

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
<input checked="" type="checkbox"/>	marketing_test	vpc-011dddcbfdc611921	Available
<input type="checkbox"/>	sales_test	vpc-0643f1eb0b017d28c	Available

Internet gateway

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

Subnet

VPC Dashboard [New](#)

Filter by VPC

Q Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs [New](#)

Subnets

Route Tables [New](#)

Internet Gateways [New](#)

Egress Only Internet Gateways [New](#)

DHCP Options Sets [New](#)

Elastic IPs [New](#)

Managed Prefix Lists [New](#)

Endpoints

Endpoint Services

NAT Gateways [New](#)

Peering Connections

Filter by tags and attributes or search by keyword

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR
sales_sur	subnet-05d39f93937c0992	available	vpc-06431feb0017d28c	10.10.10.0/24	251	-

Subnet: subnet-05d39f93937c0992

Description Flow Logs Route Table Network ACL Tags Sharing

Subnet ID subnet-05d39f93937c0992 State available

VPC vpc-06431feb0017d28c IPv4 CIDR 10.10.10.0/24

Available IPv4 Addresses 251

Availability Zone us-east-2a (us-east-2a)

Network ACL acl-0abdc4268b-f088a3

Auto-assign public IPv4 address No

Customer-owned IPv4 pool -

Output IP -

Route Table rtb-0a796e6d6f8e6e22

Owner

Route Table

Subnets

Route Tables

Internet Gateways [New](#)

Egress Only Internet Gateways [New](#)

DHCP Options Sets [New](#)

Elastic IPs [New](#)

Managed Prefix Lists [New](#)

Endpoints

Endpoint Services

NAT Gateways [New](#)

Peering Connections

Filter by tags and attributes or search by keyword

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
rtb-01012e3db4686e22	-	-	-	Yes	vpc-0119d3c0bdc611921
rtb-0aa796e6d6f8e6e22	-	-	-	Yes	vpc-06431feb0017d28c
rtb-2f205044	-	-	-	Yes	vpc-0254e169

Route Table: rtb-01012e3db4686e22

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
0.0.0.0/0	local	active	No

Security group

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group

☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	My IP	ssh allowed for private only
All ICMP - IPv4	ICMP	0 - 65535	Anywhere	e.g. SSH for Admin Desktop

[Add Rule](#)

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.

Step 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.

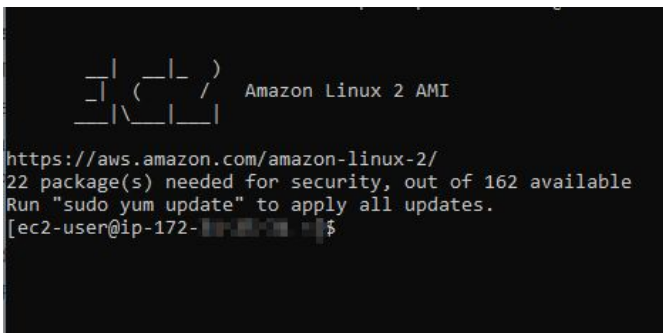
- Take a screenshot of this setting "Step 3: Configure Instance Details" in the instance creation wizard.
- Take a screenshot of the "Launch Log" indicating a successful generation of security groups, inbound rules authorization, and launch initiation.

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

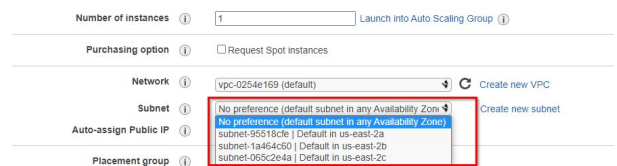


```
Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
22 package(s) needed for security, out of 162 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-25-31 ~]$
```

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of lower prices, or request Dedicated Hosts to run instances on dedicated hardware.



Number of instances 1 Launch into Auto Scaling Group

Purchasing option ☐ Request Spot instances

Network vpc-0254e169 (default) Create new VPC

Subnet No preference (default subnet in any Availability Zone) Create new subnet

Auto-assign Public IP ☐ subnet-95518c1e | Default in us-east-2a

Placement group subnet-1a464c60 | Default in us-east-2b

CIS

Run the following command and verify output shows /var is mounted:

```
# mount | grep /var
/dev/xvda1 on /var type ext4 (rw,relatime,data=ordered)
```

```
[ec2-user@ip-172-31-25-31 ~]$ mount | grep /var/
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw,relatime)
[ec2-user@ip-172-31-25-31 ~]$
```

dp-sesman.log
m.log

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

CIS Amazon Linux 2 Benchmark - Level 1

This image of Amazon Linux 2 is preconfigured by CIS to the recommendations in the associated CIS Benchmark. CIS Benchmarks are vendor agnostic, consensus-based security configuration guides both developed and accepted by government, business, industry, and academia. CIS Benchmarks also provide a foundation to comply with numerous cybersecurity ...

[More info](#)

users cannot attempt to create block or character special devices in /tmp .

Audit:

If a /tmp partition exists run the following command and verify that the `nodev` option is set on /tmp:

```
# mount | grep /tmp  
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

```
ec2-user@ip-172-31-17-13:~  
[ec2-user@ip-172-31-17-13 local-fs.target.wants]$ cd ~  
[ec2-user@ip-172-31-17-13 ~]$ mount | grep /tmp  
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)  
[ec2-user@ip-172-31-17-13 ~]$
```

run the following command and verify output shows /tmp is mounted:

```
# mount | grep /tmp  
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

run the following command and verify that tmpfs has been mounted to, or a system partition has been created for /tmp

```
# systemctl is-enabled tmp.mount  
enabled
```

```
ec2-user@ip-172-31-17-13:~  
[ec2-user@ip-172-31-17-13 local-fs.target.wants]$ cd ~  
[ec2-user@ip-172-31-17-13 ~]$ mount | grep /tmp  
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)  
[ec2-user@ip-172-31-17-13 ~]$ systemctl is-enabled tmp.mount  
disabled  
ec2-user@ip-172-31-17-13:~
```

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