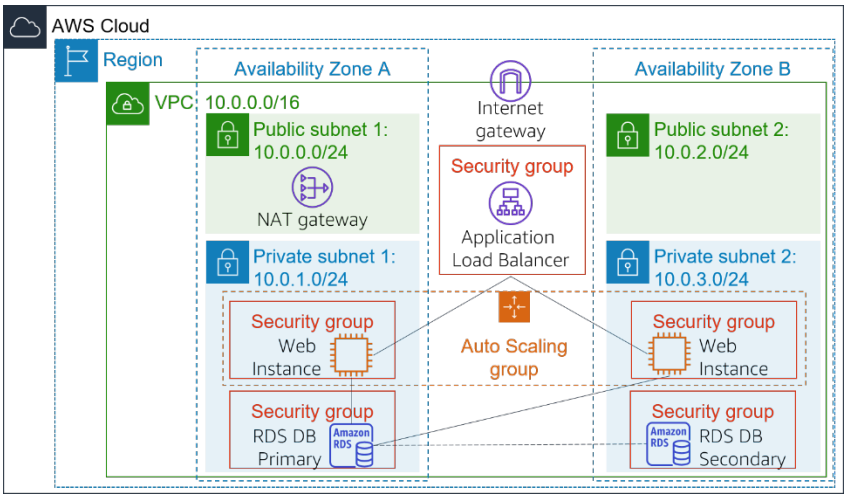


Topology (EBS)

Topology (RDS)



Topology (Auto Scaling)



Problems

No problems were encountered in this lab.

Conclusion

To wrap up, these three labs were a great addition to my understanding of the AWS cloud and management console. Through learning about Elastic Block store, I now have a deeper understanding of the inner workings of Elastic Compute Cloud. Through learning about RDS, I now have a solid foundation of knowledge about how large amounts of data with a consistent structure are stored. Through learning about auto scaling, I'm now confident that I could scale AWS services for use at a company with heavy reliance on cloud resources.

Palo Alto Networks Cybersecurity Academy – Configuring GlobalProtect RAVPN on a PA220 Firewall

Colin J. Faletto, CCNA

paloalto NETWORKS

Purpose

This lab expands upon our knowledge of the PA220 by introducing us to the world of VPNs. Setting up a remote access VPN provides valuable insight on how to create and secure a private tunnel into a firewall's internal network, which is extremely valuable to businesses requiring work-from-home cybersecurity solutions.

Background

Palo Alto Networks is a networking and cybersecurity company from Santa Clara, California. They are a member of the S&P 500. They focus mainly on the business market, creating scalable security solutions for many of the largest companies worldwide.

The Palo Alto PA220 is a firewall sold by Palo Alto Networks. Contrary to Palo Alto's main market, the PA220 is intended for small office/home office solutions. Marketed as a NGFW, or Next-Generation Firewall, the PA220 uses machine learning to identify attacks instead of relying on a simple signature check like traditional firewalls. This technology allows the PA220 to identify undocumented threats and brand-new exploits without intervention from Palo Alto networks themselves. The PA220 also prevents threats by filtering URLs and securing against DNS-based attacks. As of January 31, 2023, it is no longer being sold, and it will reach end-of-life on January 31, 2028.

The PA220 doesn't have a fan, and instead uses hexagon-shaped vents to passively filter air. The firewall's compact form factor allows it to easily fit alongside existing network devices.

Palo Alto firewalls run on an operating system called PAN-OS. PAN-OS can be controlled through two methods: a Graphical User Interface (GUI) and a Command-Line Interface (CLI). The GUI is accessible through an HTTP connection and displays in any modern web browser. The HTTP connection is available through the firewall's MGT port and by default, is accessible at http://192.168.1.1. The firewall has a default username and password of *admin*.

The latest version of PAN-OS is PAN-OS 11.2 Quasar, which was released in May 2024. In this lab, our firewall is running PAN-OS 8, which has reached end of life and is no longer supported.

PAN-OS's GUI has a variety of settings and tools to control advanced functionality of the router. The GUI's default page is a dashboard that displays vital information, such as console messages and link states of ports.

SOHO, short for Small Office/Home Office, is a network type commonly used by individuals or small businesses with less than 10 employees. This network type commonly uses smaller-scale routers, switches, and firewalls compared to their large enterprise counterparts. SOHO networks provide numerous advantages to teams of 1-

10 people as they are easier to set up and are more affordable than full-size network equipment. SOHO networks often only have a single router, and may contain switches, wireless access points, and end devices such as computers and printers.

A virtual private network, or a VPN, is a method of creating a secure tunnel between networks. VPNs allow computers that are physically located offsite to be treated the same as computers physically inside of a network. There are two primary types of VPNs: remote access (RAVPN) and site-to-site, which create private tunnels for individual computers and entire networks respectively. In the business world, VPNs are often used to allow employees working from home to access company resources located on internal servers. VPN services are commonly sold commercially, allowing consumers to connect to private network-sharing servers. These servers are often located in multiple countires or regions, enabling consumers to spoof their location and hide network traffic from their ISP.

GlobalProtect is a Remote Access VPN service developed by Palo Alto networks. The service requires a client program which runs on outside computers and supports all three major operating systems. GlobalProtect is heavily integrated into Palo Alto firewalls such as the PA220, which includes a gateway to allow connections from the service and a web portal to download the client. GlobalProtect puts a large emphasis on security, exemplifying the principle of least-privilege access and including a wide variety of configurable security options.

Remote Desktop Protocol, or RDP, is a Microsoft-proprietary protocol that allows a user to remotely view and control a connected Windows PC. RDP employs a client/server model, with the client being included on all versions of Windows and the server being exclusive to the operating system's higher tiers. RDP uses port 3389 with both TCP and UDP. RDP was introduced during Microsoft's transition from MS-DOS to the NT kernel with Windows NT 4.0 Terminal Services Edition, and the server has been included on every version of Windows (other than Home) since XP.

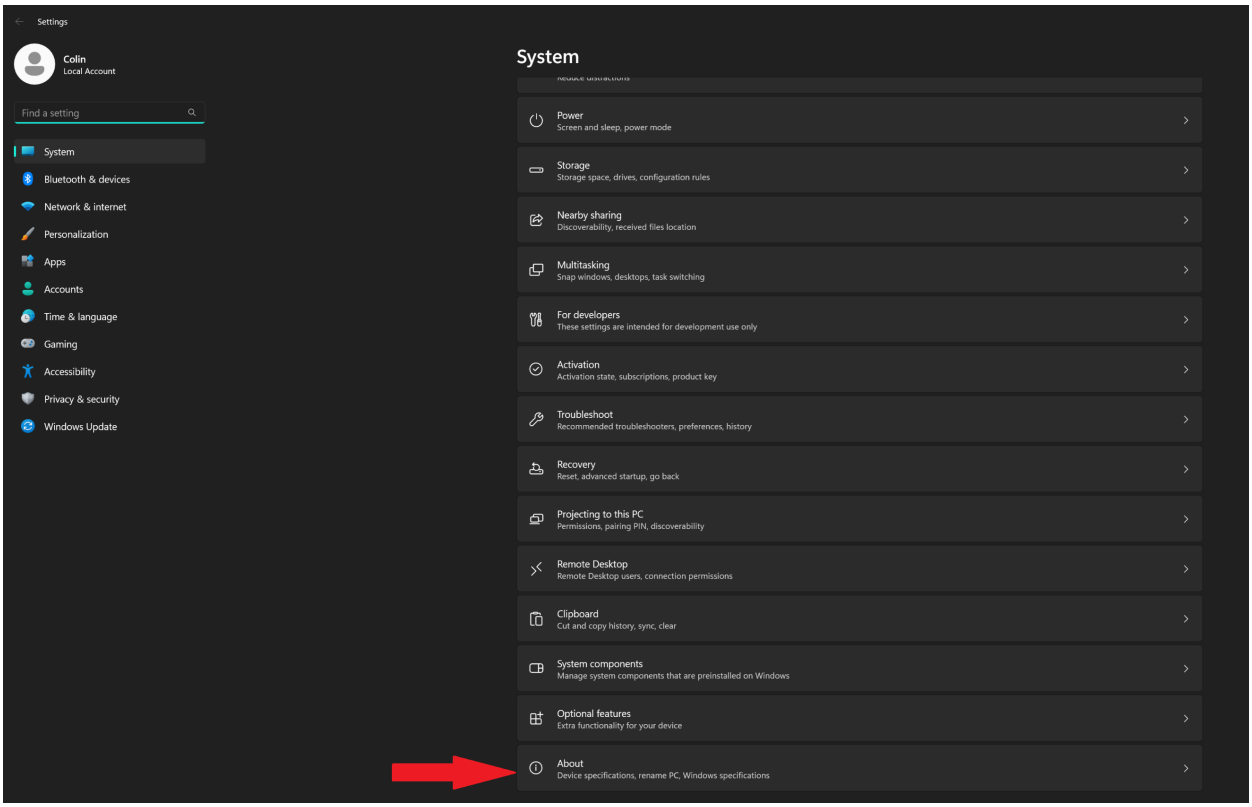
Lab Summary

In this lab, we configured Microsoft's remote desktop protocol (RDP) on two Windows computers: one on the PA220's internal network and one just outside the PA220's network. We then set up Palo Alto's GlobalProtect remote access VPN on the firewall, including credentials for the outside user and a portal page to download the GlobalProtect client.

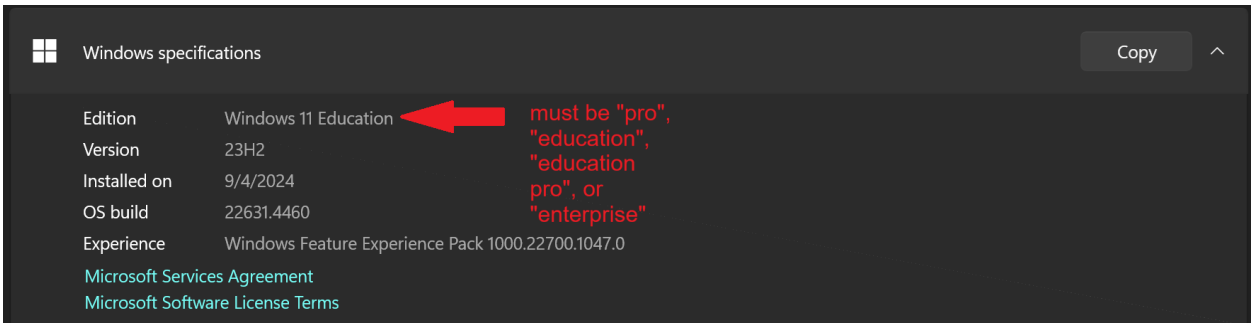
Lab Commands

Configuring Remote Desktop

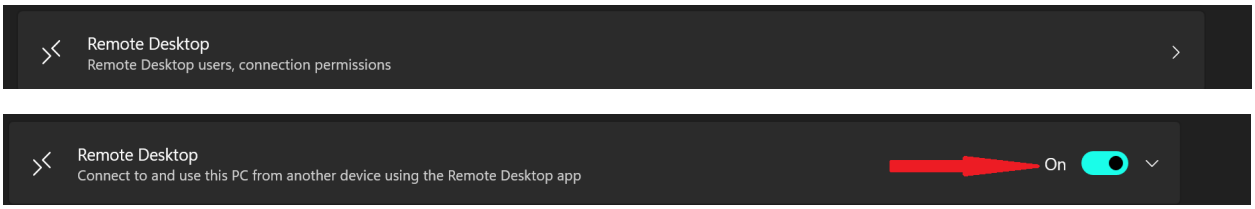
On the internal Windows PC, press (Win+I) to open the settings app. Click into the "About" section.



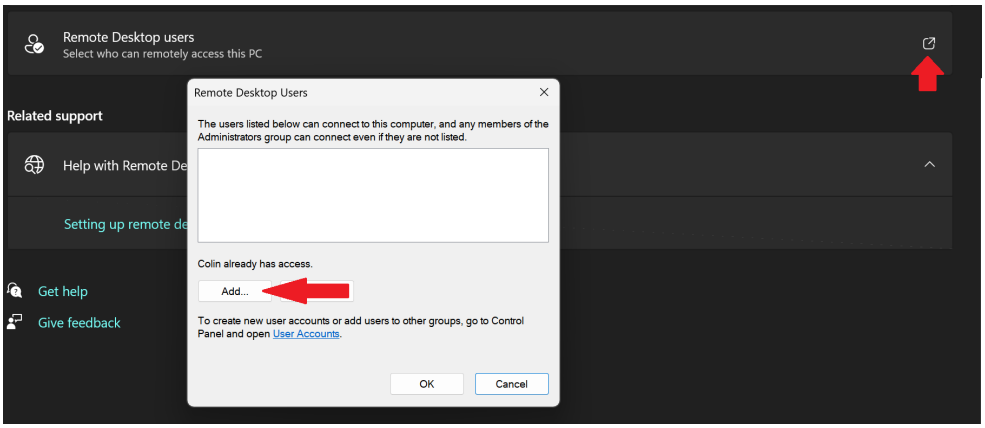
Make sure that you are running Windows 11 Pro, Education, Education Pro, or Enterprise. **Windows 11 Home doesn't support a Remote Desktop Server connection**. It can, however, be used on the external client PC.



In the settings menu, go to System > Remote Desktop and turn on "Remote Desktop".

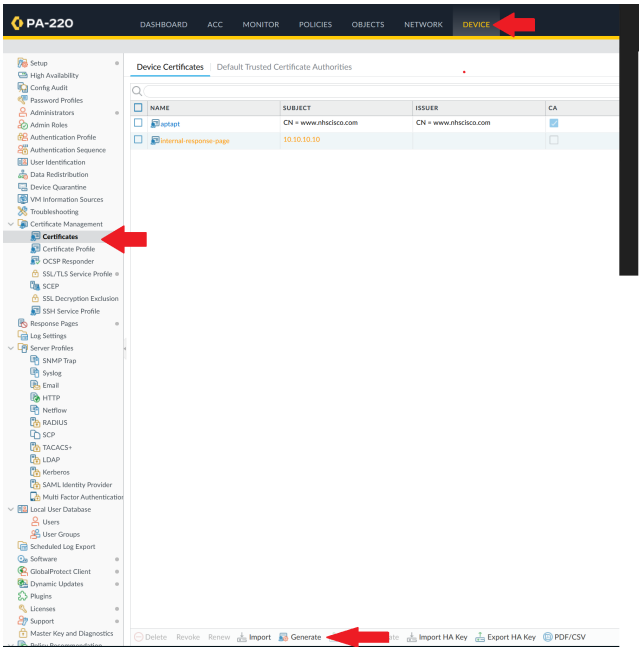


Click on "Remote Desktop Users". If the user account you want to connect to isn't an administrator, you will have to manually add it here using the "Add" button.

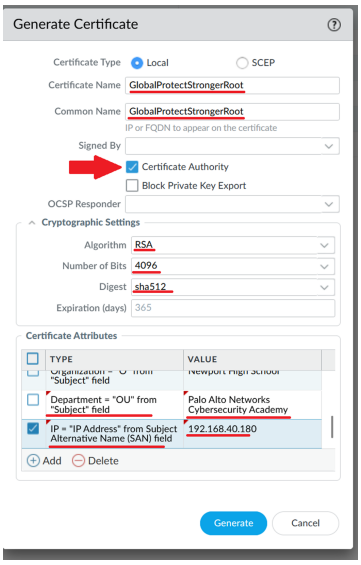


Generate Certificates

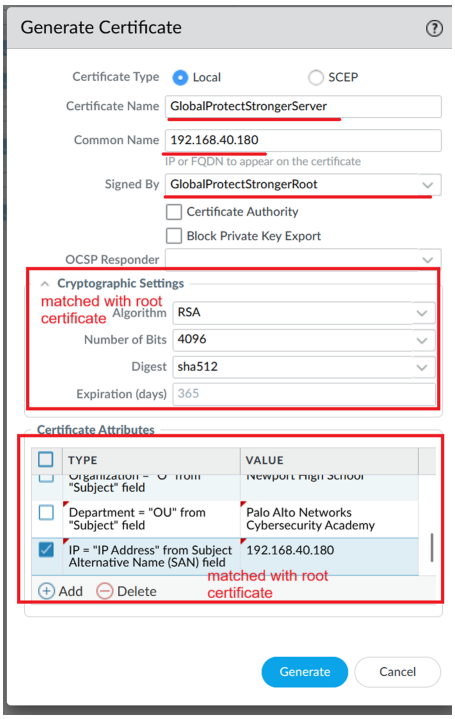
In the PA220 web interface, navigate to Device > Certificate Management > Certificates and click Generate.



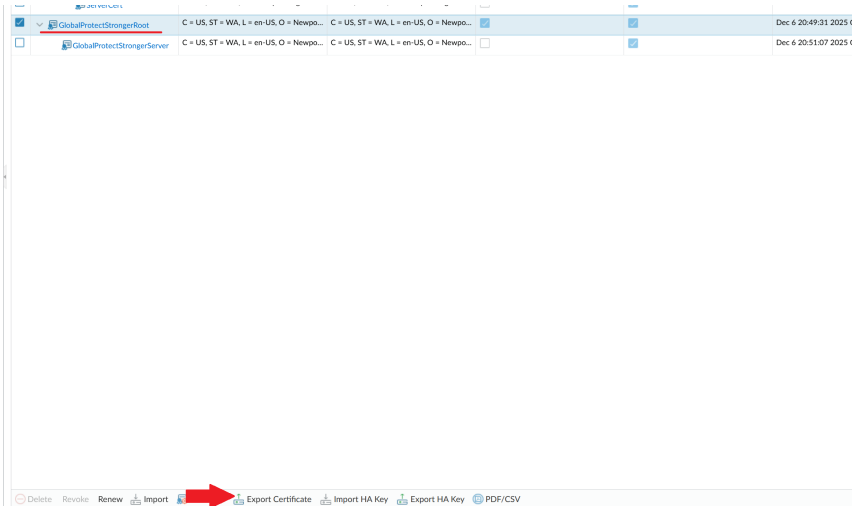
First, generate a root certificate. Give a Certificate Name and Common Name that make sense for the context, and make sure that the Certificate Authority box is checked. Under Certificate Attributes, assign appropriate values for the Country, State, Locale, Organization, and Department Fields, and make sure that the IP Address field is set to the outward-facing IP of the firewall. Optionally, increase the default cryptographic settings to higher values to increase the security of your certificates.



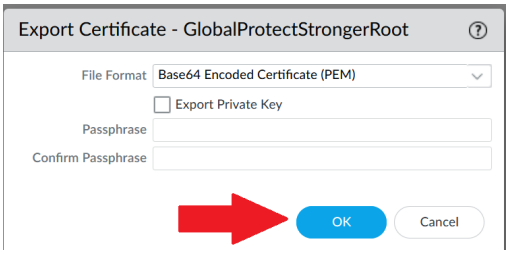
Next, generate your server certificate. Make sure that the Common Name is the outward-facing IP address of the firewall, and that the certificate is signed by the root certificate you generated earlier. Match the cryptographic settings and certificate attributes with the values configured in the root certificate.



Export your root certificate by selecting it and clicking Export Certificate.

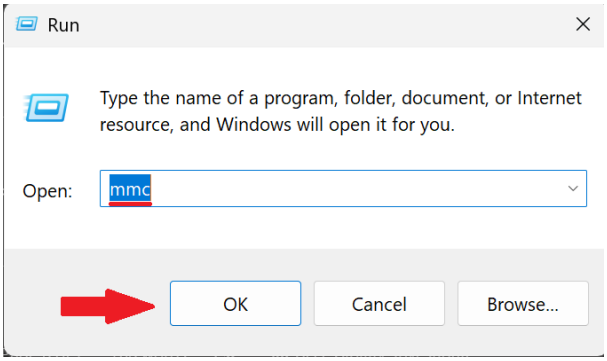


Click “OK” to confirm downloading the certificate. Make sure to note down the file’s download location.

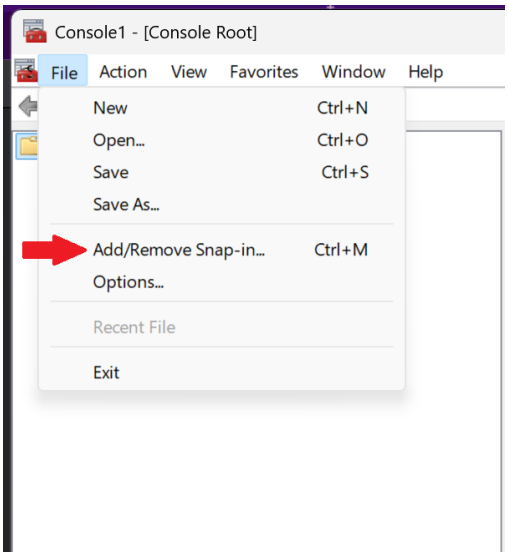


Import Certificates

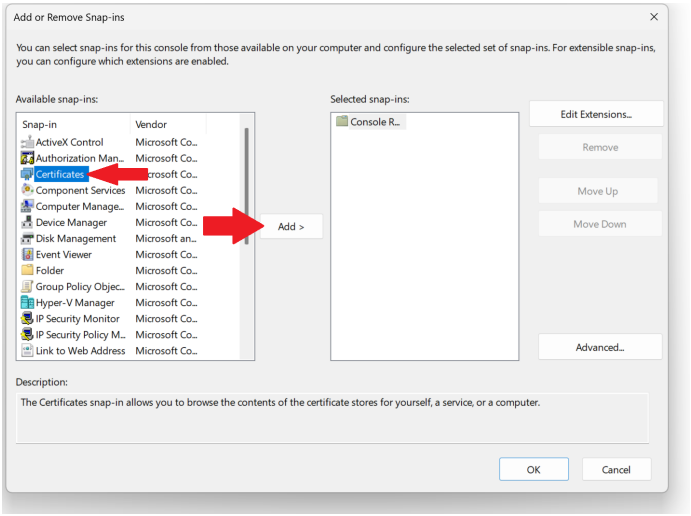
On your outside PC, open the Run dialog (Windows+R) and type “mmc”.



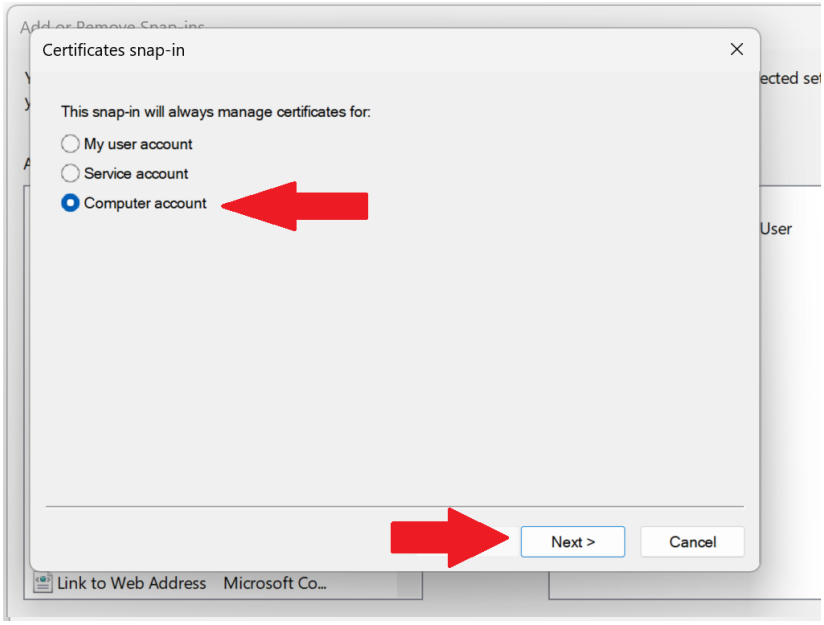
In the resulting window, click File > Add/Remove Snap-in.



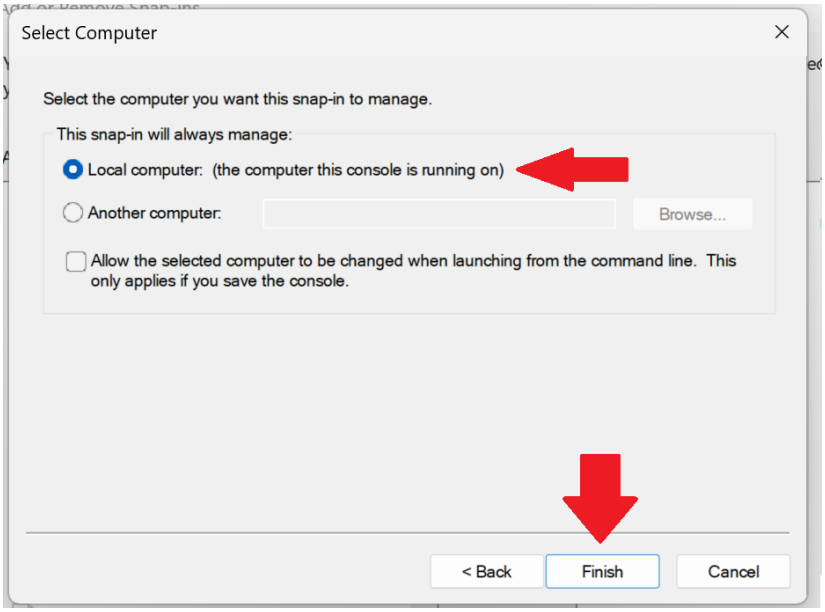
In the resulting window, click on Certificates > Add.



In the resulting window, click on Computer Account > Next.

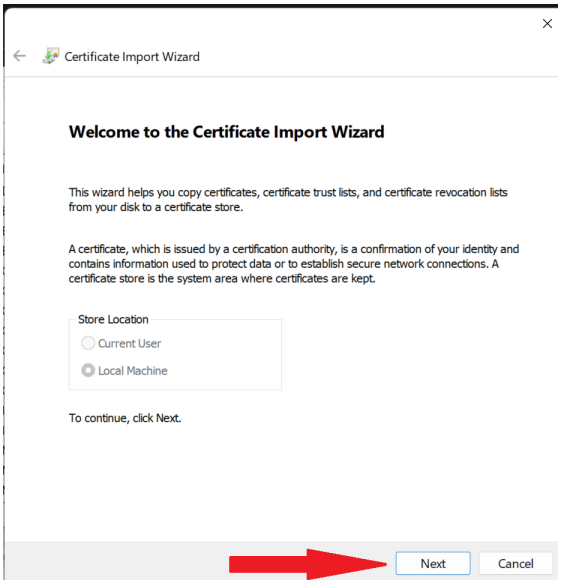


Make sure Local Computer is selected, and click Finish.

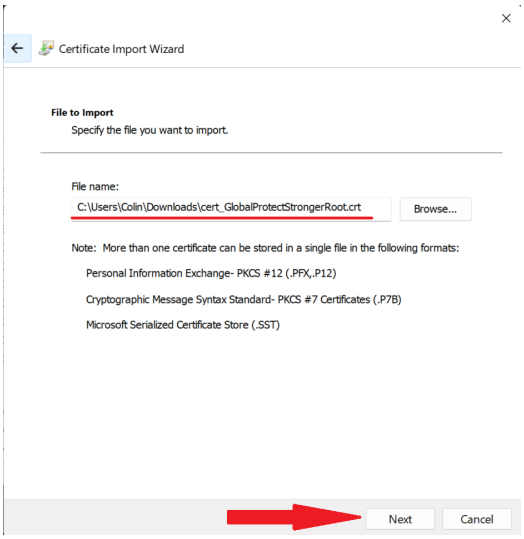


Inside Trusted Root Certification Authorities, right-click on Certificates and click on All Tasks > Import.

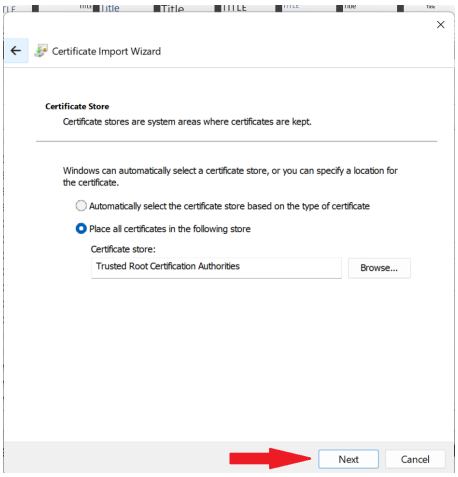
Click “Next”.



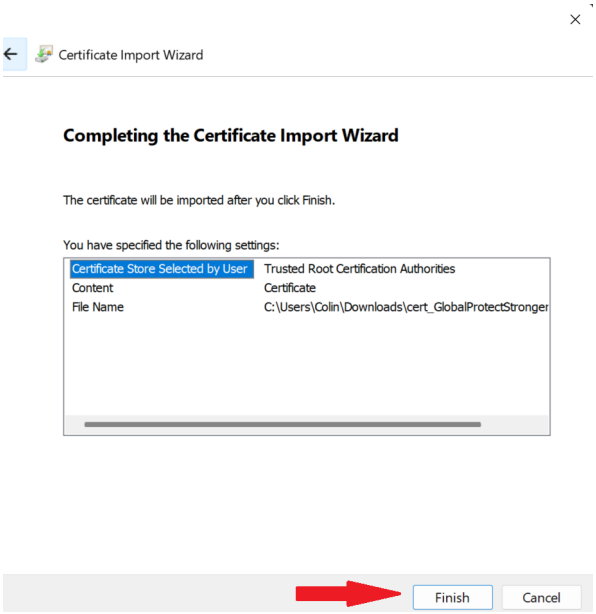
Select the certificate file downloaded earlier, then click “Next” again.



Leave the certificate store location setting as the default value, then click “Next”.

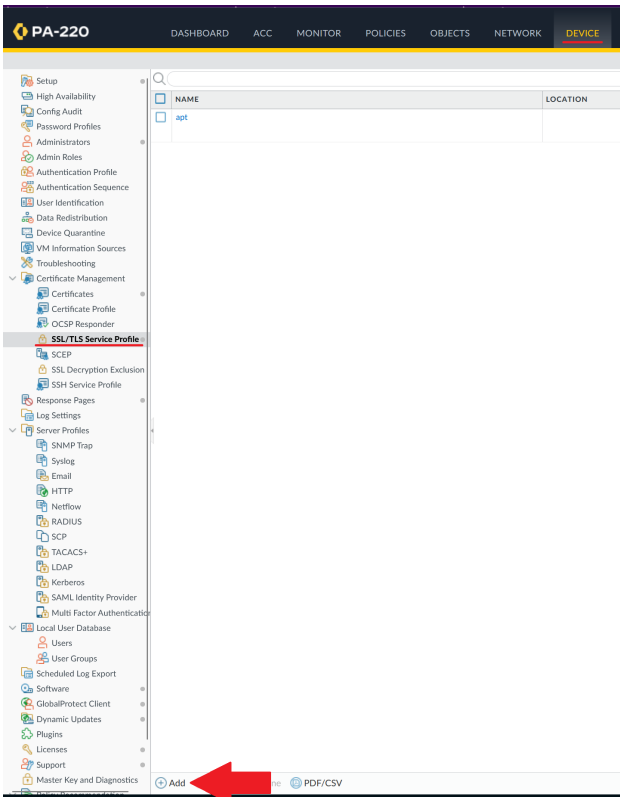


Click “Finish” to confirm the certificate import.

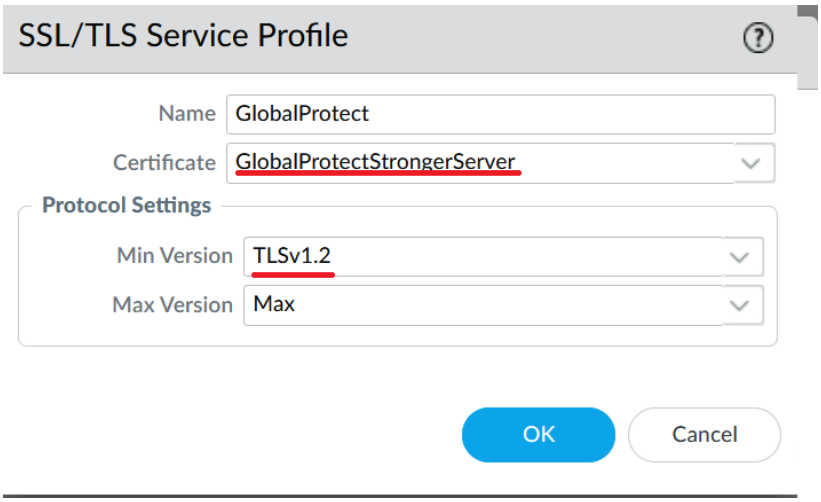


Firewall Configuration

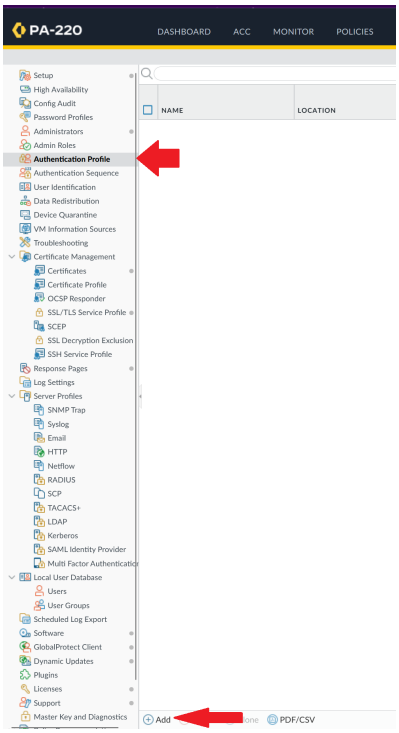
Back on the PA220, go to Device > SSL/TLS Service Profile, and click “Add”.



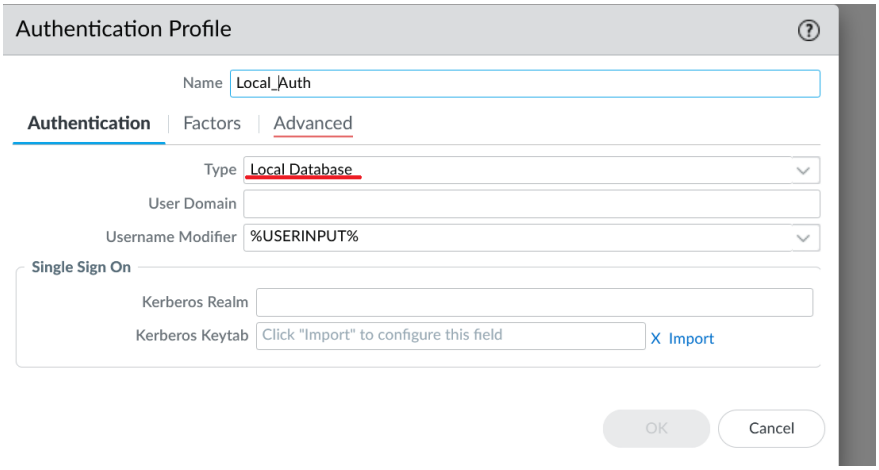
Make sure this profile uses the server certificate you set up earlier. Optionally, set the minimum TLS version to a more secure version (in this case, we used TLS 1.2)



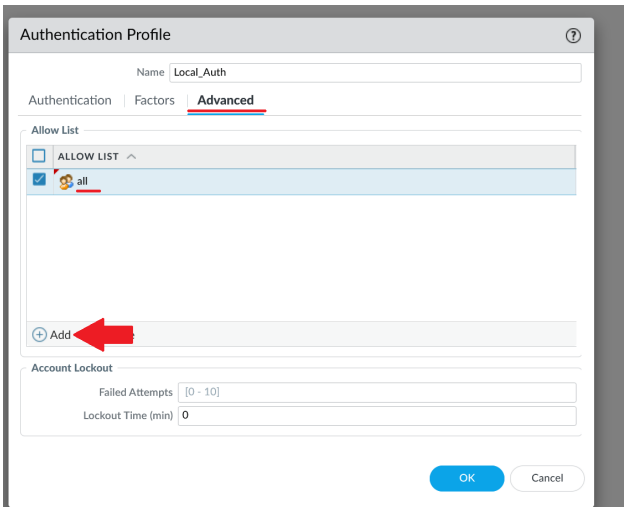
Next, go to “Authentication Profile” (still under Device) and click “Add”.



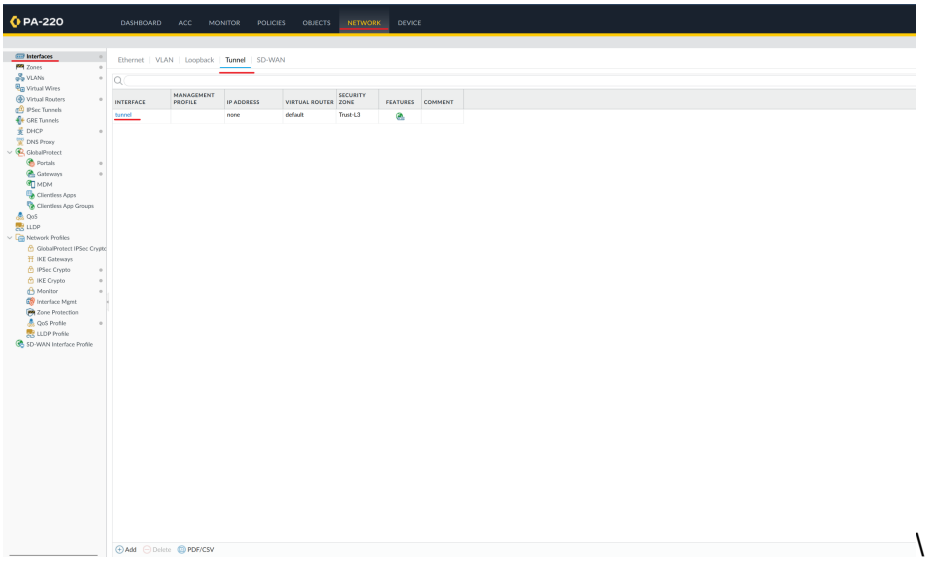
Give this profile an appropriate name and set the database type to “Local Database”.



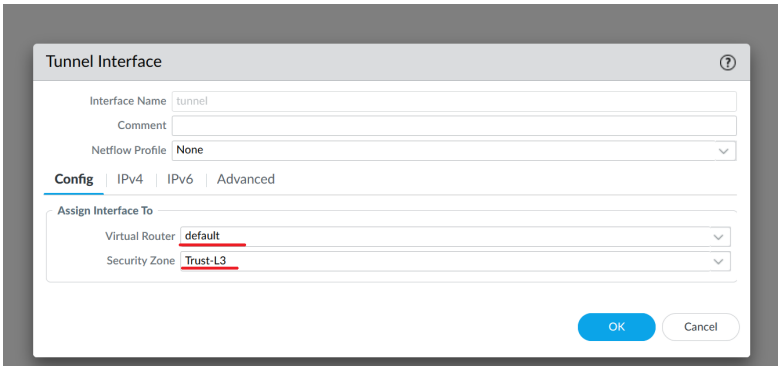
Under “Advanced”, click “Add” and type “all”.



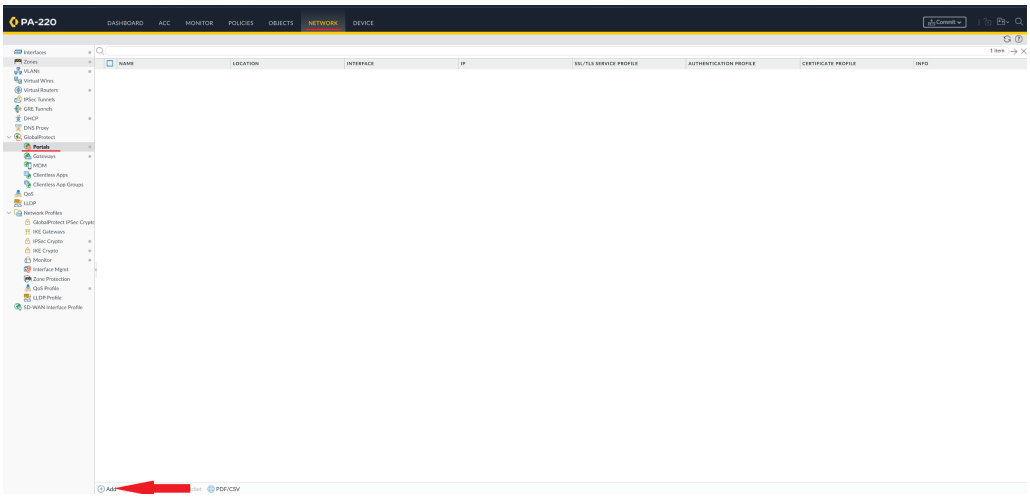
Go to Network > Interfaces > Tunnel and click on the “tunnel” interface.



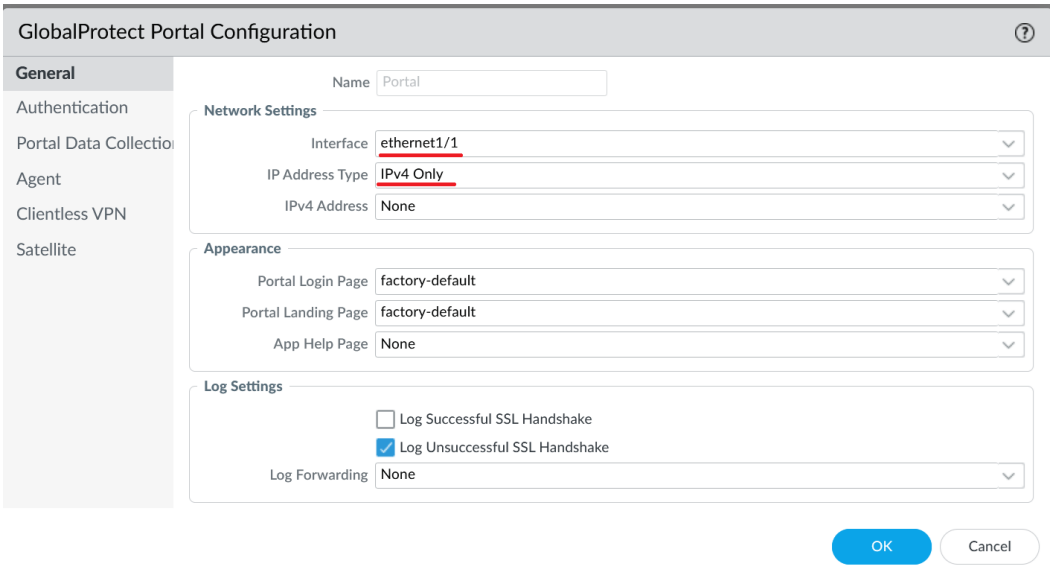
Under “Config”, configure the same virtual router and Layer 3 security zone used on your inside network.



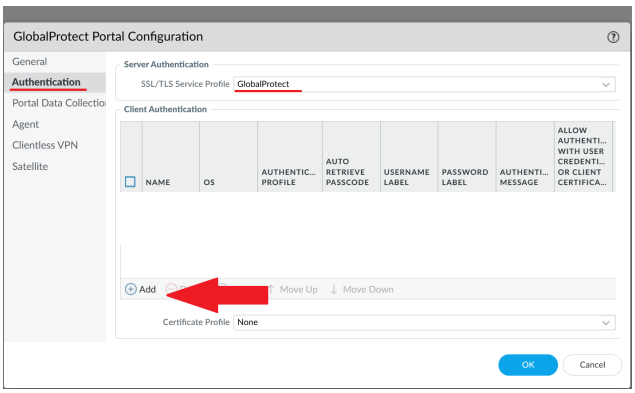
Go to Network > GlobalProtect > Portals and click “Add”.



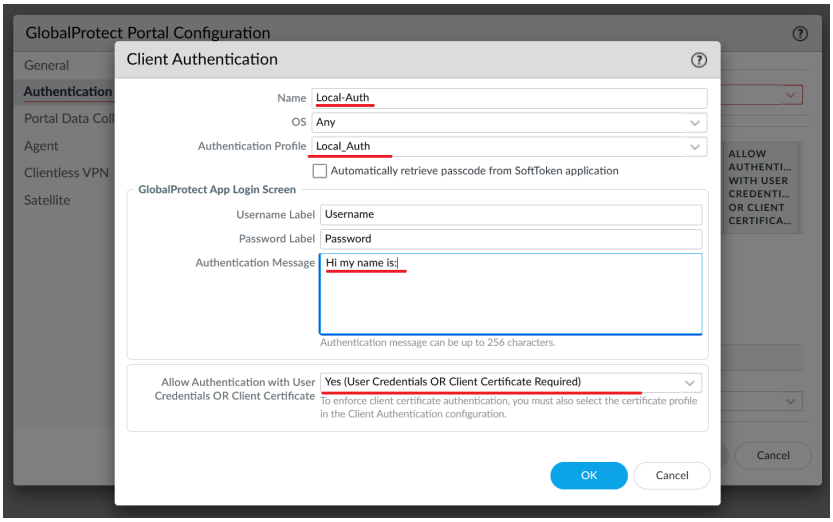
Specify the outward-facing ethernet interface and set the address type to “IPv4 only”.



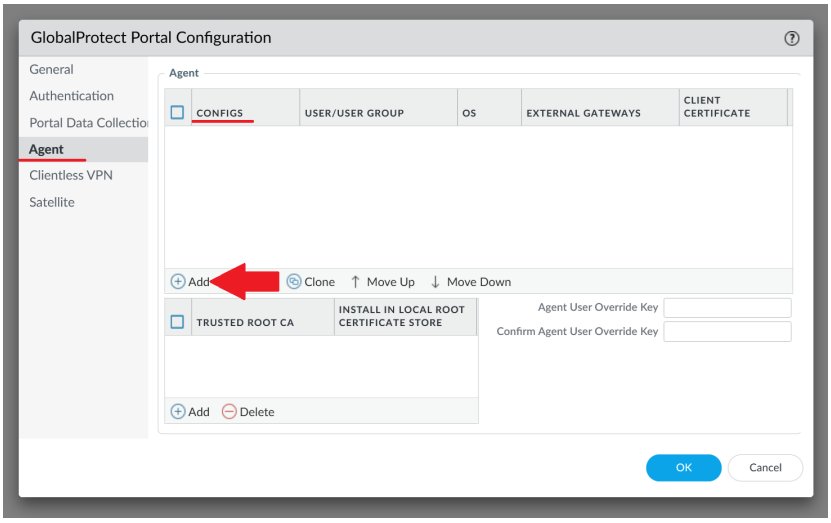
Under the “Authentication” tab, specify the SSL/TLS service profile you created earlier and click “Add”.21



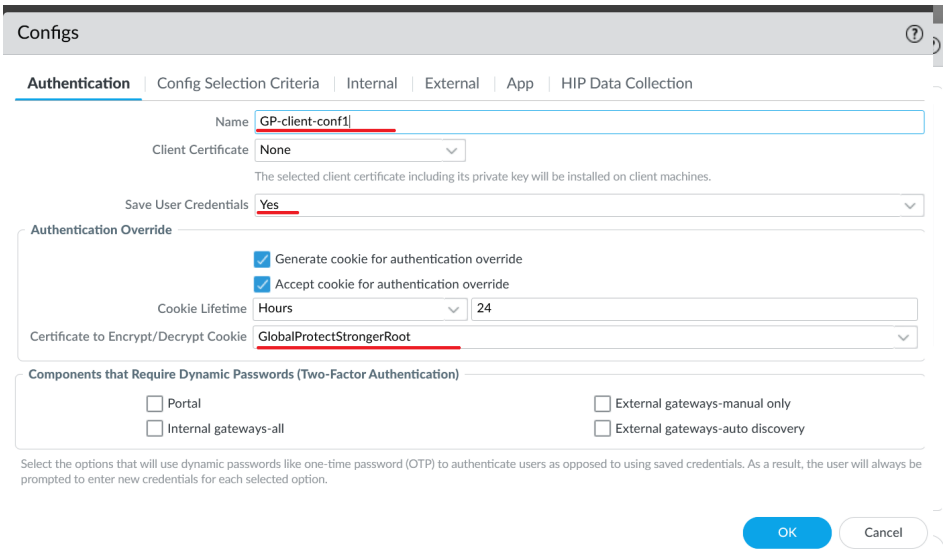
Give the client authentication profile an appropriate name and specify the authentication profile you created earlier. Create an appropriate authentication message and make sure clients can either authenticate with user credentials or client certificates.



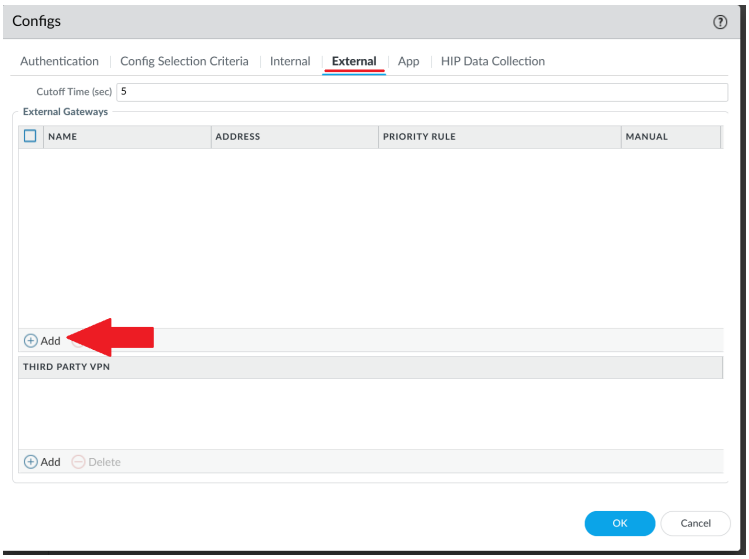
Under Agent > Configs, click “Add”.



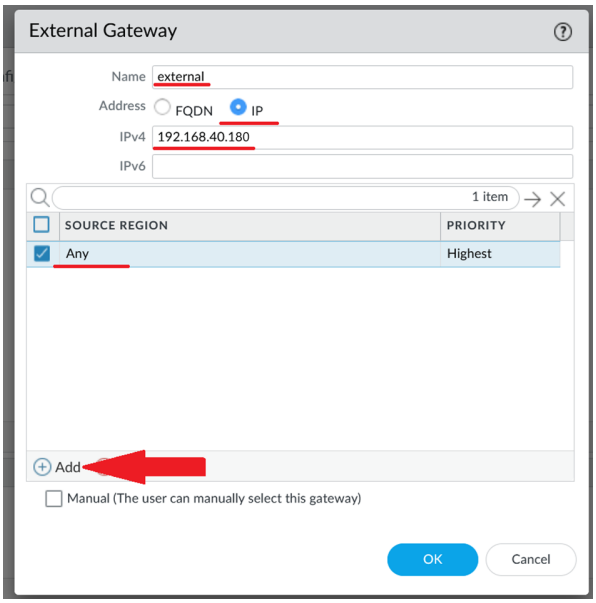
Give the config an appropriate name, and make sure to save the user credentials. Make sure the Authentication Override certificate is set to the root certificate created earlier.



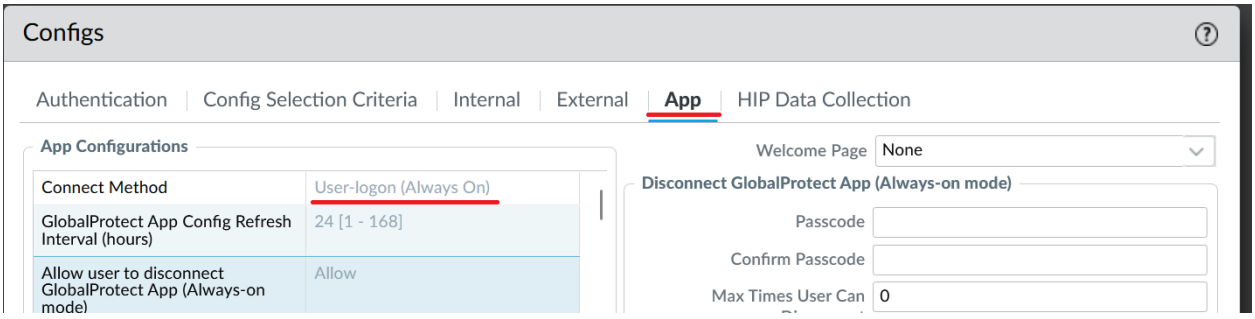
Under “External”, click “Add”.



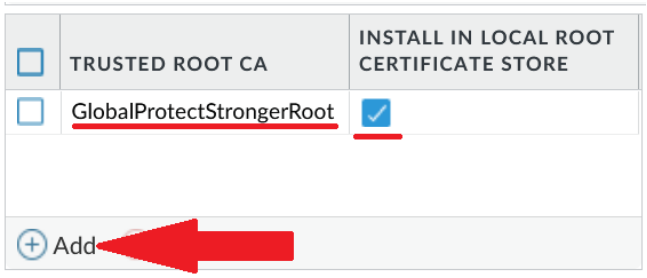
Give the gateway an appropriate name, set the mode to “IP”, and set the IP to the outward-facing IP of the gateway. Under “Source Region”, click “Add” and set it to “Any”.



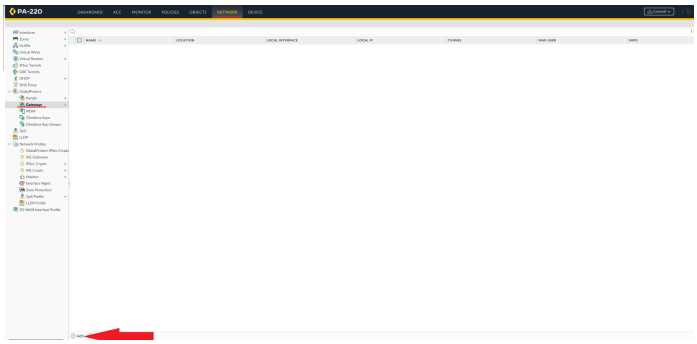
Click “OK” on the External Gateway window. Under “App”, set the connect method to “User-logon (Always On)”.



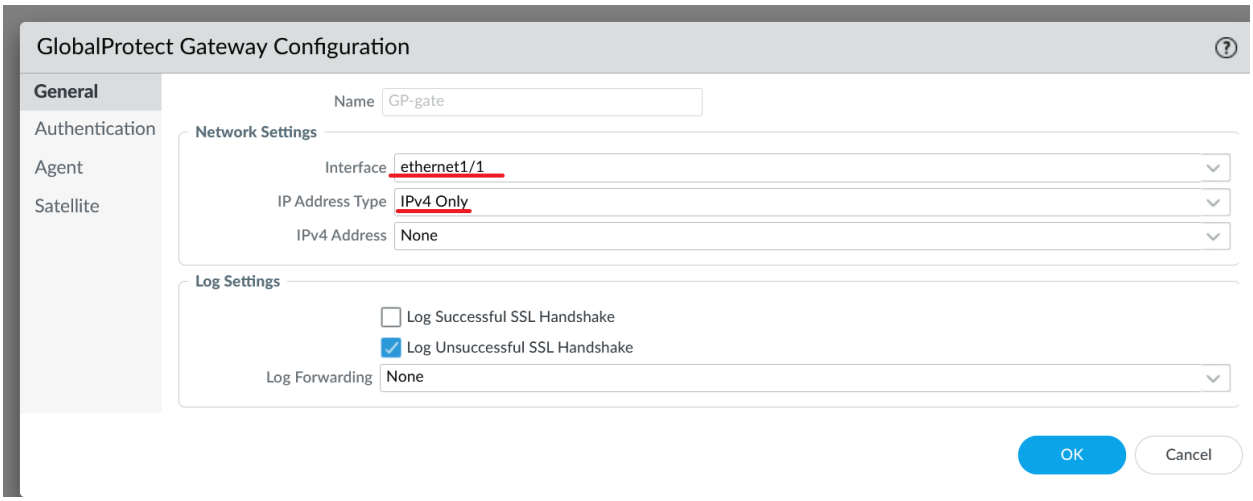
Click ok on the Configs window. Under “Trusted Root CA”, click “Add”, add the root certificate created earlier, and click “Install in local root certificate store”.



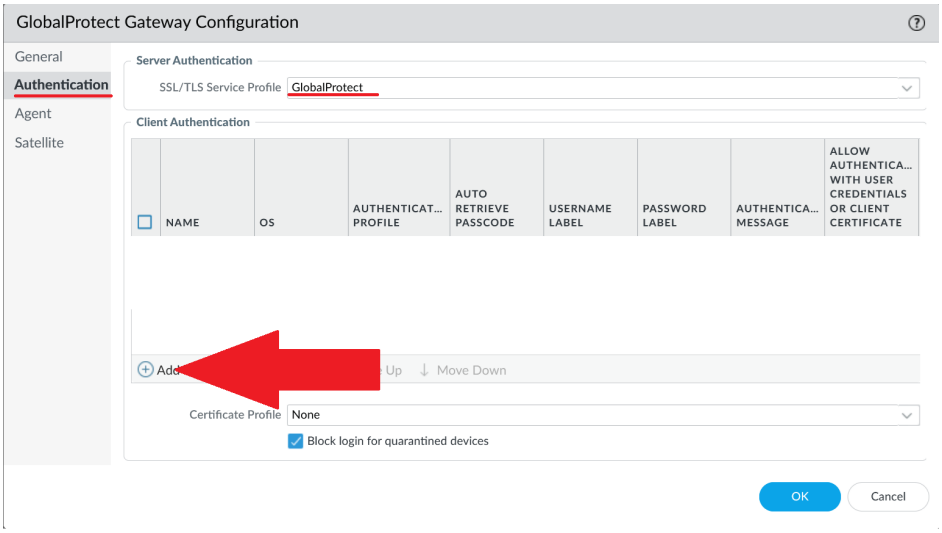
Go to Network > Gateways and click “Add”.



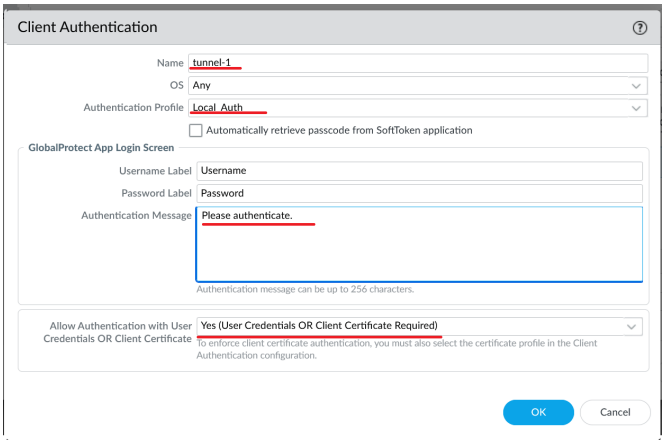
Set the interface to the outward facing interface of the firewall and leave the IP address type as “IPv4 only”.



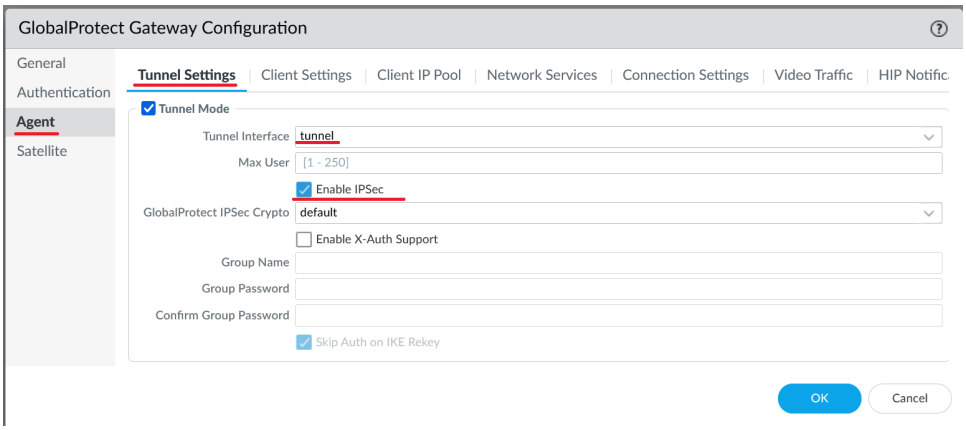
Under “Authentication”, set the SSL/TLS service profile to the profile you created earlier, and under client authentication, click “Add”.



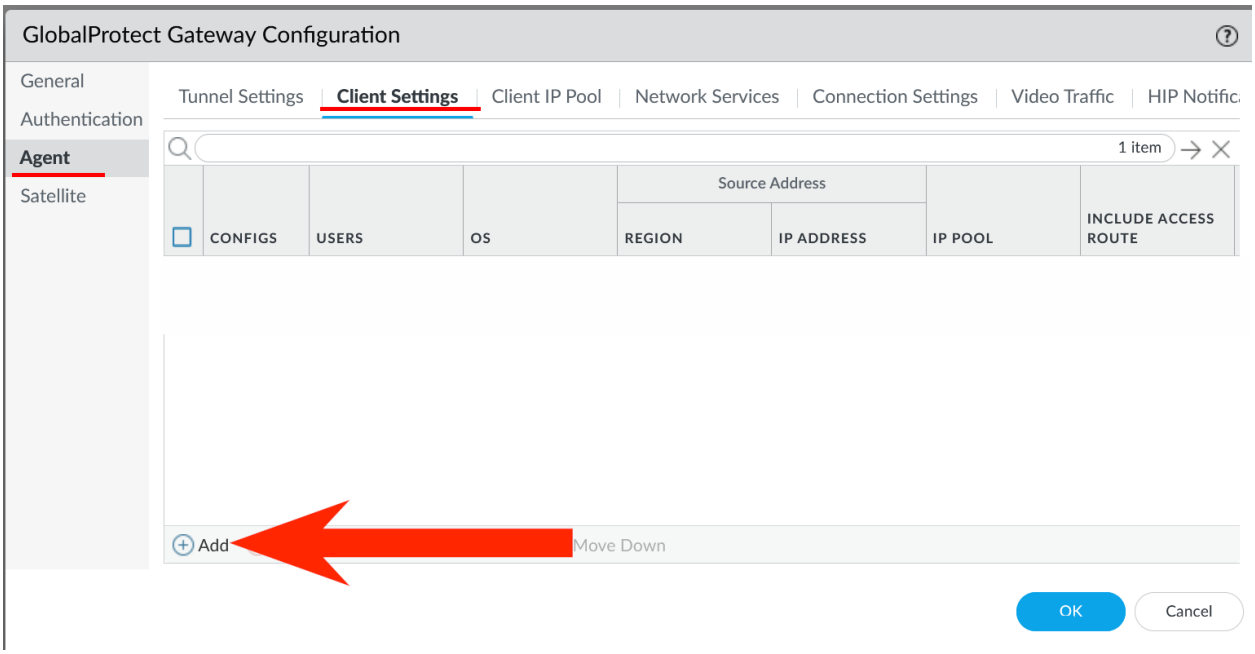
Configure an appropriate tunnel name, and set the authentication profile to the profile created earlier. Configure an appropriate authentication message, and allow authentication with user credentials OR a client certificate.



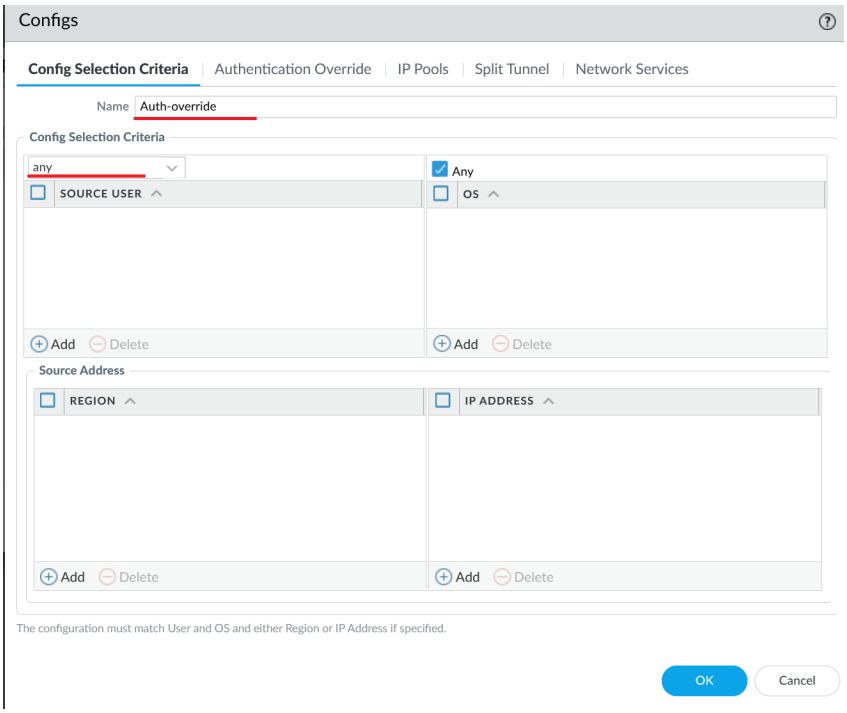
Under Agent > Tunnel Settings, set the tunnel interface to the interface created earlier, and make sure to enable IPsec.



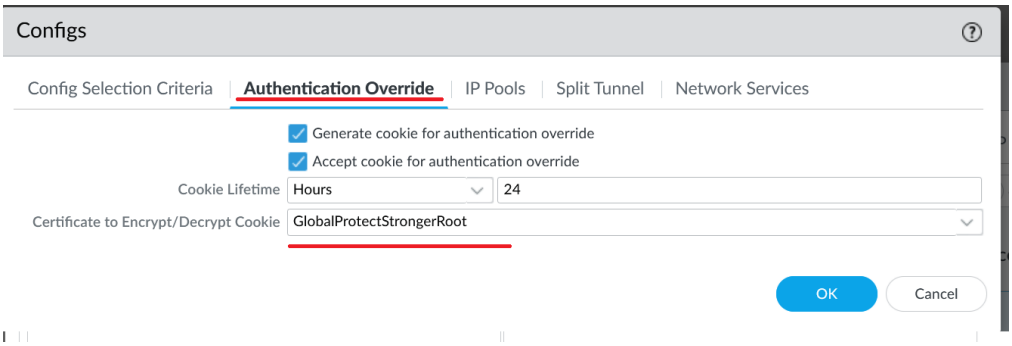
Under “Client Settings”, click “Add”.



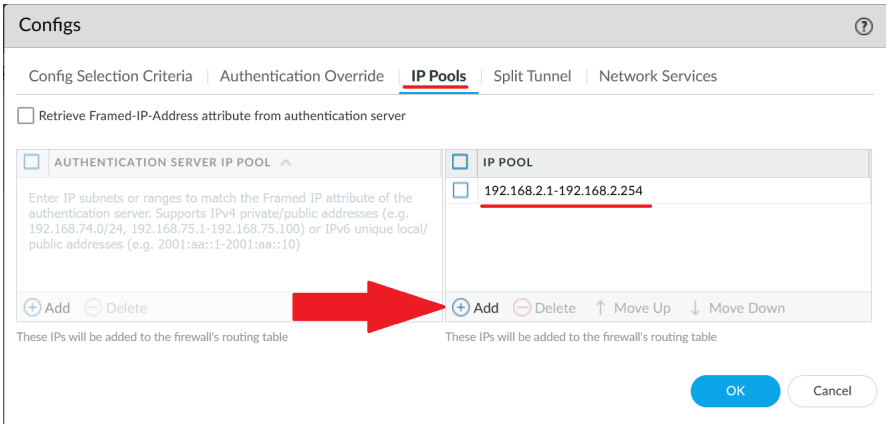
Give the configuration an appropriate name, and set the config selection criteria to "any".



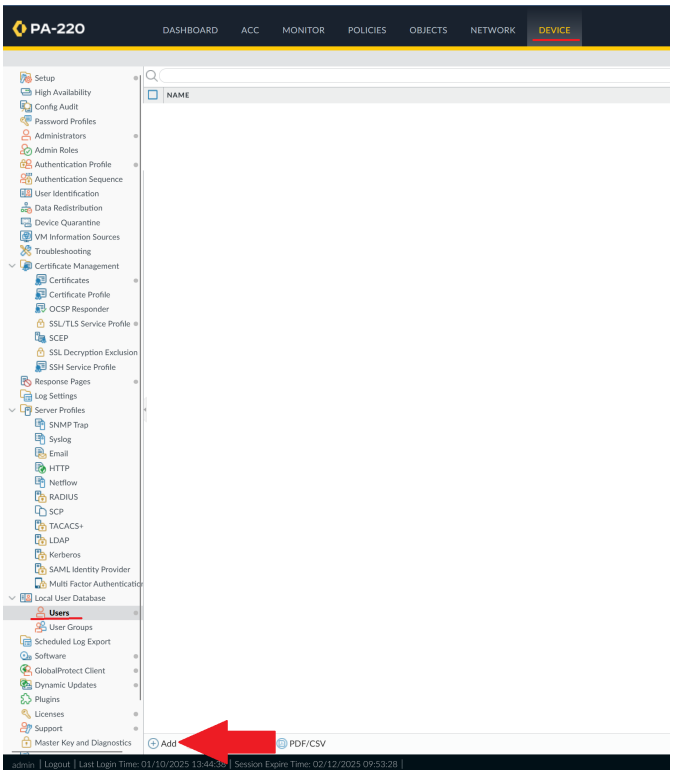
Under "Authentication Override", set the certificate to decrypt/encrypt the cookie to the root certificate created earlier.



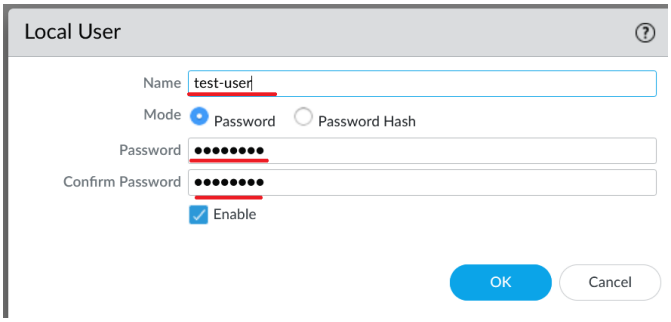
Under “IP Pools”, click “Add” and specify a valid range of IP addresses. These addresses will be dynamically allocated to clients by the GlobalProtect gateway.



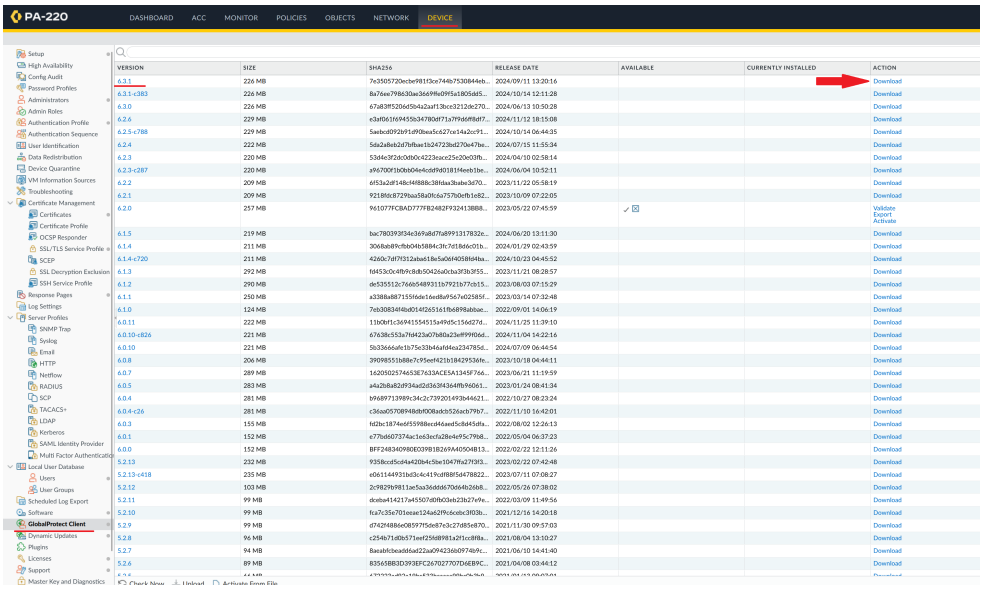
Under Device > Local User Database > Users, click “Add”.



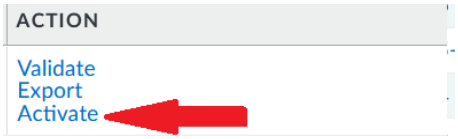
Configure an appropriate username and password.



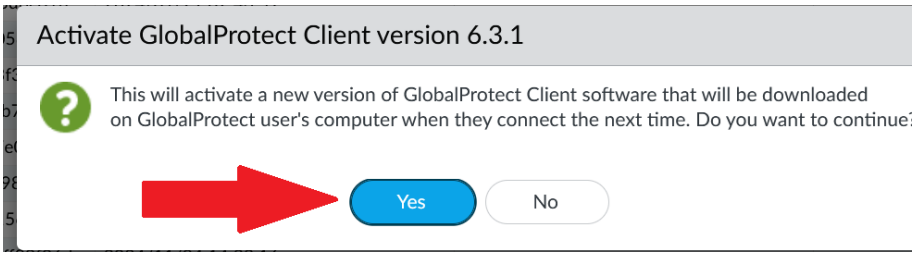
Under GlobalProtect Client, download the latest client version.



Once downloaded, click “Activate”.



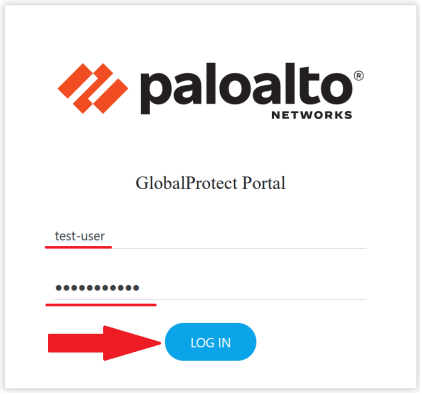
Click “Yes” to confirm.



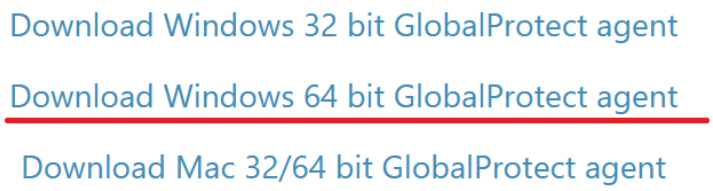
Connecting to the VPN

Switch to the outside computer. From a web browser, navigate to the outward-facing IP of the firewall.

Log in with the username and password created earlier.

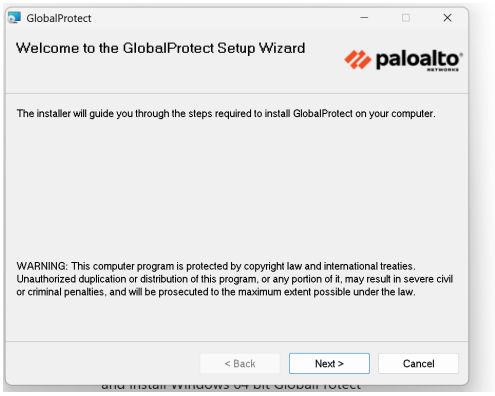


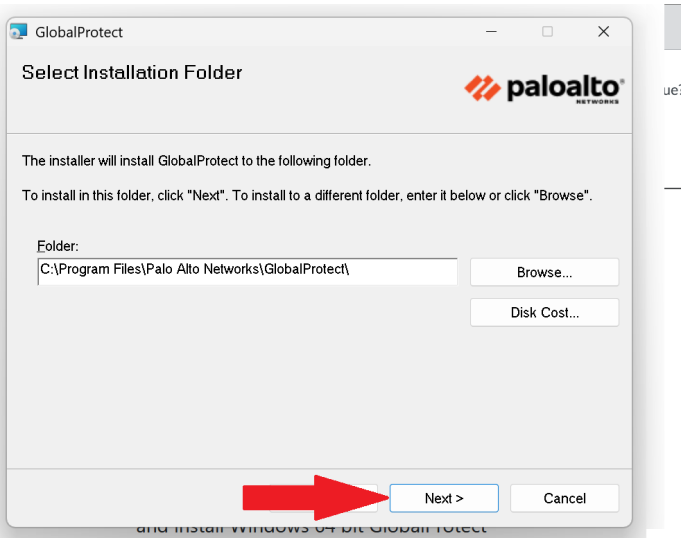
Download the appropriate GlobalProtect agent for the OS/architecture of the outside computer (in this case, Windows 64 bit).

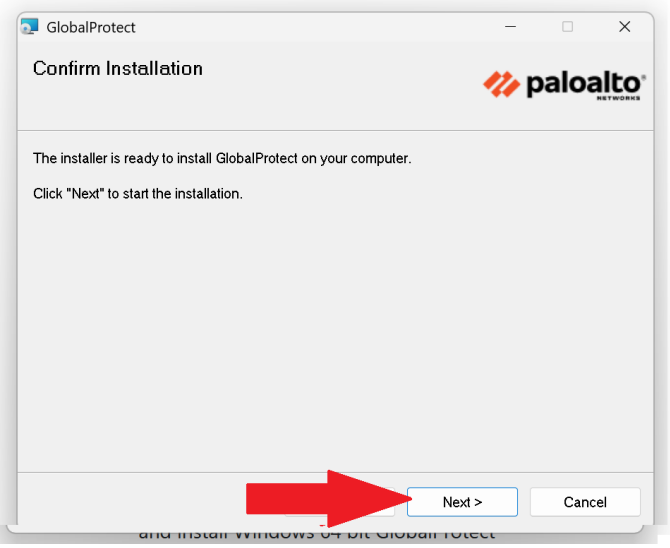


Open the downloaded installer file.

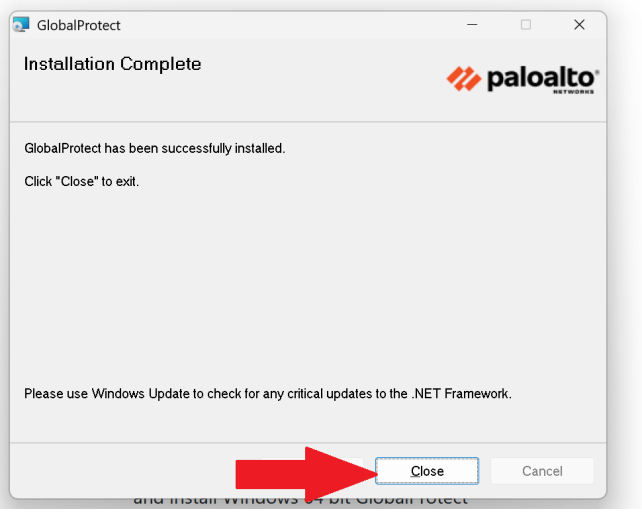
Click “Next” through the installation process.



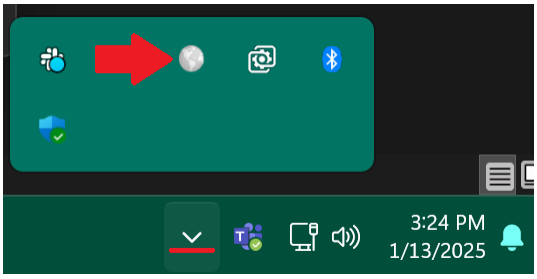




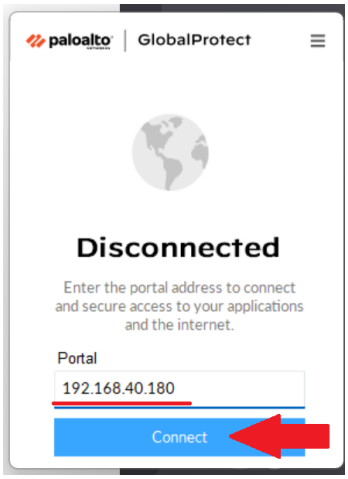
Click “Close” once the installer finishes.



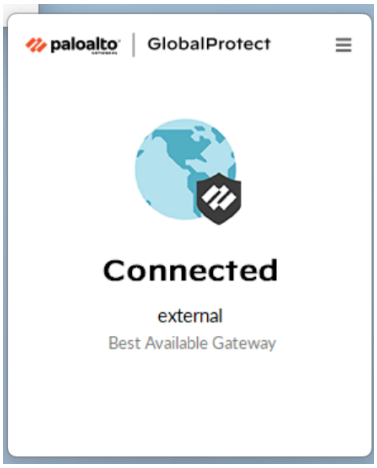
Open the GlobalProtect client from the system tray (it may be in the overflow section).



Enter the outward-facing IP of the firewall and click “Connect”.



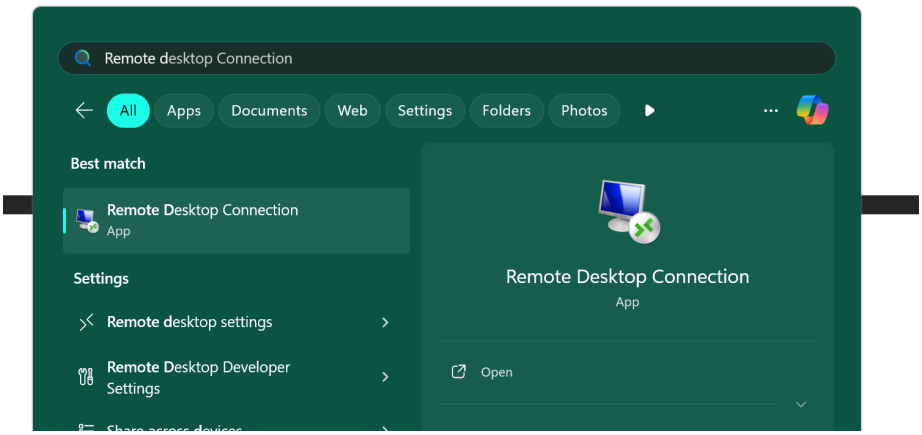
You should see the following success message:



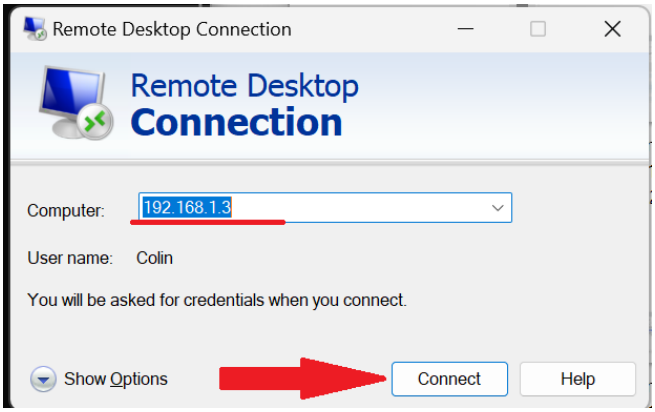
From the command prompt, run the `ipconfig` command. You should see that an address has been assigned from the IP range configured earlier.

```
C:\Users\Ram>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 5:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.2.3
```

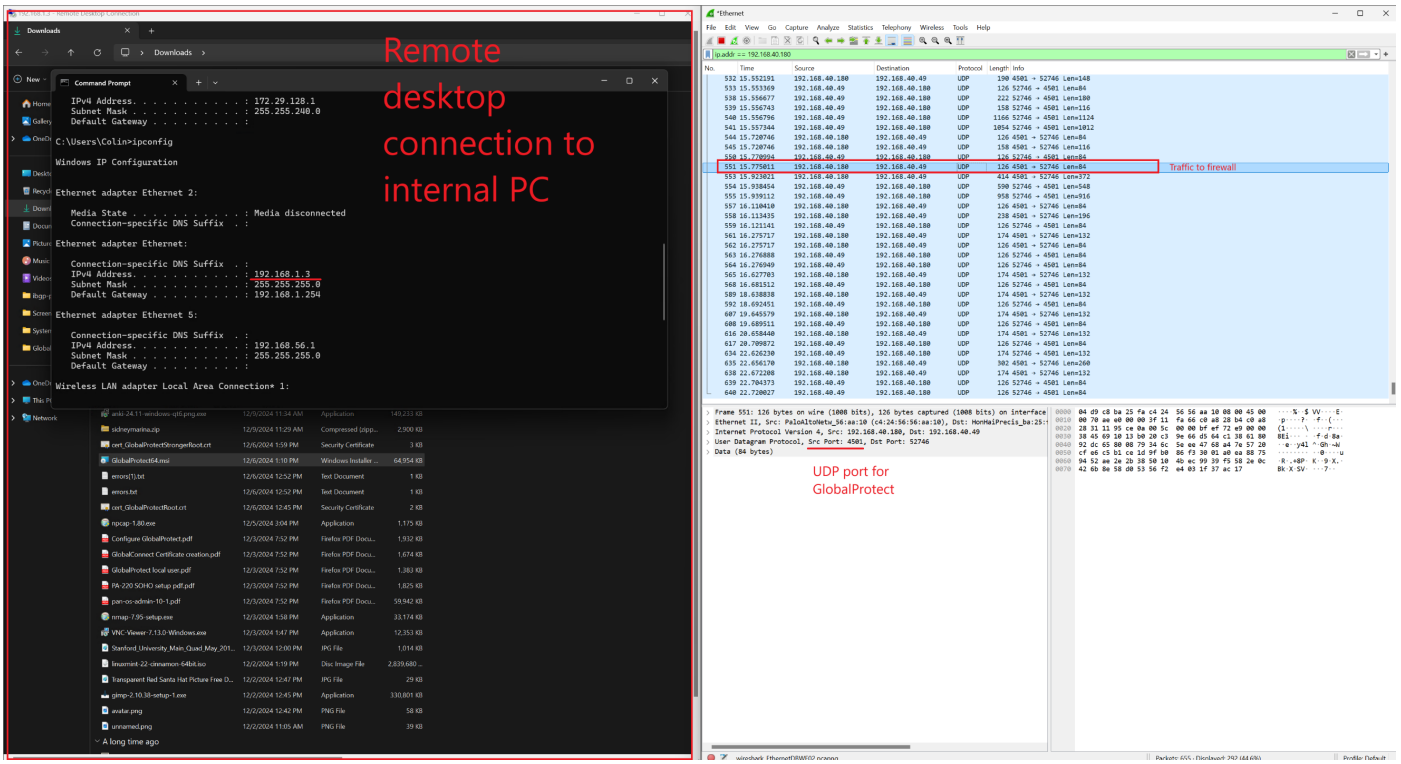
Open the remote desktop connection client.



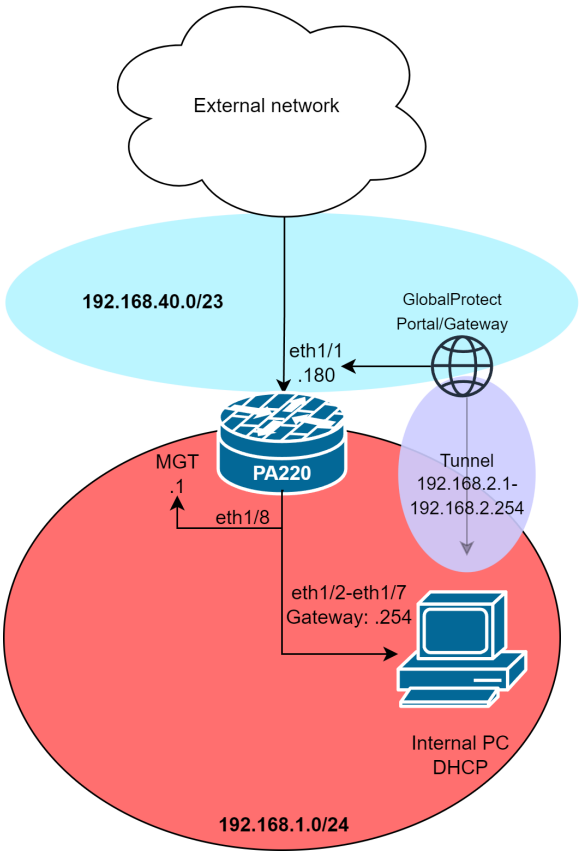
Enter the private IP of the internal computer, and click “connect”.



The remote desktop connection should establish, as shown below. By opening wireshark, you should see traffic to the firewall using port 4501 (the UDP port GlobalProtect uses).



Network Diagram



Problems

- We originally had issues with Windows RDP, which refused to connect even with both computers on the internal network. The fix for this was simply restarting both PCs.

Conclusion

To wrap up, this lab provided ample insight into the GlobalProtect VPN client and server, and how to create a secure private tunnel into a Palo Alto firewall. This information, being both niche and in-demand, is highly valued in the networking industry, and I'm very grateful to have had this opportunity to learn. Overall, this lab wasn't too difficult, and I'm very confident I could replicate this lab's setup in a real-life SOHO environment.

AWS Academy Cloud Foundations: Configuring Identity and Access Management, Virtual Private Cloud, and Elastic Compute Cloud

Colin J. Faletto, CCNA

aws academy

Purpose

This write-up is intended to document and explain the first three labs in the AWS Academy Cloud Foundations course. These labs are intended to provide an introduction to very basic AWS concepts, such as basic security, cloud networking, and virtual machines. These concepts are essential for new cloud engineers to provide parallels to the core skills of traditional IT. These labs also provide a strong foundation of knowledge for the AWS management console, as they all take place primarily inside this console.

Background

Amazon is a company based in Seattle that runs the biggest e-commerce platform in the world. They were started in 1994 by former CEO Jeff Bezos and have grown from a small online bookstore to a giant online store offering a wide variety of products. Amazon also has a strong physical retail presence in the grocery space with their Amazon Fresh and Whole Foods chains, and has a strong online media presence through Twitch, Prime Video, and Amazon Music, which provide entertainment in the form of livestreams, movies and television shows, and music respectively. Amazon also has a popular line of e-readers and tablets with their Kindle brand and has a successful brand of artificial intelligence assistants with their Amazon Alexa A.I. and their Amazon Echo line of smart speakers.

Amazon Web Services, or AWS, is Amazon's cloud computing division. It was created in 2002 to provide simple web services to customers and expanded to cloud storage and computing in 2006. It is the leading cloud service provider and is popular for its pay-as-you-go service model. AWS provides services to everyone from small businesses to massive companies like Coca-Cola and Apple, and even provides web infrastructure to government branches. AWS takes the responsibility and cost of managing a data center out of the hands of businesses and maintains a massive global network of Amazon data centers that split customer traffic among them. AWS currently has 34 geographic regions, each of which have multiple availability zones which themselves contain multiple data centers. These data centers are in undisclosed locations for security reasons, though their general position is published. AWS offers services for virtual machines, cloud storage, database management, machine learning, IoT services, cloud networking, and much more.

Amazon Elastic Compute Cloud, or EC2, is an AWS service that allows customers to create virtual machines in the AWS cloud. These machines are very versatile, as they can be allocated as many or as few resources (CPU, RAM, GPU) as needed and can run nearly any operating system. By default, EC2 instances will run Amazon Linux, which is a version of Linux optimized for AWS servers. Amazon's e-commerce platform, its primary source of revenue, has been running on EC2 instances for over a decade. EC2 instances have a variety of different types, which are optimized for different purposes such as memory (R series, X series), compute (C series), and storage (H series, I series, D series).

Amazon Virtual Private Cloud, or VPC, is an AWS service that provides a virtual network inside the AWS cloud. This service allows AWS objects, such as EC2 instances, to communicate with each other. In a VPC, each EC2 machine is assigned a

unique private IPv4 address, which is then connected via NAT to a public address on an internet gateway. Using this gateway, machines in the VPC can communicate with other AWS VPCs and other Internet-connected machines. Amazon VPC is provided at no additional charge to customers using EC2 instances.

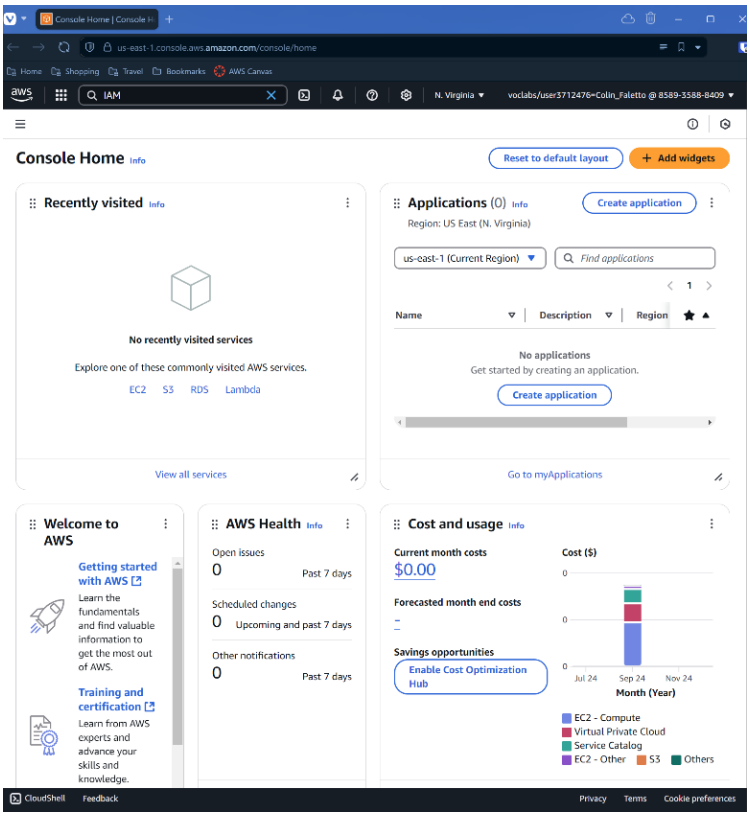
Amazon Identity and Access Management, or IAM, is an AWS service that provides a layer of security to customers by limiting the resources different users can access. IAM follows the principle of least privilege, meaning that by default, all AWS controls are blocked for users unless they have been explicitly granted permissions. IAM represents a portion of the customer responsibilities in the AWS shared responsibility model, which is a model outlining that AWS is responsible for the physical security of data centers and networks while the customer is responsible for keeping their customer data and configurations safe. One of IAM's unique features is its role feature, which creates identities with elevated permissions that can be temporarily assigned to users. This feature works similarly to the "sudo" command in unix-based operating systems.

Lab Summary

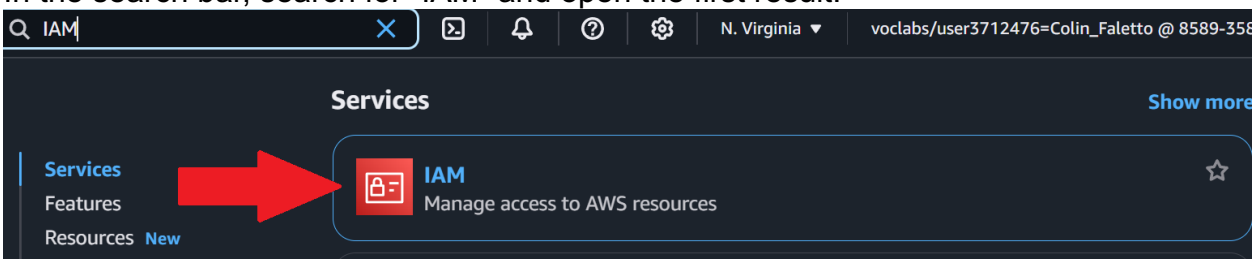
This write-up covers three different AWS labs. The first lab covers AWS IAM. The lab entails assigning permissions to three different users to allow them to interact with S3 and EC2 services. Two of these users are support users, who are assigned read-only permissions to EC2 and S3 respectively. The other user is an administrator with start and stop access to EC2 instances. The second lab covers AWS VPC, and entails creating a VPC with four different subnets, two public and two private, spread across two different availability zones. The lab also involves creating a security group to allow HTTP access to machines in the second public subnet. The third lab involves creating a web server EC2 instance, allowing HTTP access through a security group, then resizing the instance and testing the stop protection feature.

Lab Commands (Lab 1 IAM)

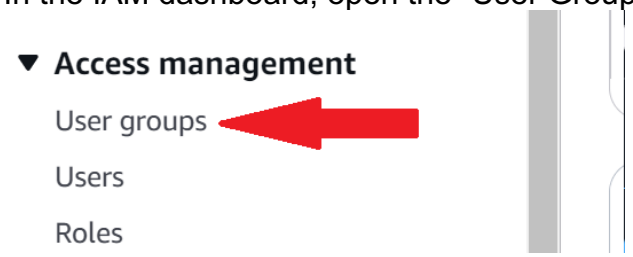
Log into the AWS management console.



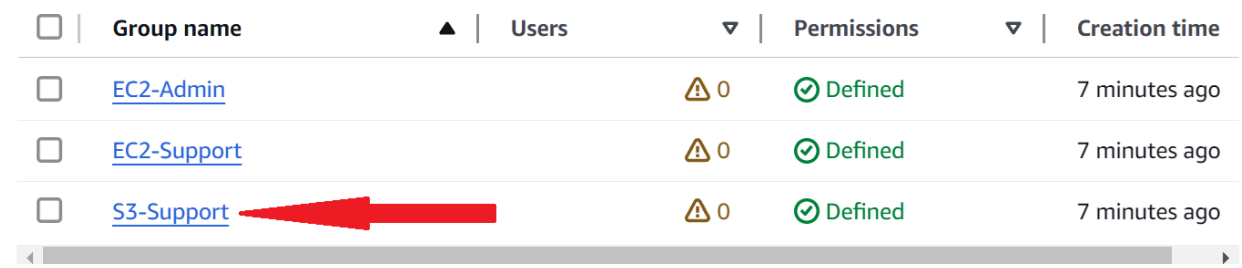
In the search bar, search for “IAM” and open the first result.



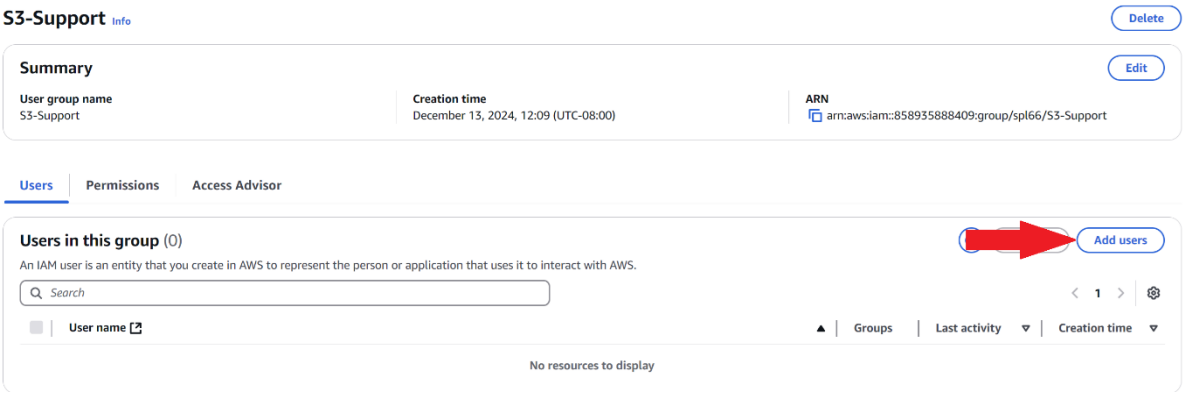
In the IAM dashboard, open the “User Groups” tab from the sidebar.



Open the “S3-Support” group.



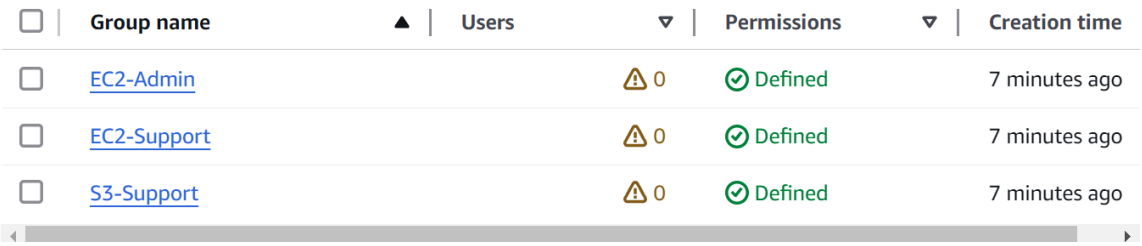
Click “Add Users”.



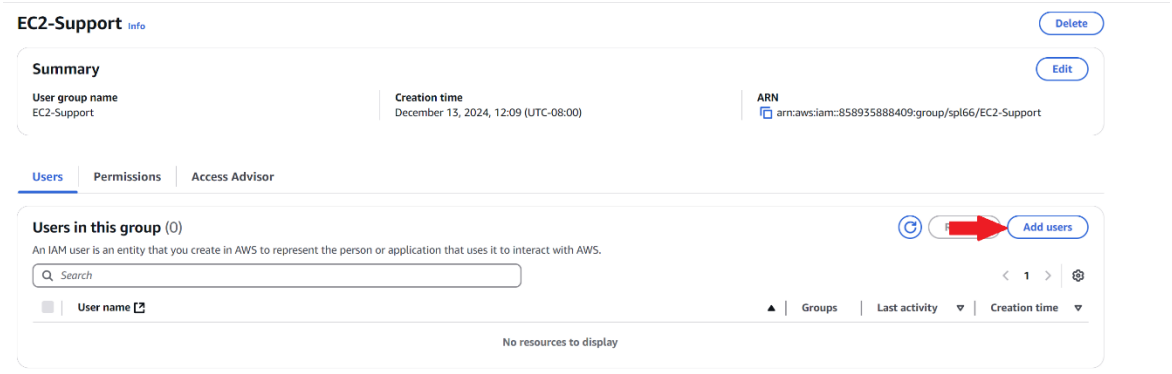
Check the box next to “user-1”.

Click “Add Users”.

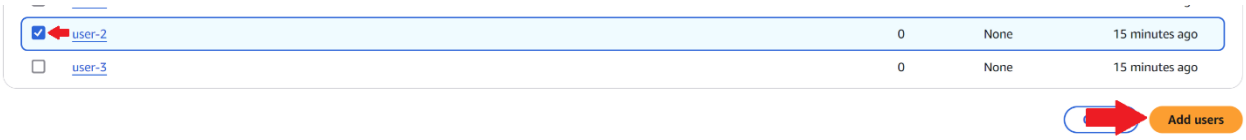
Return to the “User Groups” section and select “EC2-Support”.



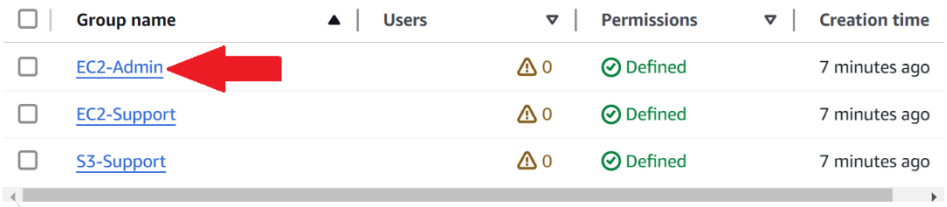
Click “Add Users”.



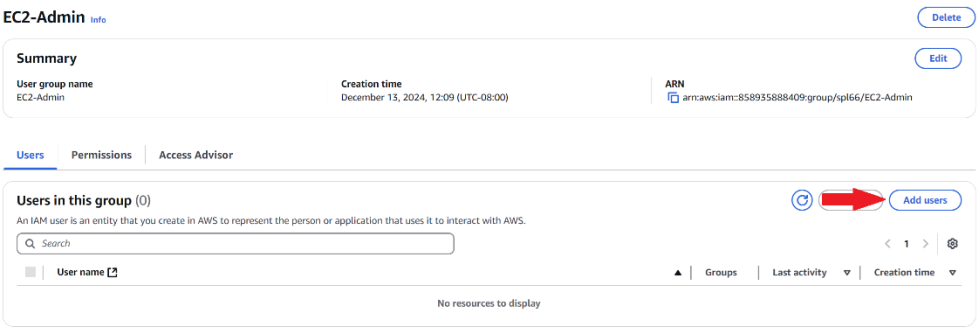
Select “user-2” and click “Add Users”.



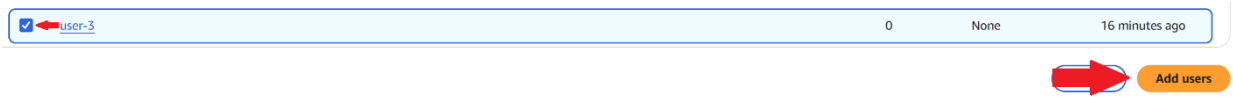
Return to the “User Groups” section and click on “EC2-Admin”.



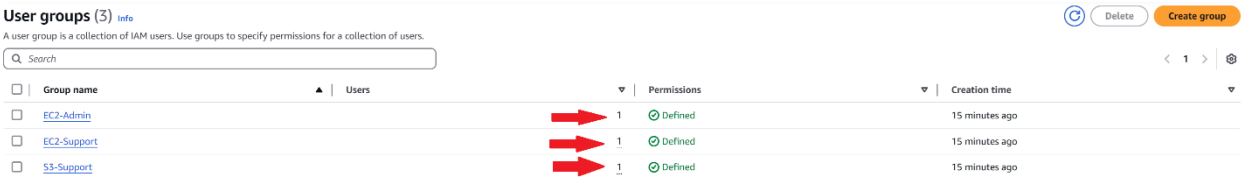
Click “Add Users”.



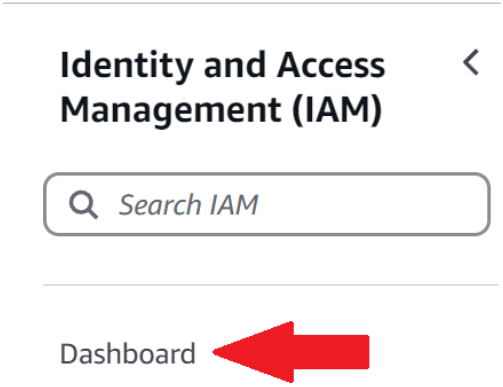
Click the checkbox next to “user-3” and click “Add Users”.



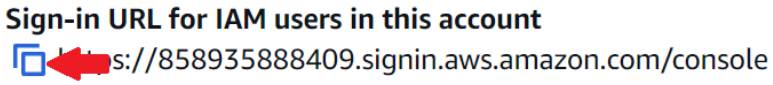
If done correctly, each user group should have a “1” next to it.



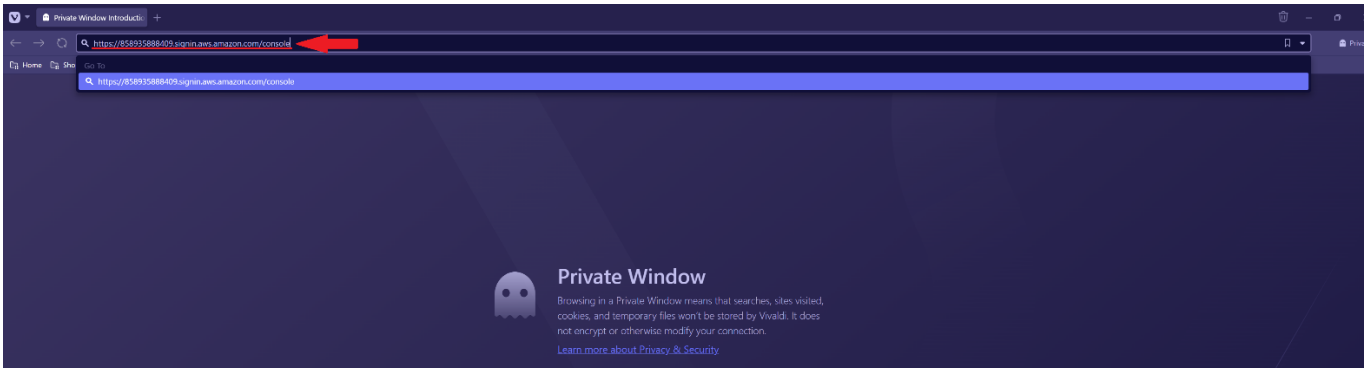
Return to the dashboard.



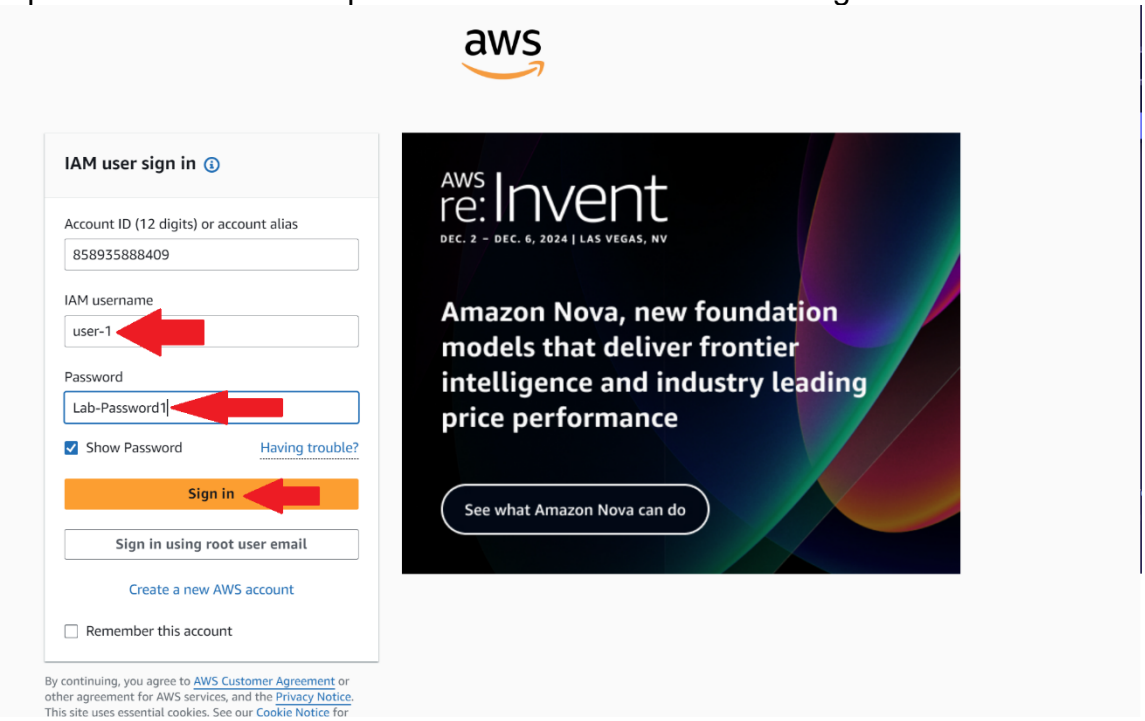
On the dashboard page, find and copy the sign-in URL for IAM users. This URL will be used to test the permissions that have just been set up.



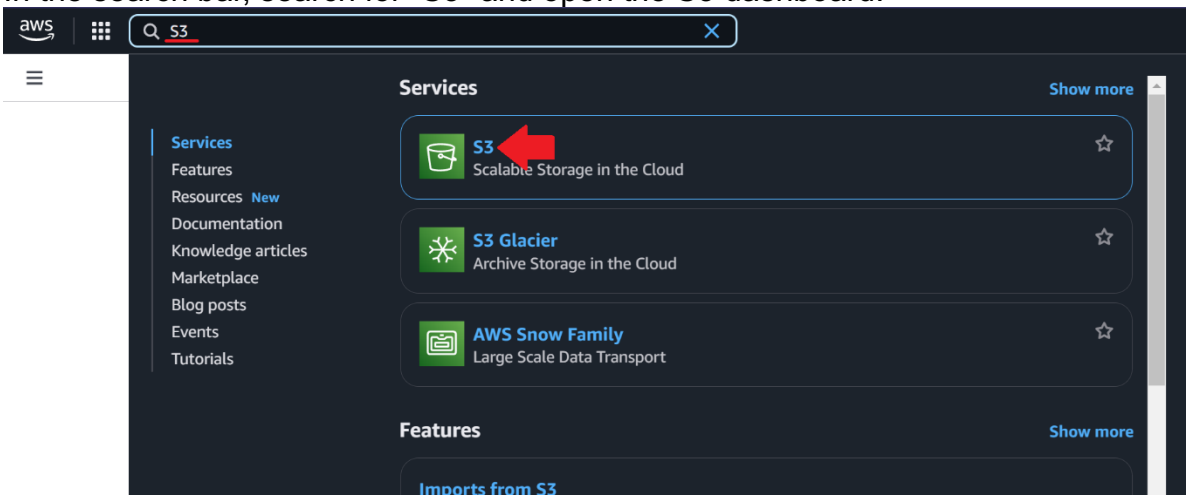
Open a new private browser window and input the URL.



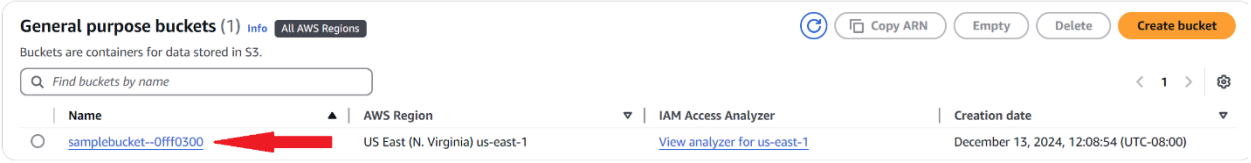
Input the username and password for “user-1” and click “Sign In”.



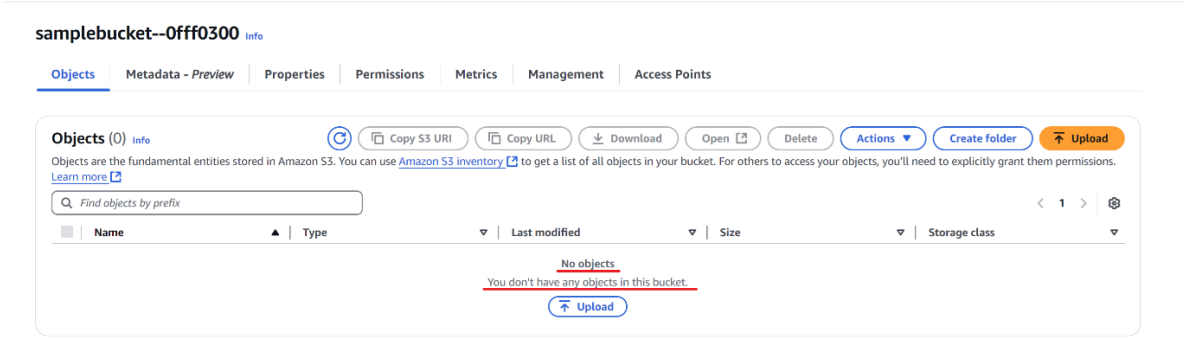
In the search bar, search for “S3” and open the S3 dashboard.



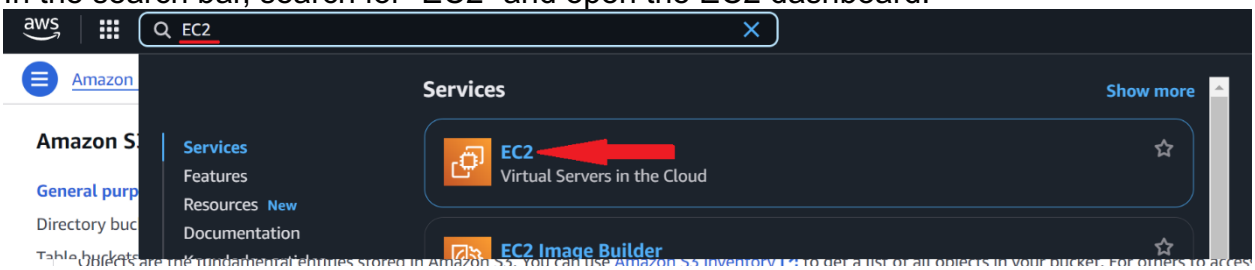
From the S3 dashboard, click on the sample bucket shown.



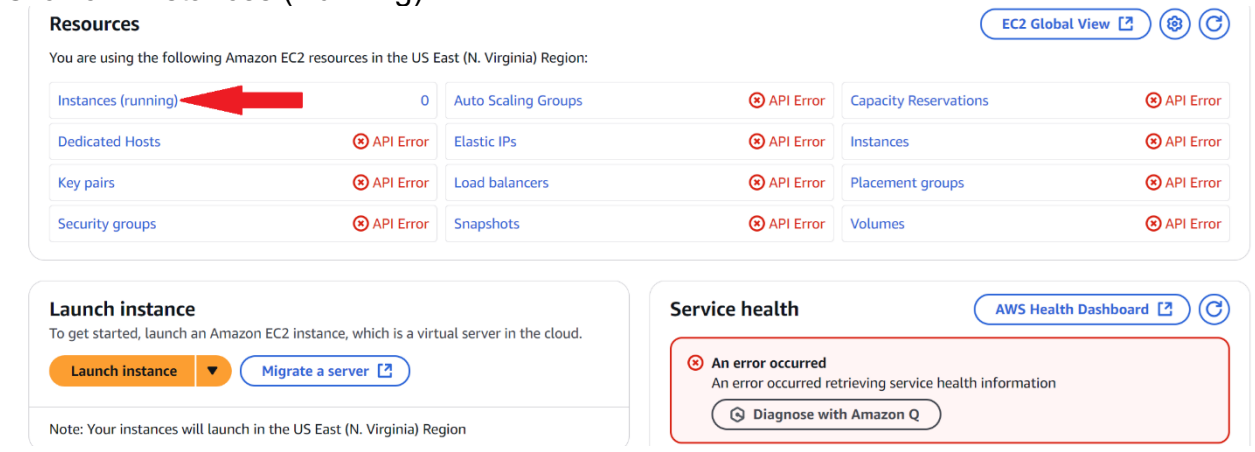
If permissions have been set correctly, user-1 should be able to see the objects in the bucket. In this case, there are no objects in the bucket, which should be evident in a message displayed to the user.



In the search bar, search for “EC2” and open the EC2 dashboard.

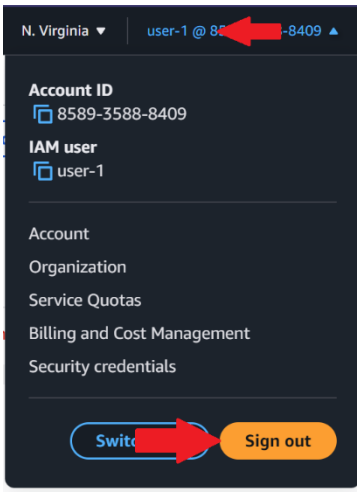


Click on “Instances (Running)”.

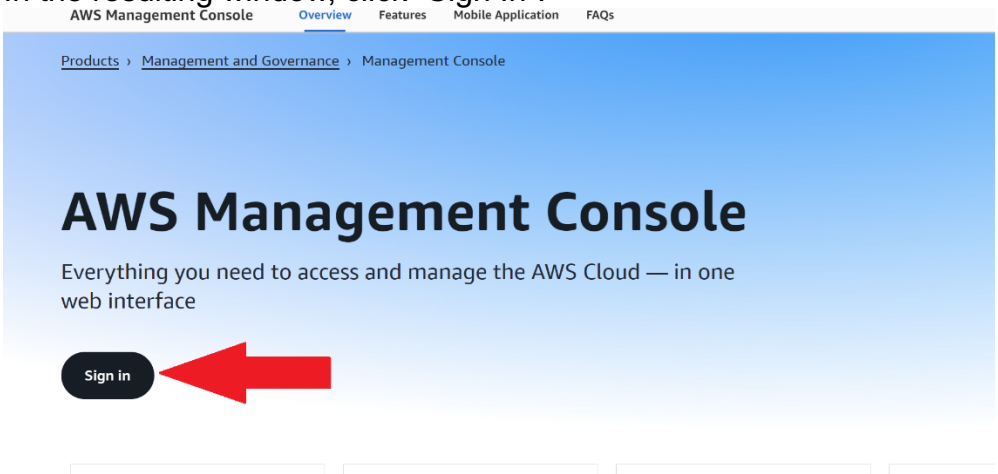


If permissions are set up correctly, the following error will occur:

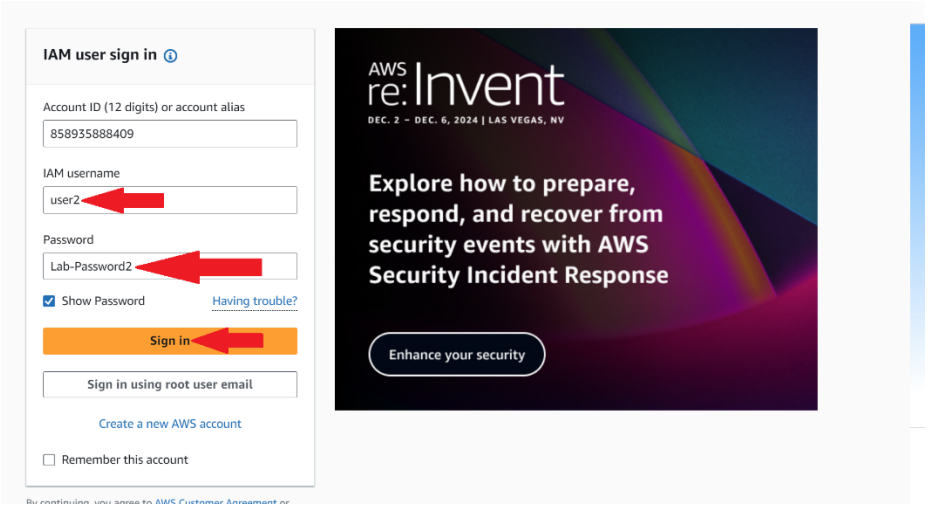
This is intended behavior, as user-1 is only authorized to access S3 services.
Click the “user-1” button in the top right corner and click “Sign Out”.



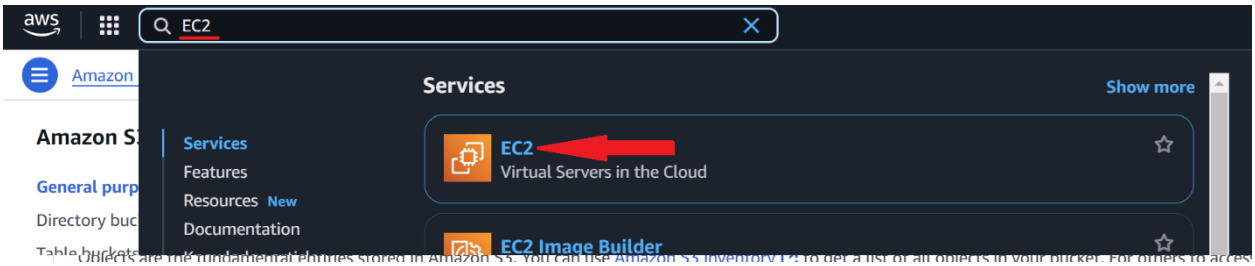
In the resulting window, click “Sign In”.



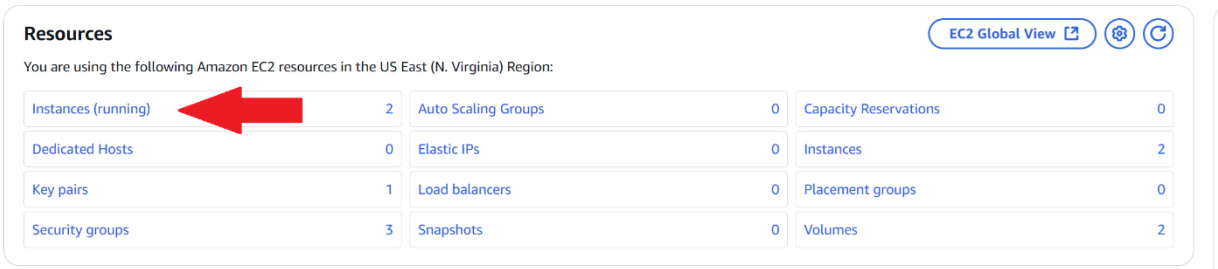
Enter the username and password for user-2 and click “Sign In”. Your AWS account ID should be automatically filled, but if it isn’t, you can paste the same sign-in URL from before.



Return to the EC2 dashboard.



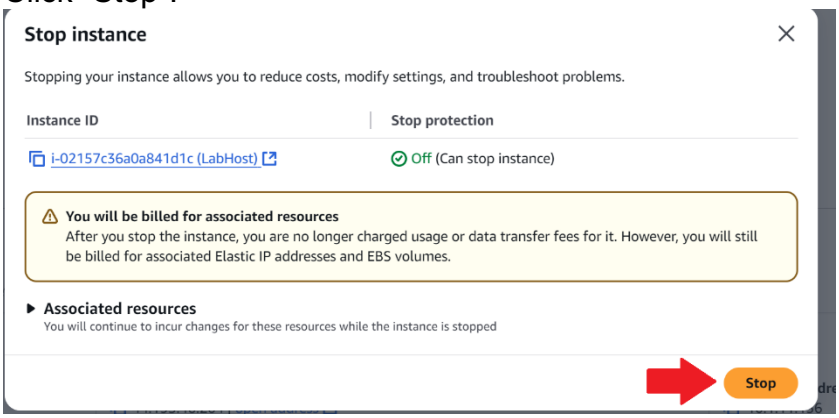
Click on “Instances (running)”. You’ll notice a distinct lack of “API Error” messages, unlike the page for user-1.



You’ll notice that the instances will properly display this time. Select the “LabHost” instance.

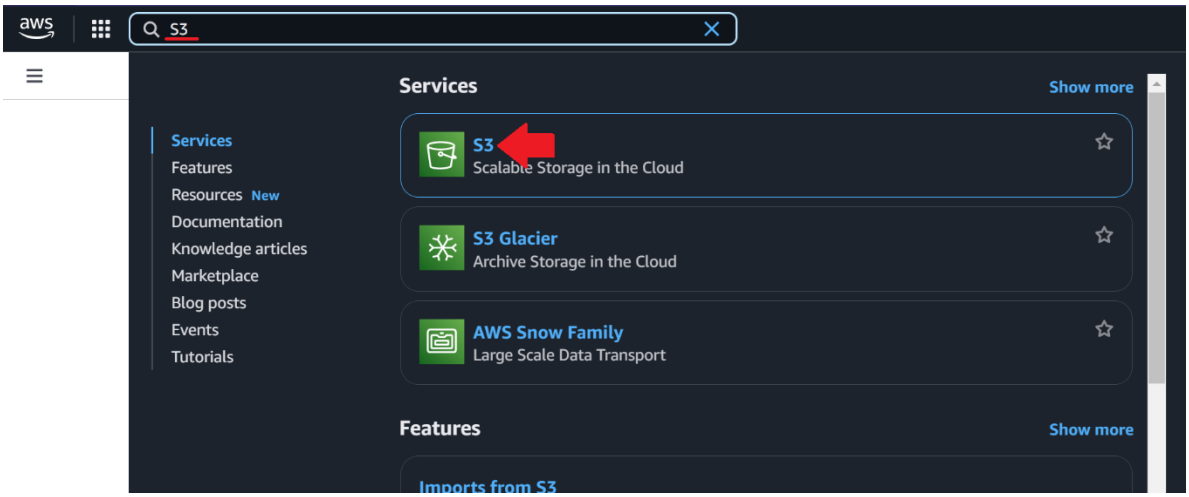
Click on “Instance state” > “Stop Instance”.

Click “Stop”.

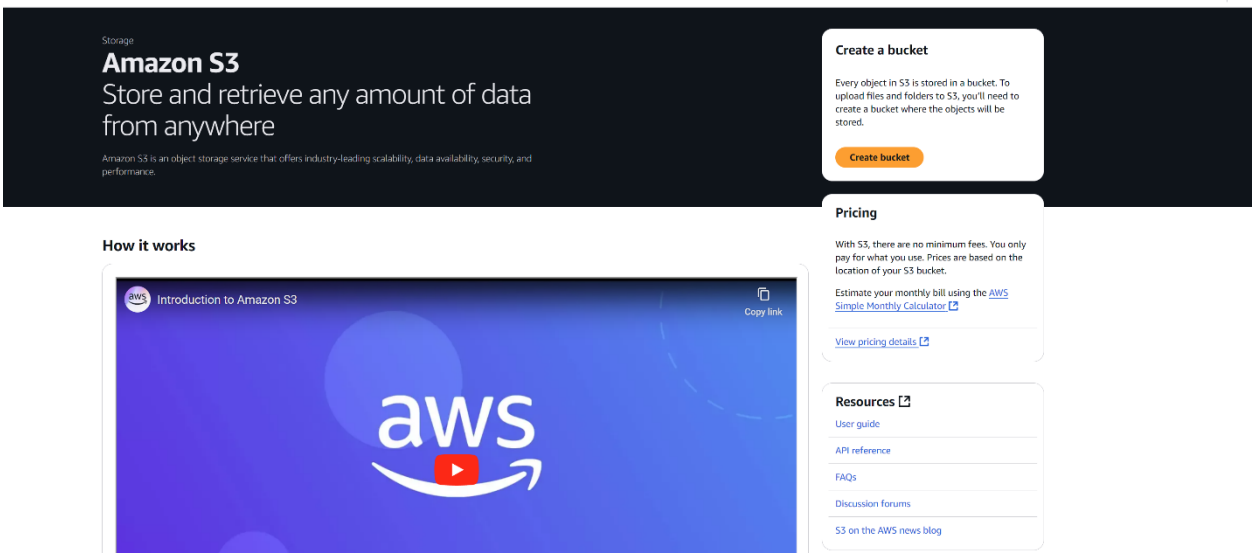


Since user-2 doesn’t have the appropriate permissions, you should get the following error message:

To confirm that user-2 doesn't have access to S3, access the S3 dashboard from the search bar.

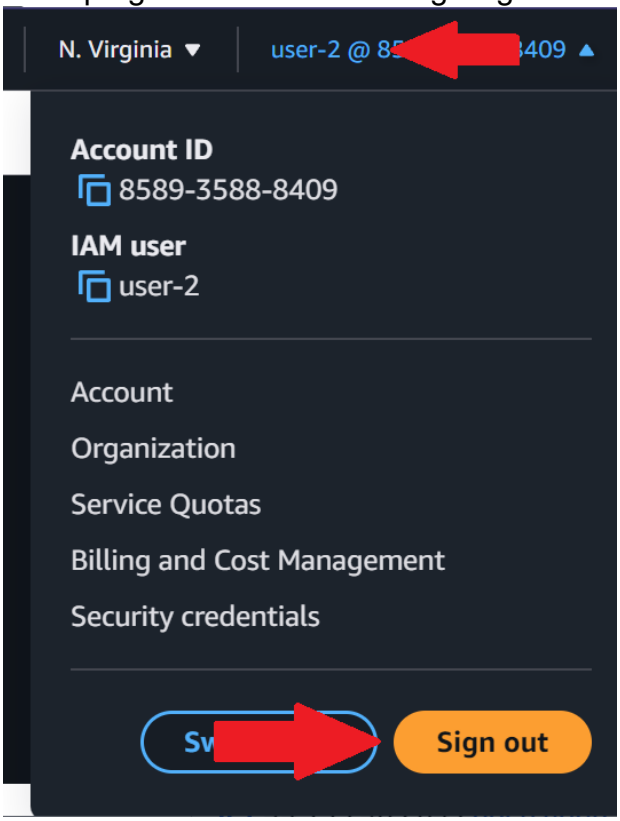


You should see the following page, where it appears that no S3 buckets have been set up (user-2 is unable to see these buckets, so AWS treats them as if they don't exist here).

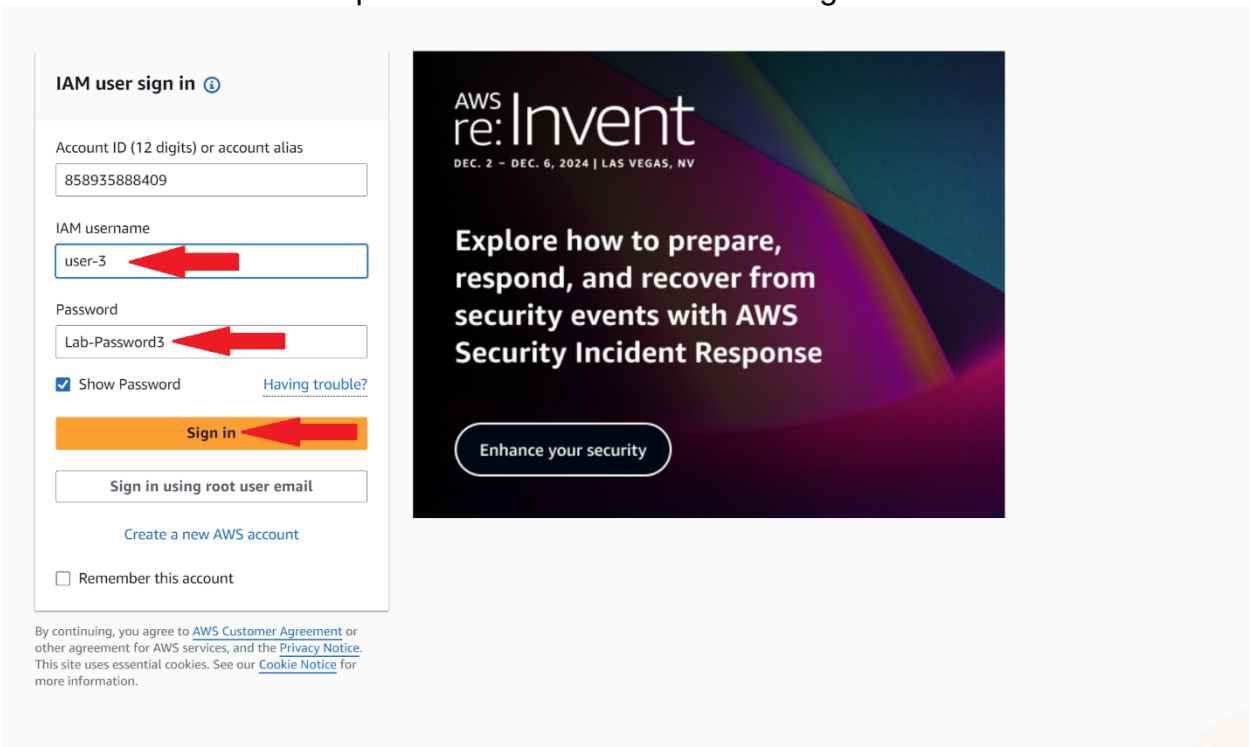


Attempting to create a bucket as user-2 will result in the following error message:

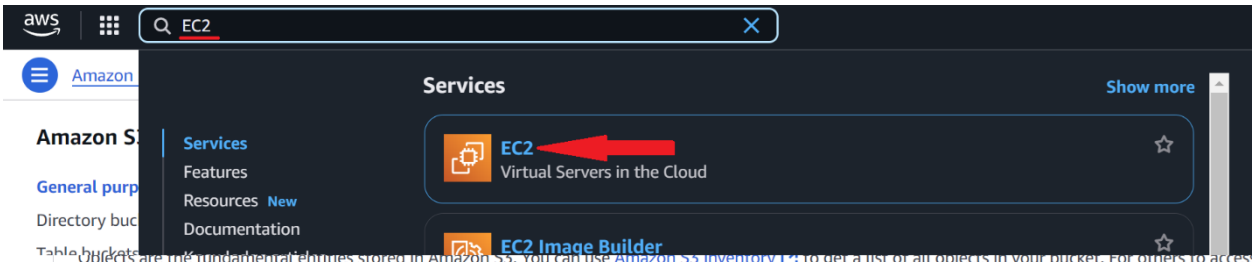
Now, switch to user-3. Sign out of the user-2 account by clicking the “user-2” button in the top right corner and clicking “Sign Out”.



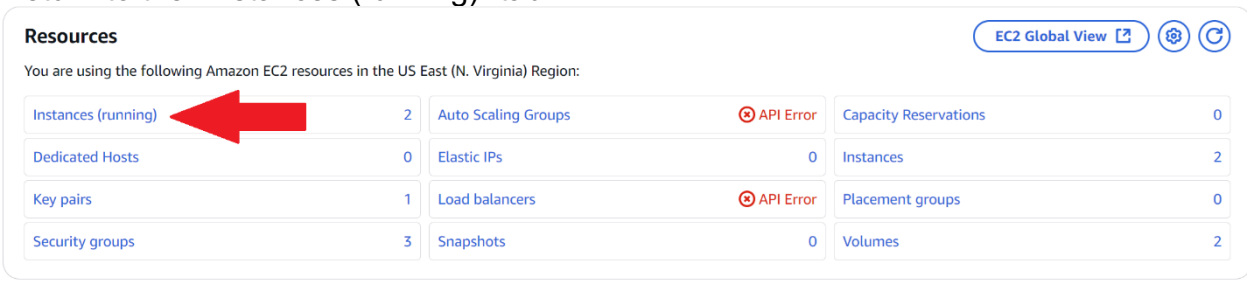
Enter the username and password for user-3 and click “Sign In”.



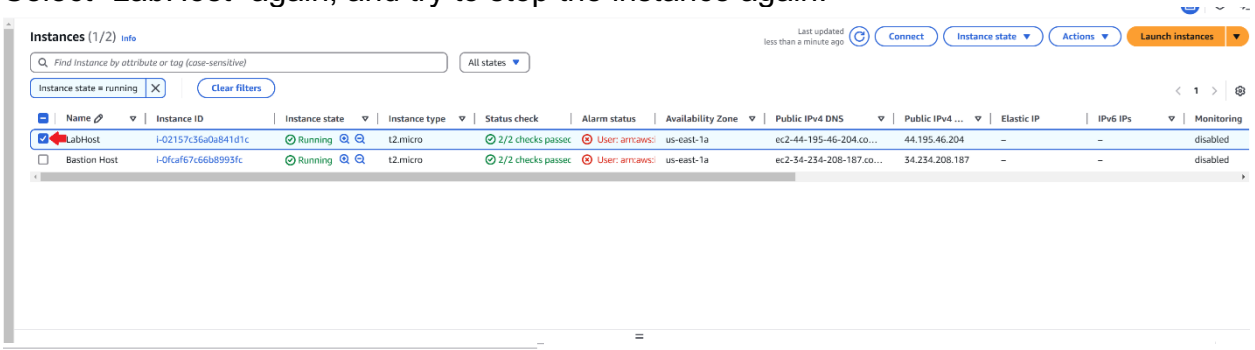
Return to the EC2 dashboard.



Return to the “Instances (running)” tab.



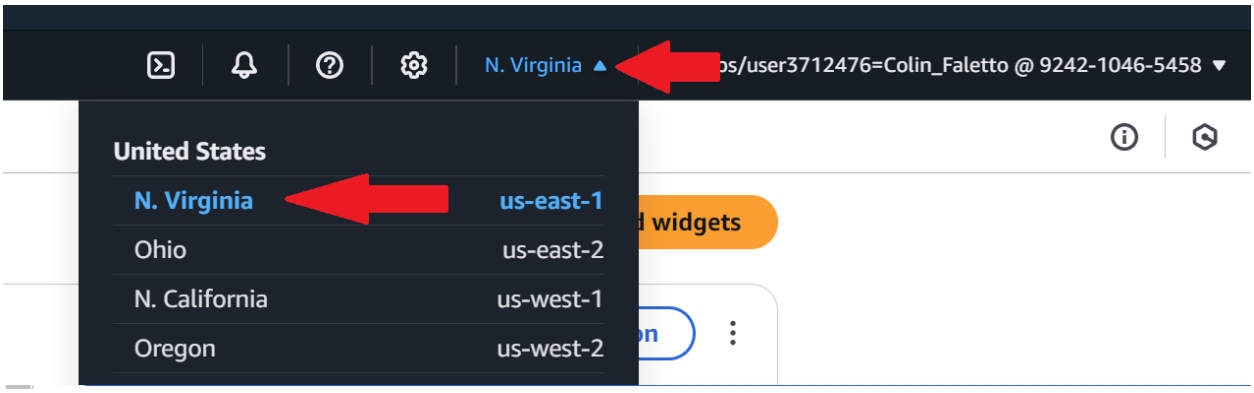
Select “LabHost” again, and try to stop the instance again.



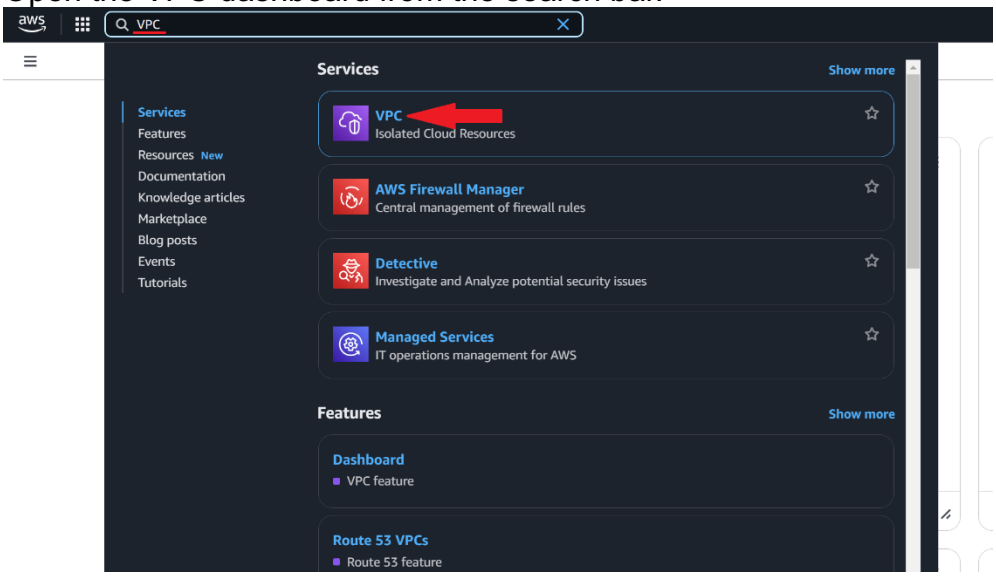
If user-3’s permissions are correctly set up, you should see the following success message:

Lab Commands (Lab 2 VPC)

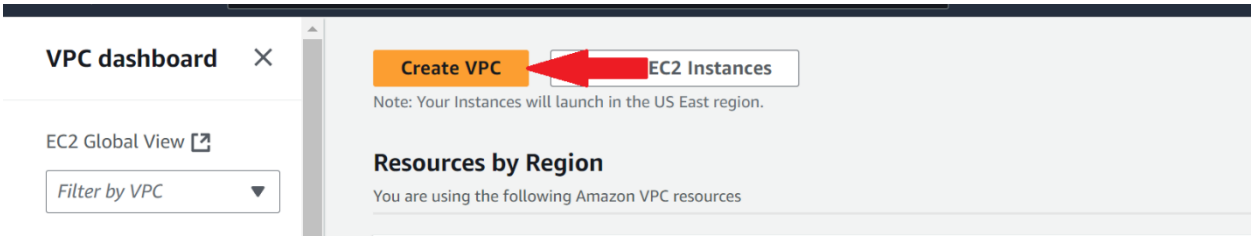
In the AWS management console, ensure that you have the “N. Virginia (us-east-1)” region selected.



Open the VPC dashboard from the search bar.

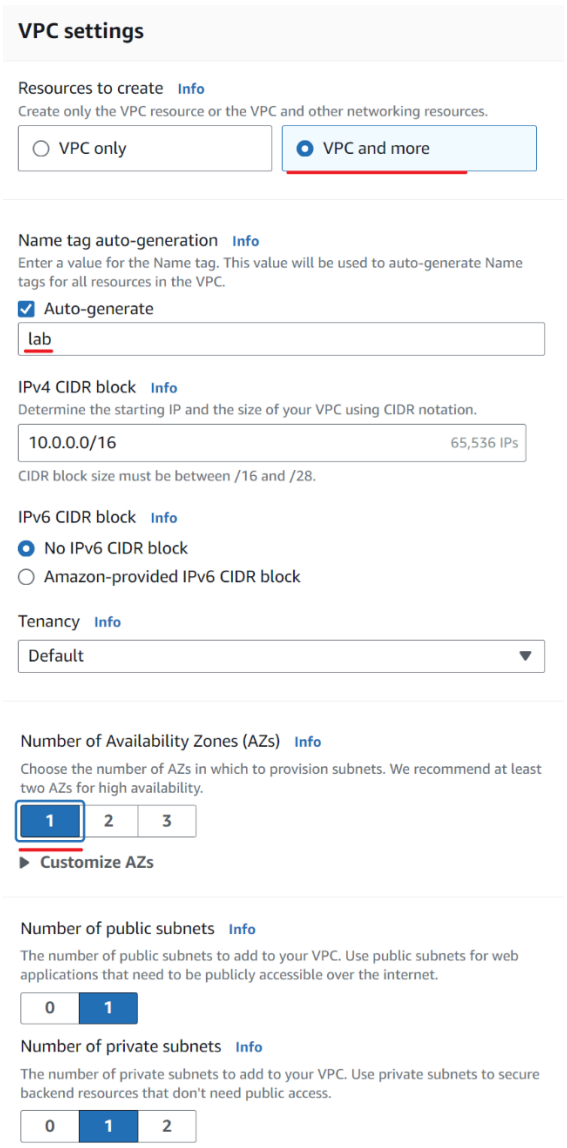


Click “Create VPC”.

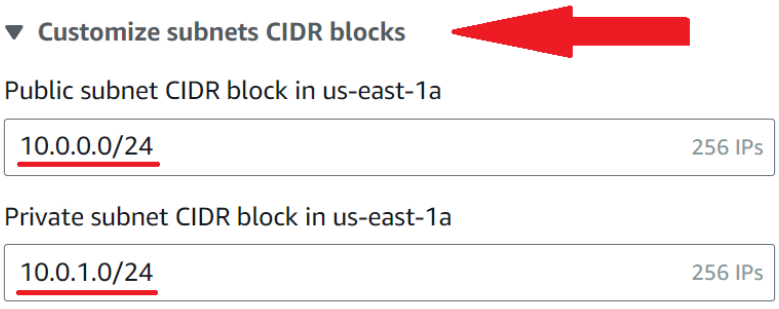


Keep all settings on their default values (ensure they match with the screenshot below) besides the following:

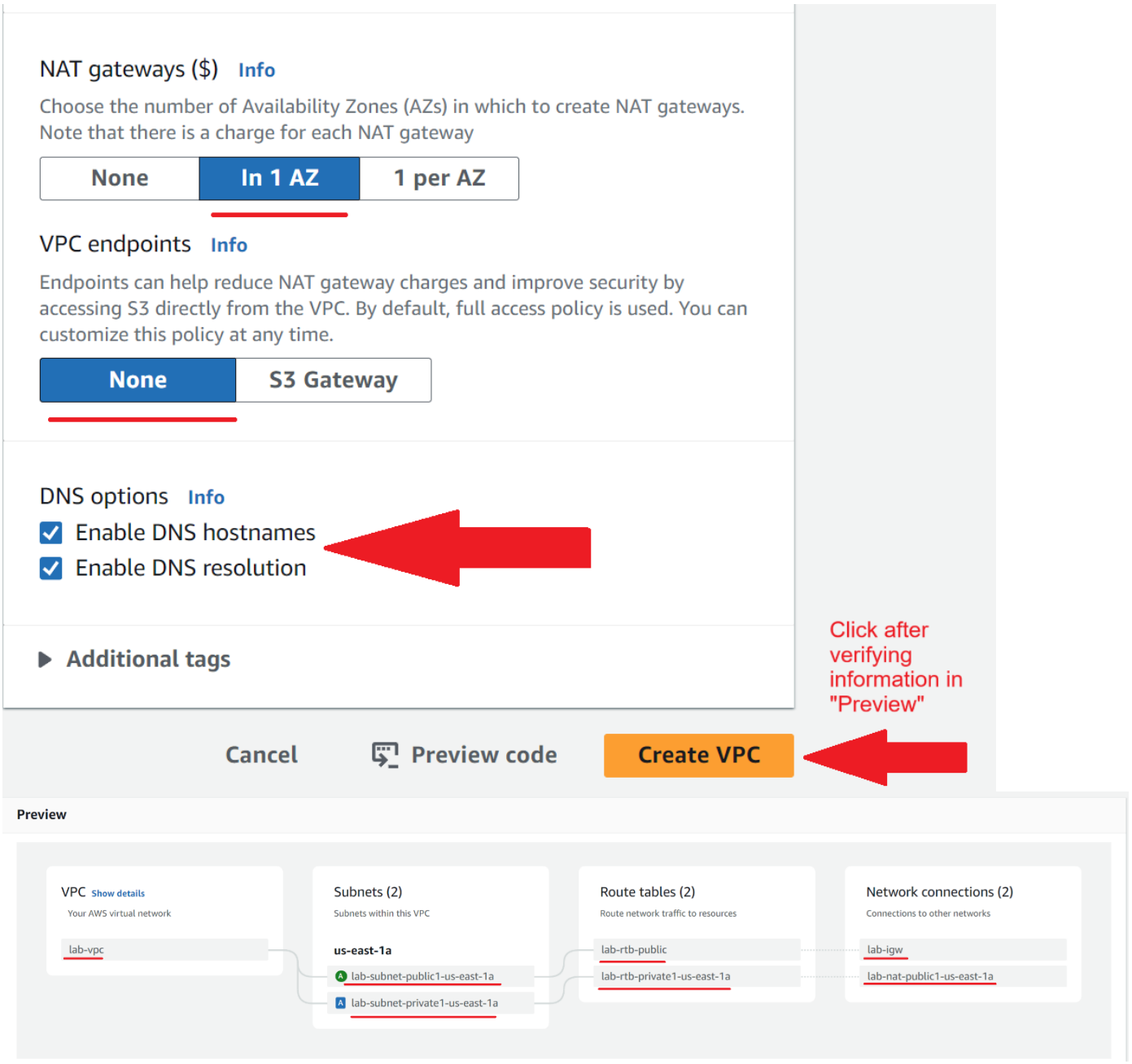
- Set “Resources to create” to “VPC and more”
- Set “Name tag auto-generation” to “lab”
- Set “Number of Availability Zones (AZs)” to “1”



Open the “Customize subnets CIDR blocks” section and ensure that the public and private subnet CIDR blocks are set to 10.0.0.0/24 and 10.0.1.0/24 respectively.

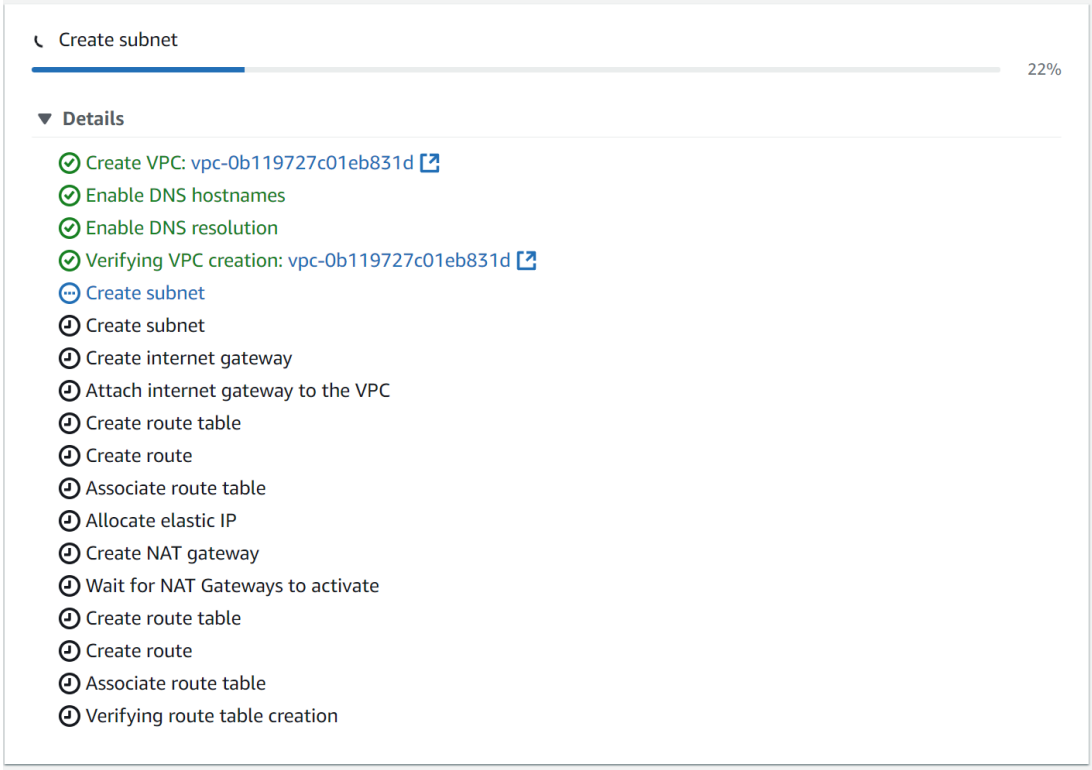


Set “NAT gateways” to “In 1 AZ”, set “VPC Endpoints” to “None”, and ensure that both boxes under “DNS options” are checked. Verify that the Subnets, Route Tables, and Network connections in the “Preview” section match the screenshot below, then click “Create VPC”.

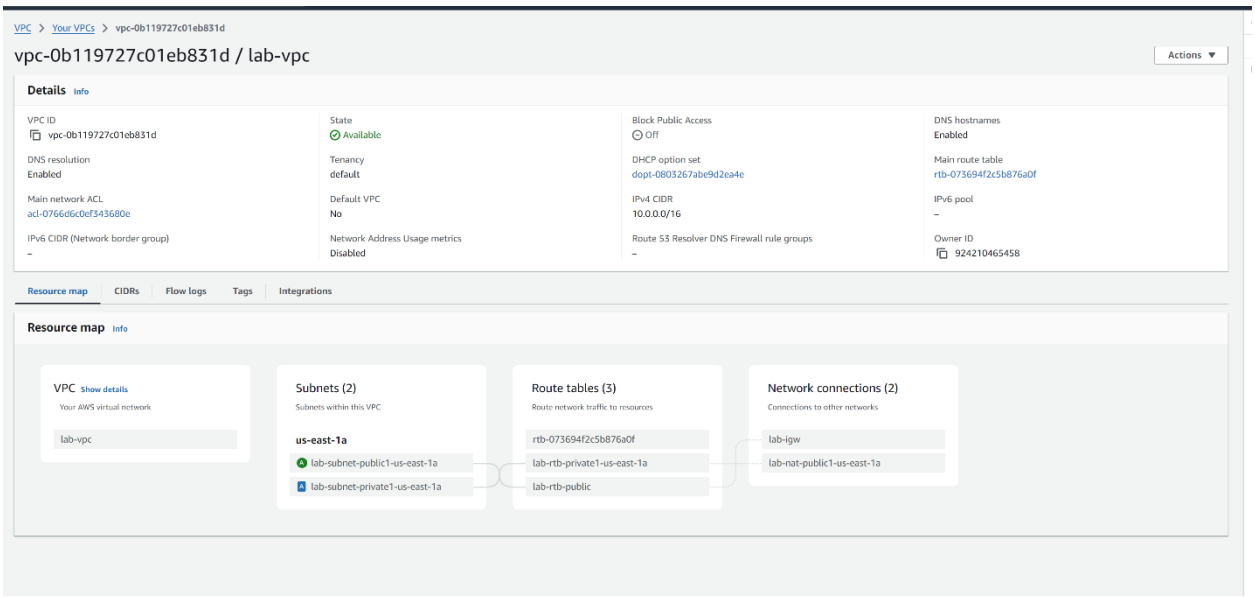


You should see a window like this while the VPC is being created:

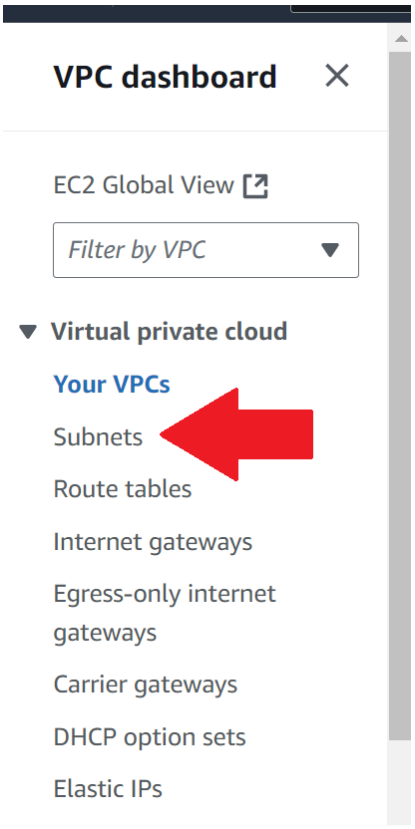
Create VPC workflow



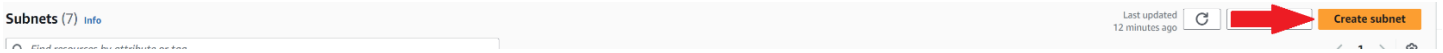
You should see a screen like this when the VPC has finished being created:



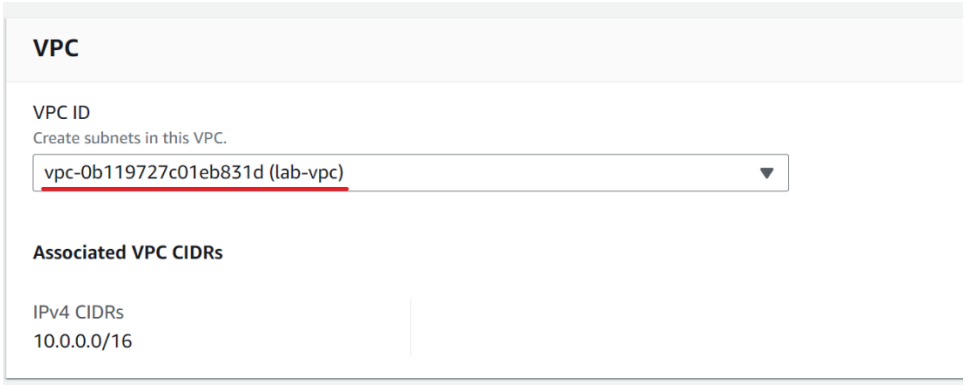
You will now create additional subnets in a second availability zone. From the sidebar, click on “Subnets”.



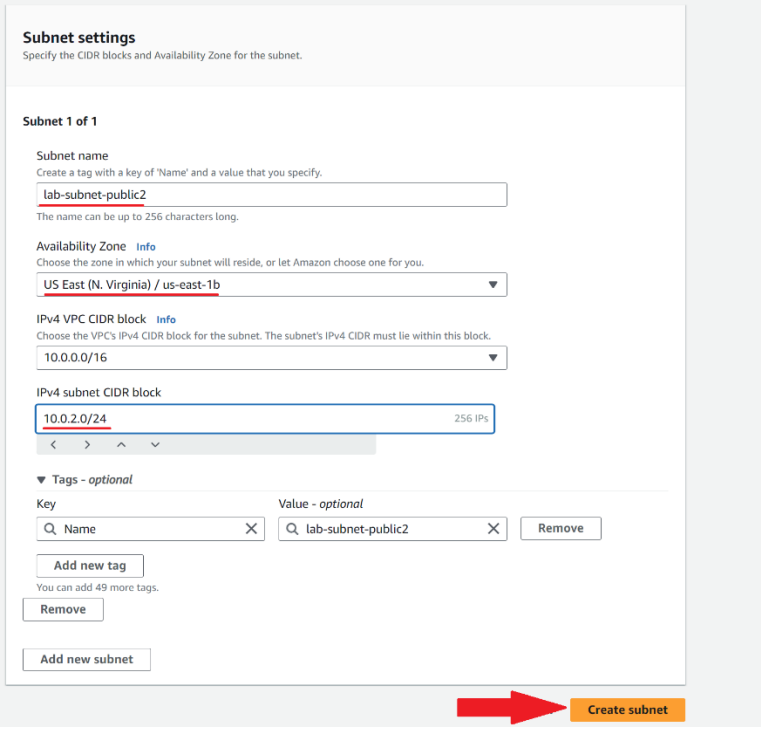
Click “Create Subnet”.



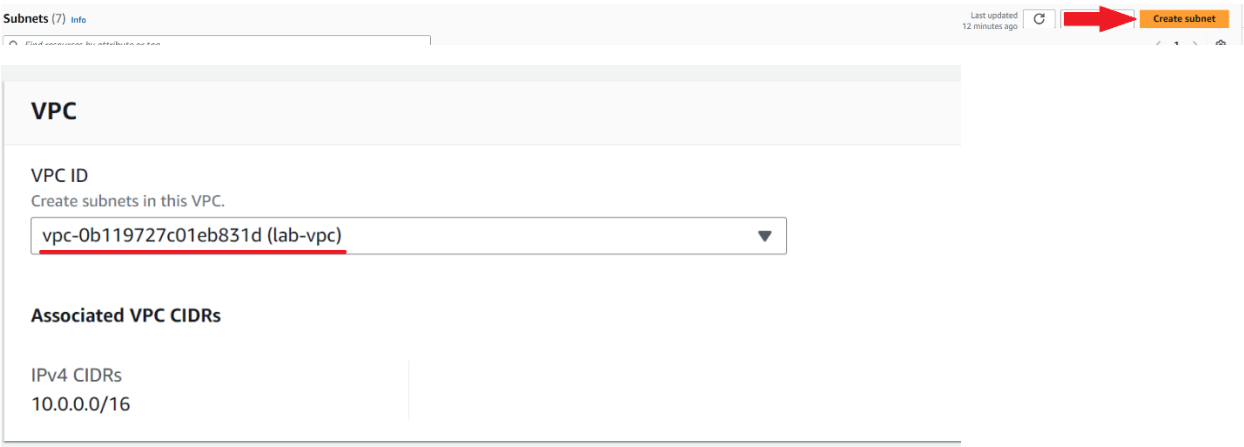
Under “VPC”, select “lab-vpc”.



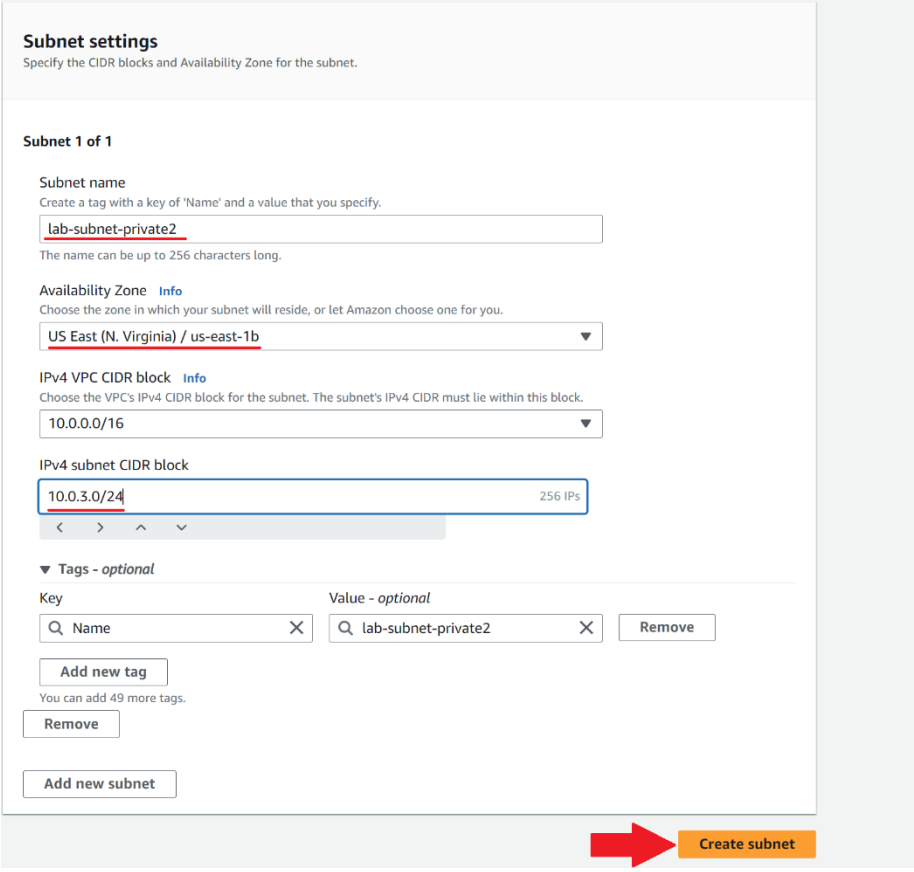
Under “Subnet settings”, set the name to “lab-subnet-public2”, the availability zone to “us-east-1b”, and the IPv4 subnet CIDR block to 10.0.2.0/24. Click “Create Subnet”.



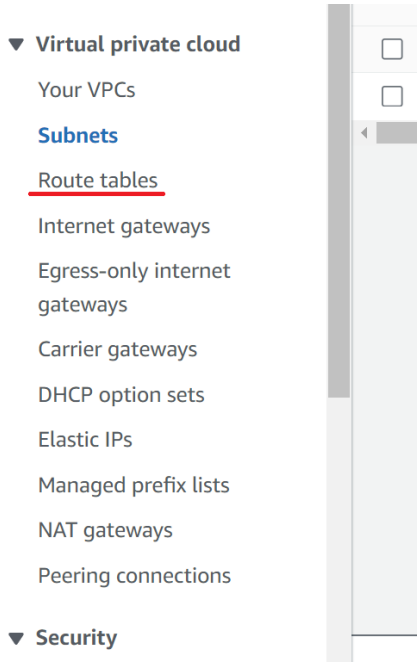
From the subnet dashboard again, select “Create Subnet” and set the VPC to “lab-vpc” again.



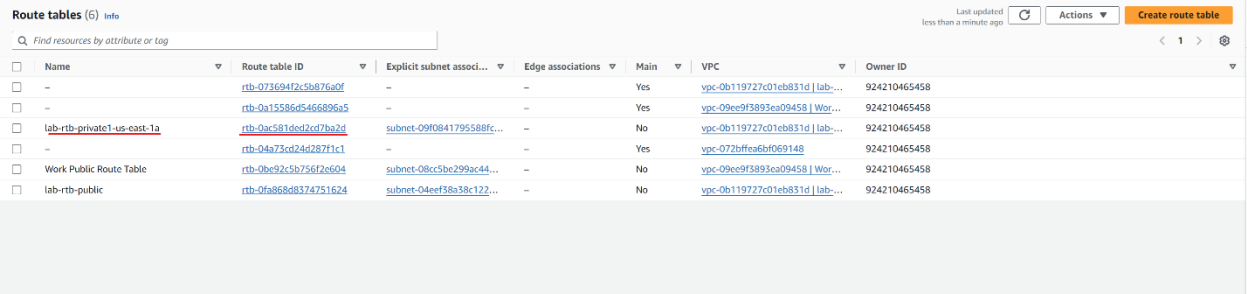
Under “Subnet settings” this time, set the name to “lab-subnet-private2”, the Availability Zone to “us-east-1b”, and the IPv4 Subnet CIDR block to 10.0.3.0/24. Click “Create Subnet”.



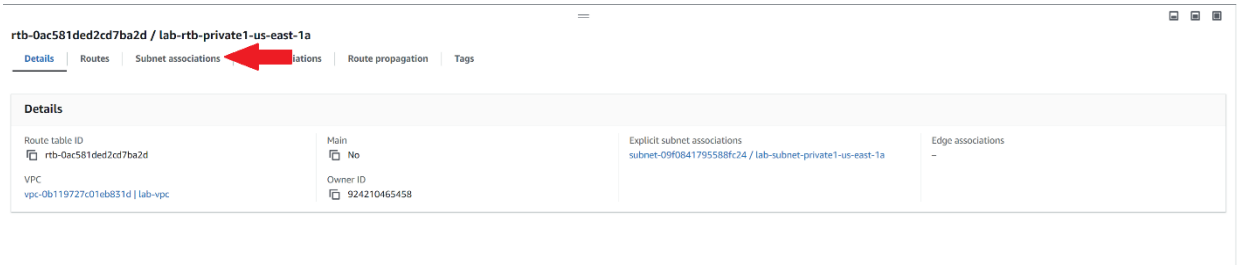
Next, set the second private subnet to share a routing table with the first private subnet. Go to the “Route tables” section from the sidebar.



Click on the “Route table ID” hyperlink associated with “lab-rtp-private1-us-east-1a”.

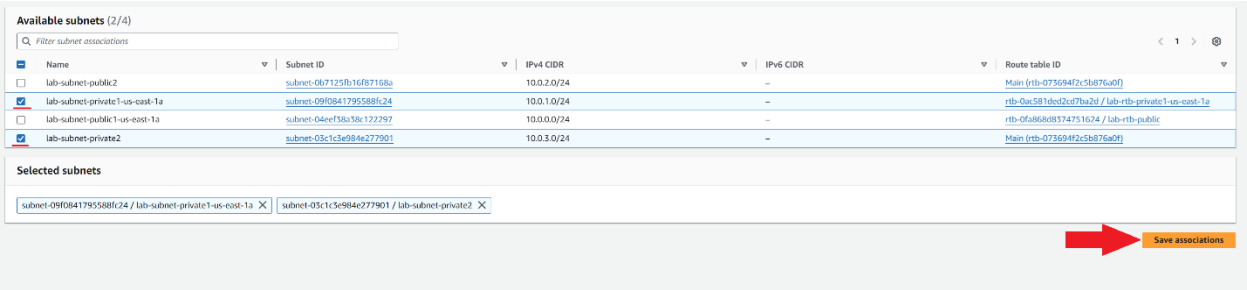


Click “Subnet associations”.

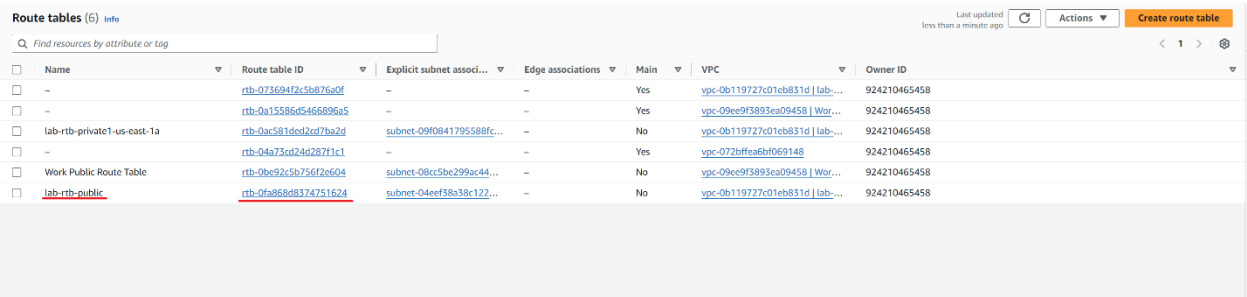


Click “Edit subnet associations”.

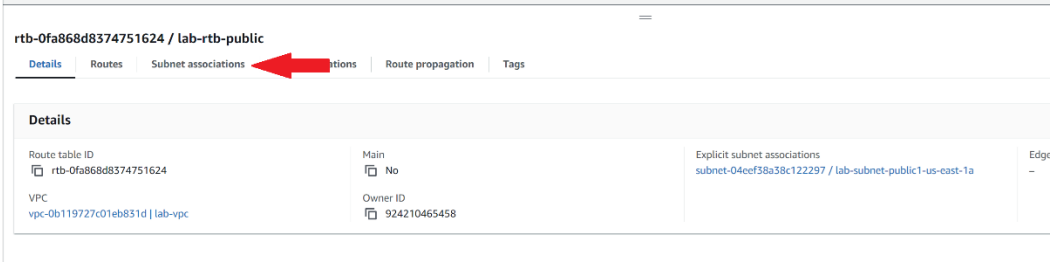
Select both private subnets, then click “Save associations”.



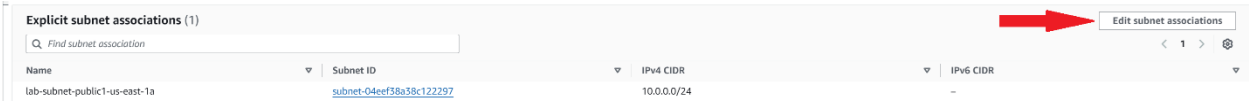
Return to the “Route tables” page. Click on the “Route table ID” hyperlink of the “lab-rtp-public” table.



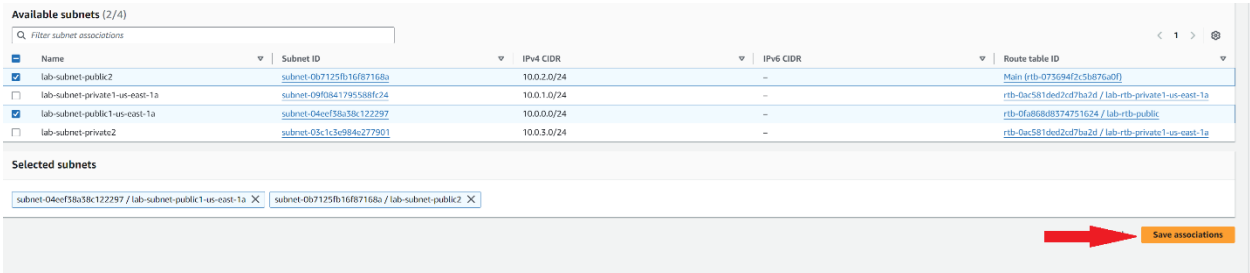
Click “Subnet associations”.



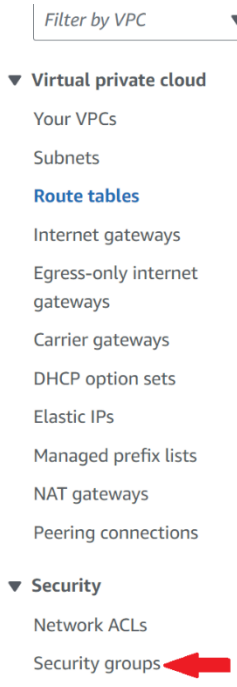
Click “Edit subnet associations”.



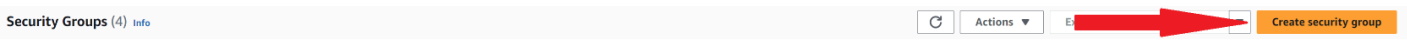
Select both public subnets, then click “Save associations”.



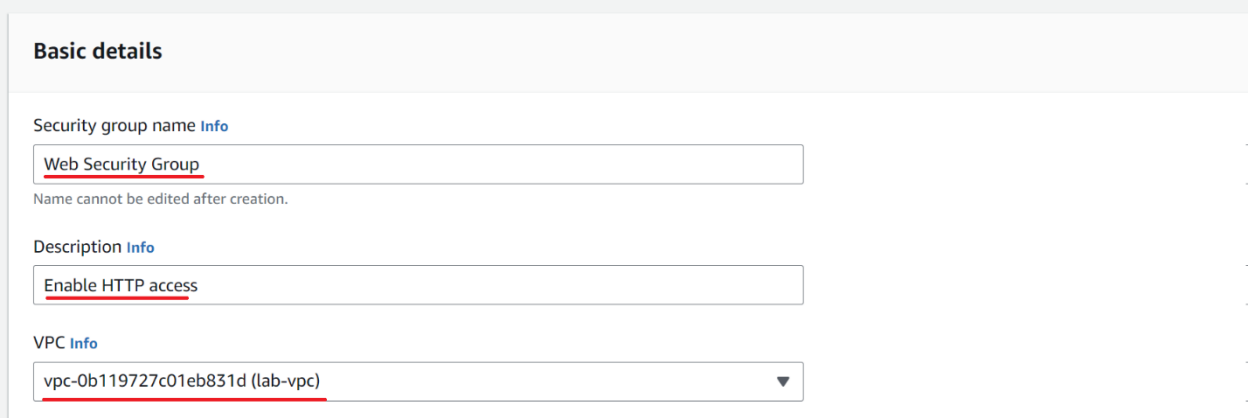
Next, you will configure a security group to permit HTTP access to a web server. Go to the “Security groups” page from the sidebar.



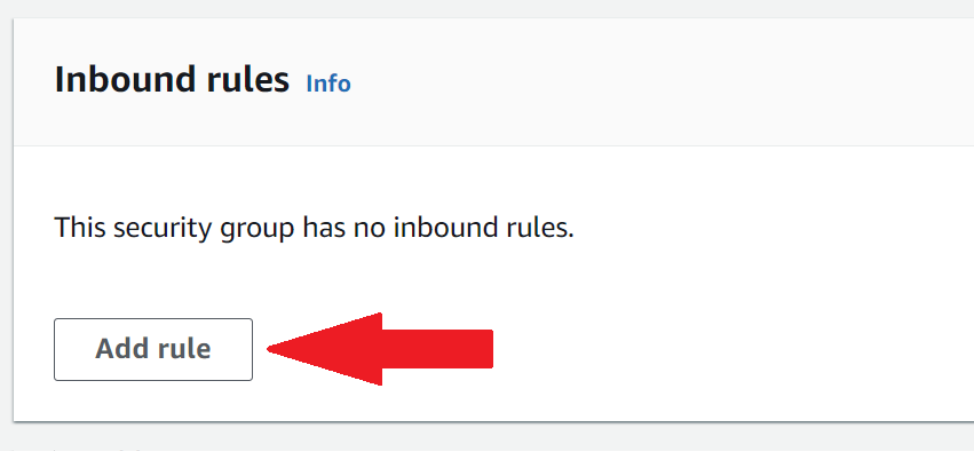
Click “Create security group”.



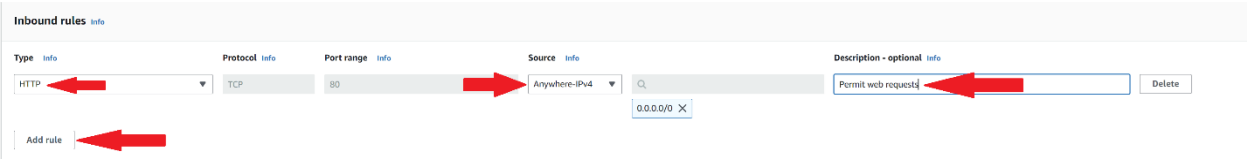
Under “Basic details”, set the name to “Web Security Group”, the description to “Enable HTTP Access”, and the VPC to “lab-vpc”.



Under “Inbound rules”, click “Add rule”.

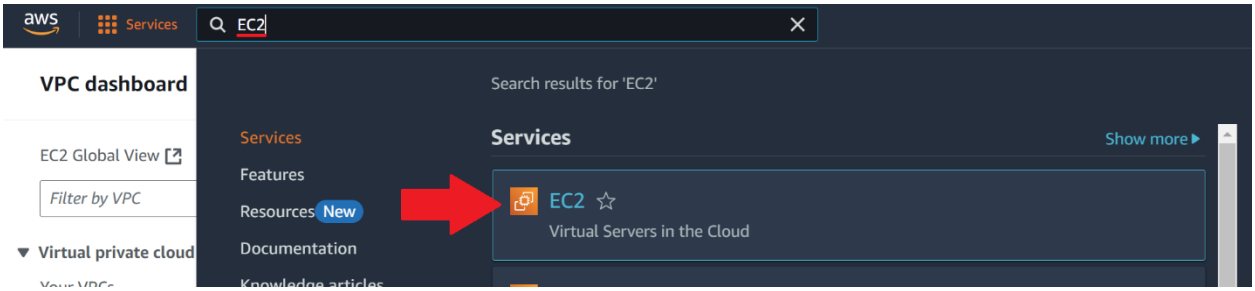


Set the rule type to “HTTP”, the source to “Anywhere-IPv4”, and the description to “Permit web requests”. Click “Add rule”.

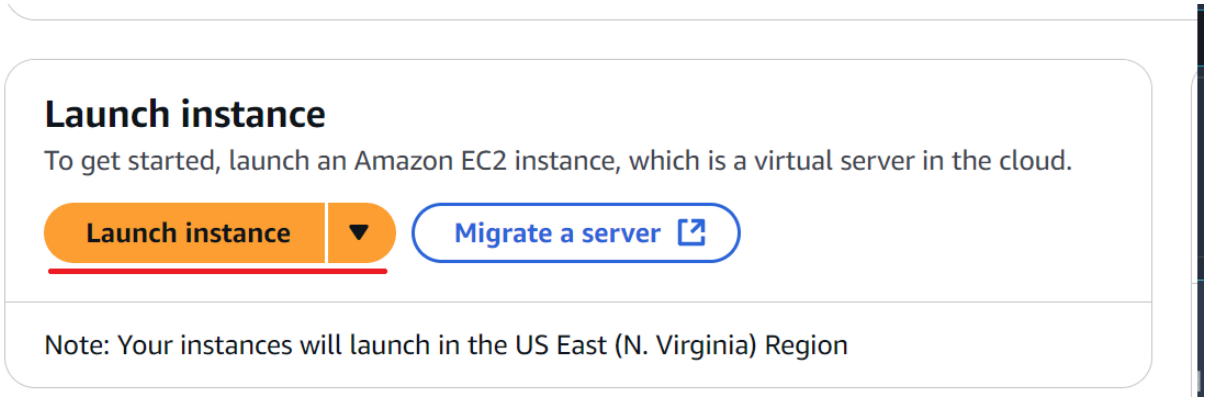


Click “Create security group”.

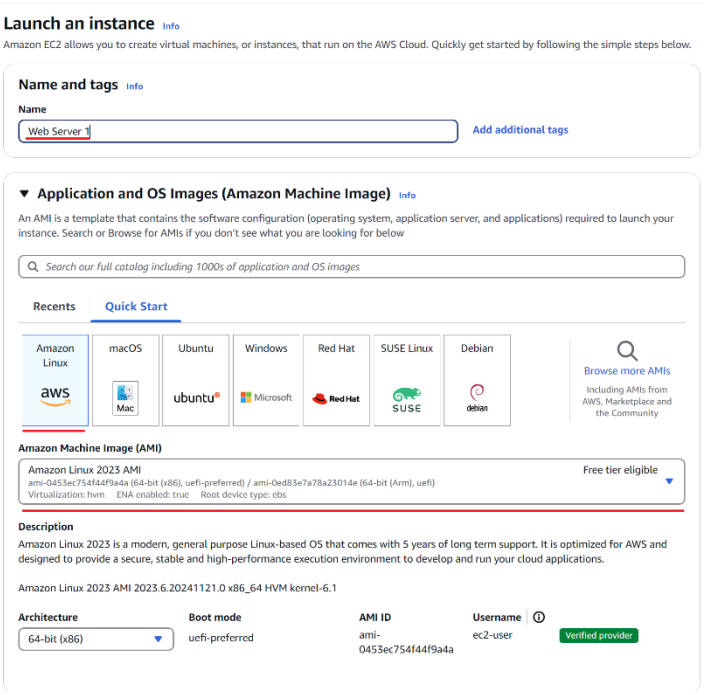
Next, we will create a web server with this security group applied. Open the EC2 dashboard from the search bar.



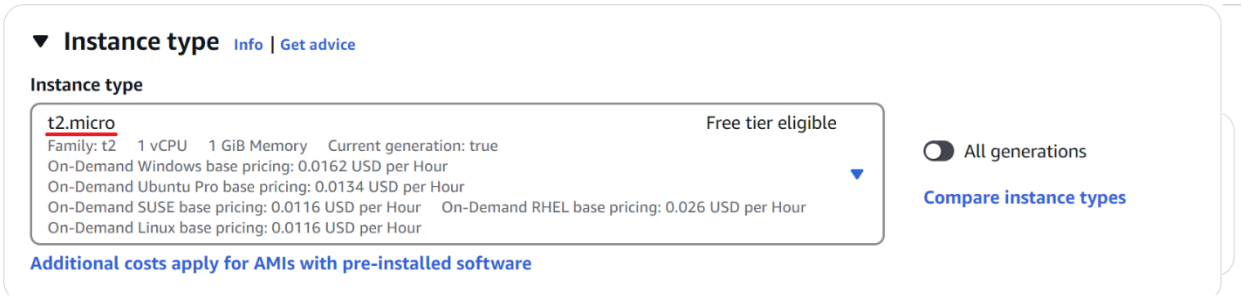
Click “Launch instance”.



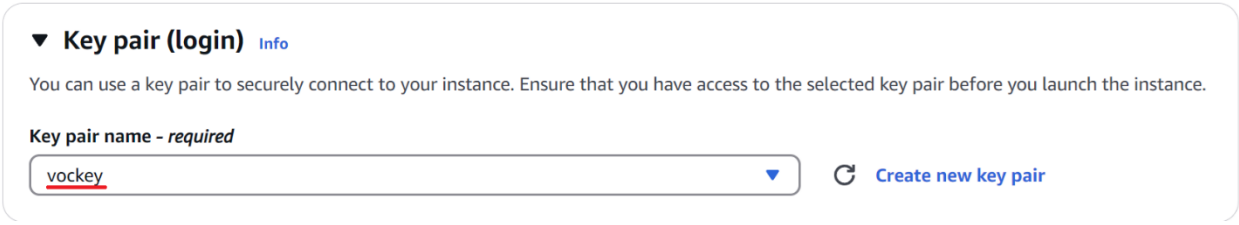
Set the name to “Web Server 1” and set the Amazon Machine Image to “Amazon Linux 2023 AMI”.



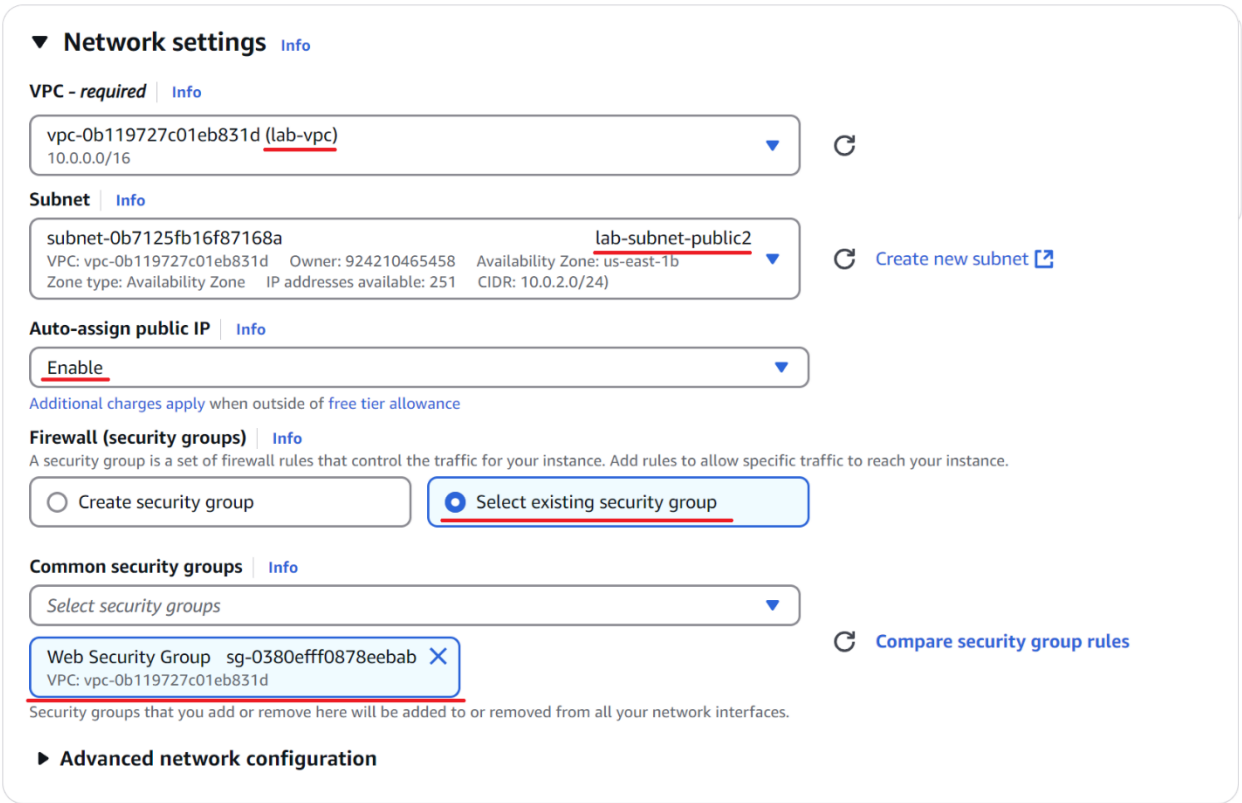
Set the instance type to “t2.micro”.



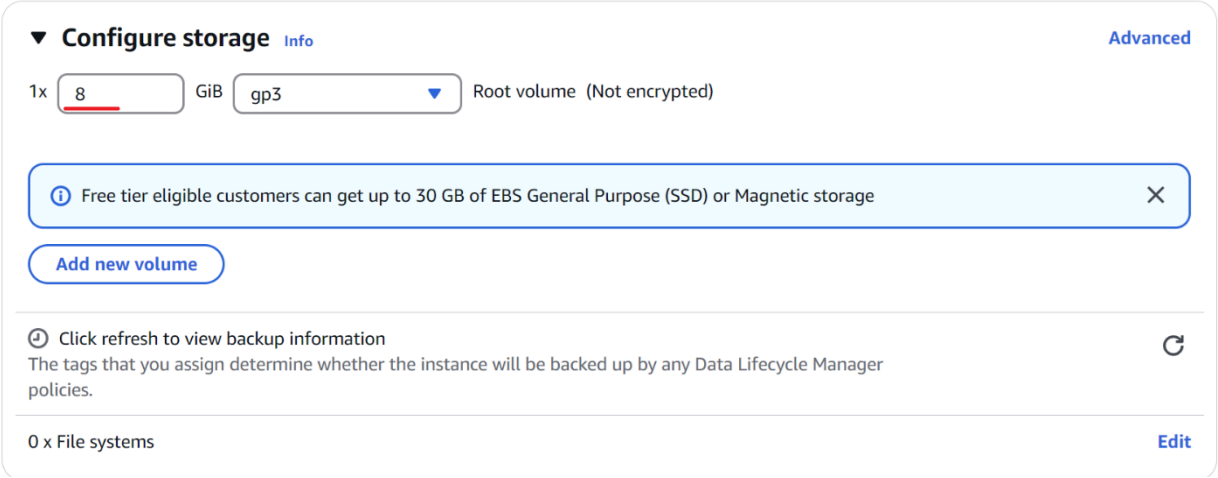
Set the Key pair to “vockey”.



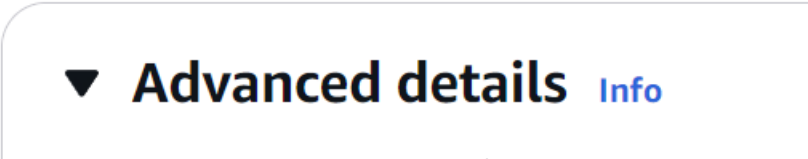
Under “Network settings”, set the VPC to “lab-vpc”, the subnet to “lab-subnet-public2”, and “Auto-assign public IP” to “Enable”. Set the “Firewall (security groups)” to “Select existing security groups” and add the “Web Security Group” created earlier.



Under “Configure storage”, set the storage to 8 Gibibytes.



Open the “Advanced details” tab.

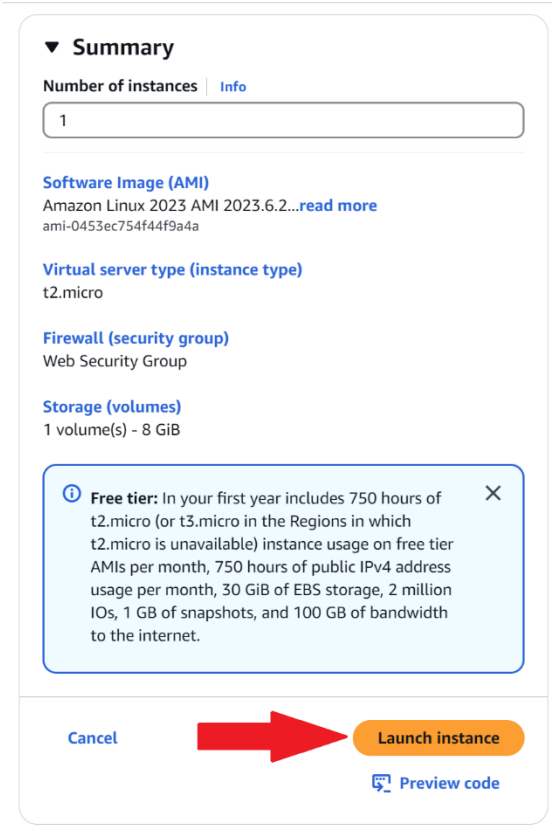


Scroll down to the “User data” section.

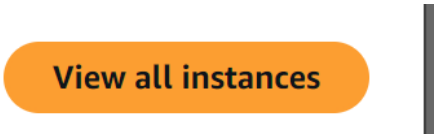
Add the following script:

```
#!/bin/bash
# Install Apache Web Server and PHP
dnf install -y httpd wget php mariadb105-server
# Download Lab files
wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-100-ACCLFO-2/2-lab2-vpc/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
# Turn on web server
chkconfig httpd on
service httpd start
```

Click “Launch Instance”.

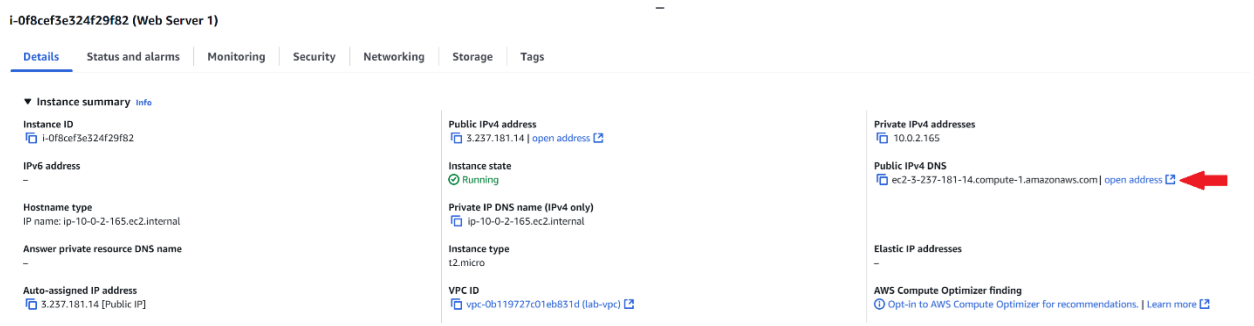


Click “View All Instances”.

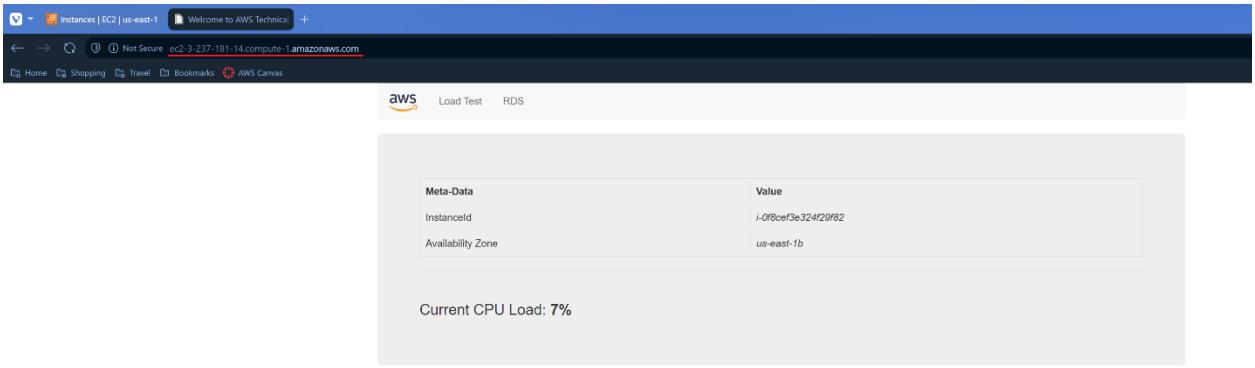


Click the checkbox next to “Web Server 1”.

After the “Status Check” section says “2/2 checks passed”, look for the public IPv4 address of the server and click the button to open the URL in a new tab:

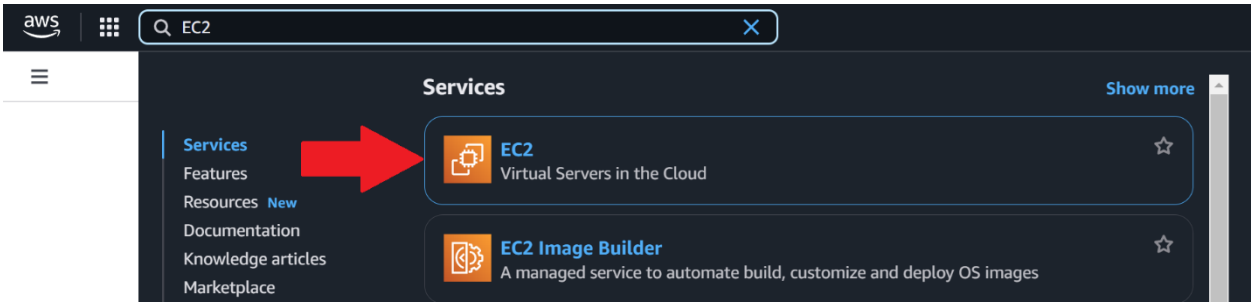


If done correctly, a page like this should open:

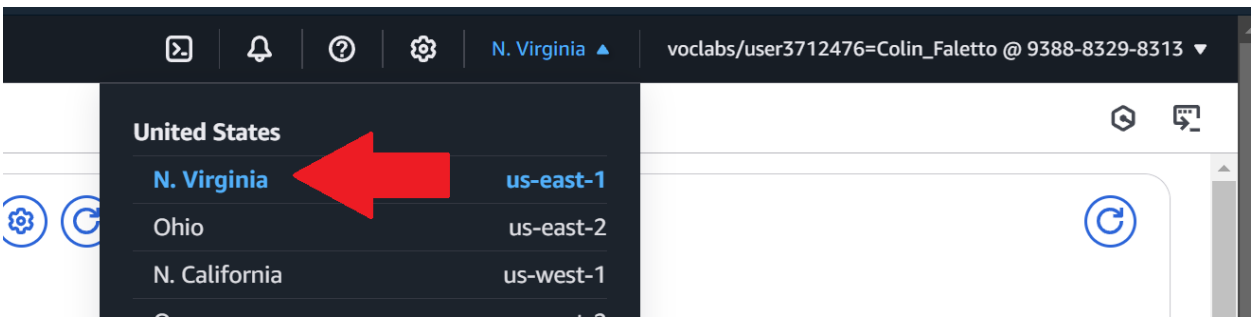


Lab Commands (Lab 3 EC2)

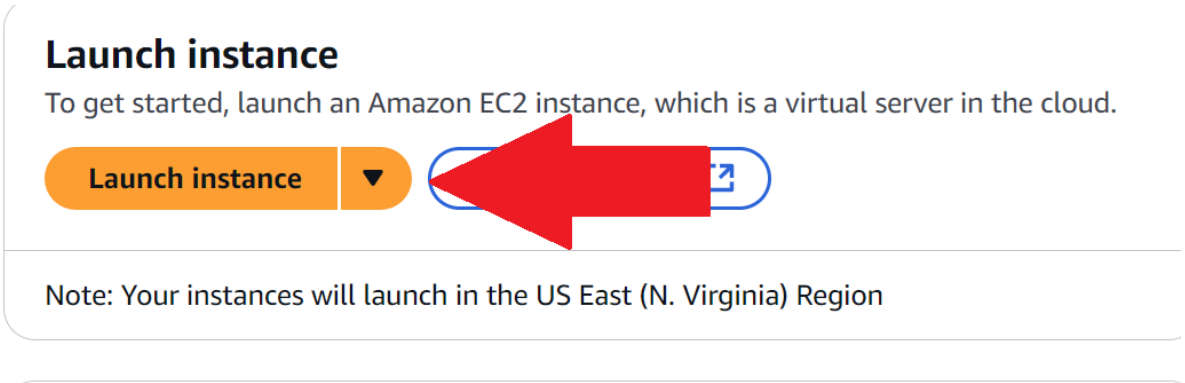
Open the EC2 console from the search bar.



Ensure you have the North Virginia region selected.

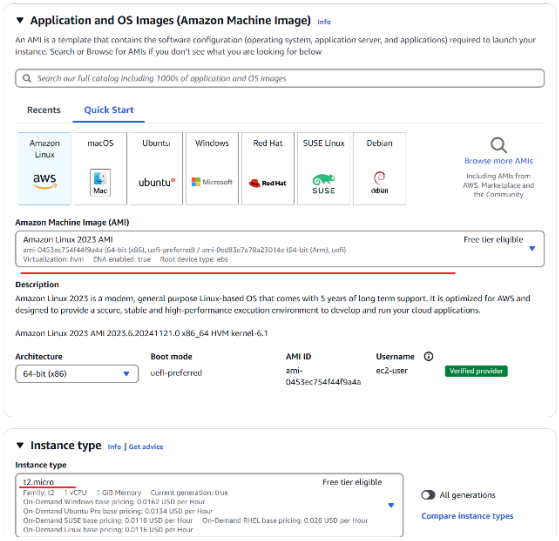


From the EC2 homepage, select “Launch Instance”.

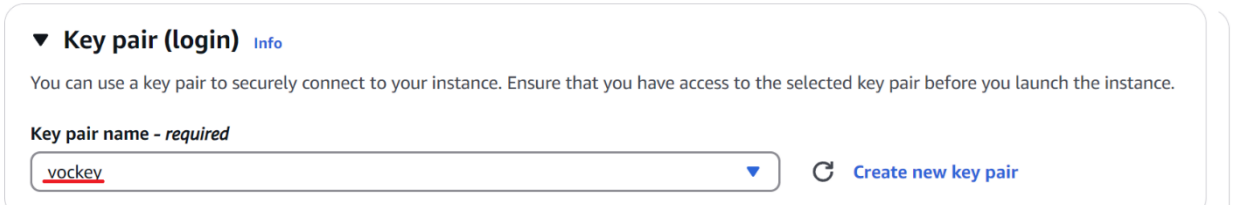


Name this instance “Web Server”.

Set the AMI to “Amazon Linux 2023 AMI” and set the instance type to “t2.micro”.

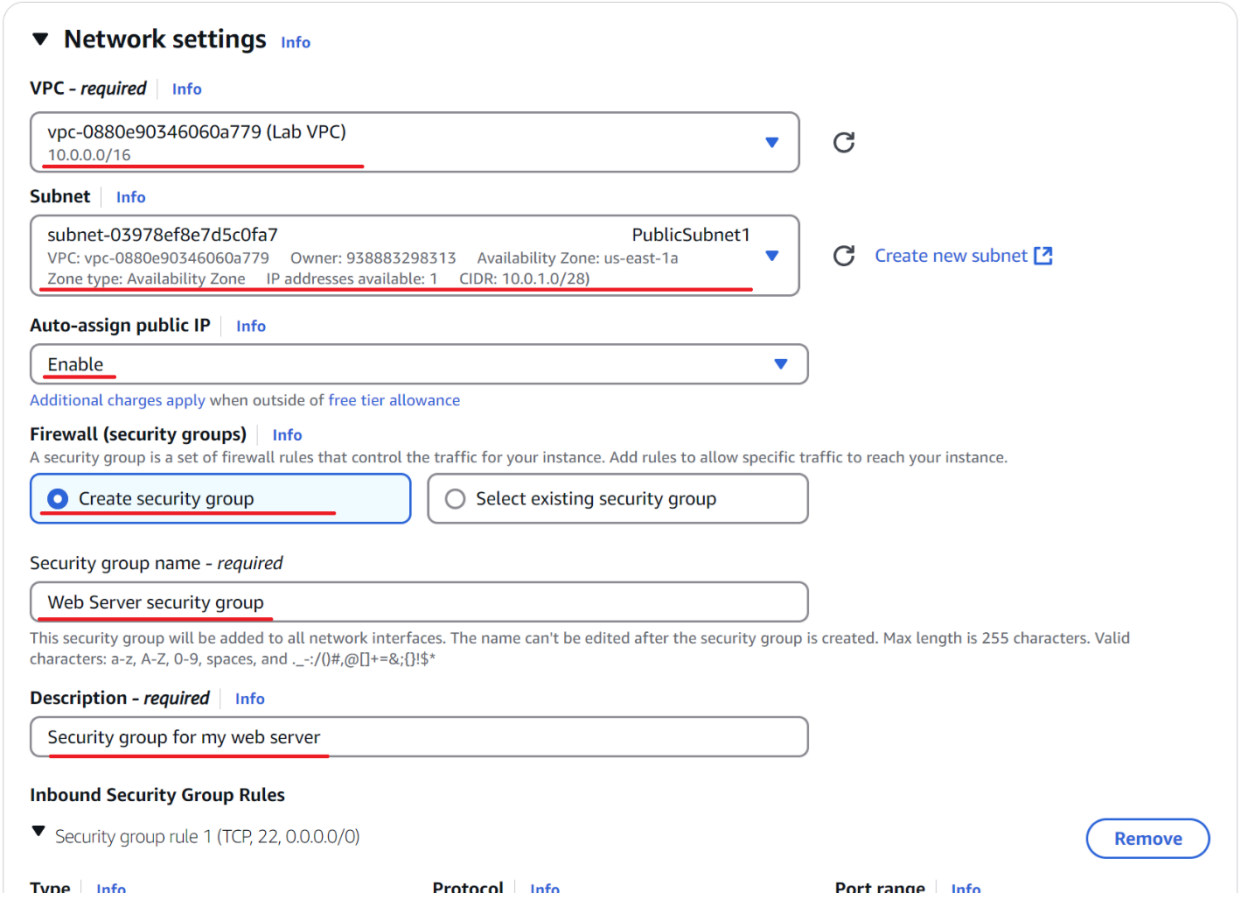


Set the key pair to “vockey”.

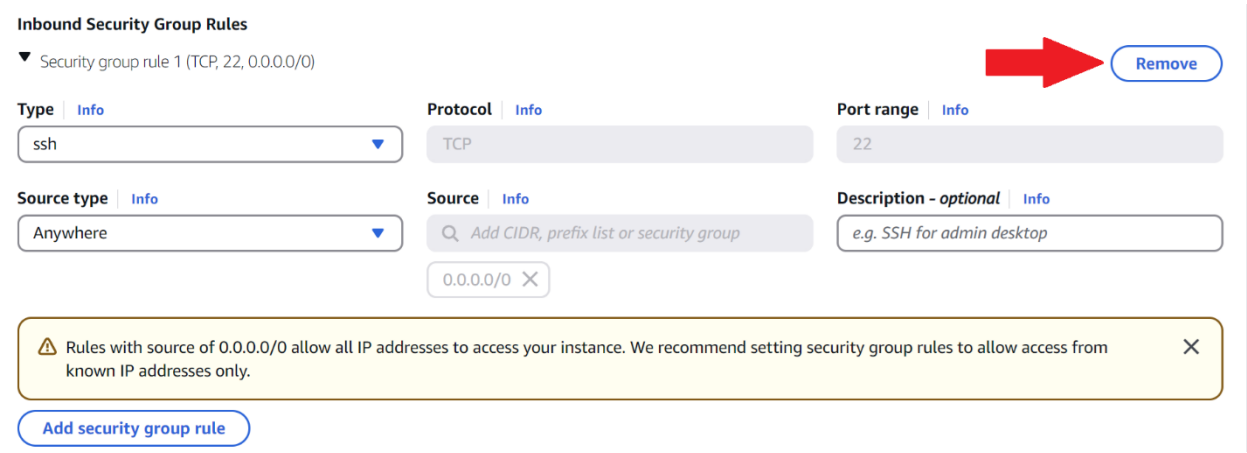


Under “Network Settings”, click “Edit”.

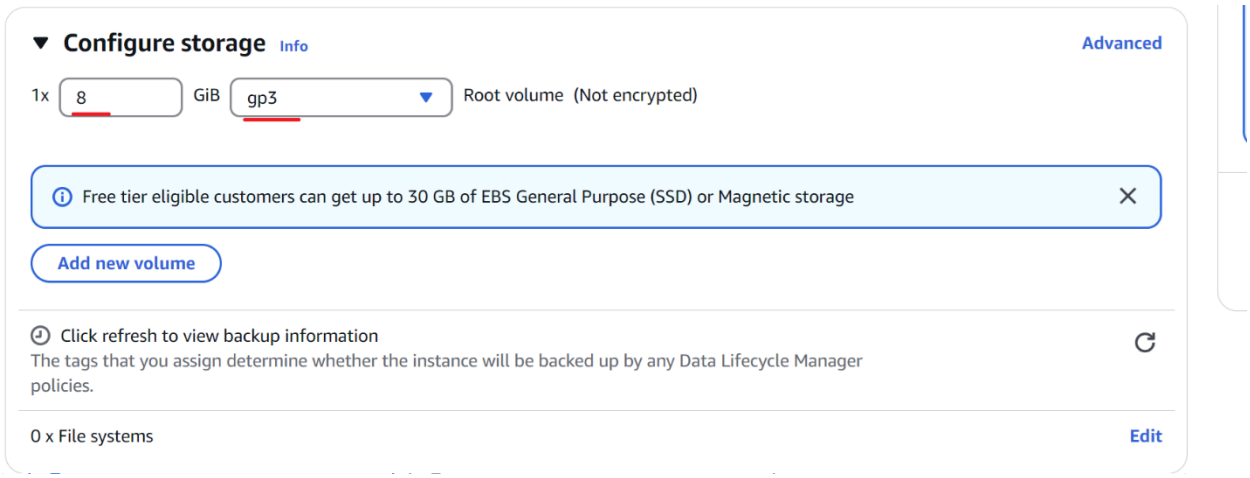
Set the VPC to “Lab VPC”, the subnet to “Public Subnet 1”, and the “Auto-Assign Public IP” setting to “enable”. Create a new security group with the name “Web Server security group” and the description “Security group for my web server”.



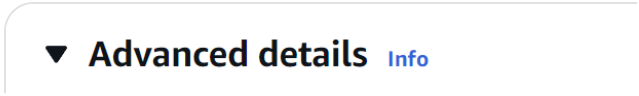
Make sure to remove “Security group rule 1”.



Under “Configure storage”, select 8 GiB of gp3.



Go the Advanced Details section.

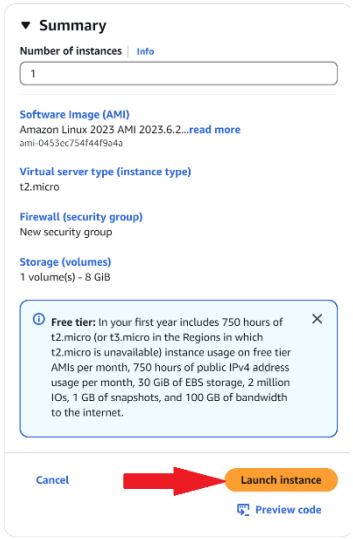


Enable termination protection.

Enter the following into the “User Data” section:

```
#!/bin/bash
dnf install -y httpd
systemctl enable httpd
systemctl start httpd
echo '<html><h1>Hello From Your Web Server!</h1></html>' >
/var/www/html/index.html
```

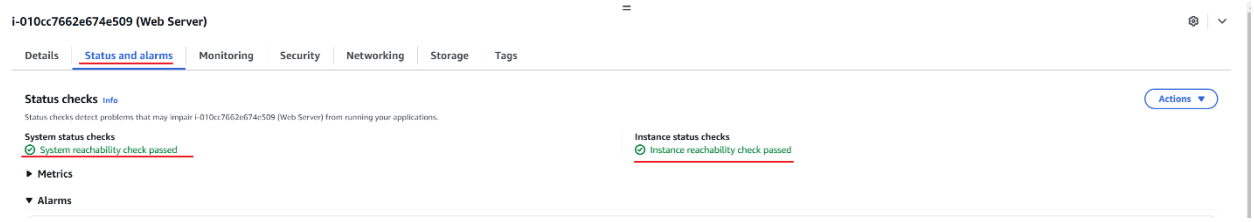
Under the “Summary” section, click “Launch Instance”.



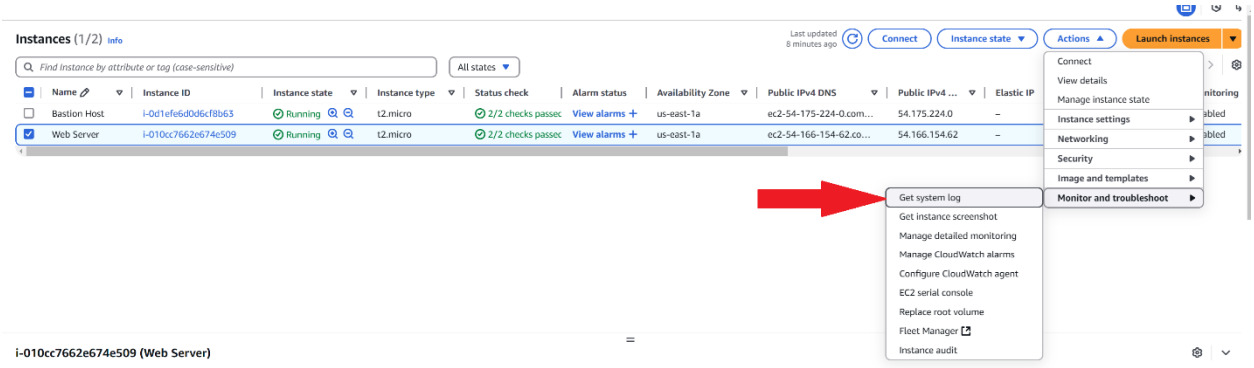
After launching the EC2 instance, click “View all instances”.

Wait for your web server to have the instance state of “Running”, then click the checkbox next to it.

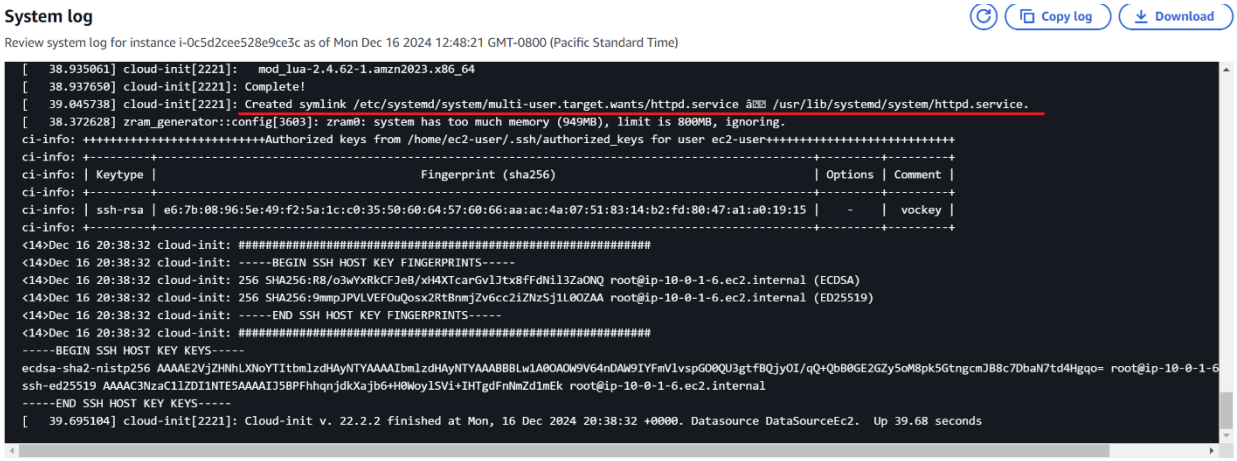
Under the “Status and Alarms” tab, ensure that both reachability checks have passed.



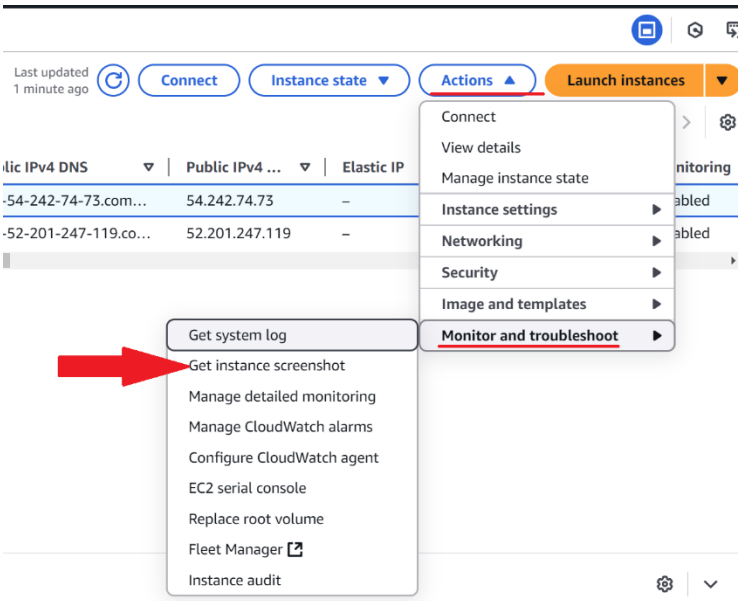
Click “Actions > Monitor and troubleshoot > Get system log”.



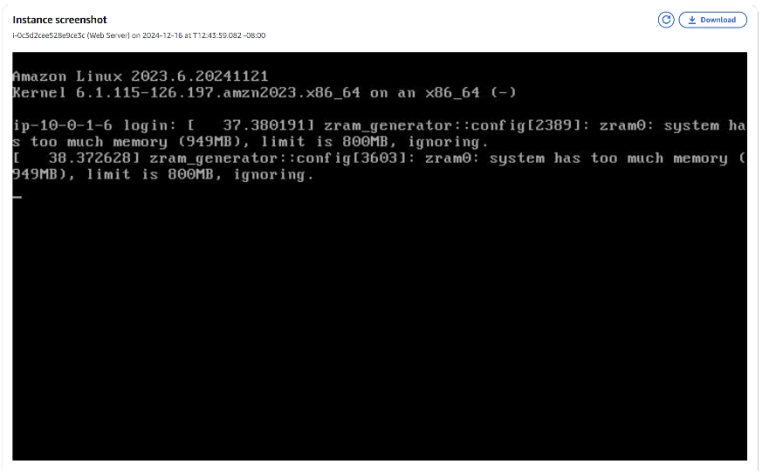
If done correctly, you should see a reference to the “httpd” service started in the User Data section.



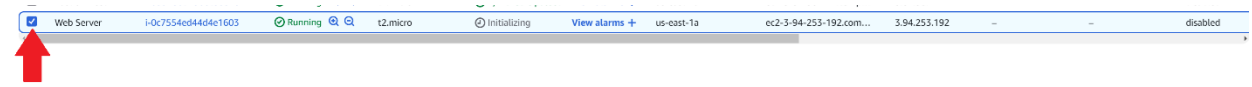
Return to the instances page and click Actrions > Monitor and troubleshoot > Get instance screenshot.

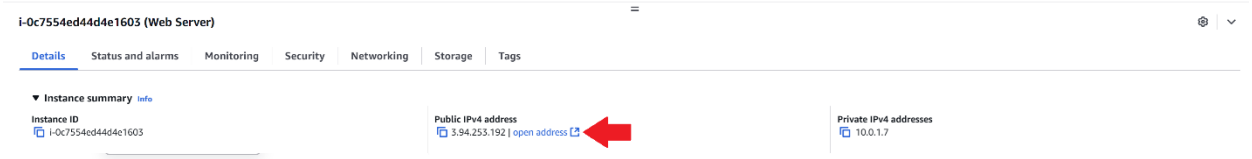


You should see a screenshot similar to this:

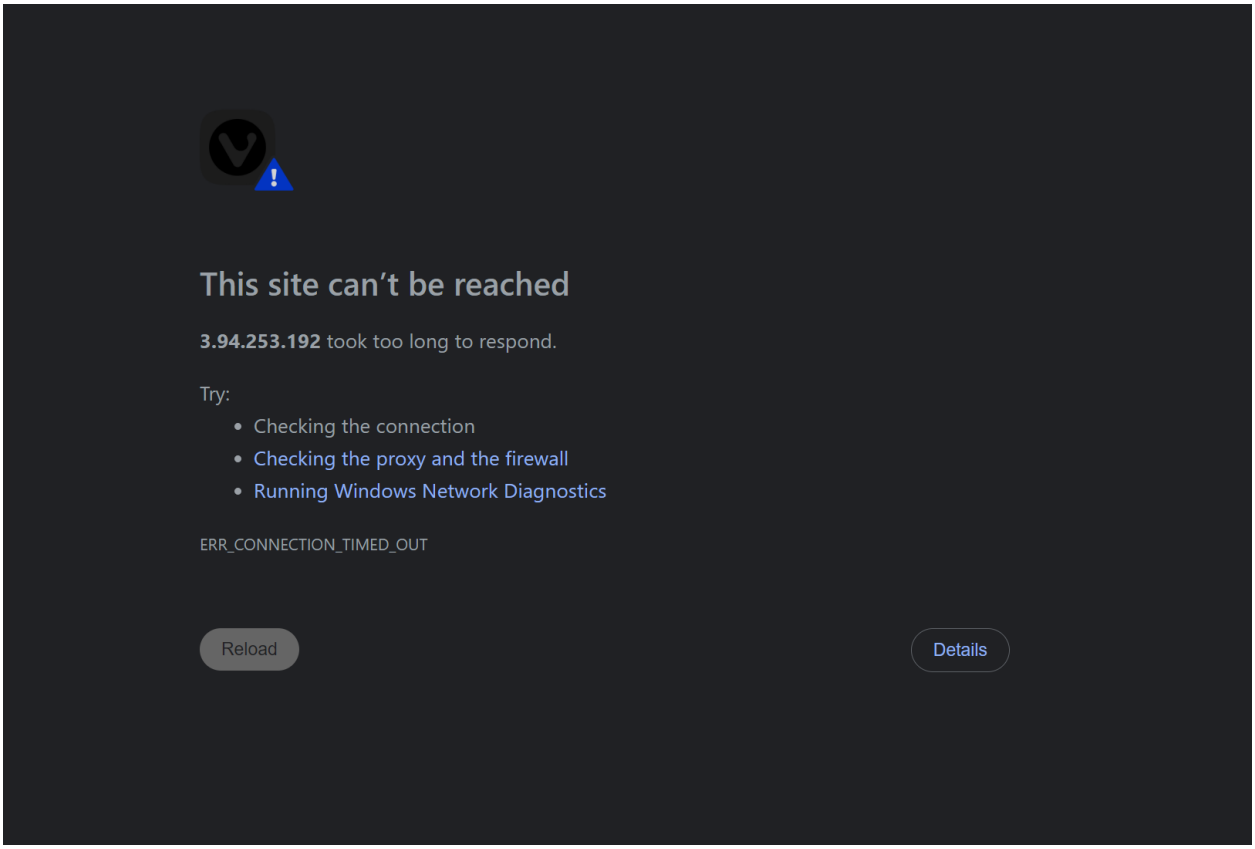


On the instances page, select Web Server and click open address under the Public IPv4 address field.

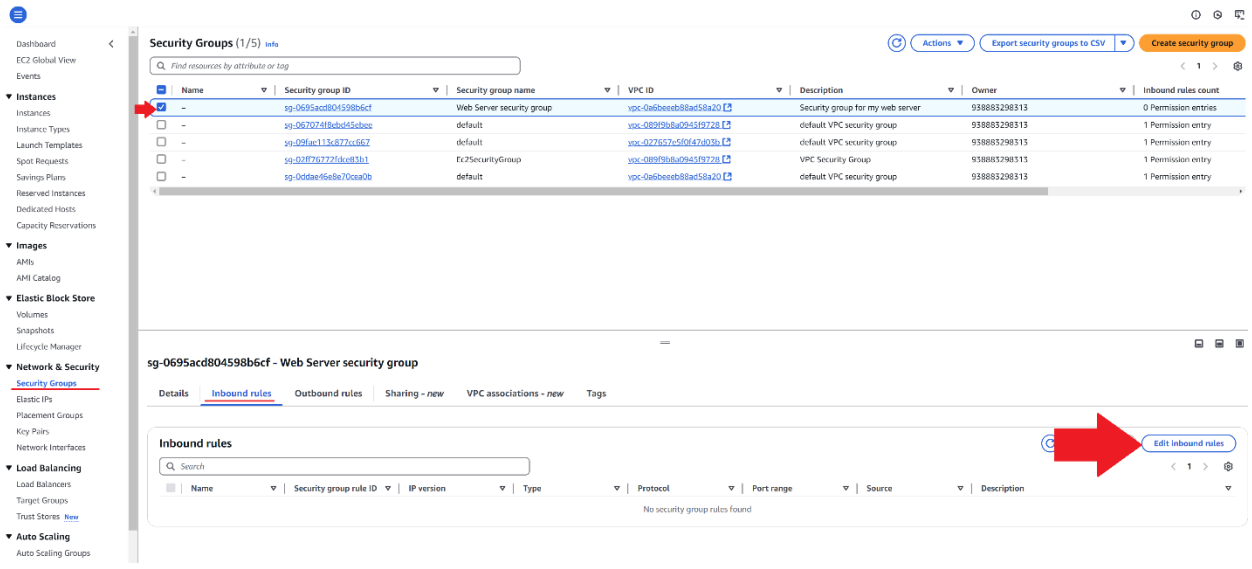




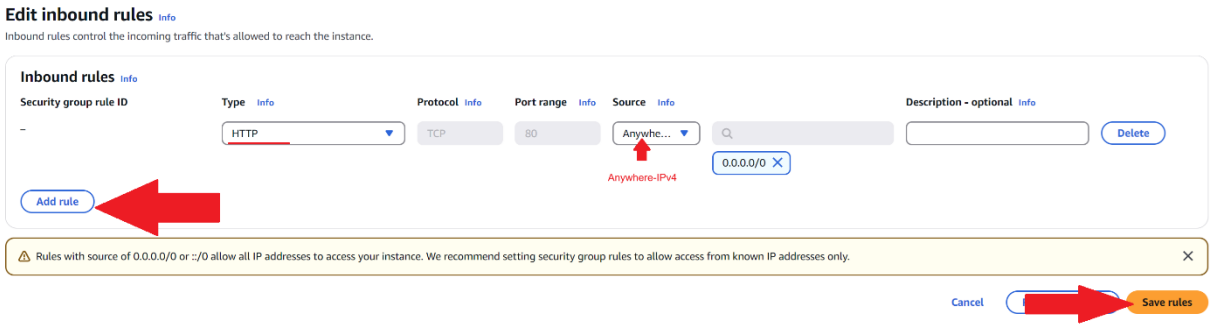
You should see an error message. This is because the security group for the instance has not yet been configured to permit HTTP access.



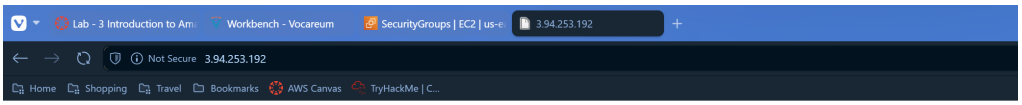
Next, you will configure a security group for the EC2 instance. Go to Security Groups > Select Web server security group > Inbound rules > Edit inbound rules.



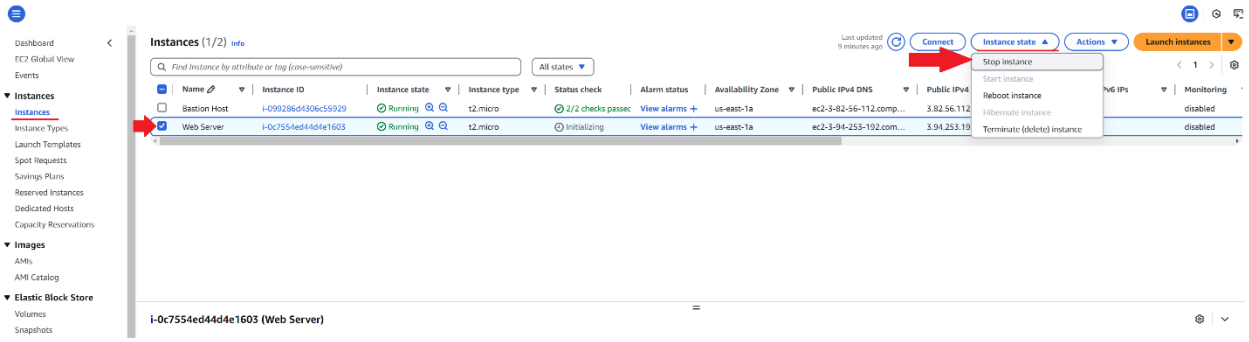
Click Add rule, set the type to HTTP, the source to Anywhere-IPv4, then click Save rules.



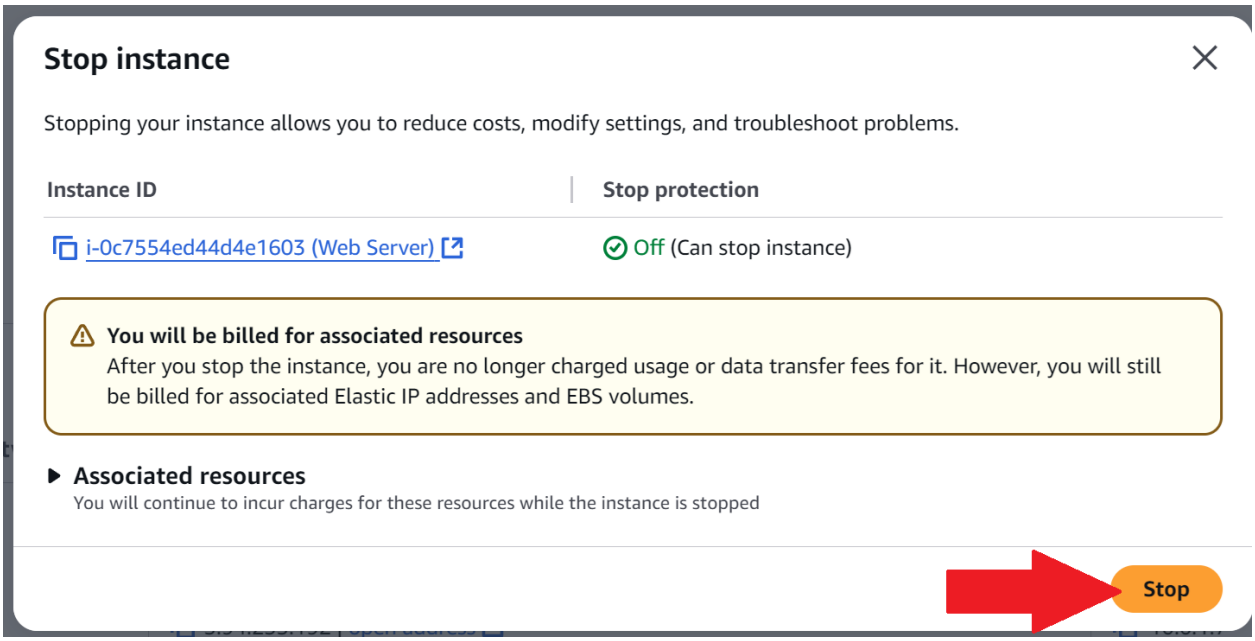
Refresh the web server page. You should see the following message:



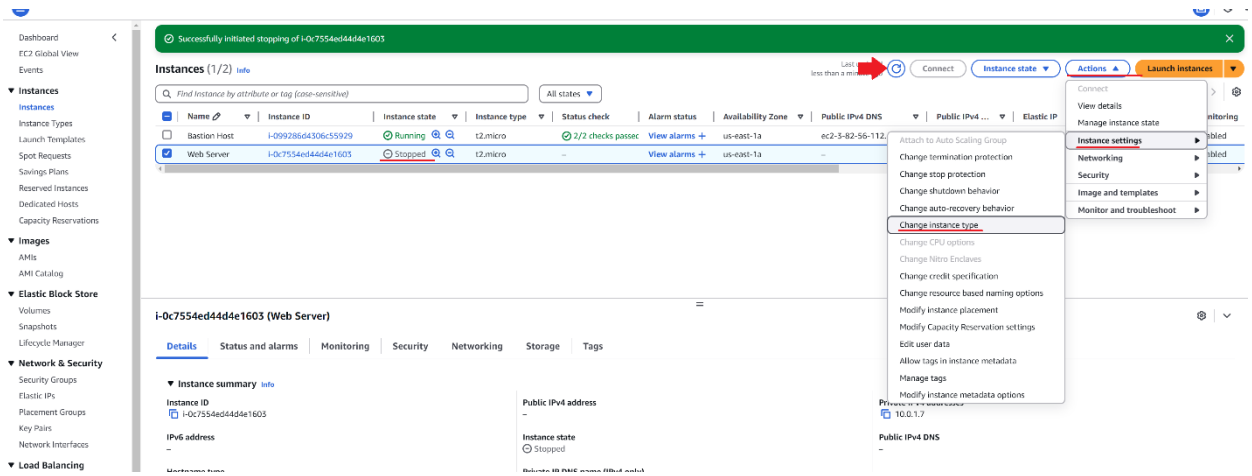
Next, you will resize the instance. Go to Instances > Select Web Server > Instance state > Stop instance.



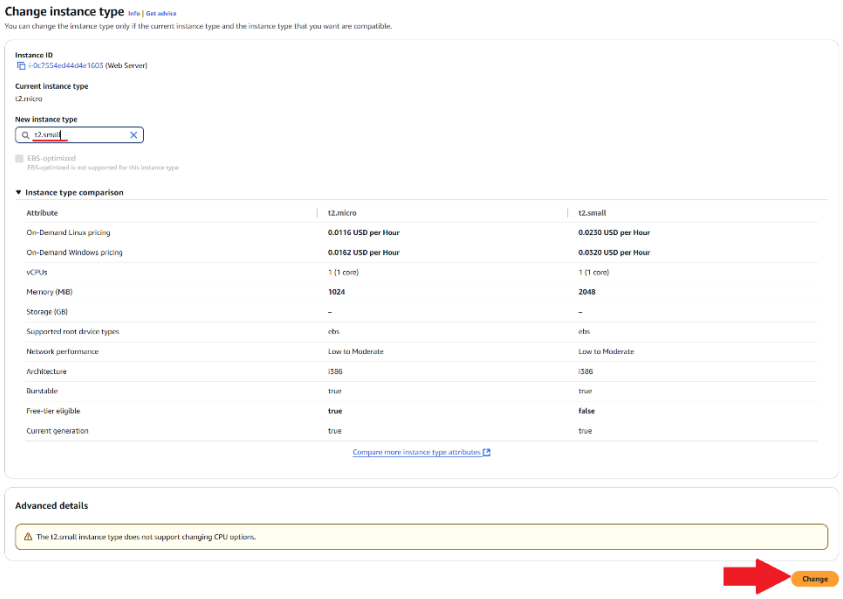
Click Stop.



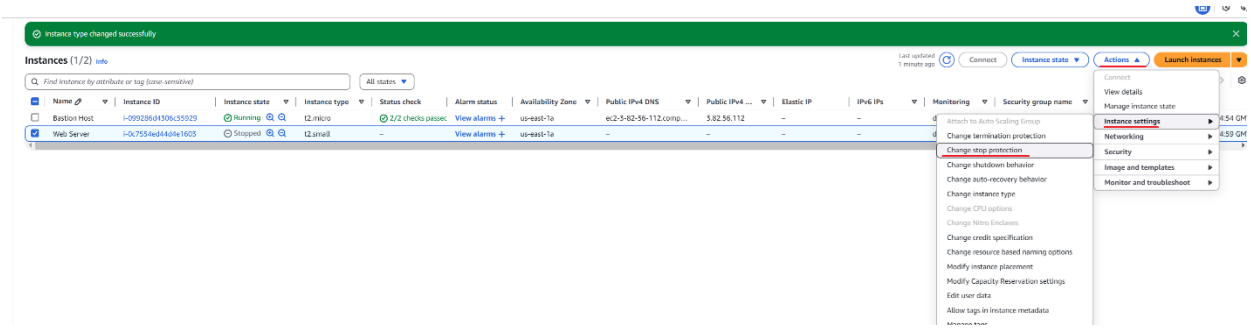
Click the refresh icon until the instance state shows Stopped, then go to Actions > Instance settings > Change instance type.



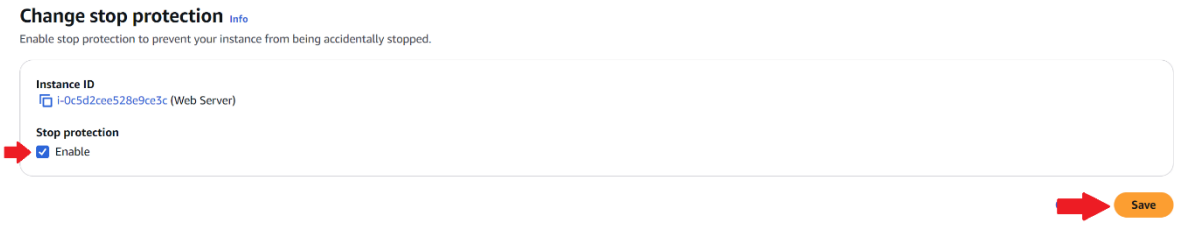
Set the instance type to t2.small, then click Change.



Go to Actions > Instance settings > Change stop protection.

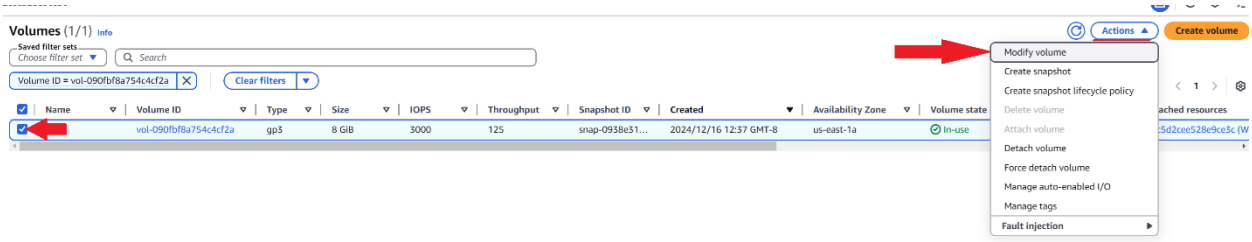


Click Enable, then click save.

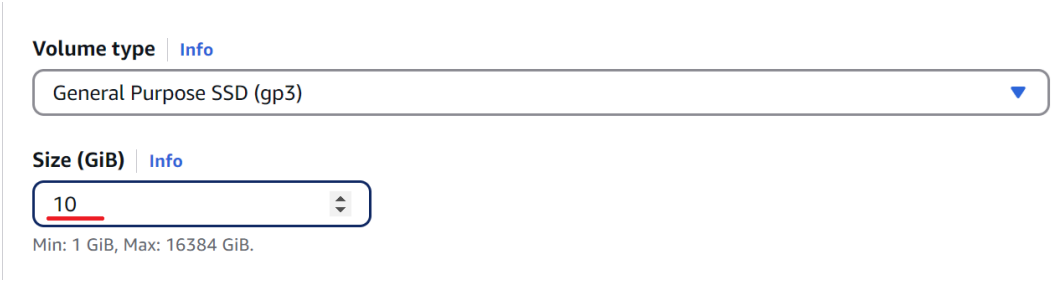


Next, go to the web server's Storage tab..

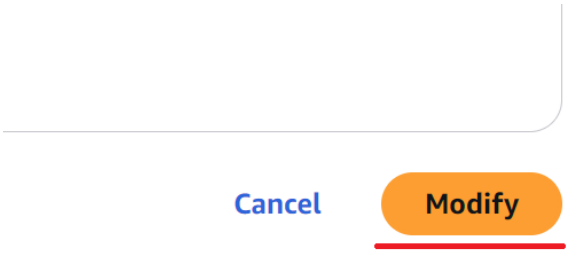
Select the volume created earlier, then click Actions > Modify volume.



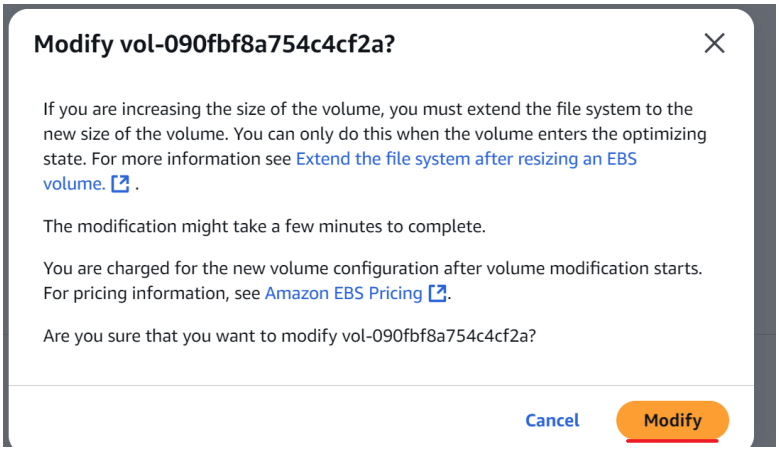
Change the size to 10 GiB.



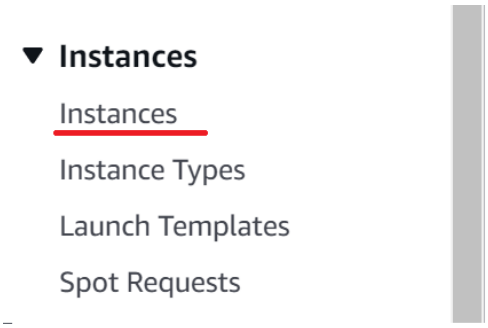
Click Modify.



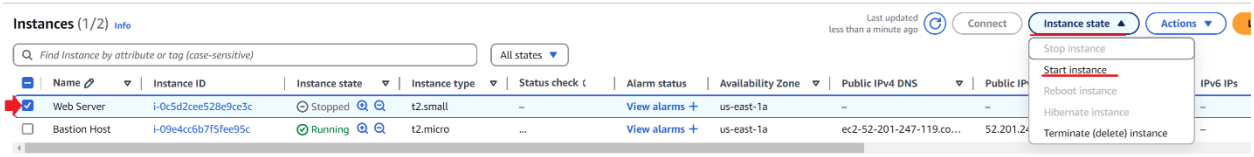
Click Modify again.



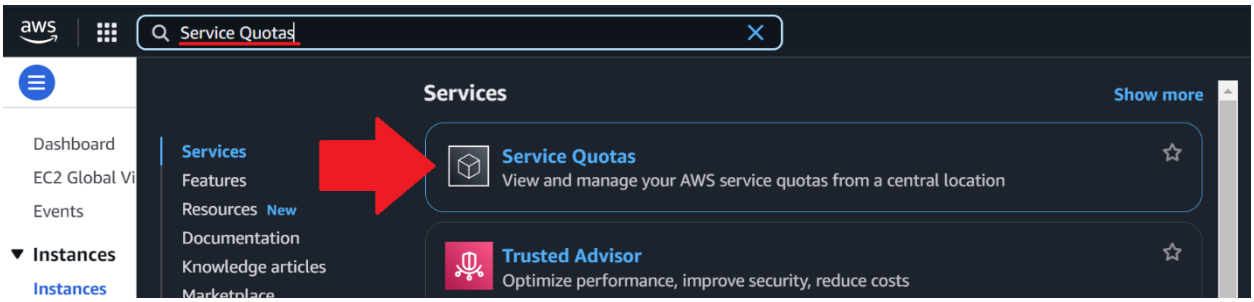
Return to the Instances section of the EC2 dashboard.



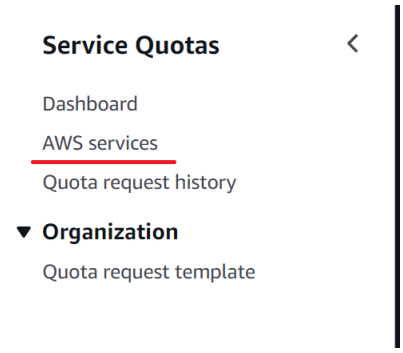
Select Web Server and click Instance state > Start instance.



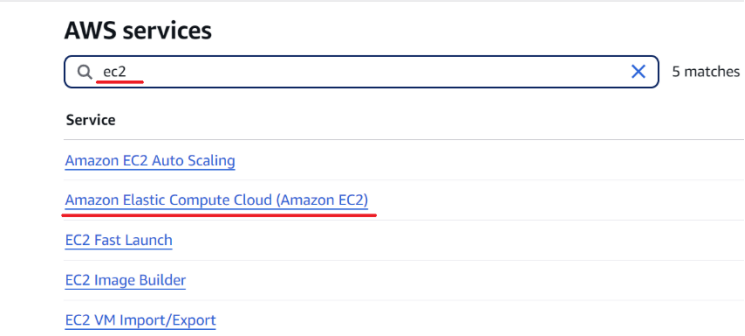
While the EC2 instance is starting, go to the Service Quotas dashboard from the search bar.



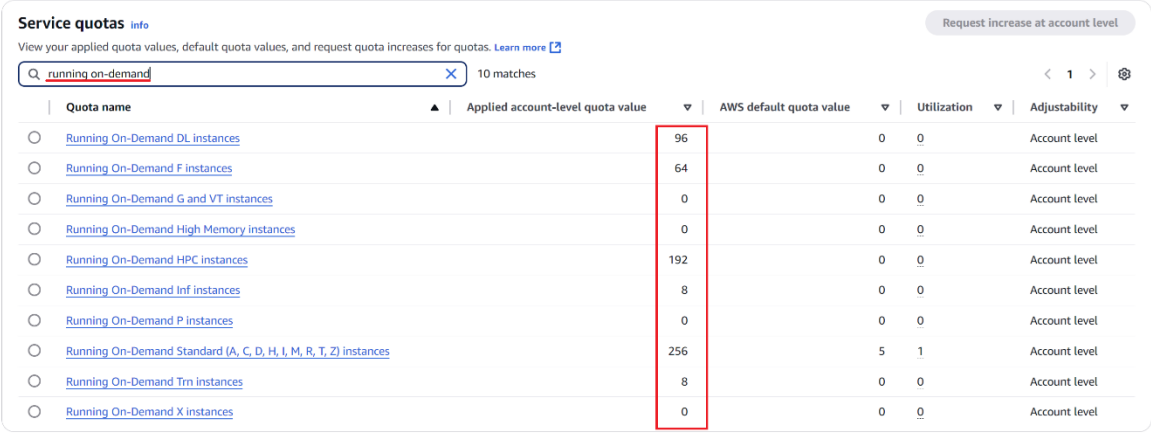
Select AWS services from the sidebar.



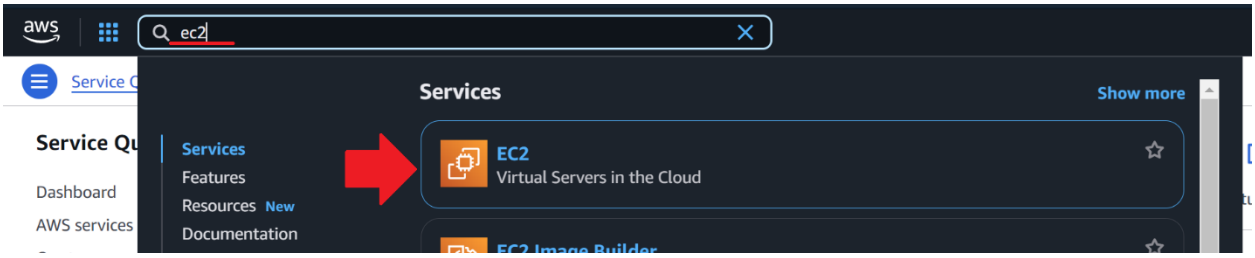
Search for and select Amazon Elastic Compute Cloud (Amazon EC2).



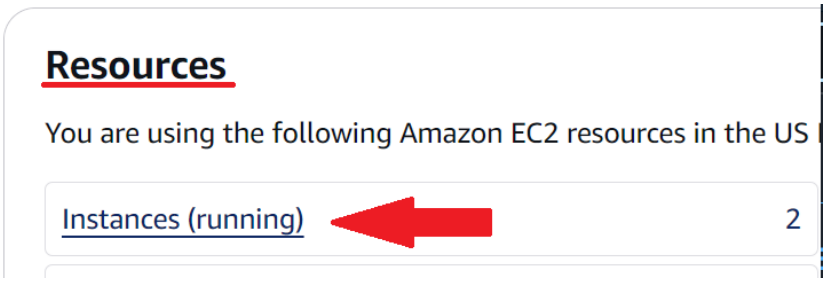
Search for running on-demand. Note the limits applied to how many concurrent EC2 instances can be run based on the instance type. Ensure that you do not surpass these limits while working with EC2.



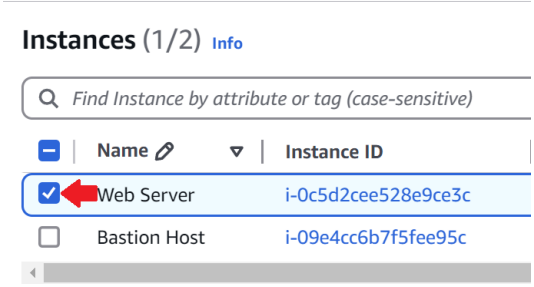
Return to the EC2 dashboard from the search bar.



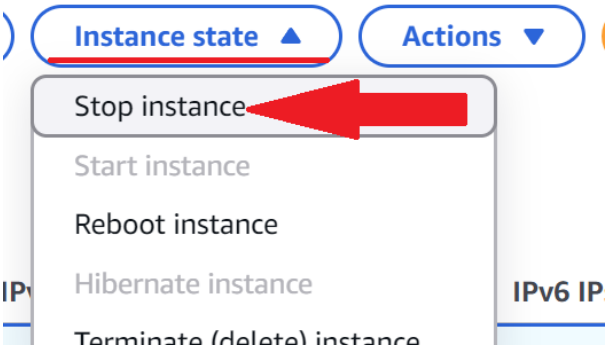
From the homepage, click Instances (running) under the Resources tab.



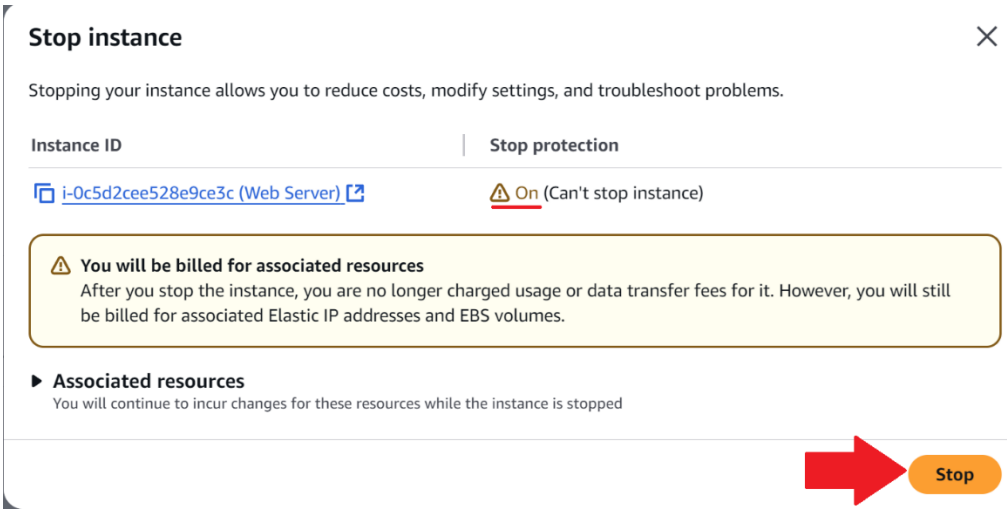
Select Web Server.



Select Instance state > Stop instance.

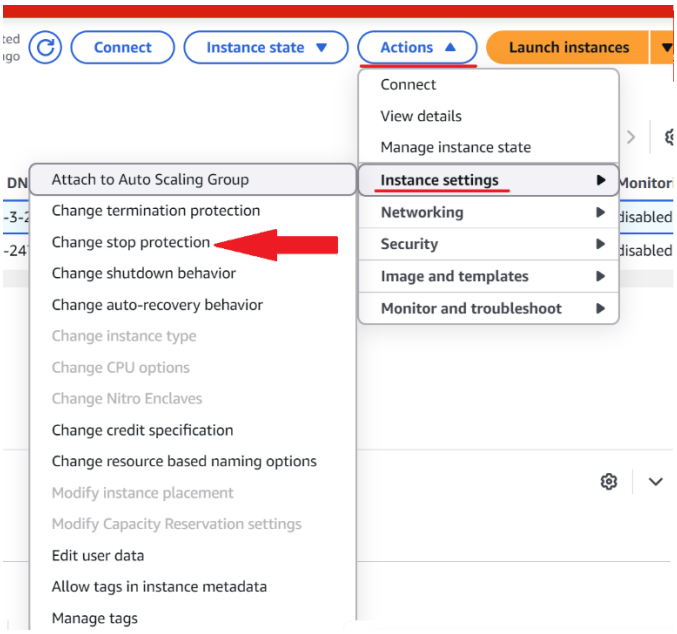


Click stop. Note the warning that stop protection is on.

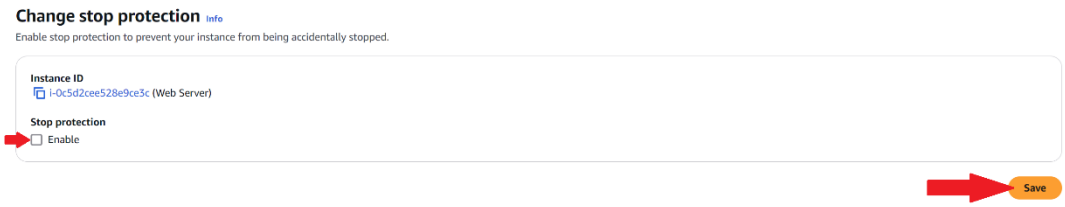


You will see the following error message.

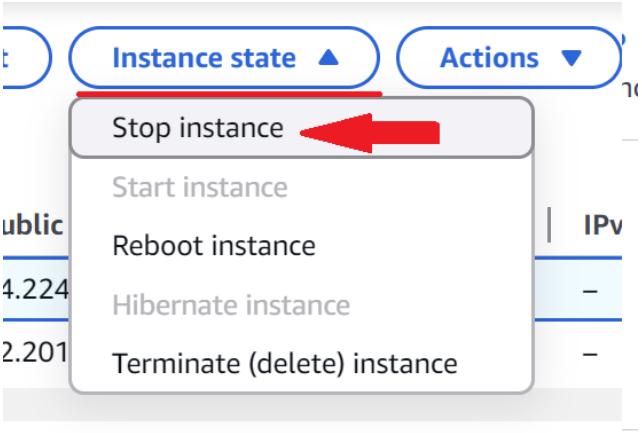
Next, you will disable stop protection. Go to Actions > Instance settings and click Change stop protection.



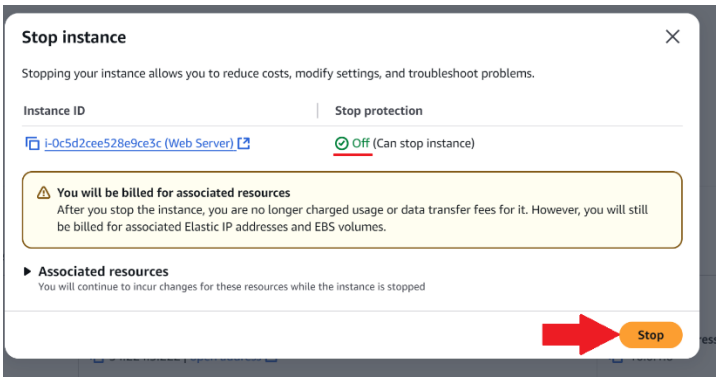
Uncheck Enable and click Save.



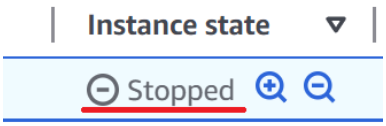
Now, click Instance state > Stop instance.



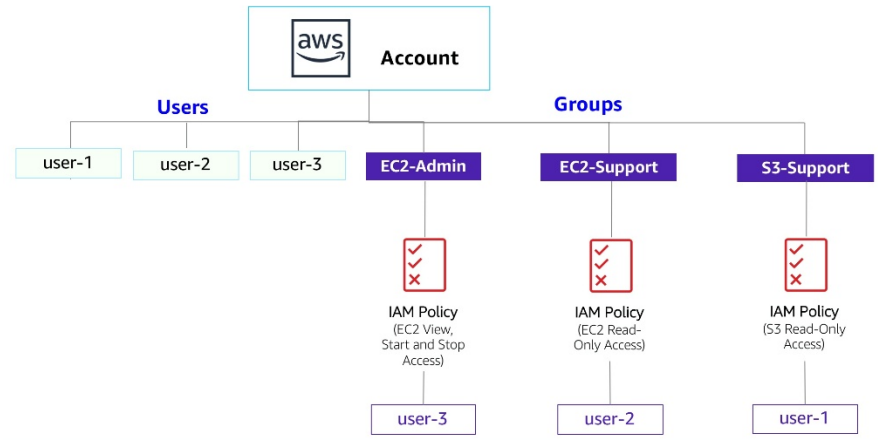
Click Stop. Note the confirmation that stop protection is now off.



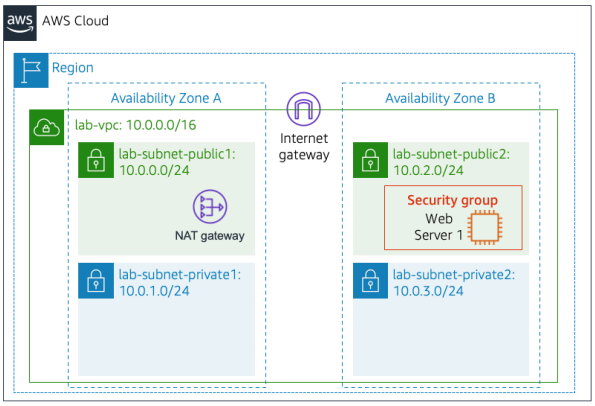
Wait a few minutes and refresh the Instances page. The web server's instance state should now show as Stopped.



Network Diagram (Lab 1 IAM)



Network Diagram (Lab 2 VPC)



Public Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	Internet gateway

Private Route Tables

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	NAT gateway

Network Diagram (Lab 3 EC2)

Problems

One problem I encountered was in Lab 3 (the EC2 lab), where even after correctly updating the Web server security group, the server's webpage refused to connect. This is because my web browser attempted to connect with HTTPS instead of HTTP. This was fixed simply by modifying the protocol in the URL to connect over HTTP.

Conclusion

To wrap up, this lab was a very useful introduction to the world of cloud computing. I'm grateful to have learned about exciting new cloud computing concepts such as complex security mechanisms, virtual routing through a private cloud, and easily scalable virtual machines. I'm now confident that I could help a company migrate basic services from traditional IT to the cloud, I'm hopeful that these foundational skills will help me secure a career in cloud services in the future.

Cover Image Attribution: Ram Venu

Advanced Cisco Networking Academy – Configuring a Cisco Wireless Access Point and WLC with WPA2-PSK and WPA2-Enterprise with a RADIUS Server

Colin J. Faletto, CCNA

Networking Academy

Purpose

This lab is intended to reintroduce the concept of managing wireless connectivity with a WLAN Controller, a concept we visited briefly in CCNA but haven't learned about since. This lab is also meant to introduce RADIUS and the process of setting it up as an external server, which indirectly teaches basic Linux skills such as navigating the terminal. This lab also revisits aspects from the CCNA course such as subinterfaces/VLANs and virtualization.

Background

Aironet is a division of Cisco that develops wireless access points. It was founded in 1986 as an independent company and acquired by Cisco 13 years later. The Cisco Aironet 1040 series was a series of access points developed by Cisco in the early 2010s, which was discontinued in 2013 and dropped from supoport in 2018. As of 2025, the Aironet line appears to be inactive or discontinued, replaced fully by the Catalyst and Meraki lines of wireless products.

Wi-Fi Protected Access, or WPA, is a security standard developed and maintained by the Wi-Fi alliance. There are three versions of WPA, being named WPA, WPA2, and WPA3 respectively. The first generation of WPA was released in 2003, with the second version releasing just a year later in 2004. In 2018, the third generation was released. WPA uses TKIP (Temporal Key Integrity Protocol) as its encryption method, while WPA2 uses CCMP (Counter-Mode/CBC-Mac Protocol) for encryption. WPA3 keeps support for CCMP but introduces GCMP (Galois/Counter Mode Protocol) as a stronger encryption method as well.

WPA can use two different methods of authentication: Personal and Enterprise. Personal authentication uses a pre-shared 256 bit key, meaning that all devices authenticate using the same password. Enterprise authentication uses a RADIUS (Remote Authentication Dial-In User Service) server, meaning that each user authenticates using their own username and password.

Ubuntu is a distribution of Linux developed by Canonical. It is built on the older Debian distribution, including well-known features from that distrubution such as the package manager Advanced Package Tool (APT). It is the most popular Linux distribution by far, with a multitude of spin-off distributions. By default, Ubuntu uses the GNOME desktop environment, which is designed with accessibility and readability in mind.

Lubuntu is a Linux distribution built on Ubuntu known for being lightweight, both in terms of CPU/Memory utilization and storage usage. Lubuntu uses the LXQt desktop environment, which is a lightweight desktop environment that still provides all the tools necessary for basic productivity and development.

Lab Summary

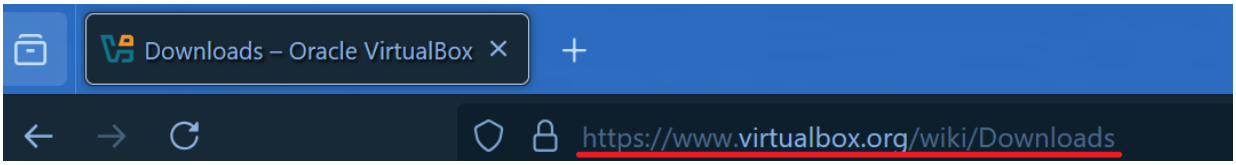
In this lab, we configured a Cisco 2504 WLAN Controller and Cisco Aironet AIR-LAP1042N Access Point with three WLANs – one configured with no security (CrunchwrapSupreme), one with WPA2-PSK (NachosBellGrande), and one with WPA2-Enterprise (CheesyGorditaCrunch). Each of these WLANs is connected to its own

VLAN, with a central router giving out addresses for each VLAN via DHCP. The central router is also connected to a management VLAN where the AP, WLAN Controller, and management PC reside.

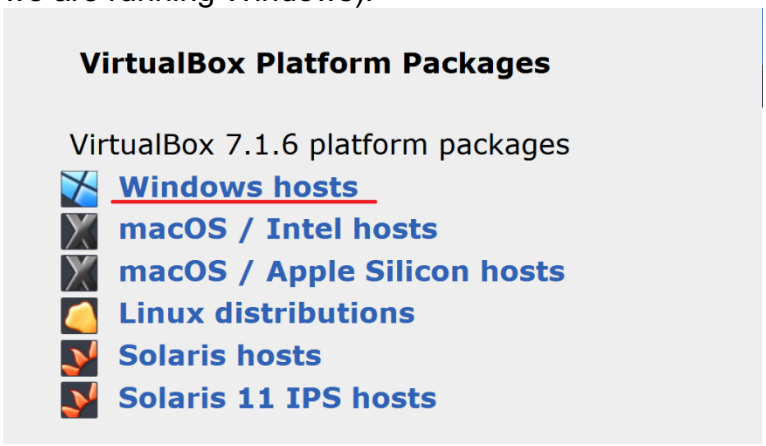
The management PC is also running a virtualized instance of Lubuntu through Virtualbox. Lubuntu is a Linux distribution we chose for its lightweight nature and similarity to the widely supported Ubuntu distribution. The Lubuntu instance runs an instance of FreeRADIUS that is used for authentication for the CheesyGorditaCrunch WLAN.

Lab Commands (Configure RADIUS Server)

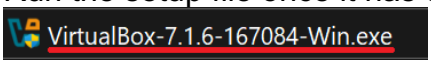
On your host PC, navigate to https://www.virtualbox.org/wiki/Downloads in a web browser.



Download the appropriate version of Virtualbox for your operating system (in this case, we are running Windows).

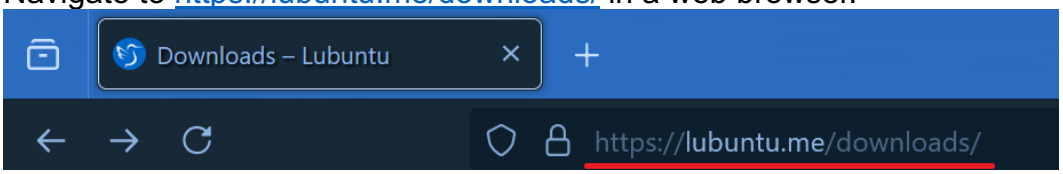


Run the setup file once it has downloaded.



Be agreeable through the setup process, clicking Next and Install when prompted.

Navigate to https://lubuntu.me/downloads/ in a web browser.



Download the ISO image for the latest stable release of the operating system.

24.10 (Oracular Oriole)

Latest stable release

Supported until July 2025

Please read the release annoucement.

LXQt Version: 2.0

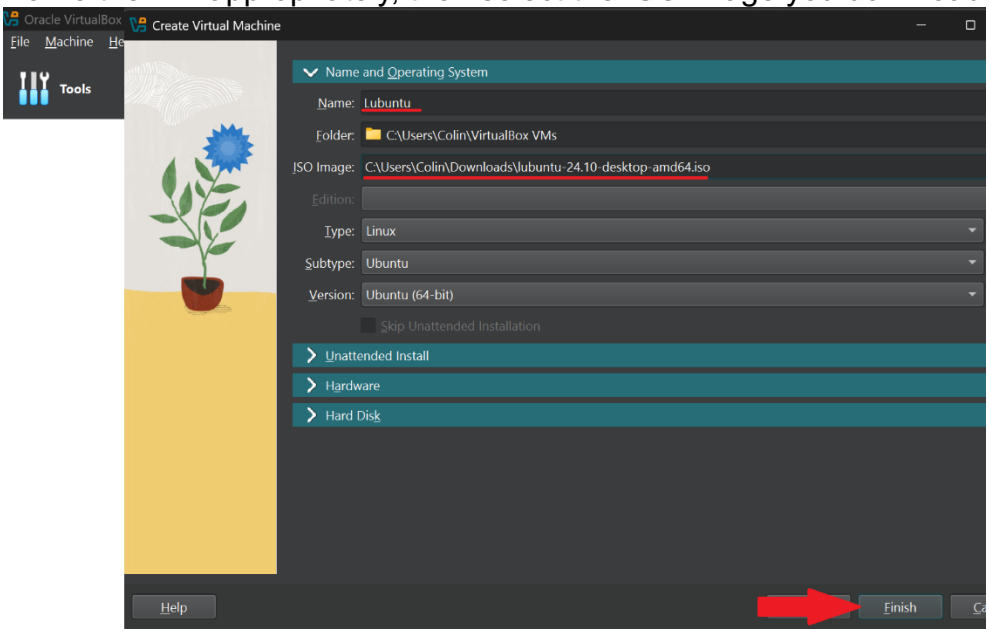
It's better to use the (magnet) link first (auto-verified downloads).

⚠ *Note: make sure to verify the integrity (SHA256SUMS) of your downloads and that they come from an official source. More info here.*

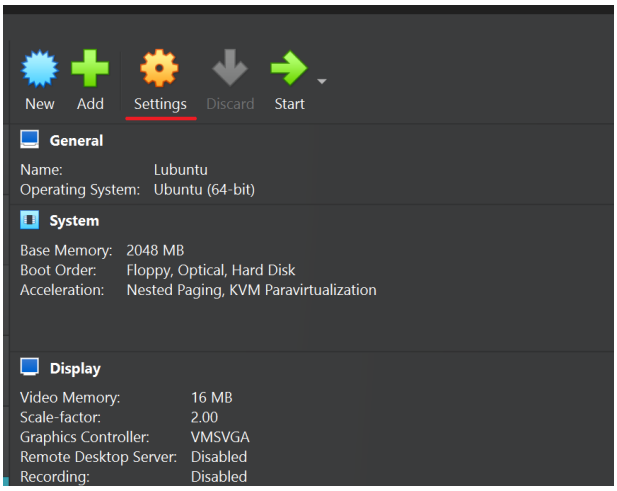
Desktop 64-bit

Open Virtualbox and click New.

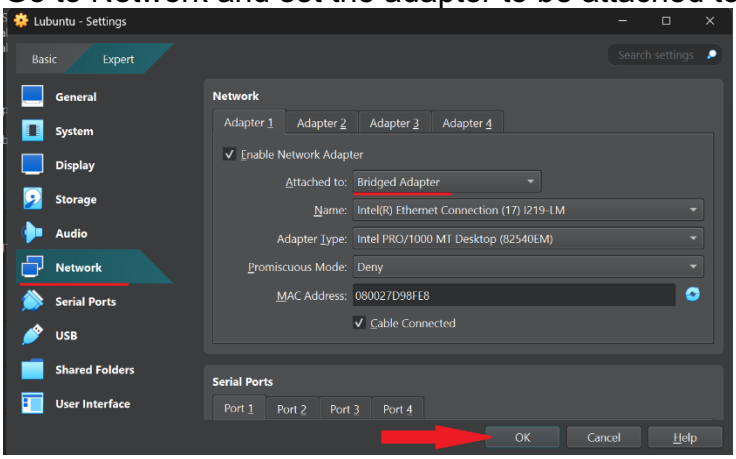
Name the VM appropriately, then select the ISO image you downloaded earlier.



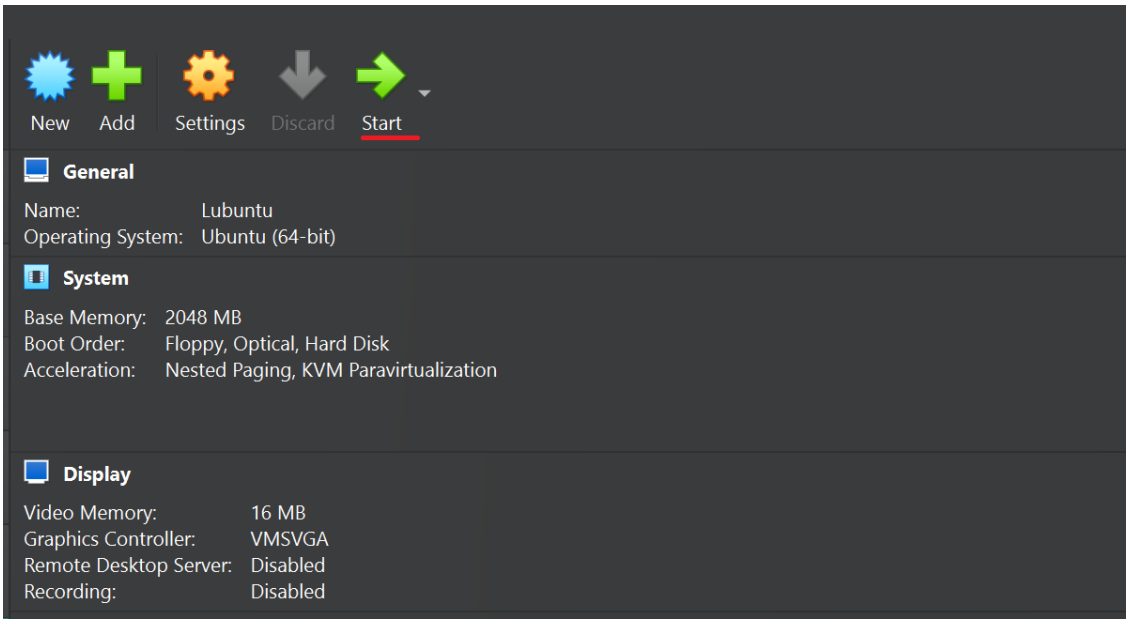
Click Settings.



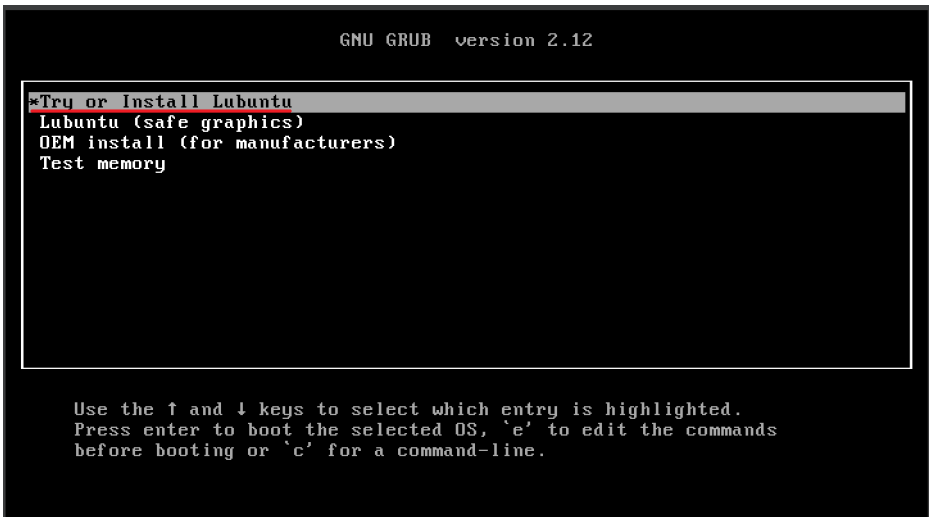
Go to Network and set the adapter to be attached to a Bridged Adapter. Click OK.



Click Start.



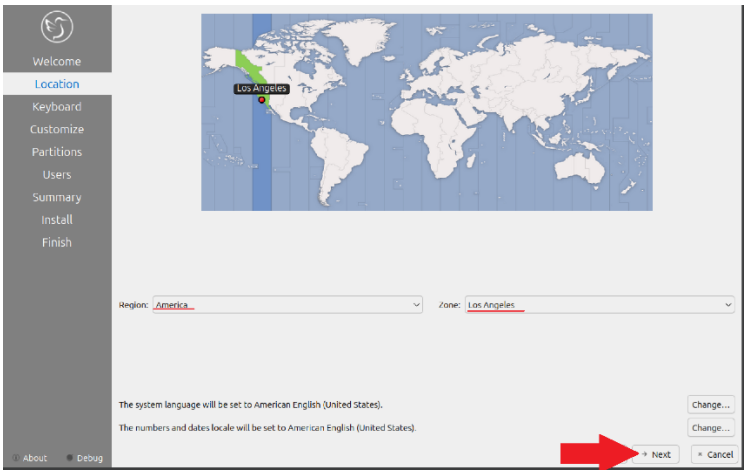
Select Try or Install Lubuntu.



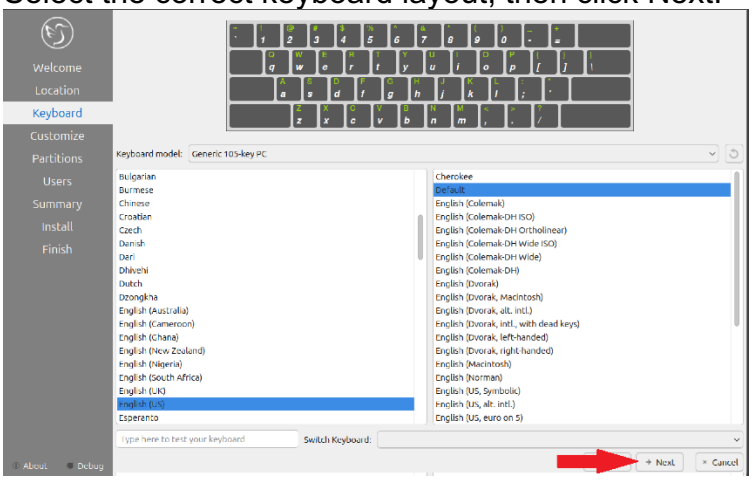
Select Install Lubuntu.

Click Next.

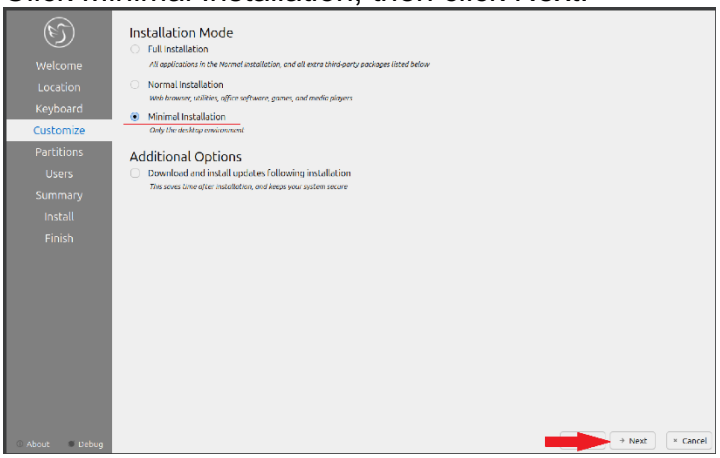
Set the correct time zone, then click Next.



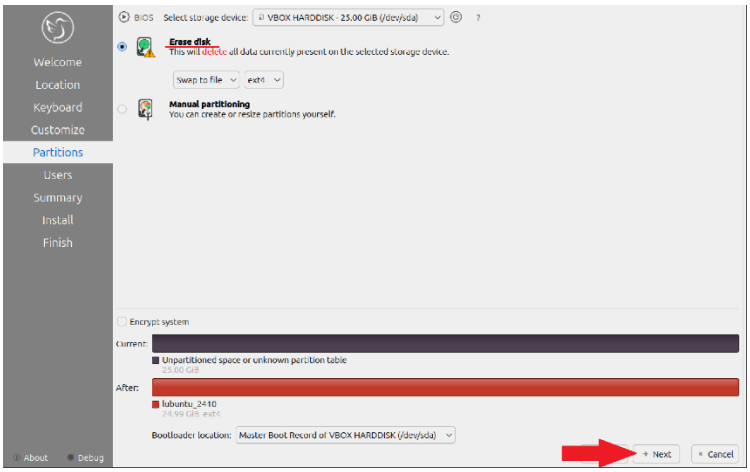
Select the correct keyboard layout, then click Next.



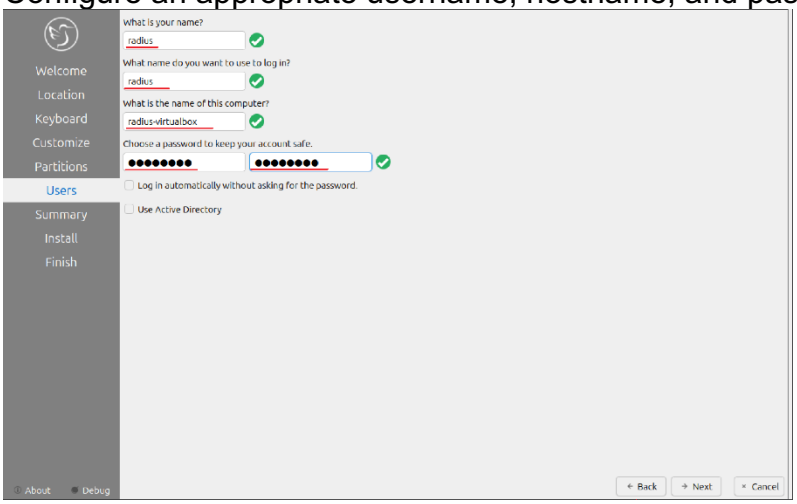
Click Minimal Installation, then click Next.



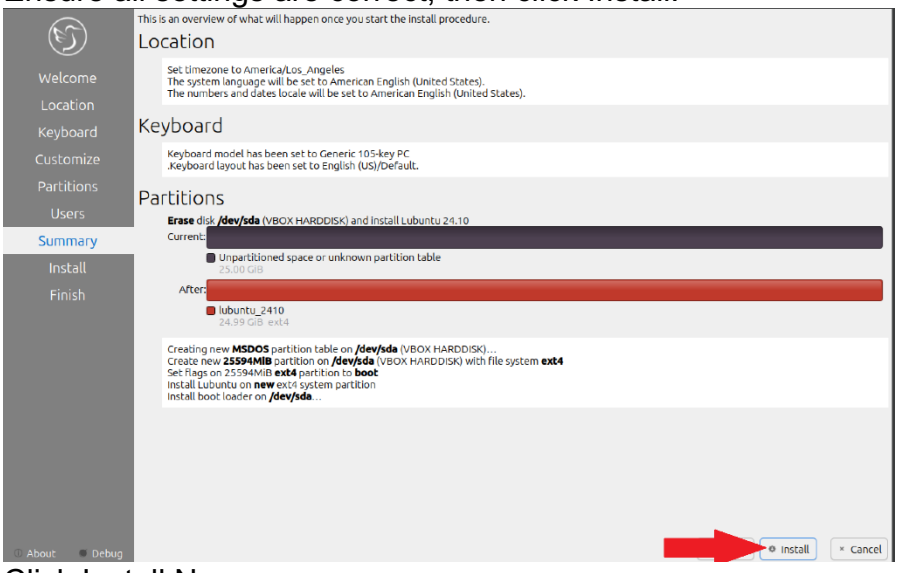
Select Erase disk, then click Next.



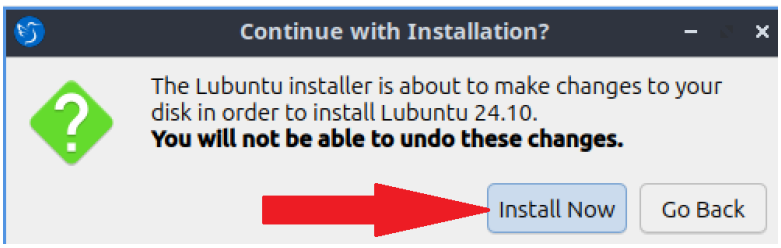
Configure an appropriate username, hostname, and password, then click Next.



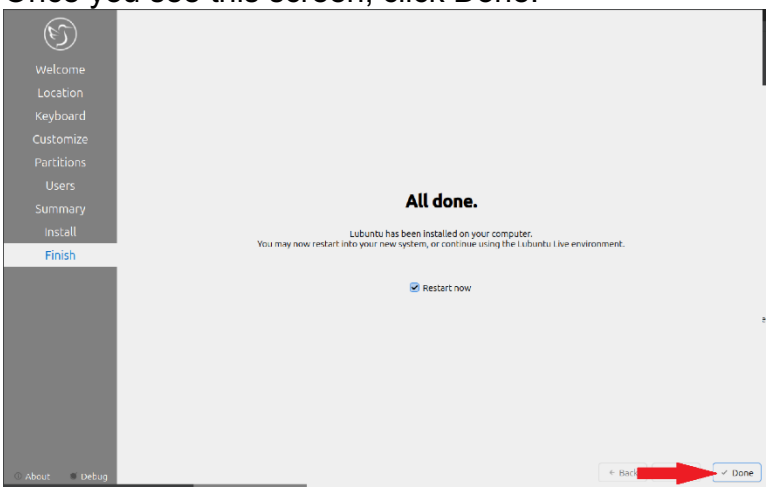
Ensure all settings are correct, then click Install.



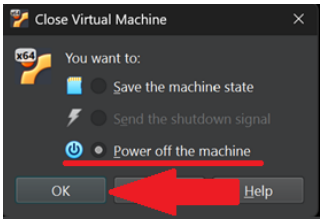
Click Install Now.



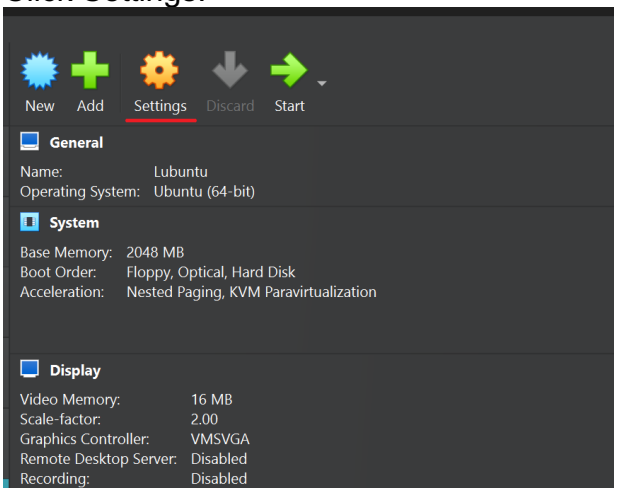
Once you see this screen, click Done.



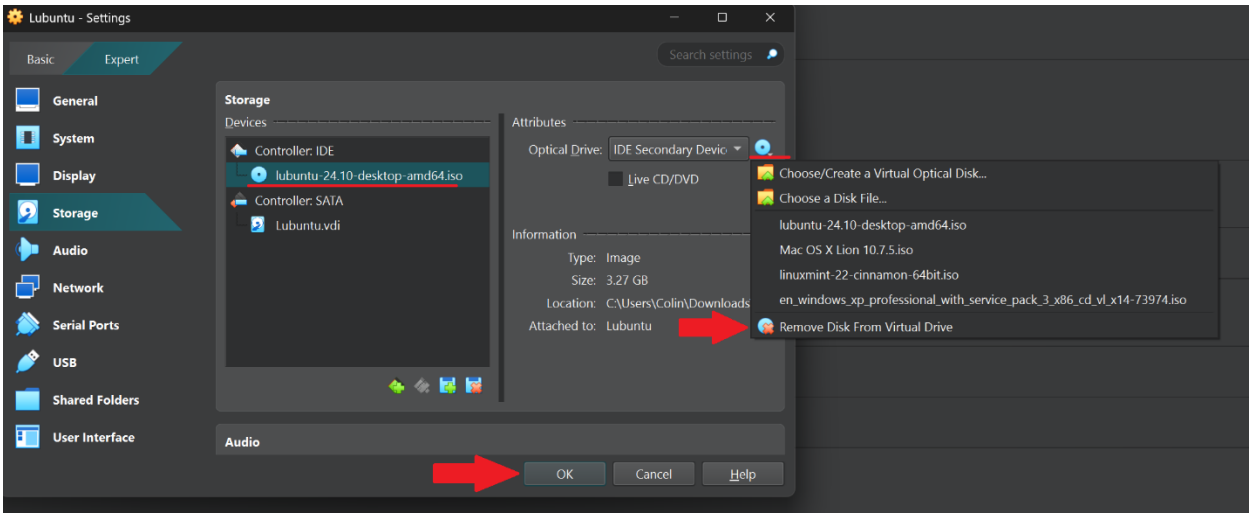
Press Right CTRL, then ALT+F4 to exit out of the VM. Select Power off the Machine, then click OK.



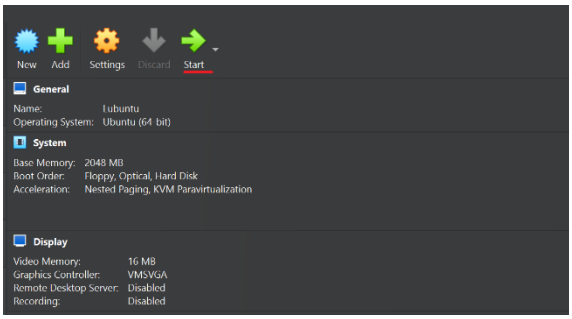
Click Settings.



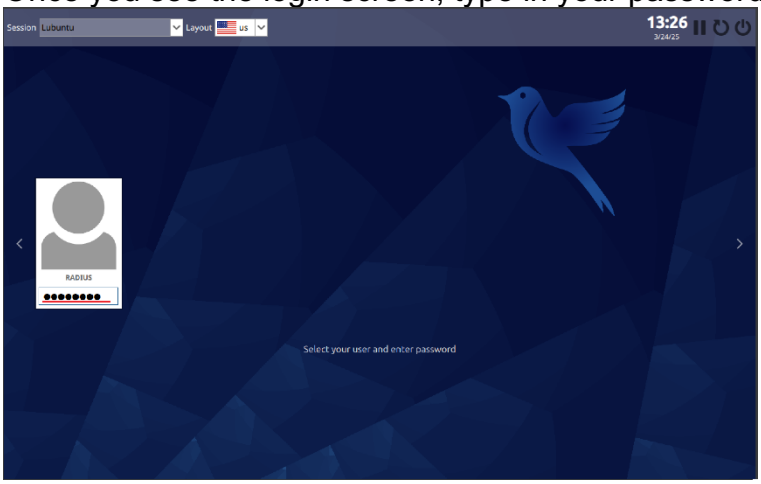
Go to Storage and click on the ISO file, click on the disk icon, then click Remove Disk from Virtual Drive. Click OK.



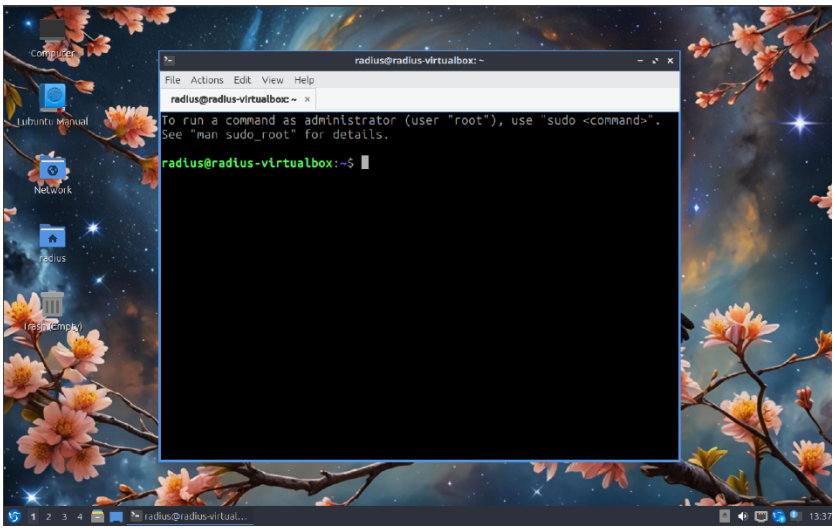
Click Start.



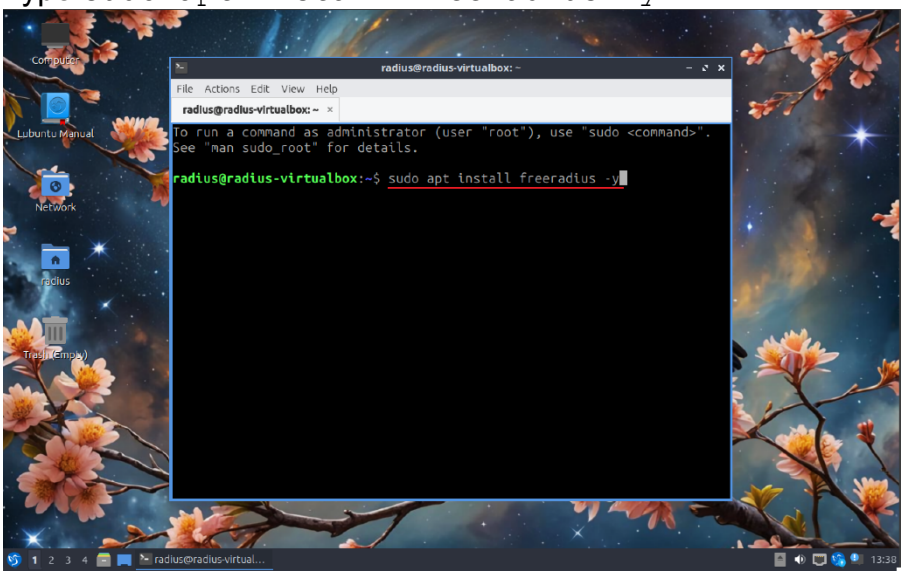
Once you see the login screen, type in your password and press Enter.



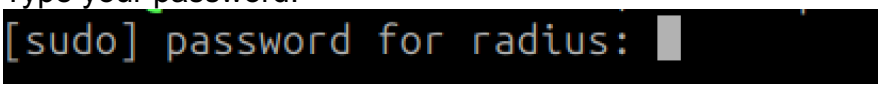
Press CTRL + ALT + T to open the terminal.



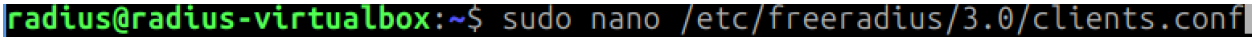
Type `sudo apt install freeradius -y`.



Type your password.



Once freeradius has installed, type `sudo nano /etc/freeradius/3.0/clients.conf`.



Add the following lines:

```
client wlc {
      ipaddr = 192.168.0.254
      secret = <secret>
}
```

With <secret> being replaced with a secure password to be specified later on the WLC.

```
client wlc {
        ipaddr = 192.168.0.254
        secret = Redbull6
}
```

Press CTRL + X, Y, then ENTER to save.

```
Save modified buffer?
 Y Yes
 N No           ^C Cancel
```

```
File Name to Write: /etc/freeradius/3.0/clients.conf
^G Help          M-D DOS Format    M-A Append        M-B Backup File
^C Cancel        M-M Mac Format    M-P Prepend       ^T Browse
```

Next, type `sudo nano /etc/freeradius/3.0/users`.

```
radius@radius-virtualbox:~$ sudo nano /etc/freeradius/3.0/users
```

Add the following lines:

```
<user>    Cleartext-Password := "<password>"
          Reply-Message := "Hello, <user>"
```

With <user> being replaced with a username and <password> being replaced with a secure password.

```
colin   Cleartext-Password := "squabbleup"
        Reply-Message := "Hello, Colin"
```

Press CTRL + X, Y, then ENTER to save.

```
Save modified buffer?
 Y Yes
 N No           ^C Cancel
```

```
File Name to Write: /etc/freeradius/3.0/users
^G Help          M-D DOS Format    M-A Append        M-B Backup File
^C Cancel        M-M Mac Format    M-P Prepend       ^T Browse
```

Lab Commands (Configuring WLC)

Connect your AP, WLC, Router, and PC to your switch as specified in the network diagram below.

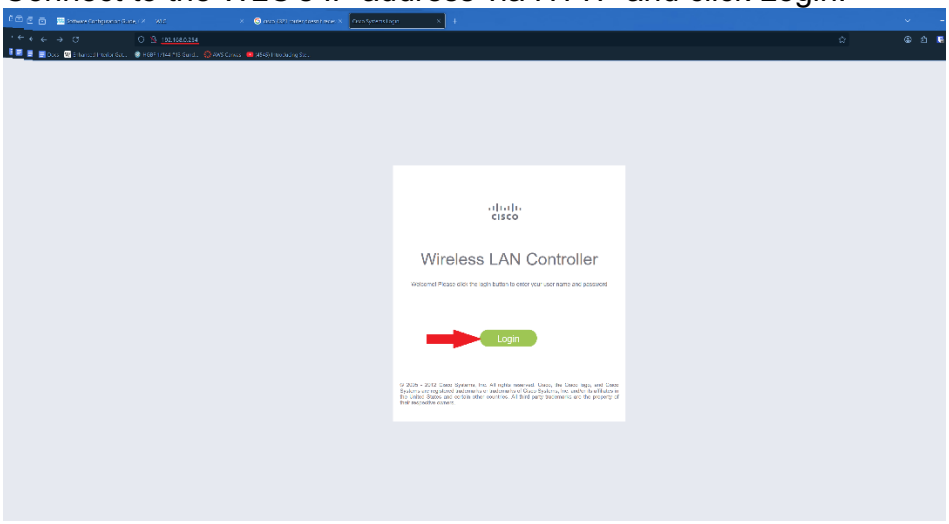
Configure your switch according to the switch configuration below (Note: the WLC should be connected to port f0/1 as a trunk, and all other devices should be on access VLAN 99.).

Configure your router according to the configuration below.

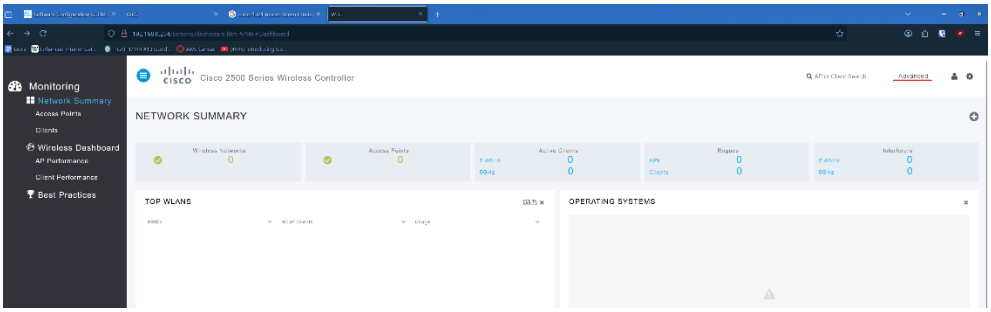
Ensure that PC is receiving an IP and that internet works.

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.0.3
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

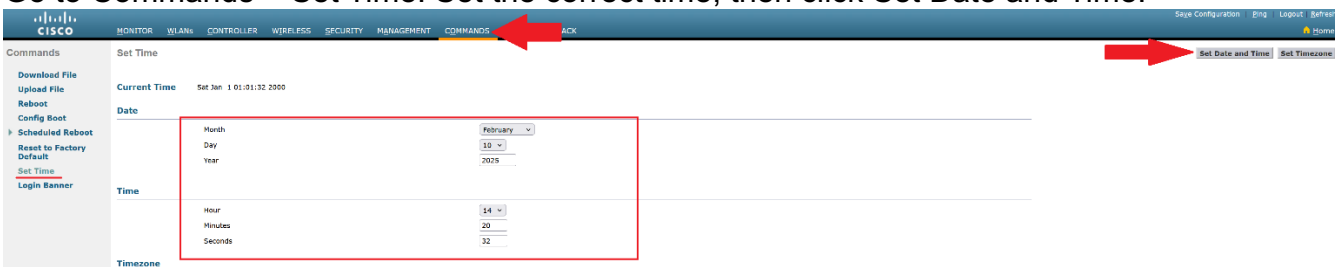
Connect to the WLC's IP address via HTTP and click Login.



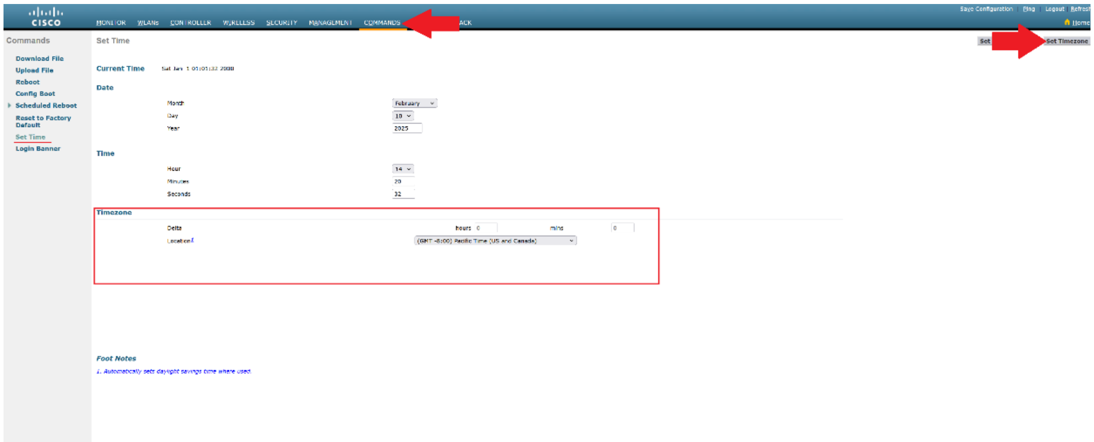
Click Advanced.



Go to Commands > Set Time. Set the correct time, then click Set Date and Time.

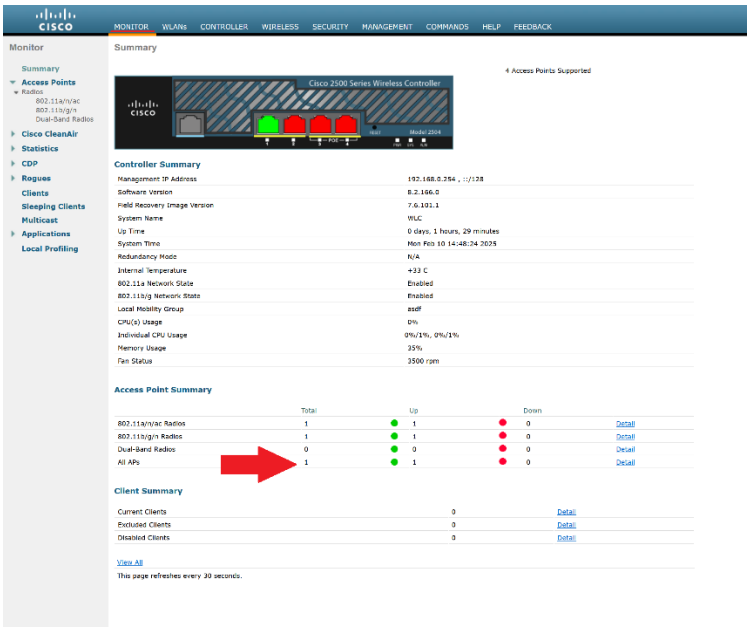


Set the timezone and click Set Timezone.

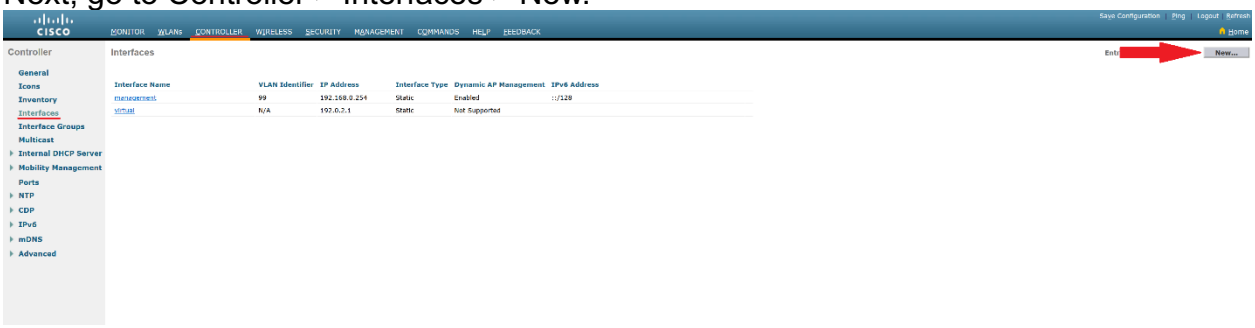


Once the correct timezone is set, the AP should automatically discover and connect to your WLC. In our case, the AP automatically downloaded and installed a software update as shown in the console log below (the image name is underlined in red):

Once the AP has finished updating, go to Monitor > Summary and ensure the WLC can see the AP (indicated by a 1 next to the All APs section)



Next, go to Controller > Interfaces > New.

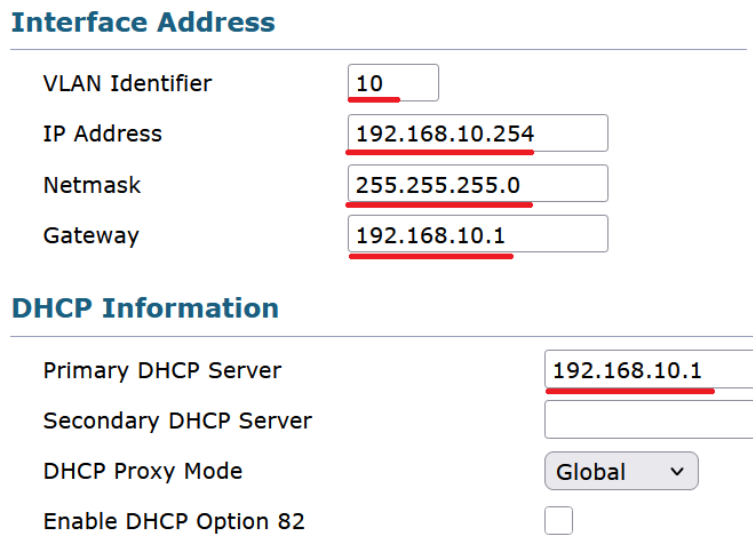


Create the Guest VLAN, setting the VLAN ID to 10.

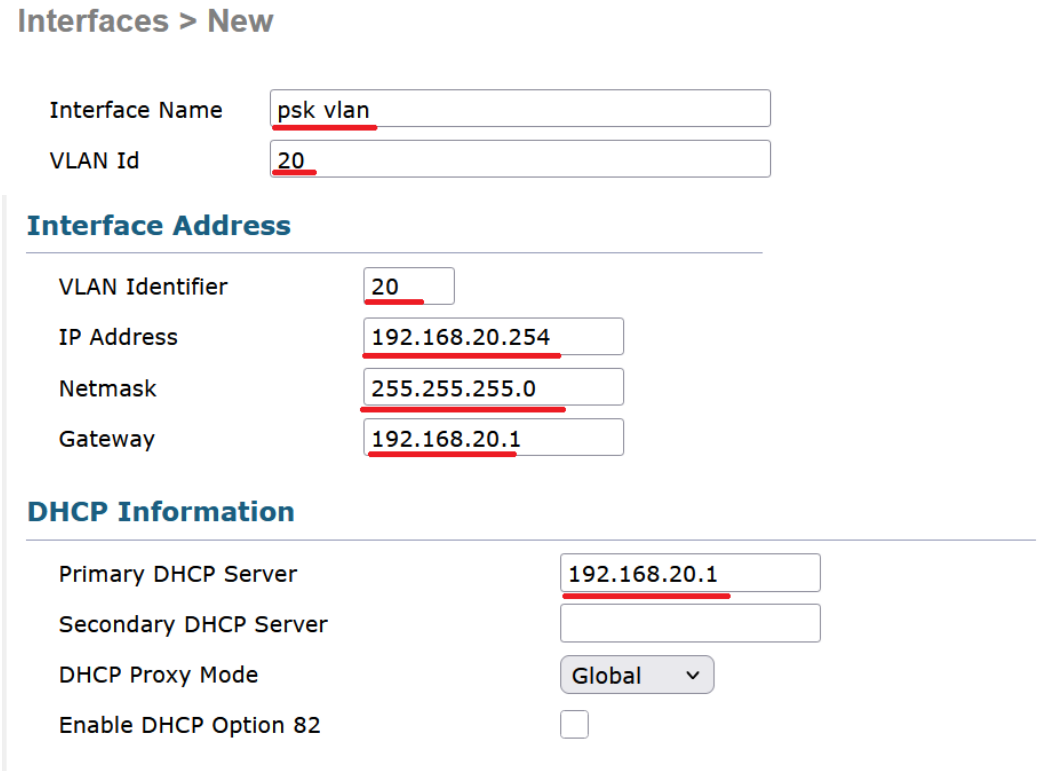
Interfaces > New

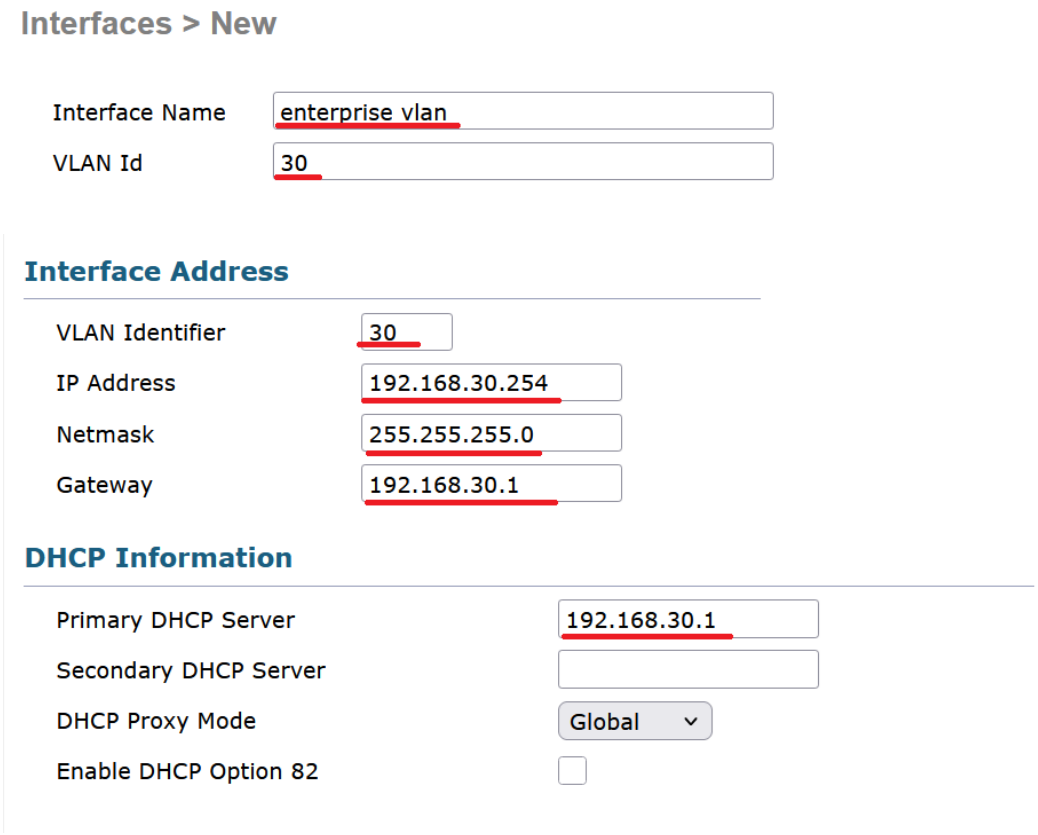
Interface Name	Guest VLAN
VLAN Id	10

Configure the VLAN ID, IP Address, Netmask, Gateway, and Primary DHCP Server for VLAN 10:

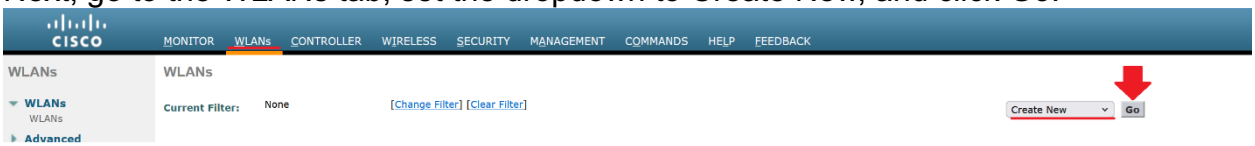


Create the PSK and Enterprise VLANs, using the VLAN information for VLANs 20 and 30 respectively:

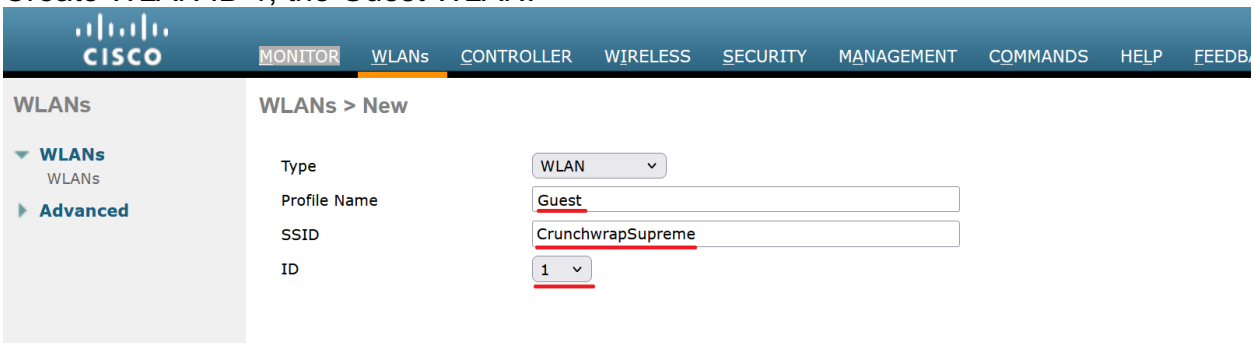




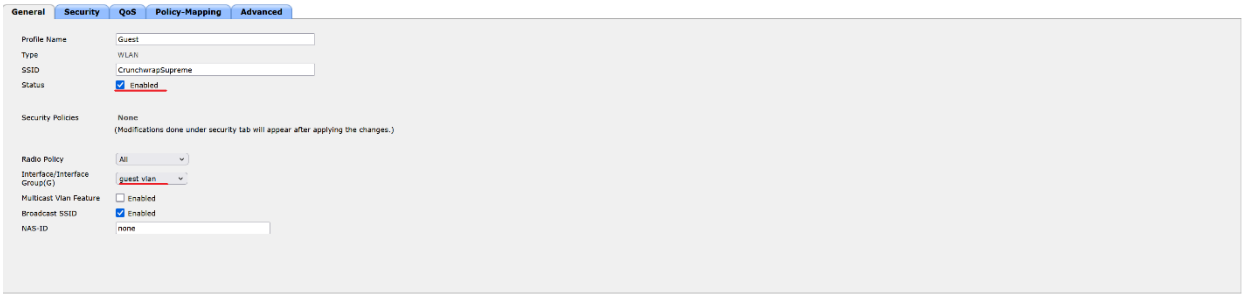
Next, go to the WLANs tab, set the dropdown to Create New, and click Go.



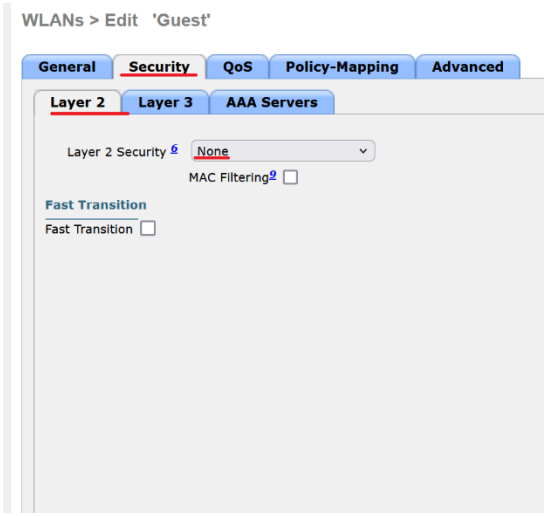
Create WLAN ID 1, the Guest WLAN:



Ensure the WLAN is enabled, and the interface is set to the guest VLAN:

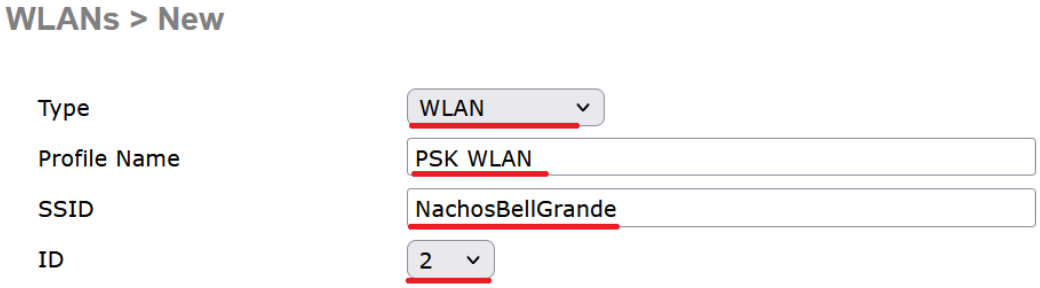


Under Security > Layer 2, set Layer 2 Security to None.

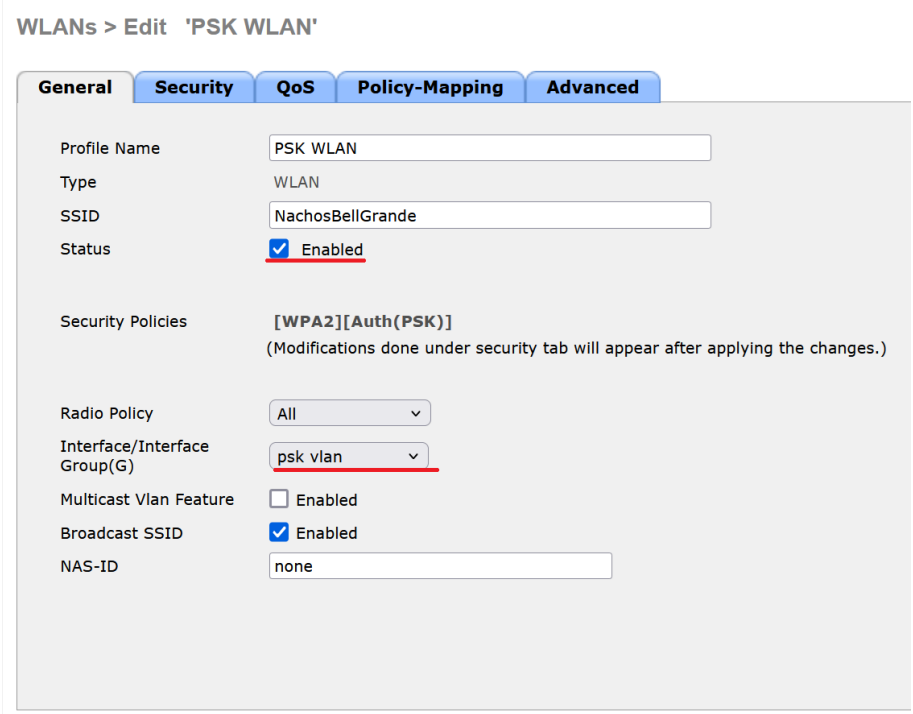


Click Apply.

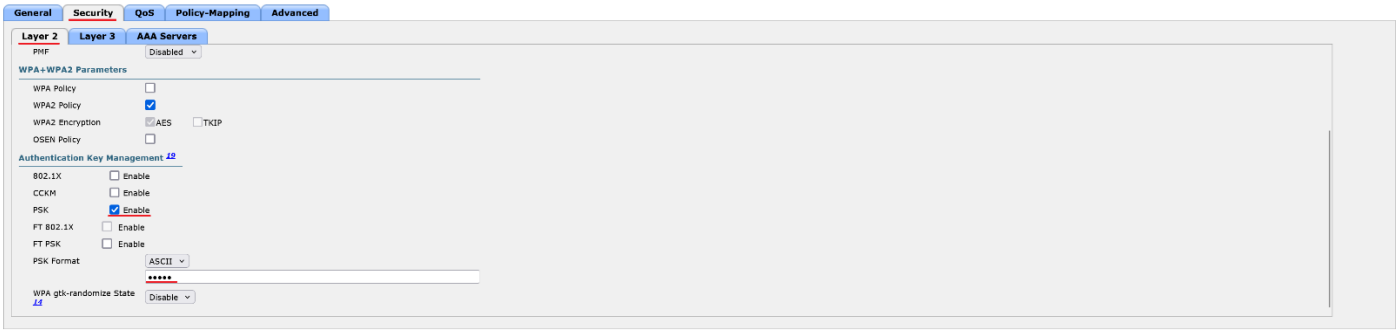
Next, configure the PSK WLAN (NachosBellGrande) with VLAN ID 2.



Ensure the WLAN is enabled and the interface is set to the PSK VLAN.

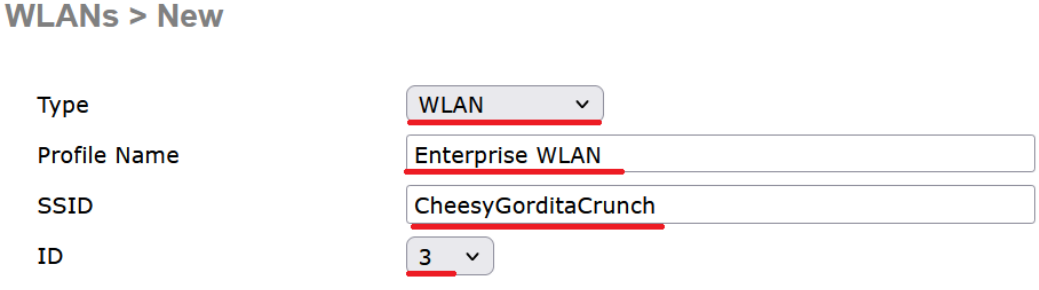


Under Security > Layer 2, Enable PSK, and under PSK Format, set a strong password.

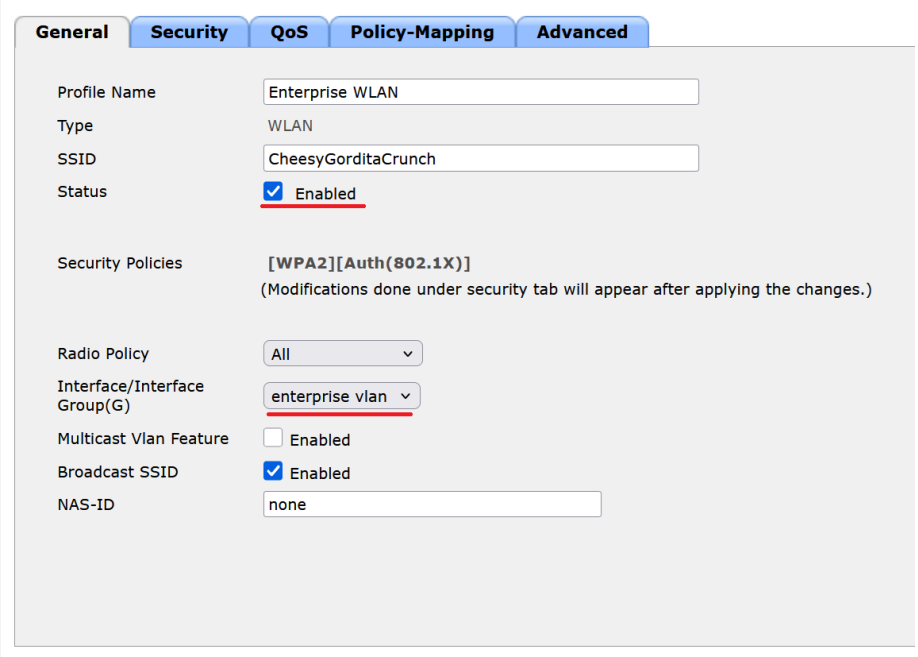


Click Apply.

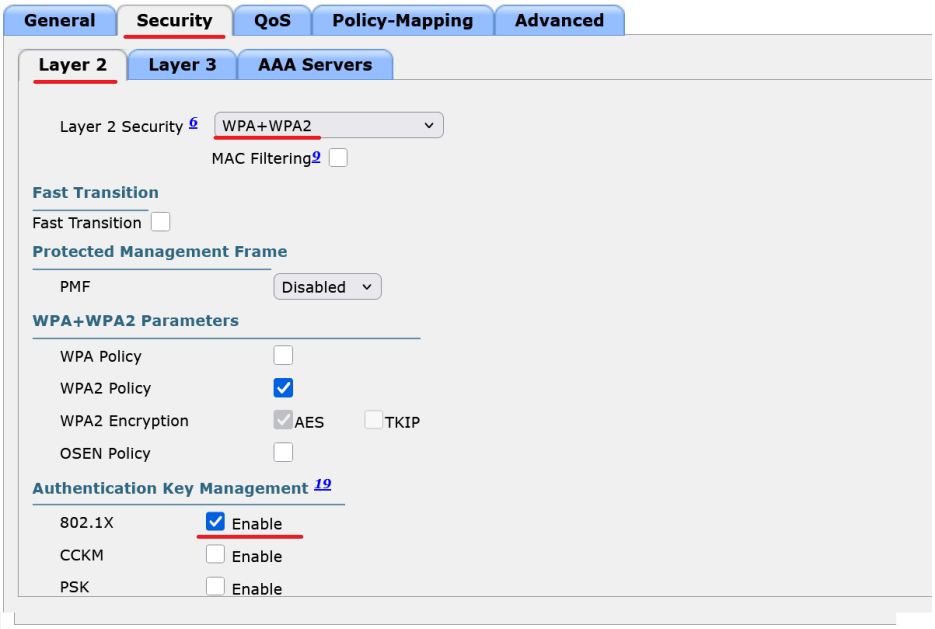
Next, Create the Enterprise WLAN.



Ensure the WLAN is enabled and set the interface to the Enterprise VLAN.

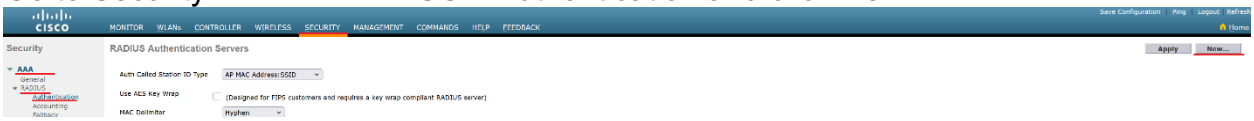


Under Security > Layer 2, set the Layer 2 securitty to WPA+WPA2, and under Authentication Key Management, ensure that 802.1X is enabled.

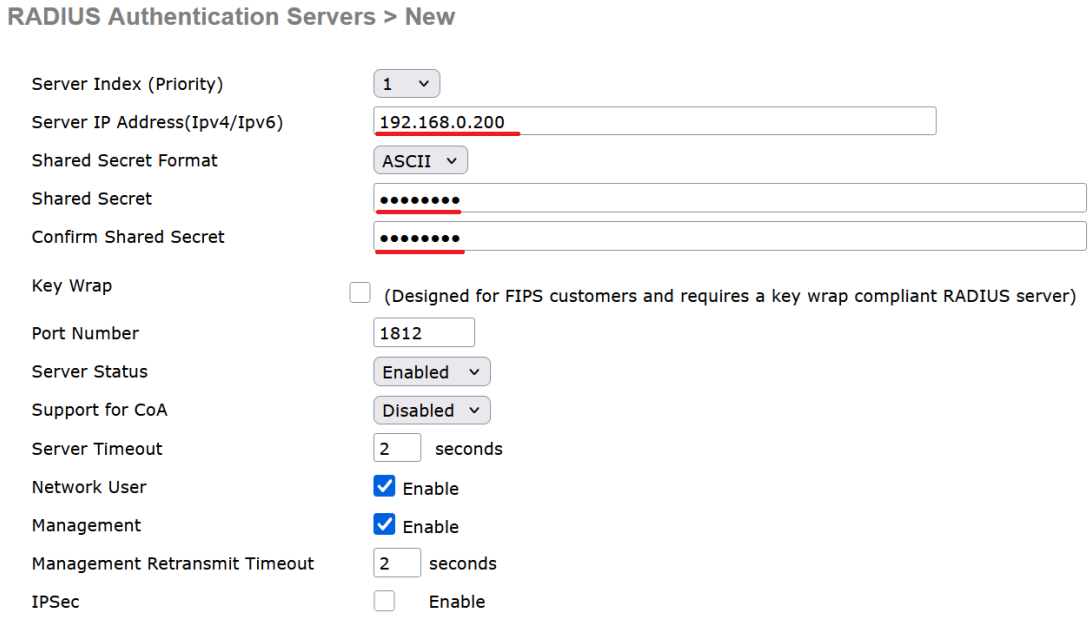


Click Apply.

Go to Security > AAA > RADIUS > Authentication and click New.



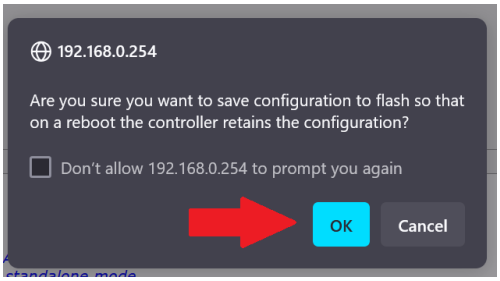
Enter the IP address of the RADIUS server, then enter the shared secret configured in the server's `clients.conf` file.



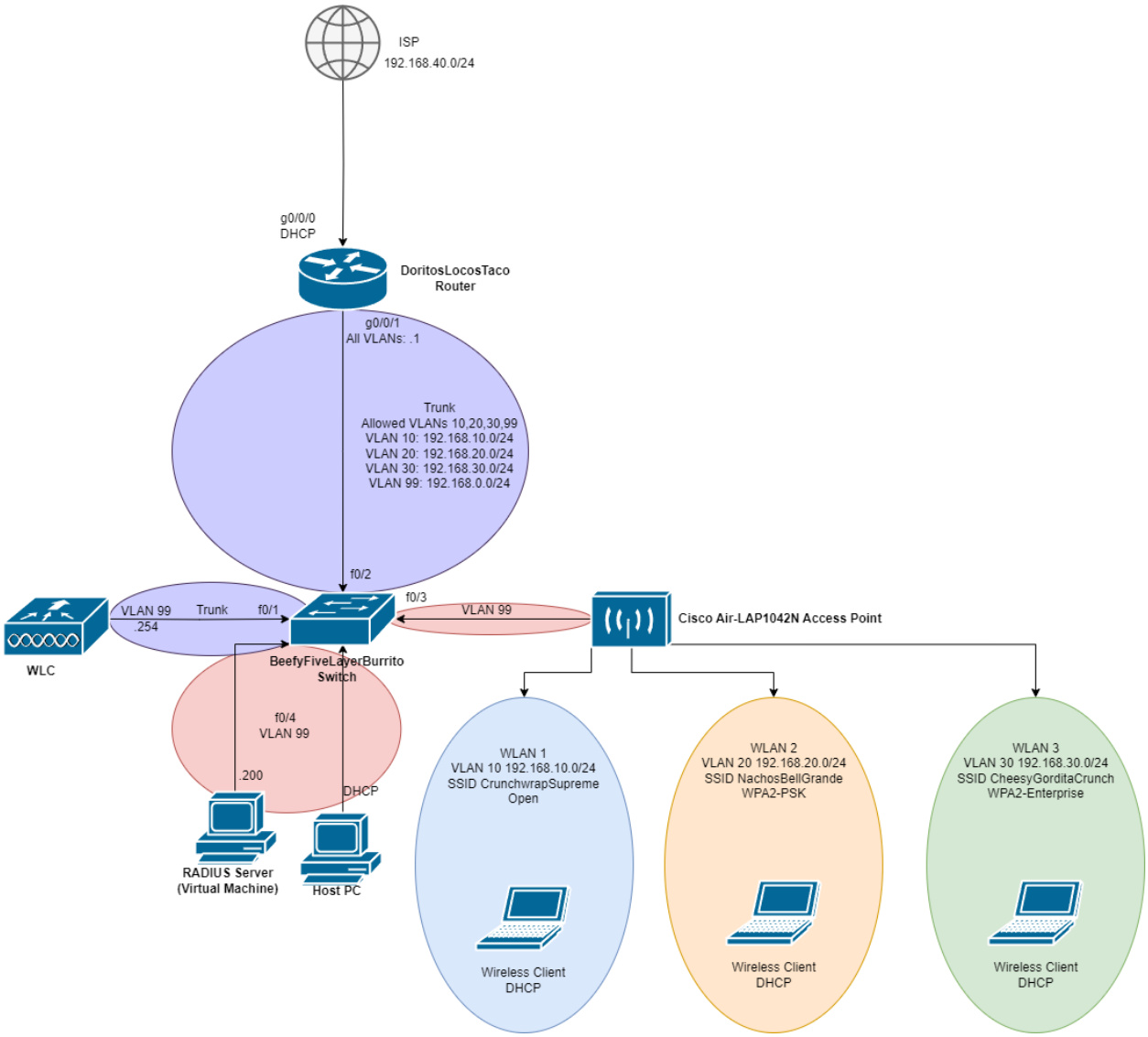
Click Apply.

Finally, click Save Configuration.

Click OK.



Network Diagram



Configuration for DoritosLocosTaco (Router)

```
Current configuration : 5312 bytes
Last configuration change at 22:07:55 UTC Tue Mar 11 2025
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
hostname DoritosLocosTaco
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
 address-family ipv4
 exit-address-family
 address-family ipv6
```

```
 exit-address-family
no aaa new-model
ip name-server 8.8.8.8 1.1.1.1
ip dhcp excluded-address 192.168.0.254
ip dhcp excluded-address 192.168.0.1
ip dhcp excluded-address 192.168.0.1 192.168.0.10
ip dhcp excluded-address 192.168.0.30 192.168.0.254
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.20.1
ip dhcp excluded-address 192.168.30.1
ip dhcp excluded-address 192.168.0.200
ip dhcp pool AP-POOL
 network 192.168.0.0 255.255.255.0
 default-router 192.168.0.1
 dns-server 8.8.8.8 8.8.4.4
ip dhcp pool GUEST-VLAN
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 8.8.8.8
ip dhcp pool PSK-VLAN
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 8.8.8.8
ip dhcp pool ENTERPRISE-VLAN
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 8.8.8.8
login on-success log
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214421D1
no license smart enable
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
 mode none
interface GigabitEthernet0/0/0
 ip address dhcp
 ip nat outside
 negotiation auto
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
interface GigabitEthernet0/0/1.10
 encapsulation dot1Q 10
```

```
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
interface GigabitEthernet0/0/1.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
 ip nat inside
interface GigabitEthernet0/0/1.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip nat inside
interface GigabitEthernet0/0/1.99
 encapsulation dot1Q 99
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
interface Serial0/1/0
interface Serial0/1/1
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 negotiation auto
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip http client source-interface GigabitEthernet0/0/0
ip nat inside source list 1 interface GigabitEthernet0/0/0
overload
ip nat inside source list 10 interface GigabitEthernet0/0/0
overload
ip nat inside source list 20 interface GigabitEthernet0/0/0
overload
ip nat inside source list 30 interface GigabitEthernet0/0/0
overload
ip route 0.0.0.0 0.0.0.0 dhcp
access-list 1 permit 192.168.0.0 0.0.0.255
access-list 10 permit 192.168.10.0 0.0.0.255
access-list 20 permit 192.168.20.0 0.0.0.255
access-list 30 permit 192.168.30.0 0.0.0.255
ip access-list extended 101
control-plane
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
```

```
end
```

Configuration for BeefyFiveLayerBurrito (Switch)

```
Current configuration : 5307 bytes
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname BeefyFiveLayerBurrito
boot-start-marker
boot-end-marker
no aaa new-model
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
vlan internal allocation policy ascending
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface FastEthernet0/2
 switchport access vlan 99
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30,99
 switchport mode trunk
interface FastEthernet0/3
 switchport access vlan 99
interface FastEthernet0/4
 switchport access vlan 99
interface FastEthernet0/5
 switchport access vlan 99
interface FastEthernet0/6
 switchport access vlan 99
interface FastEthernet0/7
 switchport access vlan 99
interface FastEthernet0/8
 switchport access vlan 99
interface FastEthernet0/9
 switchport access vlan 99
interface FastEthernet0/10
 switchport access vlan 99
interface FastEthernet0/11
 switchport access vlan 99
interface FastEthernet0/12
```

```
 switchport access vlan 99
interface FastEthernet0/13
 switchport access vlan 99
interface FastEthernet0/14
 switchport access vlan 99
interface FastEthernet0/15
 switchport access vlan 99
interface FastEthernet0/16
 switchport access vlan 99
interface FastEthernet0/17
 switchport access vlan 99
interface FastEthernet0/18
 switchport access vlan 99
interface FastEthernet0/19
 switchport access vlan 99
interface FastEthernet0/20
 switchport access vlan 99
interface FastEthernet0/21
 switchport access vlan 99
interface FastEthernet0/22
 switchport access vlan 99
interface FastEthernet0/23
 switchport access vlan 99
interface FastEthernet0/24
 switchport access vlan 99
interface FastEthernet0/25
 switchport access vlan 99
interface FastEthernet0/26
 switchport access vlan 99
interface FastEthernet0/27
 switchport access vlan 99
interface FastEthernet0/28
 switchport access vlan 99
interface FastEthernet0/29
 switchport access vlan 99
interface FastEthernet0/30
 switchport access vlan 99
interface FastEthernet0/31
 switchport access vlan 99
interface FastEthernet0/32
 switchport access vlan 99
interface FastEthernet0/33
 switchport access vlan 99
interface FastEthernet0/34
 switchport access vlan 99
interface FastEthernet0/35
 switchport access vlan 99
```

```
interface FastEthernet0/36
 switchport access vlan 99
interface FastEthernet0/37
 switchport access vlan 99
interface FastEthernet0/38
 switchport access vlan 99
interface FastEthernet0/39
 switchport access vlan 99
interface FastEthernet0/40
 switchport access vlan 99
interface FastEthernet0/41
 switchport access vlan 99
interface FastEthernet0/42
 switchport access vlan 99
interface FastEthernet0/43
 switchport access vlan 99
interface FastEthernet0/44
 switchport access vlan 99
interface FastEthernet0/45
 switchport access vlan 99
interface FastEthernet0/46
 switchport access vlan 99
 switchport mode access
interface FastEthernet0/47
 switchport access vlan 99
 switchport mode access
interface FastEthernet0/48
 switchport access vlan 99
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface GigabitEthernet0/3
interface GigabitEthernet0/4
interface Vlan1
 no ip address
ip classless
ip http server
ip http secure-server
ip sla enable reaction-alerts
line con 0
line vty 0 4
 login
line vty 5 15
 login
end
```

Routing Table for DoritosLocosTaco

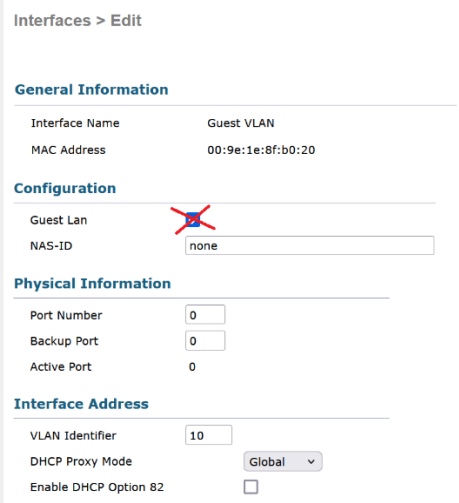
```
S*    0.0.0.0/0 [1/0] via 192.168.40.1
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
```

```
C        192.168.0.0/24 is directly connected, GigabitEthernet0/0/1.99
L        192.168.0.1/32 is directly connected, GigabitEthernet0/0/1.99
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected,
GigabitEthernet0/0/1.10
L        192.168.10.1/32 is directly connected,
GigabitEthernet0/0/1.10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected,
GigabitEthernet0/0/1.20
L        192.168.20.1/32 is directly connected,
GigabitEthernet0/0/1.20
      192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.30.0/24 is directly connected,
GigabitEthernet0/0/1.30
L        192.168.30.1/32 is directly connected,
GigabitEthernet0/0/1.30
C     192.168.40.0/23 is directly connected, GigabitEthernet0/0/0
      192.168.40.0/32 is subnetted, 1 subnets
L        192.168.40.110 is directly connected, GigabitEthernet0/0/0
```

Problems

Originally, our AP did not connect to the WLC, and we couldn't figure out why. It turns out that this was due to the time being set incorrectly on the WLC. The time is set to January 1, 2000 at 12:00AM by default, which prevents an HTTPS connection from being formed between the AP and the WLC as the AP's certificates are set to only work after a certain date. This problem is the reason that setting the time on the WLC is one of the first configuration steps we outline in this lab.

Originally, we checked the "Guest LAN" box for the Guest VLAN interface, assuming that this option was necessary. It turns out that the Guest Lan option is meant for guest authentication for wired clients, and will not work for a wireless guest network.



Conclusion

To wrap up, I am now much more confident in my skills setting up wireless networks, especially in their addressing and security settings. I also now understand RADIUS and its open-source implementations to a much greater extent, and am confident that I could replicate this setup in a real-world environment. This type of

network with three WLANs, one for guest use, personal use, and secure use, is especially useful in the real world, and is very similar to the WLAN configuration that our school district uses for tens of thousands of students and staff.

Fortinet Cybersecurity Academy: Configuring a FortiGate 40F Firewall for a SOHO Environment/Configuring a Fortinet 421E AP with WPA2-PSK and WPA2-Enterprise Local Auth

Colin J. Faletto, CCNA

FORTINET

Purpose

This lab is intended to introduce the Fortinet ecosystem, providing basic knowledge of the FortiGate firewall console and GUI interface. The lab also provides insight into the default configuration of a FortiGate firewall and how it can be used for a SOHO environment. In addition, the lab teaches how to set up a FortiAP access point, connect it to a FortiGate, and configure WLANs with a variety of different security options.

Background

SOHO, short for Small Office/Home Office, is a network type commonly used by individuals or small businesses with less than 10 employees. This network type commonly uses smaller-scale routers, switches, and firewalls compared to their large enterprise counterparts. SOHO networks provide numerous advantages to teams of 1-10 people as they are easier to set up and are more affordable than full-size network equipment. SOHO networks often only have a single router, and may contain switches, wireless access points, and end devices such as computers and printers.

Wi-Fi Protected Access, or WPA, is a security standard developed and maintained by the Wi-Fi alliance. There are three versions of WPA, being named WPA, WPA2, and WPA3 respectively. The first generation of WPA was released in 2003, with the second version releasing just a year later in 2004. In 2018, the third generation was released. WPA uses TKIP (Temporal Key Integrity Protocol) as its encryption method, while WPA2 uses CCMP (Counter-Mode/CBC-Mac Protocol) for encryption. WPA3 keeps support for CCMP but introduces GCMP (Galois/Counter Mode Protocol) as a stronger encryption method as well.

WPA can use two different methods of authentication: Personal and Enterprise. Personal authentication uses a pre-shared 256 bit key, meaning that all devices authenticate using the same password. Enterprise authentication uses a RADIUS (Remote Authentication Dial In User Service) server, meaning that each user authenticates using their own username and password.

Fortinet is a cybersecurity company founded in 2000 in Sunnyvale, CA. They are known for their flagship product, the FortiGate firewall, as well as a wide variety of other networking and security devices, such as the FortiSwitch and the FortiAP, and services such as FortiSandbox, FortiAuthenticator, FortiVoice, and FortiDDoS. Fortigate is an S&P 500 component and is listed on the NASDAQ as $FTNT.

The FortiGate 40-F is a firewall developed by Fortinet. It has capabilities expected of a modern firewall such as full routing capability, DHCP server capability, and support for a variety of filtering methods. **The 40-F also supports running its own local RADIUS server with a feature called Local Auth (Authentication).** The 40-F uses a fanless design, allowing it to operate silently. The 40-F has a small form factor at 1.5 x 8.5 x 6.3 inches, meaning it can easily fit into existing networking setups. By

default, the 40-F gives out DHCP addresses in the 192.168.1.0/24 subnet to its clients (from .110-.210, specifically) and its GUI client can be accessed via HTTPS at 192.168.1.99.

The FortiAP 421E is an access point developed by Fortinet. It has 8 internal antennae and 2 internal radios broadcasting on 2.4 GHz and 5 GHz respectively. It supports a variety of authentication methods, including WPA and WPA2 with either 802.1X or PSK, WEP, and a MAC blacklist/whitelist. It can form a mesh with other FortiAP devices to ensure more uniform connectivity across a site. The 421E can also handle a maximum of 512 clients per radio split across a maximum of 16 SSIDs.

Lab Summary

In this lab, we factory reset a FortiGate 40F firewall and upgraded it to version 7.4, which was the most recent mature version of FortiOS at the time, striking a balance between new features and stability. We configured basic settings and verified that essential firewall functions were working. We then connected a FortiAP 421E and set up two WLANs, running WPA2-Personal with PSK and WPA2-Enterprise with Local Authentication respectively.

Lab Commands

Cable all lab devices according to the topology.

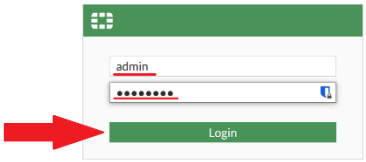
Turn on your firewall and wait for the login screen to show. Within 60 seconds, press the reset button next to the firewall's power connector. You will see a message like this:

```
AadiAndKevin login:
System is resetting to factory default...
```

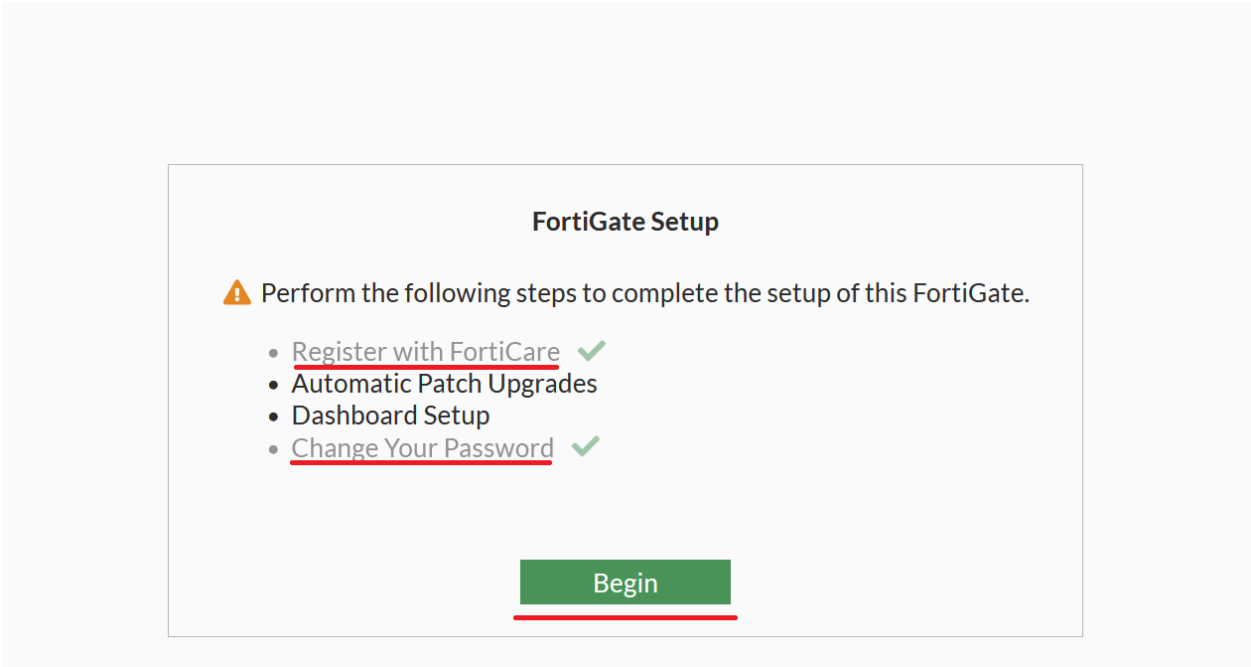
You should see the prompt `Fortigate-40F login:` Type in the username `admin` with no password. Change your password when prompted.

```
FortiGate-40F login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome!

FortiGate-40F #
```

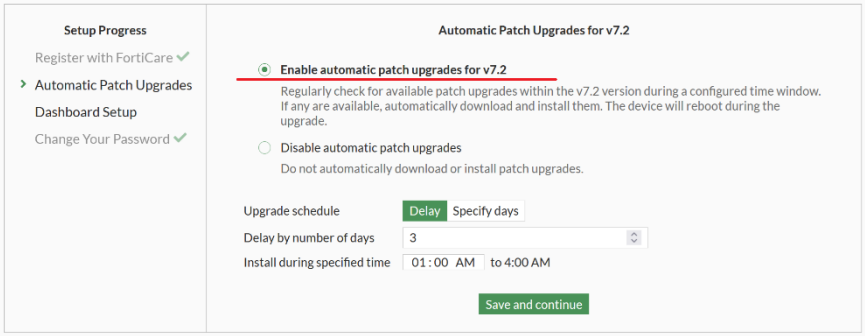
Connect your PC to the firewall via ethernet. Go to https://192.168.1.99 and log in with the username and password you set.



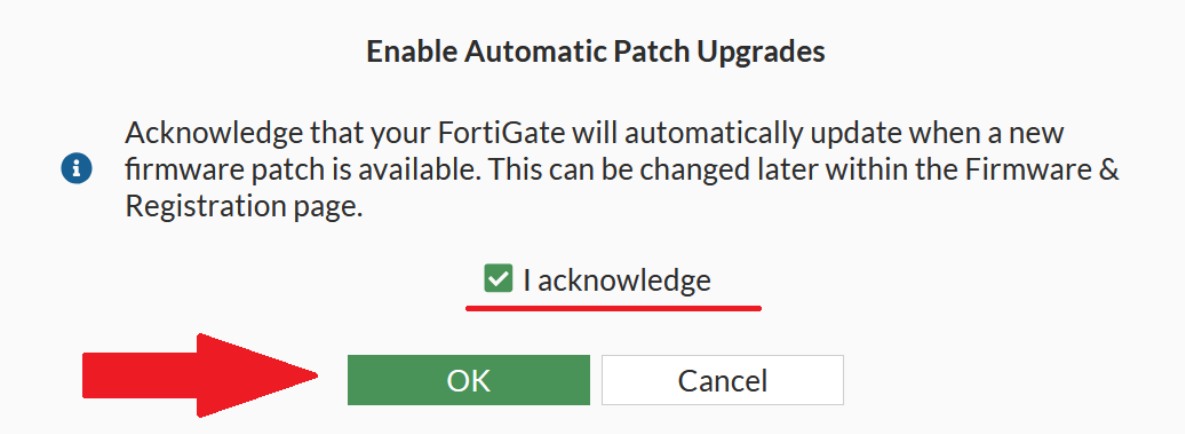
You should see the following setup screen. Note that the Change Your Password checklist item has already been completed, as we completed this earlier. (Also, the firewall used in this lab had already been registered to my cybersecurity academy, so the Register with Forticare item is also checked off.) Click Begin.



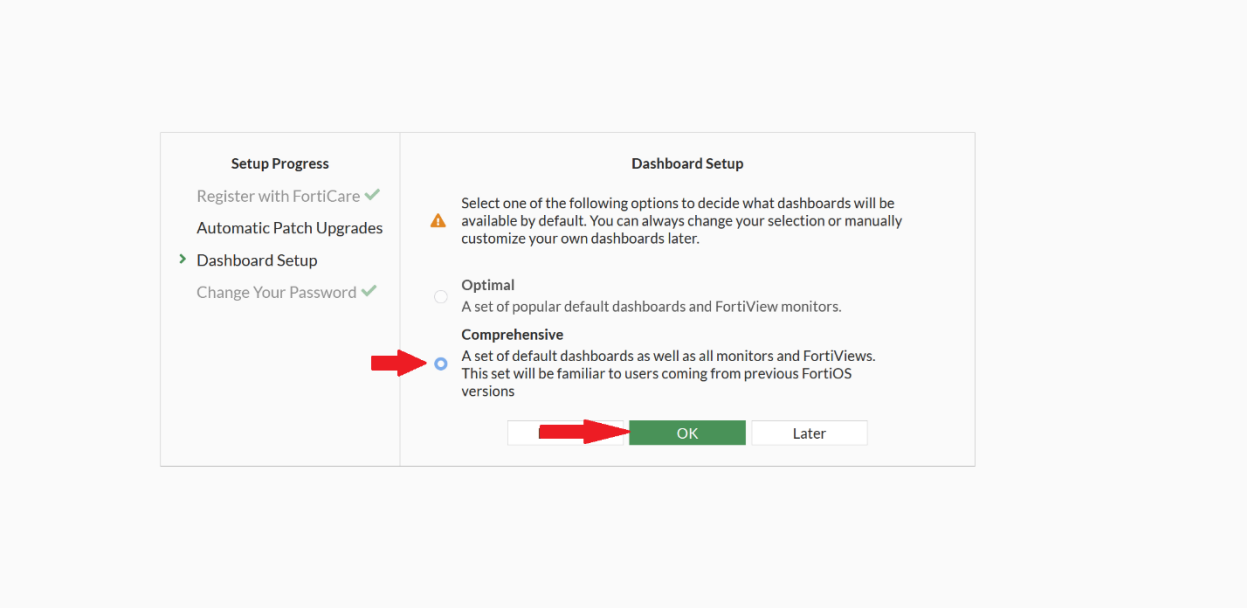
Click Enable Automatic Patch Upgrades and leave the other settings as default.



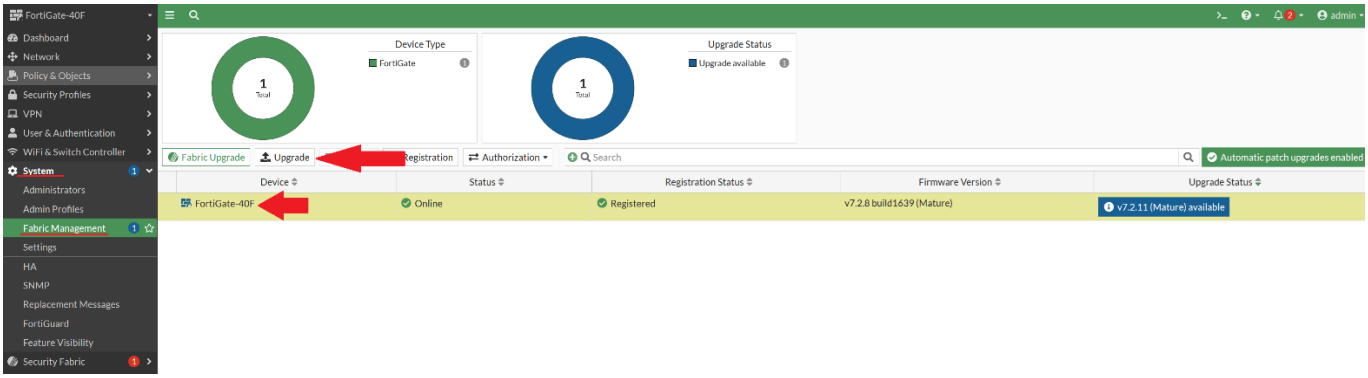
Click I acknowledge and click OK.



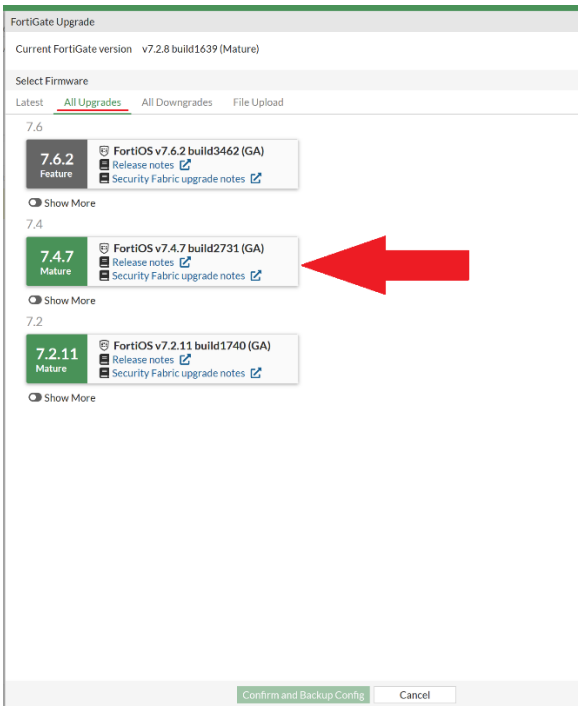
Choose the comprehensive dashboard and click OK.



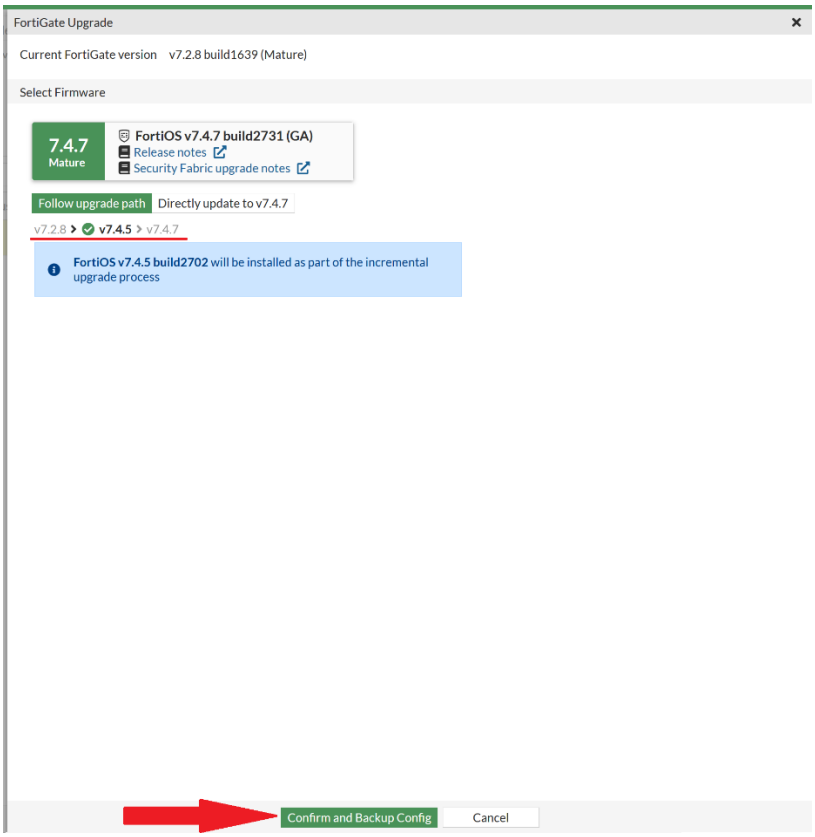
You should now see the main fortigate dashboard page. Next, we will update the system firmware. Click on System > Fabric Management (may be called Firmware and Registration in newer versions), click on the Fortigate 40F, then click Upgrade.



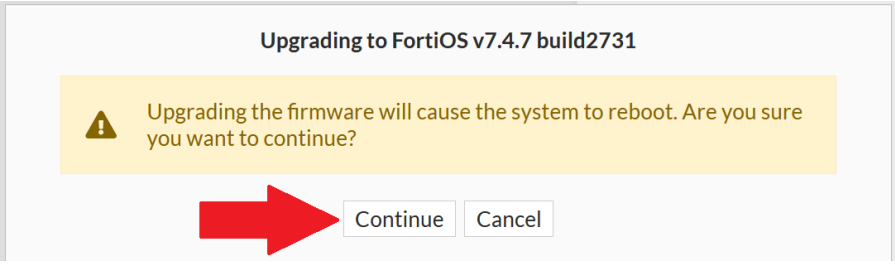
Click All Upgrades, then select the version you would like to upgrade to. In this lab, we opted to update to the latest version of FortiOS 7.4, as at the time, it was the latest version with a focus on bugfixes and stability (7.6 focused on feature updates, and wasn't as stable)



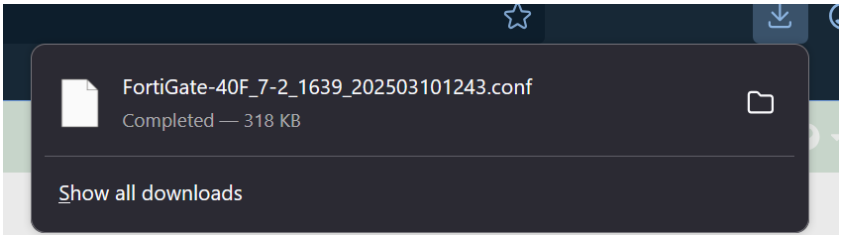
Click Confirm and Backup Config. Note that in most cases, multiple different versions of FortiOS will be installed as part of an incremental upgrade process. While there is an option to directly update between versions, following an upgrade path can decrease the chances of corrupting your configuration.



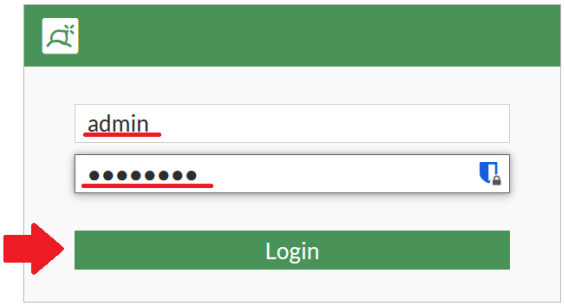
Click Continue, and wait for the upgrade process to complete.



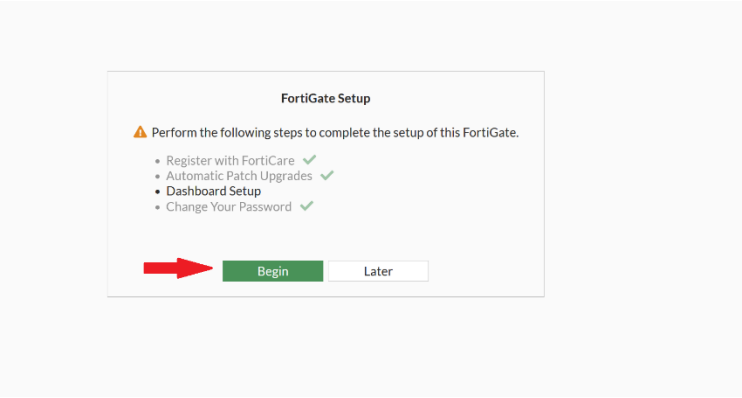
Note that a backup configuration file will be downloaded locally.

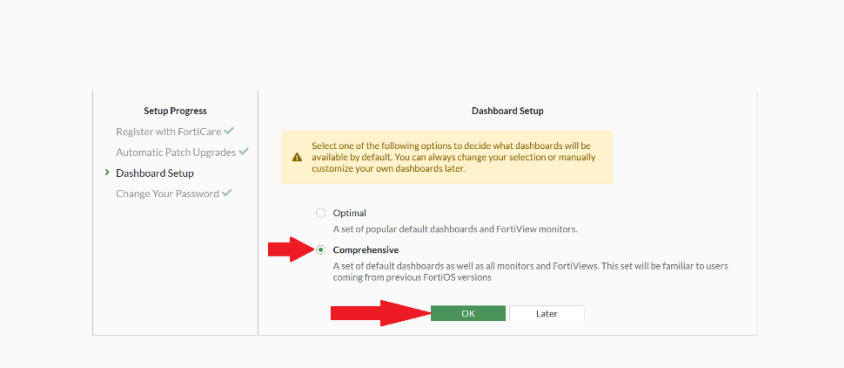


When the upgrade process is complete, reload the page and log in again.

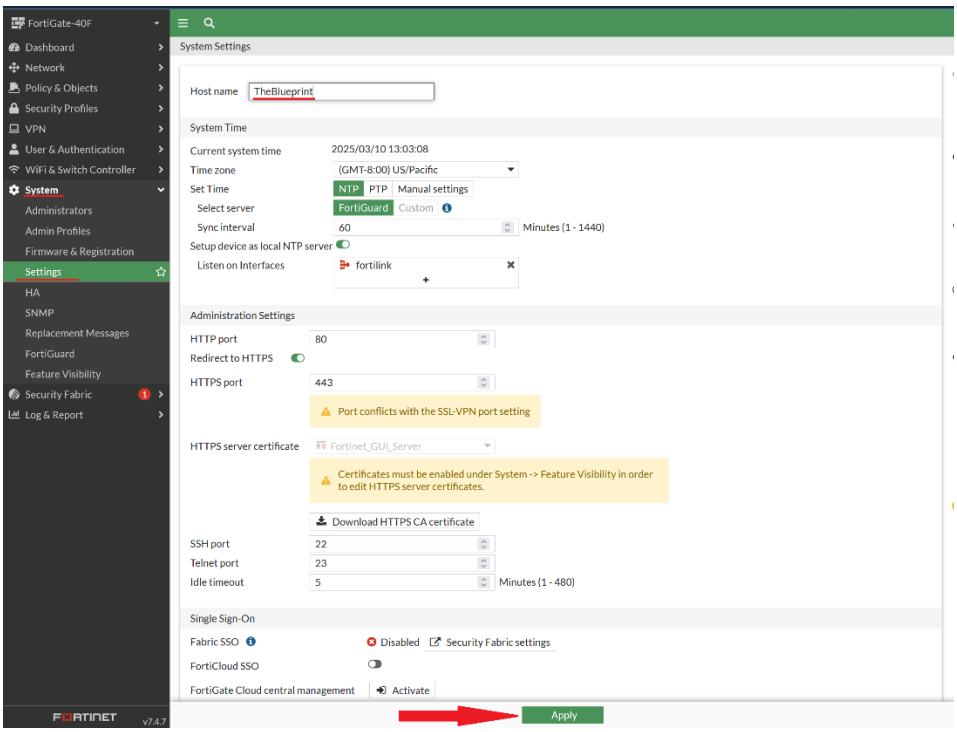


You may be asked to complete dashboard setup again. In this case, choose the Comprehensive dashboard like before.

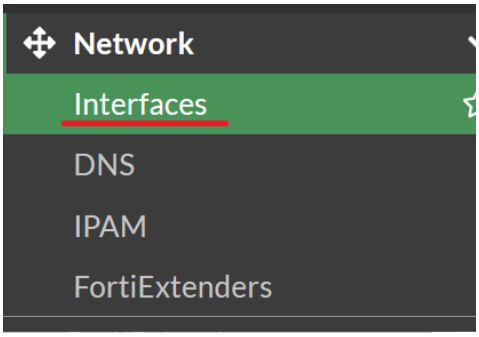




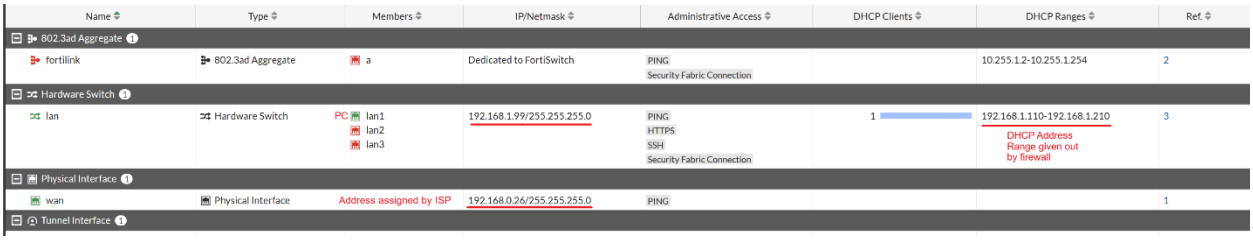
You should now see the firewall's dashboard. Next, we will configure a hostname for the firewall. Go to System > Settings, enter a host name, and click Apply.



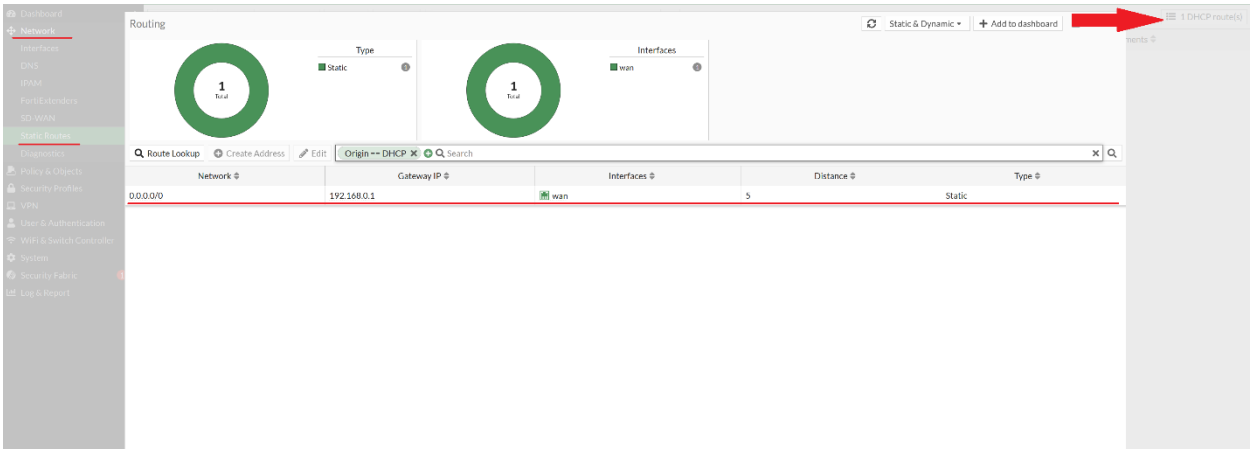
We will now verify the firewall's basic configuration. Go to Network > Interfaces.



You should see that the LAN interface is configured to give out addresses on the 192.168.1.0/24 network, with one device (your PC) connected. You should also see that the WAN interface has an IP given out by your ISP.



Next, click on Network > Static Routes and click on DHCP routes. You should see that a default route out the WAN interface has automatically been configured.



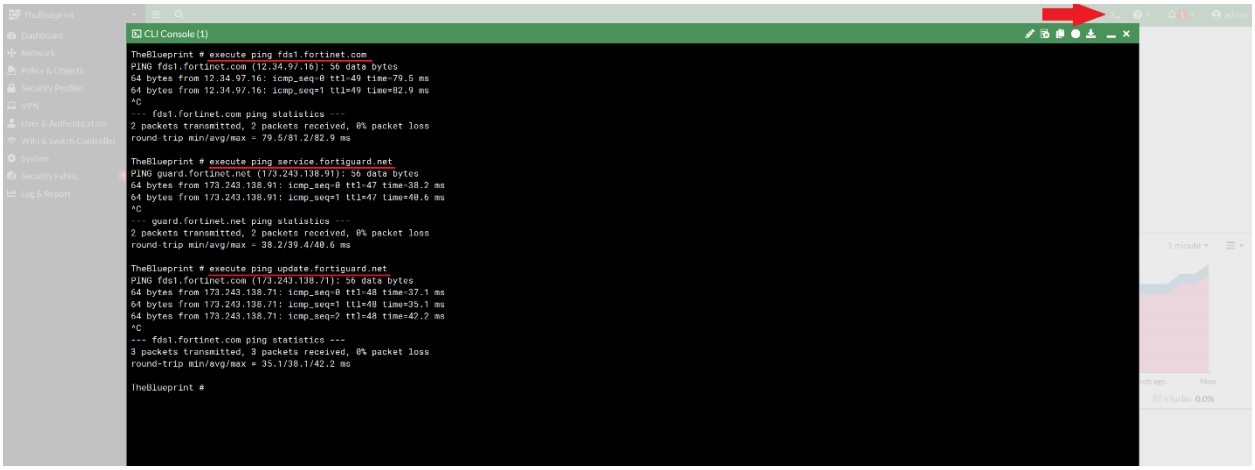
Click the CLI Console icon in the top right corner and run the following commands:

```
execute ping fds1.fortinet.com
```

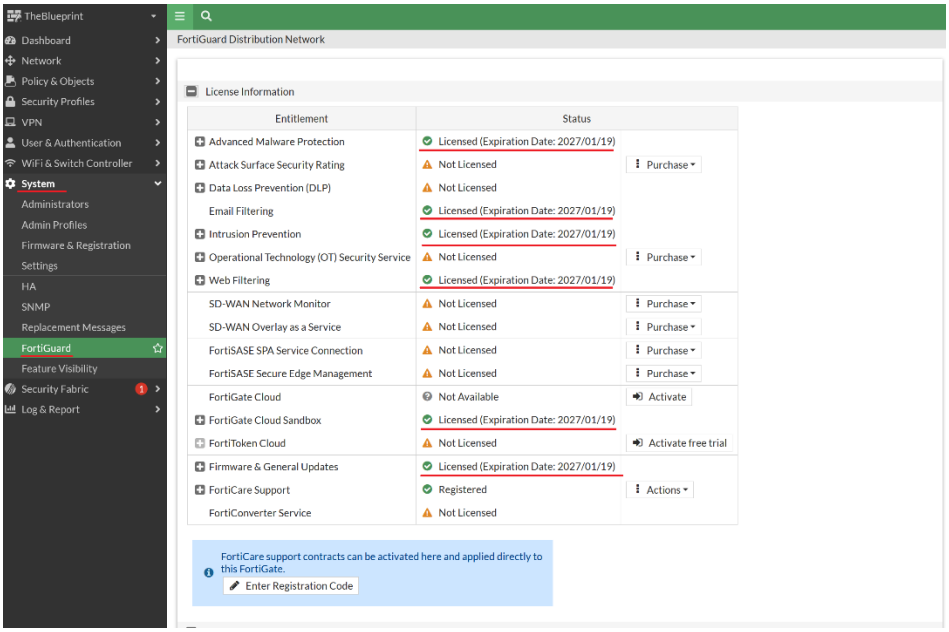
```
execute ping service.fortiguard.net
```

```
execute ping update.fortiguard.net
```

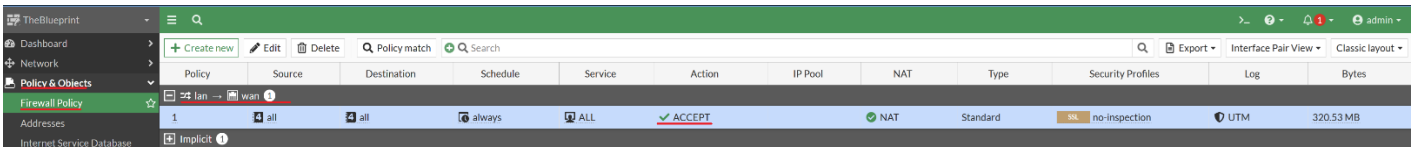
Ensure that you receive a response from each of these servers.



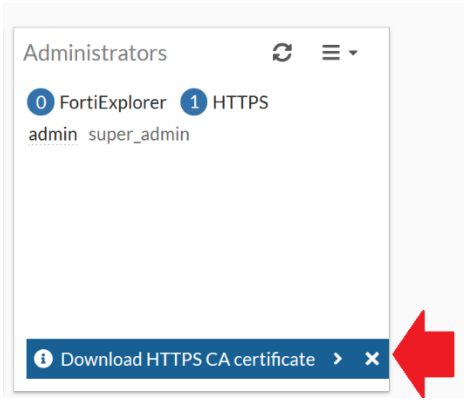
Next, go to System > FortiGuard and ensure your firewall has licenses for essential firewall functions, such as Email filtering, Web filtering, and Firmware updates.



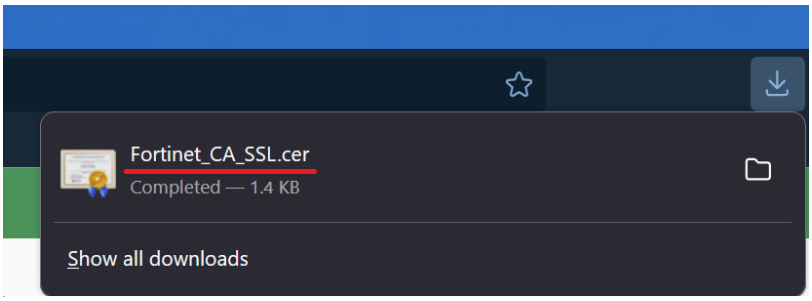
Next, go to Policy & Objects > Firewall Policy and ensure there is a policy allowing traffic between the LAN and WAN interfactes.



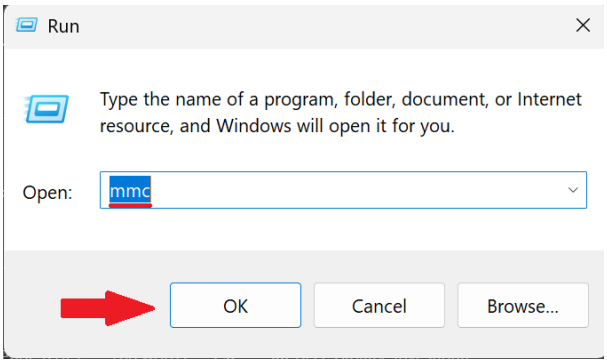
Return to the dashboard page, and under Administrators, click Download HTTPS CA certificate.



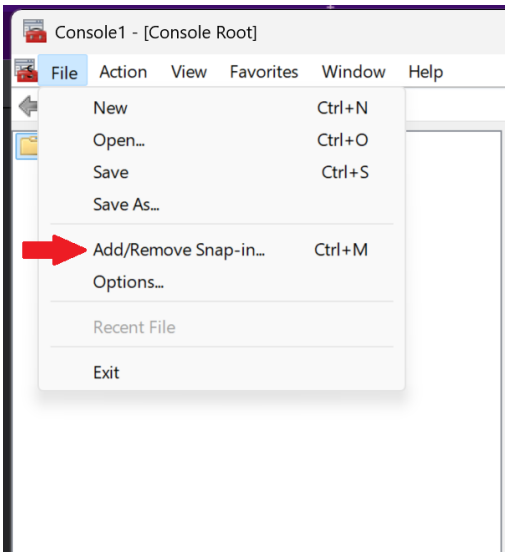
You should see a certificate file download to your PC.



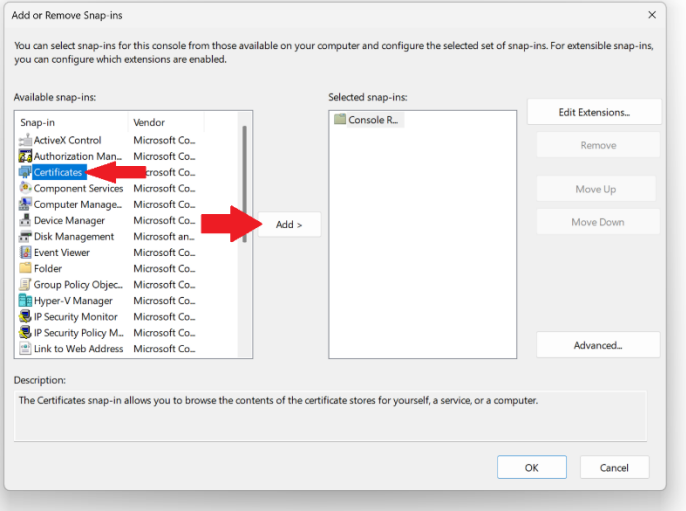
Next, we will install this certificate. On your PC, open the Run dialog (Windows+R) and type “mmc”.



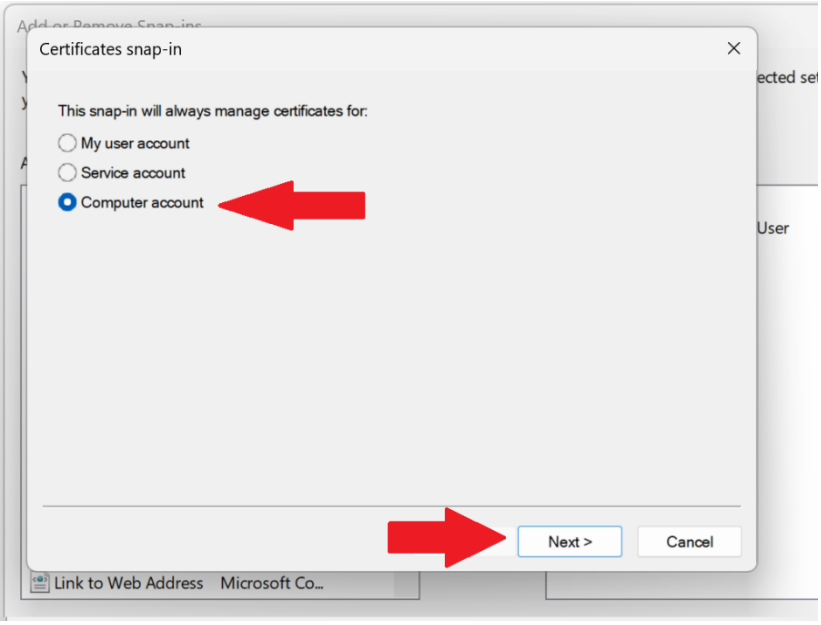
In the resulting window, click File > Add/Remove Snap-in.



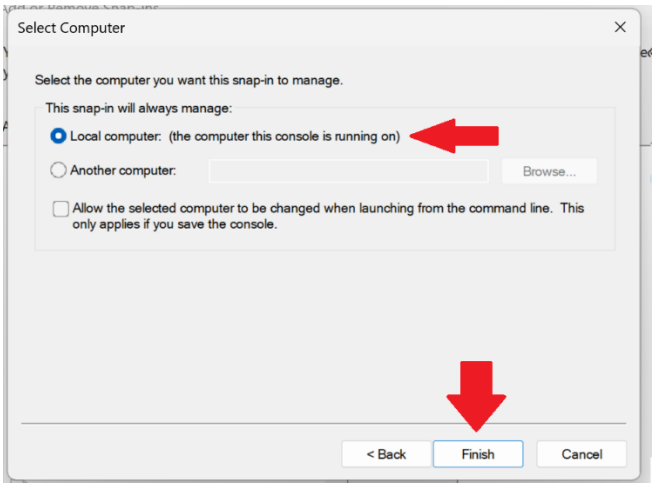
In the resulting window, click on Certificates > Add.



In the resulting window, click on Computer Account > Next.

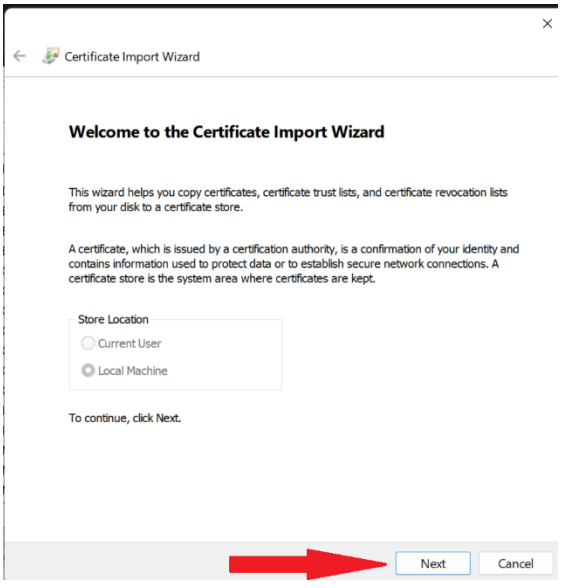


Make sure Local Computer is selected and click Finish.

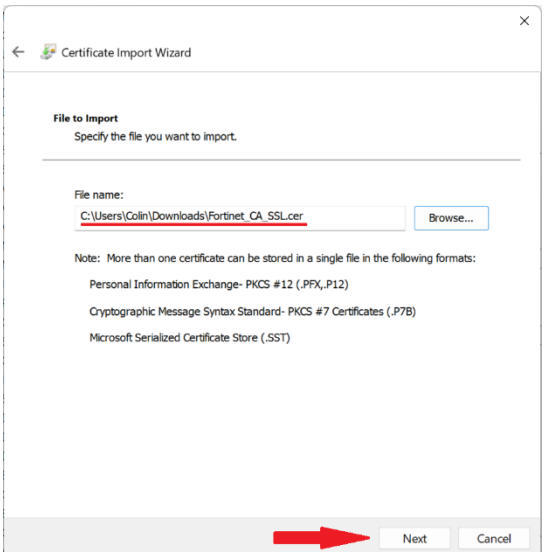


Inside Trusted Root Certification Authorities, right-click on Certificates and click on All Tasks > Import.

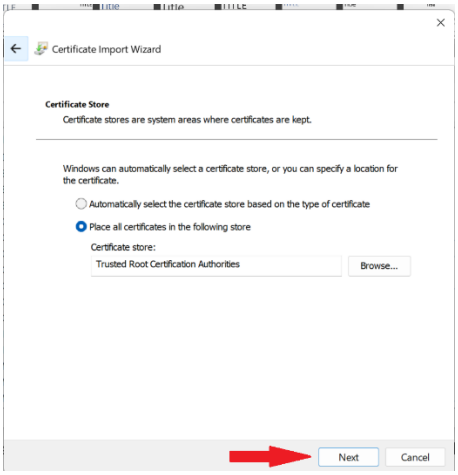
Click “Next”.



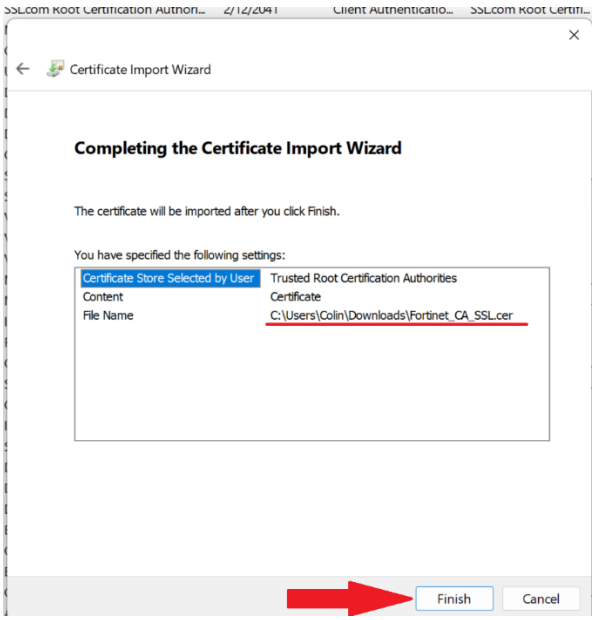
Select the certificate file downloaded earlier, then click “Next” again.



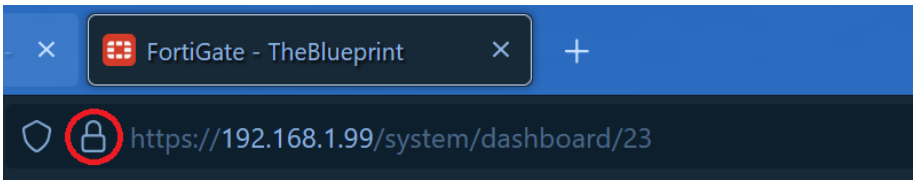
Leave the certificate store location setting as the default value, then click “Next”.



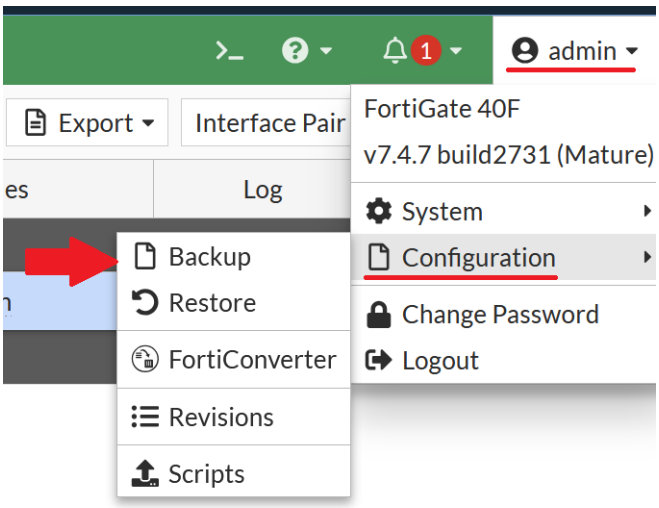
Click “Finish” to confirm the certificate import.



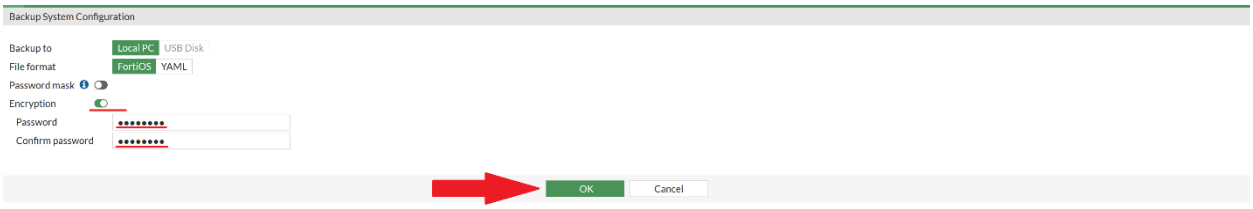
Close and reopen your browser, and ensure that the HTTPS lock icon appears when opening the firewall's management page.



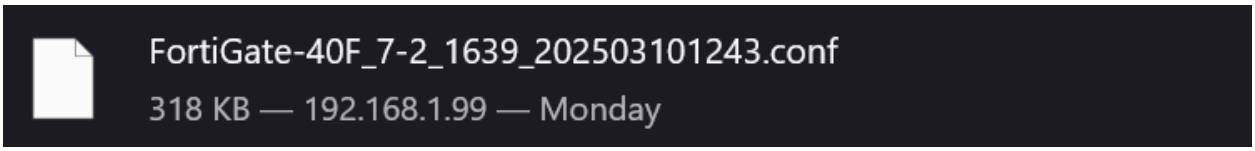
Next, we will back up the firewall's configuration. Click on the admin profile picture in the top right, then click on Configuration > Backup.



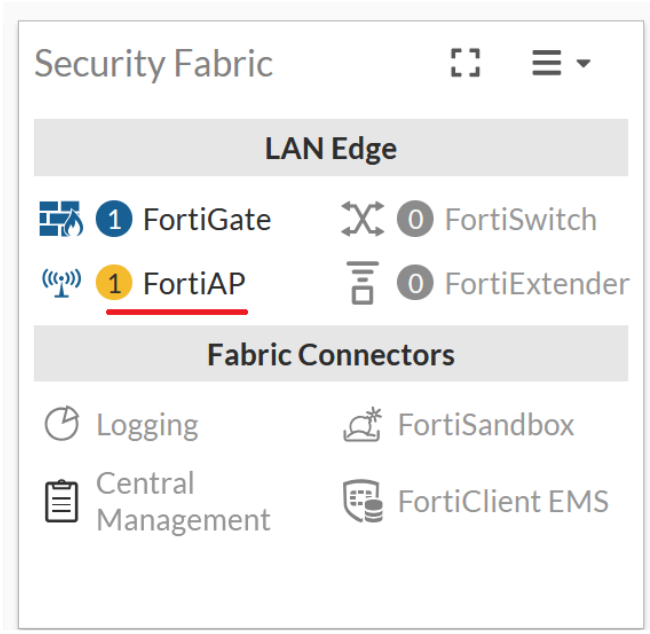
Enable Encryption and enter a secure password for the backup. Click OK.



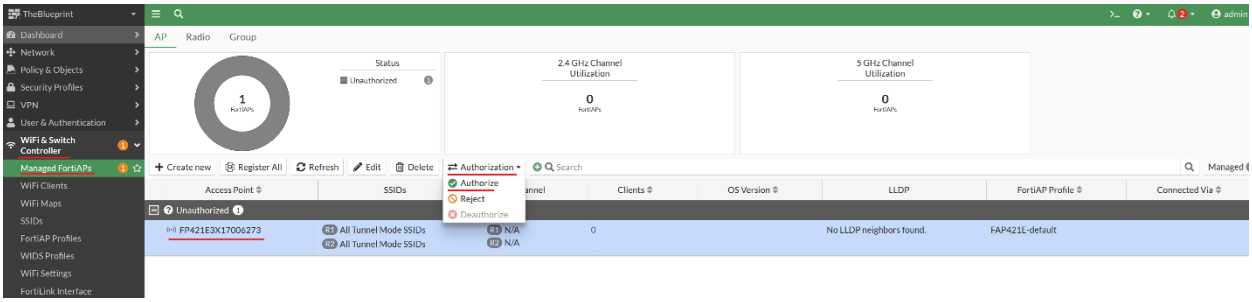
The backup file will be downloaded to your PC.



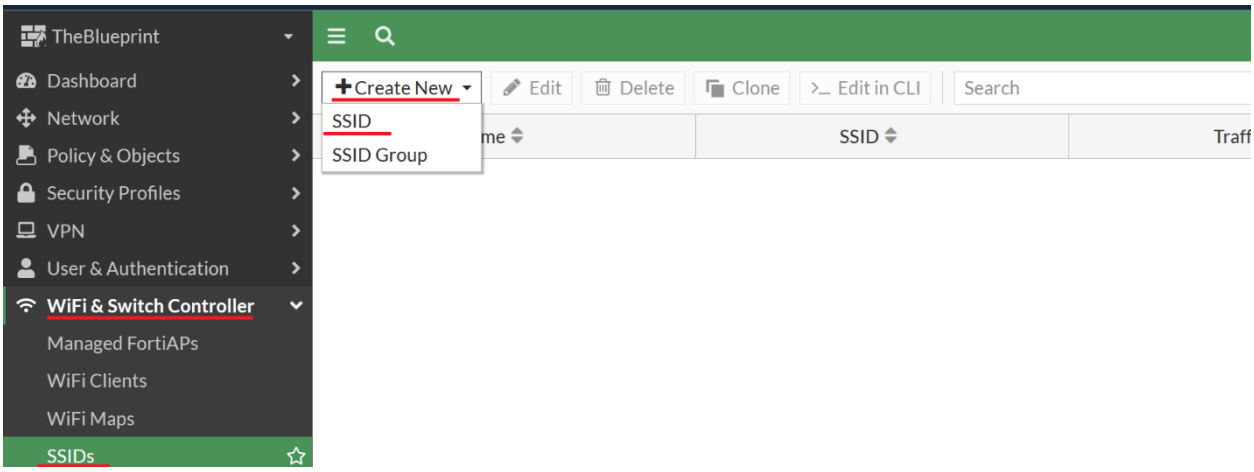
Next, we will set up the AP. Return to the Dashboard, and under Security Fabric, ensure that one (1) FortiAP device is visible.



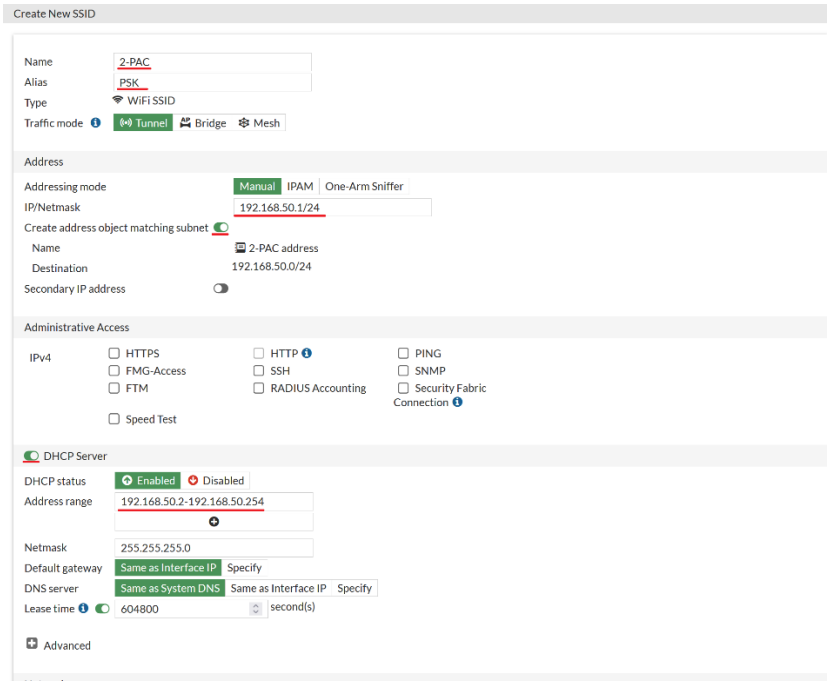
Go to WiFi & Switch Controller > Managed FortiAPs, click on the unauthorized AP, and click Authorization > Authorize.



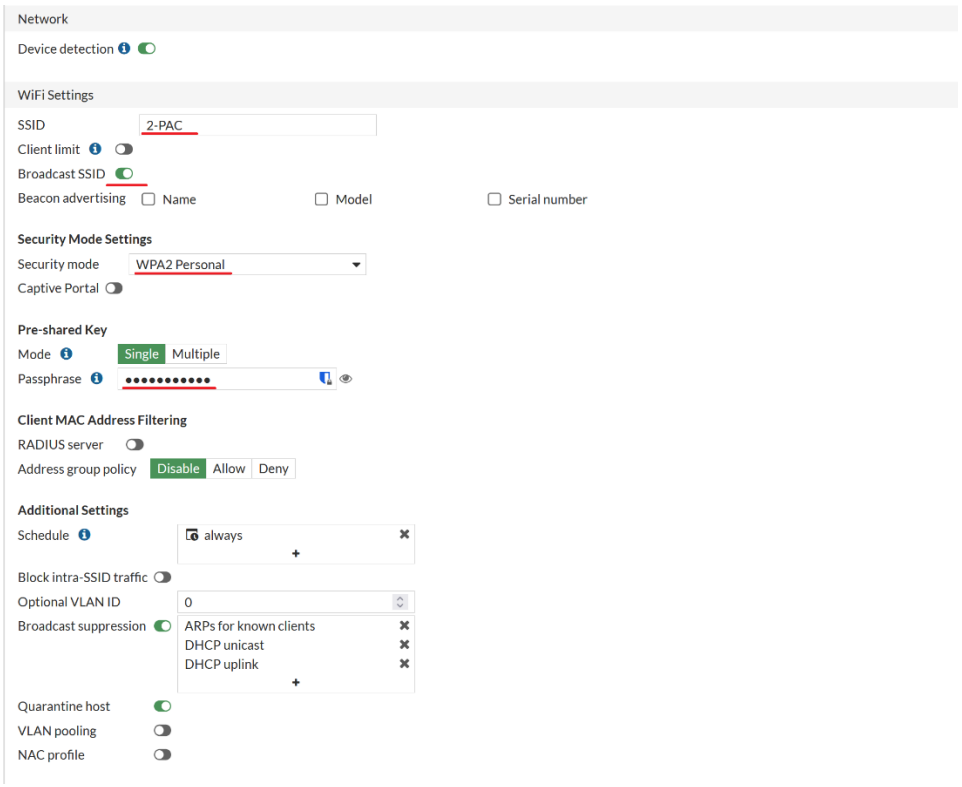
Next, we will set up the WPA2-PSK SSID. Go to WiFi & Switch Controller > SSIDs, and click Create New > SSID.



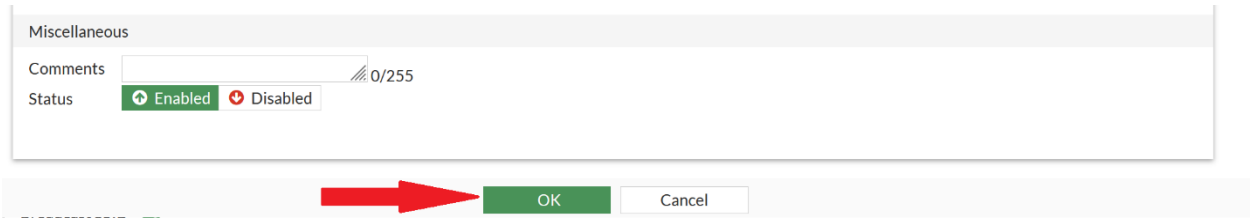
Configure an appropriate name (in this case, we called it 2-PAC) and alias. Give the SSID an appropriate IP and netmask, and ensure that an address object matching the subnet is created. Ensure that the DHCP server option is enabled. The DHCP server settings should automatically match the network settings configured in the Address section.



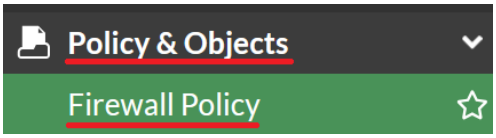
Set the SSID to the same as the name, ensure that the SSID is being broadcasted, set the security mode to WPA2 Personal, and configure an appropriate passphrase.



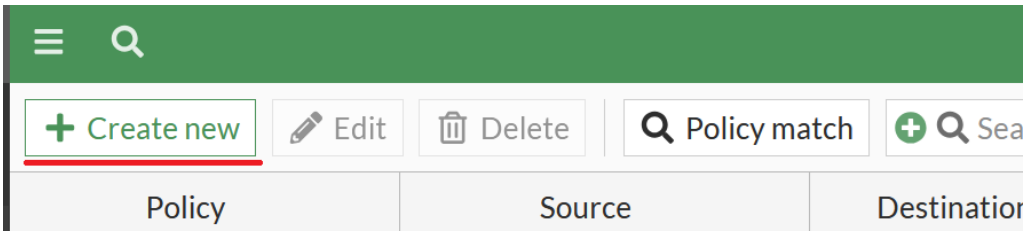
Click OK.



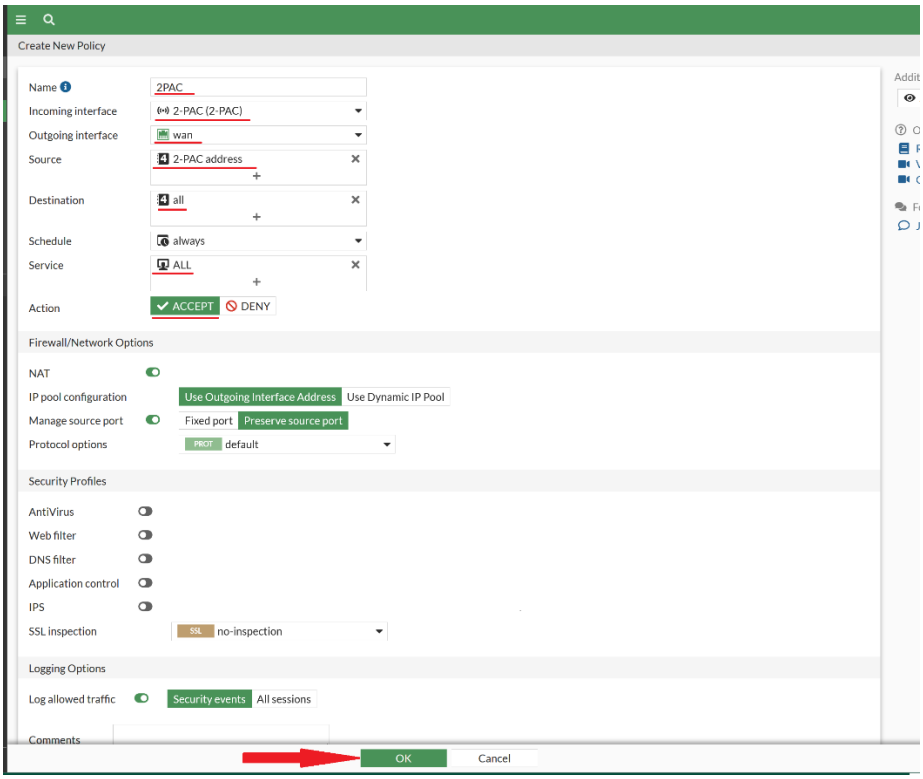
Go to Policy & Objects > Firewall Policy.



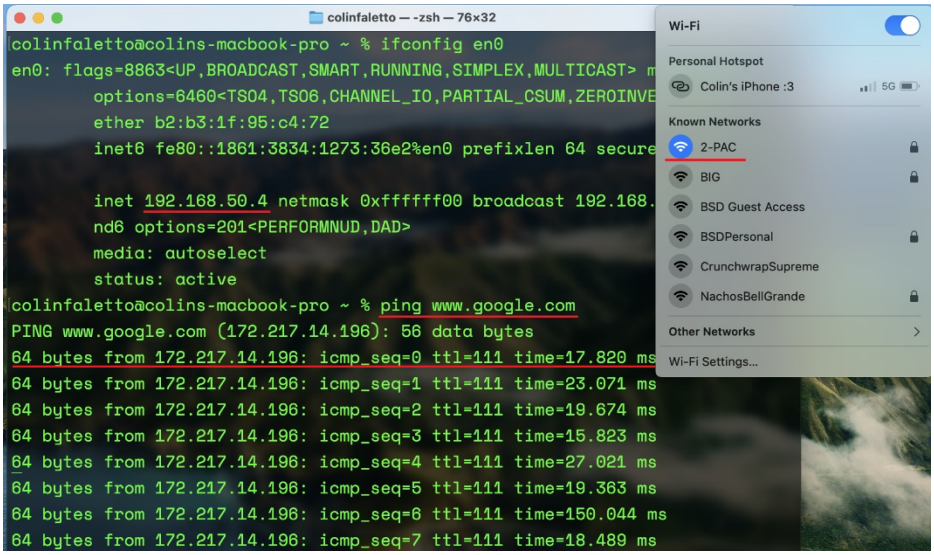
Click Create new.



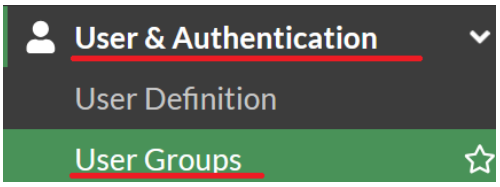
Configure an appropriate name. Set the incoming/outgoing interface to the PSK WLAN and the WAN respectively. Set the source and destination to the PSK address object and “all” respectively. Set the action to Accept and click OK.



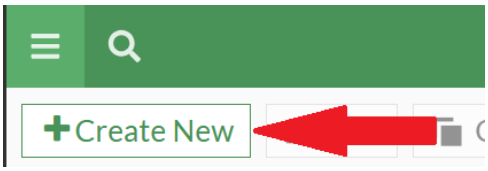
Your PSK WLAN should now be fully set up. Confirm that it works by connecting another device, inputting the password configured earlier. As seen in the screenshot below, when connected to the 2-PAC network, my laptop recieves an address in the 192.168.50.0/24 network, and can successfully ping outside of the network.



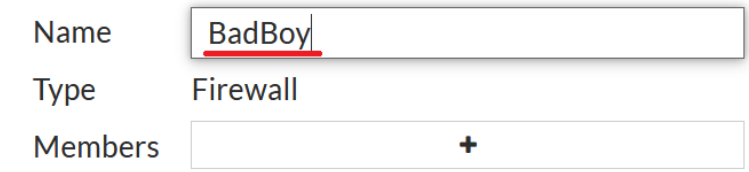
Next, you will configure Local User authentication for the WPA2 Enterprise WLAN. Go to User & Authentication > User Groups.



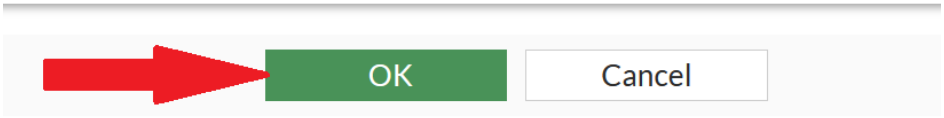
Click Create New.



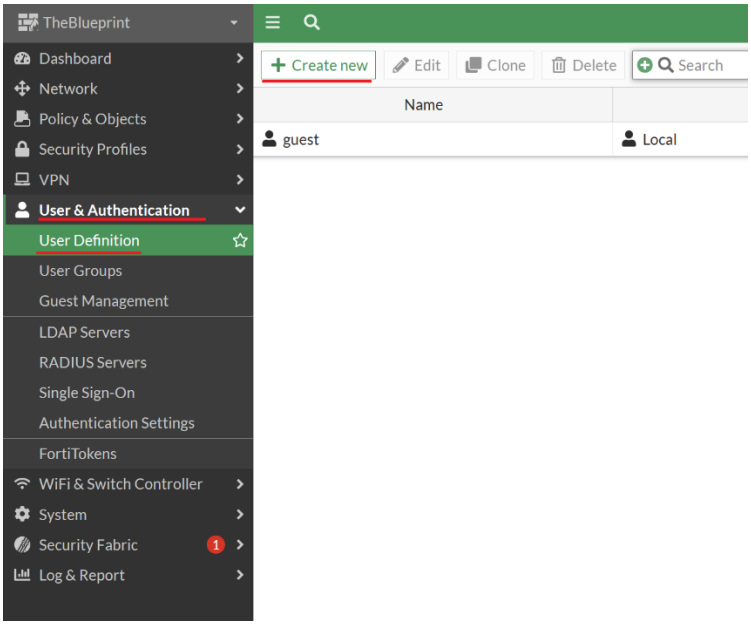
Choose an appropriate group name.



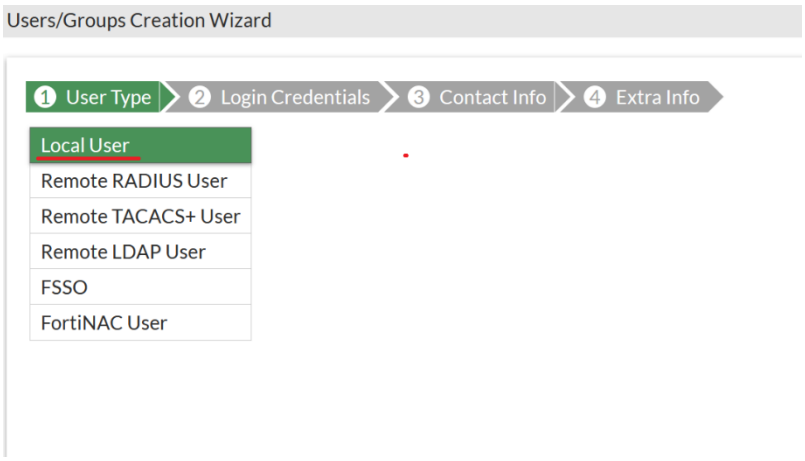
Click OK.



Go to User & Authentication > User Definition and click Create new.

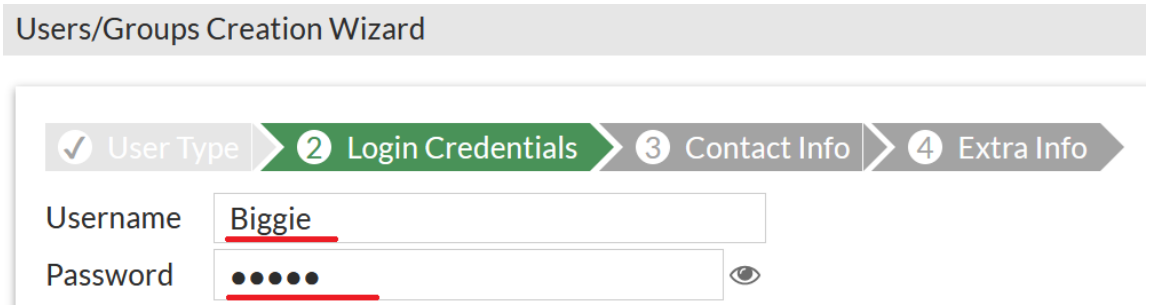


Set the User Type to Local User.



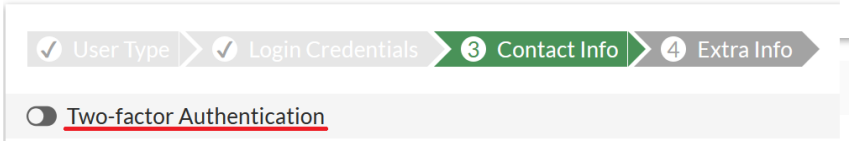
Click Next.

Set an appropriate username and password.



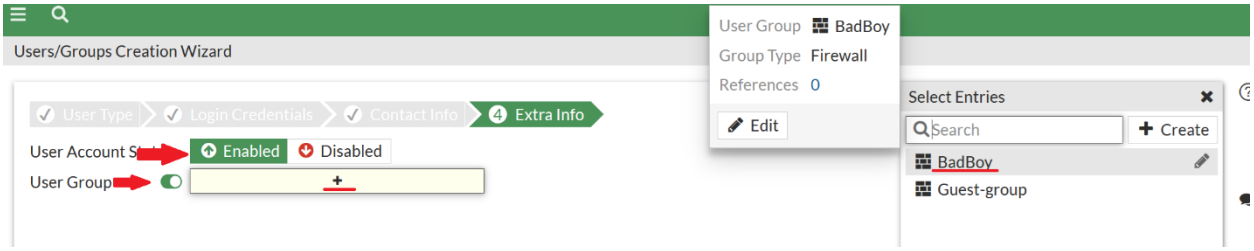
Click Next.

Under Contact Info, leave two-factor authentication off.

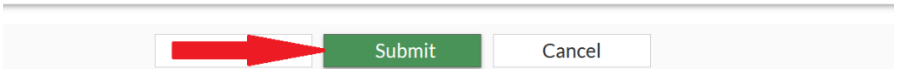


Click Next.

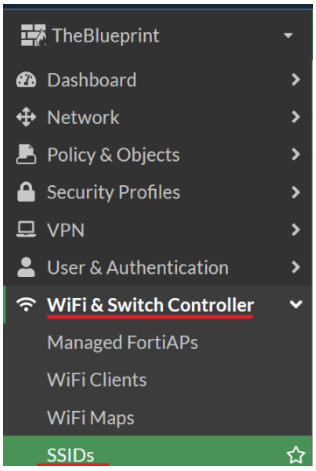
Set the User Account Status to Enabled, enable User Group, click the plus icon, and select the User Group created earlier.

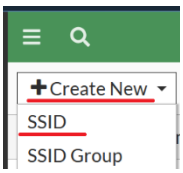


Click Submit.

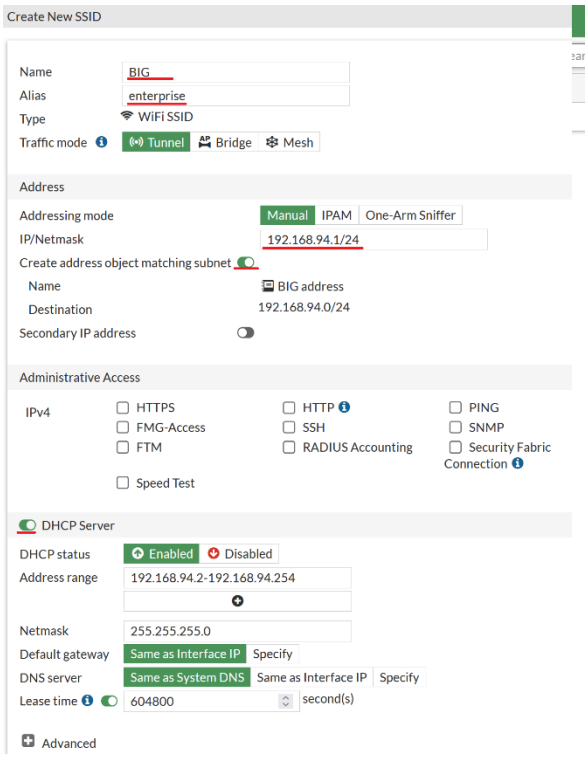


Next, we will set up the WPA2-Enterprise SSID. Go to WiFi & Switch Controller > SSIDs and click Create New > SSID.

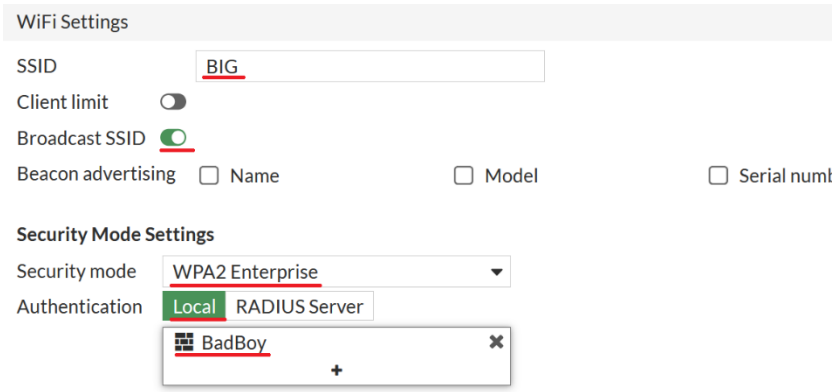




Assign an appropriate name (in this case, we chose BIG) and alias. Assign an appropriate IP/netmask, and ensure that an address object is created matching the subnet. Ensure that a DHCP server for the subnet is created.

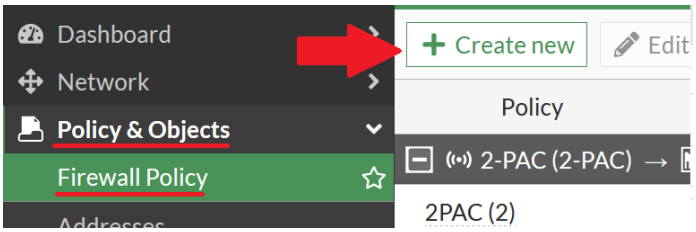


Set the SSID to the same as the name, ensure the SSID is broadcast, set the security mode to WPA2 Enterprise, set the authentication to Local, and add the user group created earlier.

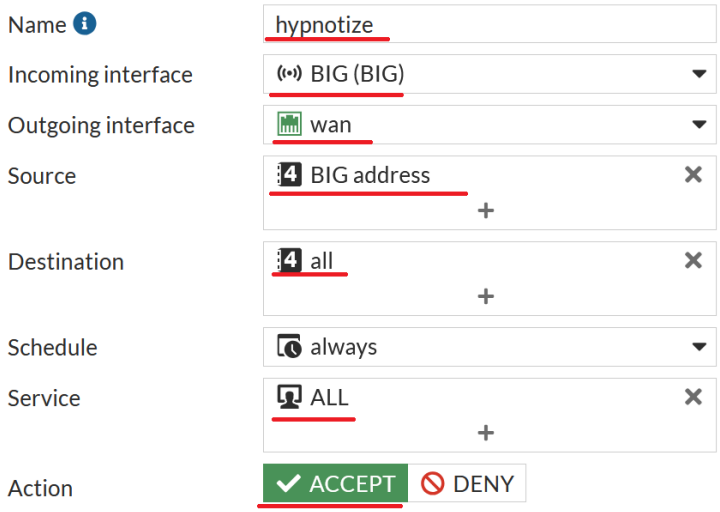


Click OK.

Next, we will configure a firewall policy to allow traffic from the Enterprise WLAN to reach the WAN.

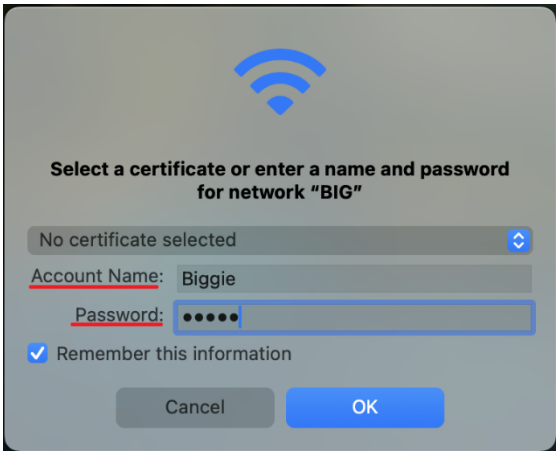


Configure an appropriate name. Set the incoming/outgoing interface to the Enterprise WLAN/WAN interfaces respectively. Set the source/destination to the address object for the WLAN and “all” respectively. Set the service to ALL and the action to ACCEPT.



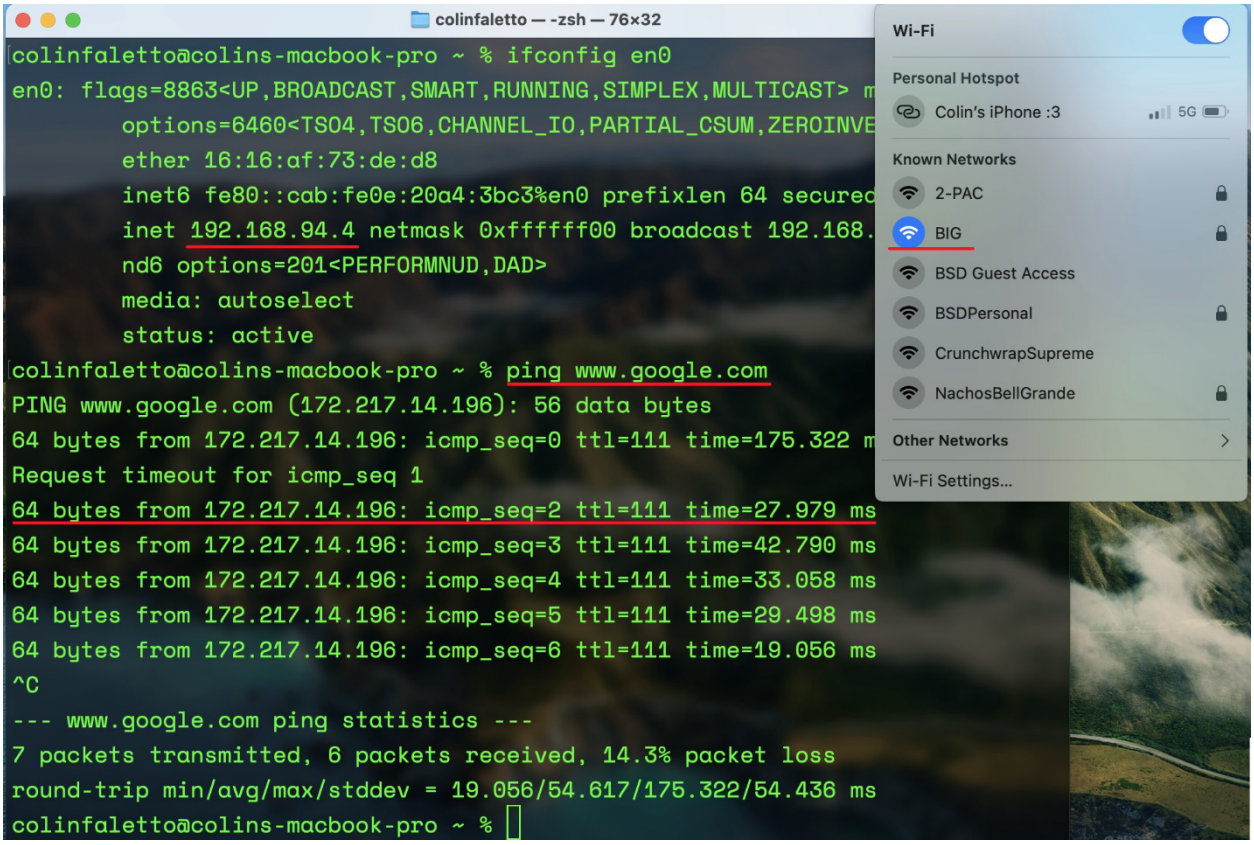
Click OK.

Your Enterprise WLAN has now been set up. To test it, connect from another WiFi-capable device. You should see a login prompt similar to this:

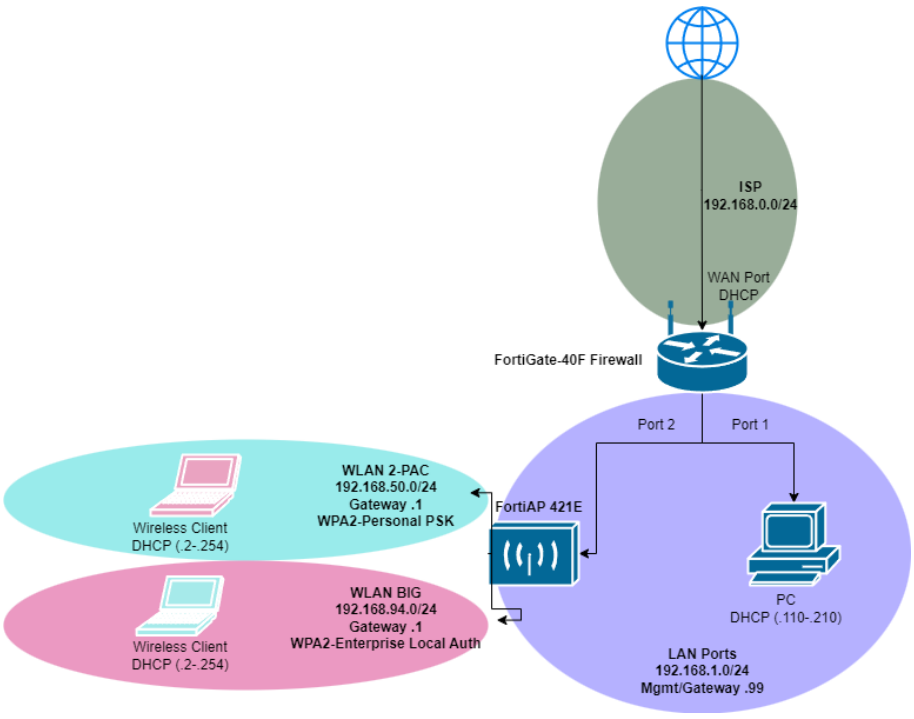


Enter the username and password configured for the local user, then connect. Ensure that you trust the firewall’s certificate when connecting. As seen in the screenshot

below, when connected to the BIG network, my laptop recieves an address in the 192.168.94.0/24 subnet and can successfully ping outside the network.



Network Diagram (IPv4)



Problems

We found that the FortiAP cannot be plugged directly into the FortiGate without a separate power source, as the FortiGate does not provide power over ethernet. We fixed this by placing a standard 48V PoE injector in between the firewall and the access point.

Conclusion

To wrap up, I now have a strong understanding of the basic Fortinet ecosystem, the FortiOS GUI interface, and various WPA2 security policies. I am now confident that I could replicate this setup in a real SOHO environment.