Linux Academy

Hands-on Lab

Building a VPC from Scratch

Contents

Lab Connection Information

- Labs may take up to five minutes to build
- Access to an AWS Console is provided on the Live! Lab page, along with your login credentials
- Ensure you are using the N. Virginia region
- Labs will automatically end once the alloted amount of time finishes

Related Courses

AWS CSA - Associate

Related Videos

Introduction to VPC and AWS Networking

Building a VPC from Scratch

VPC Networking

VPC Security

Need Help?

Linux Academy Community

... and you can always send in a support ticket on our website to talk to an instructor!

In this lab, we will be creating a virtual private cloud (VPC) containing an Internet Gateway, two route tables, and four subnets across two Availability Zones; additionally, we will define an Access Control List (ACL) and a security group for any instances added to the VPC.

Create the VPC

Navigate to the **VPC Dashboard**. Since we are creating this VPC "from scratch" we are *not* using the VPC wizard provided by AWS. Instead, click on **Your VPCs** on the left menu. **Create VPC**.

First, give the VPC a **Name tag**. We used *LabVPC*. We also need to define a CIDR block range for the VPC to use; set **IPv4 CIDR block** to *10.0.0.0/16*. More information on CIDR block ranges can be found in the *Guide to Subnetting* in the Downloads section of this course.

AWS also allows us to enable IPv6 CIDR block ranges; leave this at the default (*No IPv6 CIDR Block*). Set the **Tenancy** to *default*; tenancy determines whether your VPC shares resources with other AWS users. Setting dedicated tenancy will increase the cost of running your VPC. Press **Yes, Create**.

Internet Gateway and Route Tables

Click on **Internet Gateways** on the left menu. **Create Internet Gateway**. We gave ours a **Name tag** of *LabIGW*. **Create**. Notice that the gateway is current not attached to a VPC. Press **Attach to VPC** at the top of the screen, and select *LabVPC* from the list. **Yes, Attach**.

Next, we need to configure our two routing tables. We want one to point to the Internet Gateway, while the other remains private. Click **Route Tables** from the left menu.

Press **Create Route Table**. We gave ours a **Name tag** of *LabRT-Public* with the intention of this being the route table pointing to our Internet Gateway. Ensure the **VPC** selected is the *LabVPC*. **Yes, Create**.

Press **Create Route Table** again. We named the second route table *LabRT-Private*. Ensure the **VPC** is set to *LabVPC* and press **Yes, Create**.

Select *LabRT-Public* and click the **Routes** tab on the table below. We want to point our route table to the Internet Gateway. Press **Edit**, **Add another route**. Set the **Destination** to *0.0.0.0/0* and the **Target** to the *LabIGW* gateway. **Save**.

Subnets

We want four different subnets – two public and two private across two Availability Zones.

While still in the VPC Dashboard, select **Subnets** from the left menu. **Create Subnet**. Set the **Name tag** to *LabSubnet1-Public* – this is our first public subnet. Ensure the appropriate VPC is selected and set the **Availabity Zone** to *us-east-1a*. Set the **IPv4 CIDR block** to *10.0.1.0/24*. **Yes, Create**.

Create the second public subnet, *LabSubnet2-Public*, in the *us-east-1b* Availability Zone with a CIDR block of *10.0.2.0/24*.

Create the third subnet, *LabSubnet3-Private*, in the *us-east-1a* Availability Zone with a CIDR block of *10.0.3.0/24*.

Create the fourth subnet, *LabSubnet4-Private*, in the *us-east-1b* Availability Zone with a CIDR block of *10.0.4.0/24*.

We now need to associate our subnets with the correct route tables. Return to the **Route Tables** page, and select the public route table. Click on the **Subnet Associations** tab below. **Edit**. Select both subnets labeled *public* and **Save**. Select the private route table and repeat the process, this time adding both *private* subnets to the associated subnets.

Security Layers

With our VPC set up, we want to define two network access control lists and configure two security groups to use within our VPC.

Network Access Control Lists

Click on **Network ACLs** on the left menu. **Create Network ACL**. We gave ours the **Name tag** of *LabNACL1* and set the **VPC** to the *LabVPC*. **Yes, Create**. Repeat this process for a network ACL with the name of *LabNACL2*.

We want out first NACL to have both inbound and outbound rules for HTTP and SSH. Select *LabNACL1* and click on the **Inbound Rules** tab below. Press **Edit**. **Add another rule**. Set the **Rule #** to *100* and the **Type** to *SSH (22)*. Set the **Source** to *0.0.0.0/0* to allow all sources to use SSH. **Add another rule**. Set the **Rule #** to *110* and the **Type** to *HTTP (80)*, with a **Source** of *0.0.0.0/0*. **Save**.

Click **Outbound Rules**. **Edit**. Use the same settings as above for the outbound rules.

The NACL is still not associated with any subnets, however. Select the **Subnet Associations** tab and press **Edit**. Select *LabSubnet1-Public* and *LabSubnet3-Private* (both us-east-1a subnets) and **Save**.

Select *LabNACL2*. For this NACL, we want to allow RDP rules and ensure we can access any EC2 instanced with SSH and HTTP. Select **Inbound Rules** and set the SSH and HTTP rules as before, using the same rule numbers. Add a third rule with a **Rule #** of *120*, a **Type** of *RDP (3389)*, and a **Source** of *0.0.0.0/0*. **Save**. Repeat this process for the **Outbound Rules**.

Select **Subnet Associations**. **Edit**. Choose the *LabSubnet2-Public* and *LabSubnet4-Private* (us-east-1b) subnets. **Save**.

Security Groups

While we can create the security groups right now, we cannot attach them until any instances are provisioned.

Press **Security Groups** on the left menu. **Create Security Group**. We gave ours a **Name tag**, **Group name**, and **Description** of *LabSG-EC2*. Ensure the **VPC** is the *LabVPC*. **Yes, Create**.

Press **Create Security Group** again, this time giving it a **Name tag**, **Group name**, and **Description** of *LabSG-RDS*. Ensure the correct VPC is selected. **Yes, Create**.

Select the *LabSG-RDS* group and click **Inbound Rules**. As with NACLs, we need to set up any inbound and outbound rules. Press **Edit**. For **Type**, select *RDP (3389)*, and set the **Source** to *0.0.0.0/0*. **Add another rule**. Set the **Type** for this new rule to *SSH (22)* and the **Source** to *0.0.0.0/0*. Add a third rule for *HTTP (80)*, also with a source of *0.0.0.0/0*. **Save**. Currently, by default, our outbound rules allow all connections. We do not need to make changes to these rules for this lab.

Now select the *LabSB-EC2* security group. Add the SSH and HTTP rules as we have done above. **Save**. We now have both security groups set up.

With our VPC set up and security layers created to ensure some protection for any future EC2 or RDS instances, this lab is now complete.