Dom Moore
Cloud Architecture Security

Overview

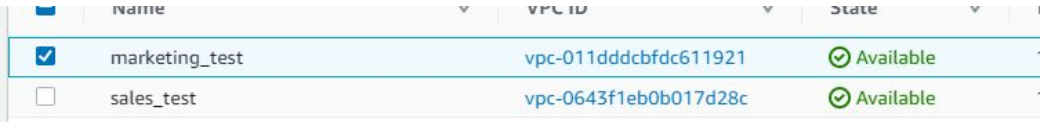
Configure an AWS Virtual Private Cloud (VPC) and also evaluate the CIS standards as they relate to OS hardening.

Part 1: Create a VPC

In this part of the lab, you'll deploy your first VPC. If you're an advanced user, looking for a challenge, or wish to enhance your AWS infrastructure knowledge, perform the below steps without the assistance of the VPC Wizard. Document with screenshots and descriptions of the steps you will take below.

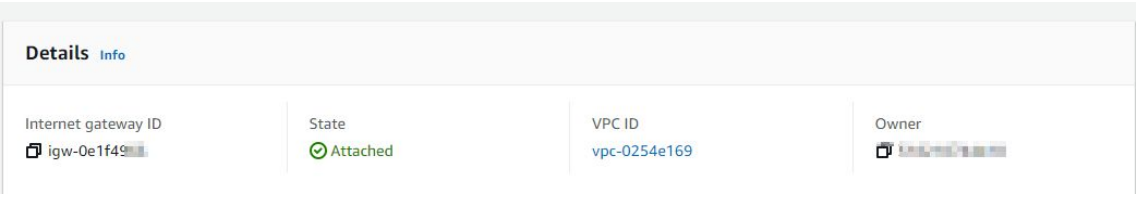
Step 1- Create a non-default Amazon VPC with network address
Step 2- Attach an Internet gateway to the VPC.
Step 3- Create an IPv4 subnet with network address
Step 4- Create a custom route table and associate it with your subnet.
Step 5- Launch an EC2 instance into your VPC.
Step 6- Establish remote internet connectivity to your new instance.
Step 7- Restrict inbound traffic to only allow your home network's public IP address.

Vpc network



Name	VPC ID	State
marketing_test	vpc-011dddcbfdc611921	Available
sales_test	vpc-0643f1eb0b017d28c	Available

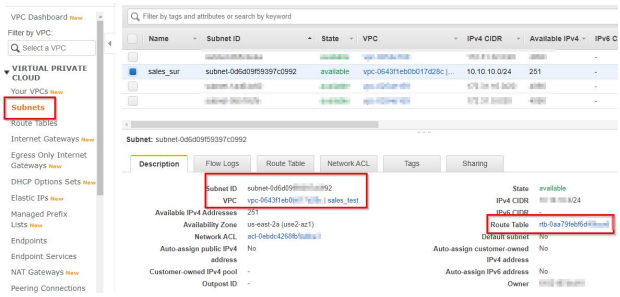
Internet gateway



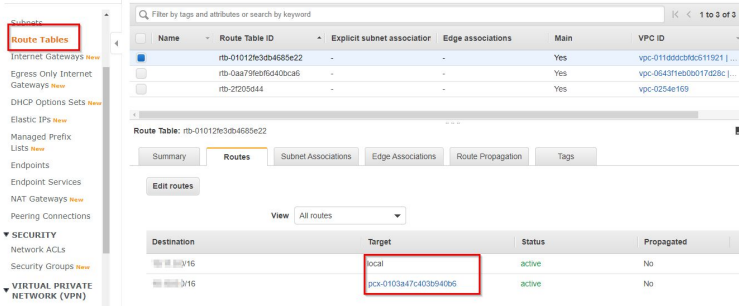
Details Info

Internet gateway ID	State	VPC ID	Owner
igw-0e1f49	Attached	vpc-0254e169	

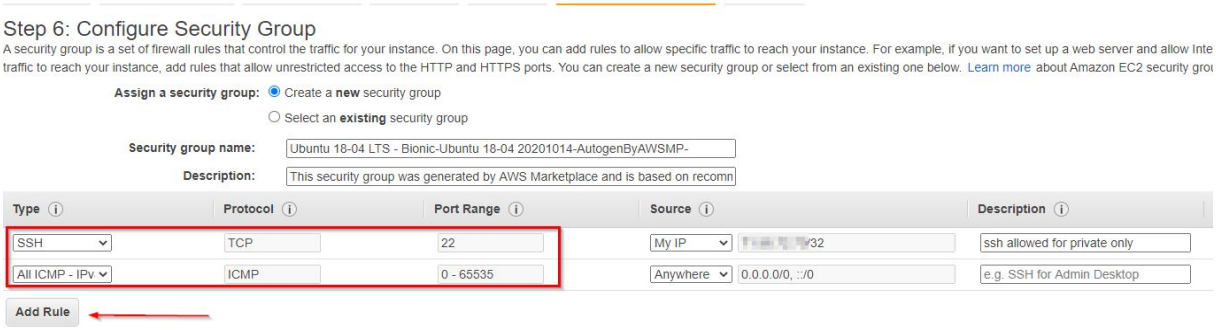
Subnet



Route Table



Security group



Part 2: Manual EC2 instance hardening with CIS

Next up, let's install an AMI on your new VPC and harden it according to CIS standards. Note: There are CIS-compliant AMIs that are prehardened, but for this part of the lab use regular AMIs.

Ste[1- launch a new instance in the same region as your VPC.

Step 2- Select an AMI that also appears in the CIS benchmark list.

Step 3- Deploy the instance to your VPC's subnet.

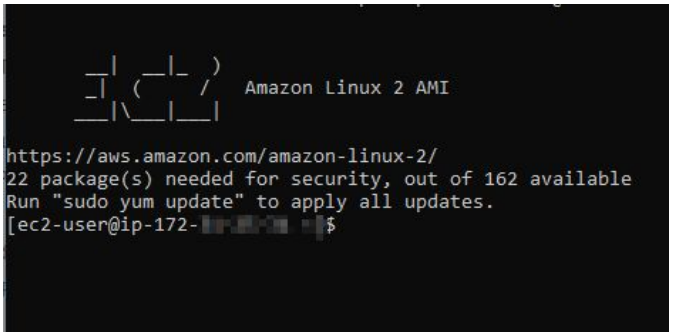
- Take a screenshot of this setting "Step 3: Configure Instance Details" in the instance creation wizard.
- Take a screenshot of the "Launch Log" indicating a successful generation of security groups, inbound rules authorization, and launch initiation.

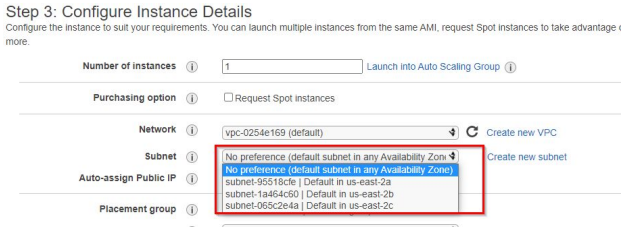
Step 4- Establish remote connectivity to your new instance.

Step 5- Select three benchmarks from your AMI's benchmark document in the CIS benchmark list and reconfigure your AMI to achieve the standard indicated.

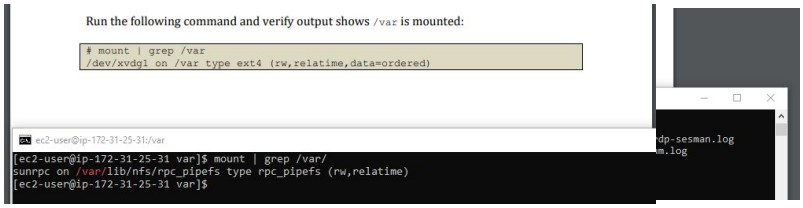
- Take a screenshot of each configuration change in your instance session.

New ami





CIS



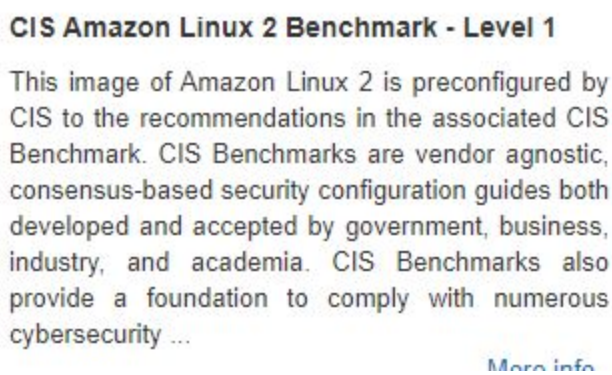
Part 3: Pre-hardened EC2 instance deployment

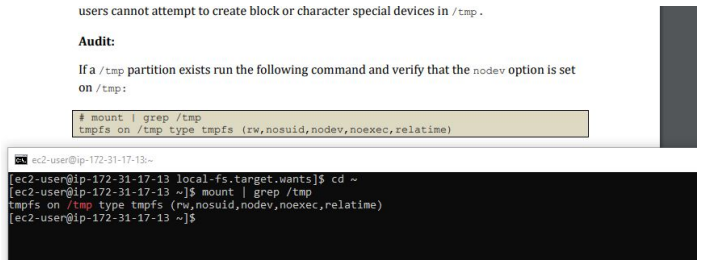
Step 1- Deploy a pre-hardened AMI in your non-VPC EC2.

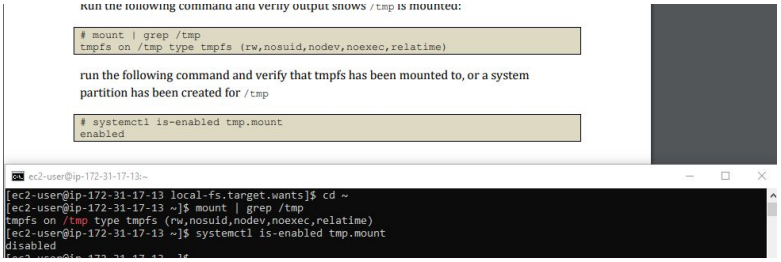
Step 2- Access the CIS standards and verify three benchmarks are achieved on the hardened instance.

- Take a screenshot verifying each benchmark in your pre-hardened instance. Does the hardened instance achieve the security standard on deployment?

CIS instance







Part 4: Reporting

- While deploying a VPC for a client company, you've determined that all employees at the office will need access to VPC resources. How will you configure employee access to VPC resources? Assume employees are working from a single office LAN.
    - I would configure the vpc for peering and allow the employees to access the resources by adding them to the VPS and using a routing table to direct the networks.
- What are the advantages and disadvantages of deploying pre-hardened AMIs?
    - The advantages are that they should be configured with some existing rules that may be better than the default ami rules but a disadvantage is that the preset rules may not fit your use case therefore you may still have to configure and add personalized rules.
- How does a VPC compare to the network architecture of a physical LAN?
    - The overall concept is the same in theory, you are on a public network the internet but the vpc is an encrypted network that provides privacy the basic networking principles still apply in the case of LAN or VPC