AWS Concepts2-EC2 First Half

EC2: Elastic Compute Cloud= Infrastructure as a Service

- 🔸 Definitions
  - Consists in the capability of: Renting virtual machines/ Storing data on virtual machines (EBS)/ Distributing load across machines (ELB)/ Scaling the services using an auto-scaling group (ASG)
  - EC2 is the fundamental of the Cloud works
- 🔸 Sizing and Configuration Options
  - Operation systems: linux, windows, macos
  - CPU
  - How much random access memory (RAM)
  - How much storage space: network-attached (EBS, EFS)/ hardware (EC2 Instance Store)
  - Network Card: speed of the card, Public IP Address
  - Firewall rules: security group
  - Bootstrap script: EC2 User Data—bootstrapping 在启动时运行且仅有一次; run with root user
- 🔸 AMI: Amazon Machine Image. Launch instance *(OMG...the setting process is so complicated)*


- 🔸 EC2 Instance Type Basic: https://aws.amazon.com/cn/ec2/instance-types/

  Seven different types; naming convention: m5.2xlarge
  - M: instance class. 5: generation of the instance. 2xlarge: size within the instance class
  - General purpose: we use *t2.macro* which is a general purpose EC2 instance
  - Compute Optimize: used for machine learning, dedicated game servers, media transcoding, high performance web servers/computing, batch processing
  - Memory Optimize: used for relational/non-relational databases, optimize for BI, for real time processing of big unstructured data
  - Storage Optimize: used for relational or NoSQL databases, distributed file systems, data warehousing applications
- 🔸 Security Groups and Classic Ports
  - Is the fundamental of network security in AWS
  - How traffic gets into or out your EC2 instances
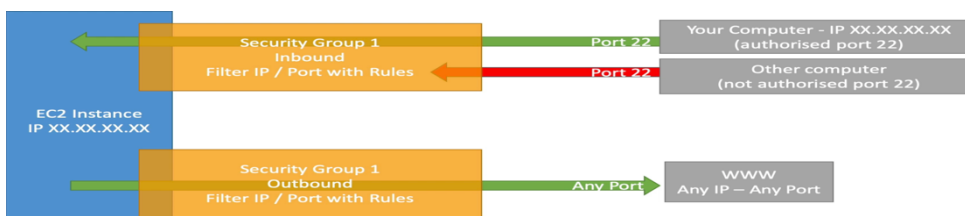
- Regulate: access to ports, authorize IP ranges, control inbound/outbound network

- Locked down into a region/VPC combination
- Can be attached to multiple instances
- It is better to maintain a separate security group for SSH access
- "Connection refuse" error→the security group works
- By default, all inbound traffic is blocked, all outbound traffic is authorized
- Classical Ports to know
- 22=SSH (Secure Shell)- log into a Linux instance
- 21=FTP (File Transfer Protocol)-upload files into a file share
- 22=SFTP (Secure File Transfer Protocol)-upload files using SSH
- 80-HTTP-access unsecured websites
- 443-HTTPS-access secured websites
- 3389-RDP (Remote Desktop Protocol)-log into a windows instance

Security Groups (1/3) Info

[C] [Actions ▼] [Export security groups to CSV] [▼] [**Create security group**]

Q Filter security groups   < 1 > ⚙

■	Name ▽	Security group... ▽	Security grou... ▽	VPC ID ▽	Description ▽	Own
☑	–	sg-0f3fd9068161...	launch-wizard-1	vpc-094f0966e7ac...	launch-wizard-1...	6461
☐	–	sg-07bc7da7c4cc...	default	vpc-094f0966e7ac...	default VPC sec...	6461
☐	–	sg-08e839f315ce...	launch-wizard-2	vpc-094f0966e7ac...	launch-wizard-2...	6461

Details   Inbound rules   Outbound rules   Tags

Details

Security group name	Security group ID	Description	VPC ID
🗇 launch-wizard-1	🗇 sg-0f3fd90681618b156	🗇 launch-wizard-1 created 2022-06-16T12:56:41.864Z	🗇 vpc-094f0966e7ac3f7f4 ↗

⬡ SSH

- Definition: control a remote machine, all using command line.
- Public DNS and Public IP of instance

```
Last login: Sun Jun 12 12:33:30 on ttys000
[(base) macbookpro@ip-192-168-43-11 ~ % ssh ec2-user@44.202.4.240
The authenticity of host '44.202.4.240 (44.202.4.240)' can't be established.
ECDSA key fingerprint is SHA256:19J/jAFVoiO8A0X3nN23FxRmHqsL8udEMg0EyV5N1Mg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '44.202.4.240' (ECDSA) to the list of known hosts.
ec2-user@44.202.4.240: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).

[(base) macbookpro@ip-192-168-43-11 ~ % ssh -i key1.pem ec2-user@44.202.4.240
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@           WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'key1.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "key1.pem": bad permissions
ec2-user@44.202.4.240: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[(base) macbookpro@ip-192-168-43-11 ~ % chmod 0400 key1.pem
[(base) macbookpro@ip-192-168-43-11 ~ % ssh -i key1.pem ec2-user@44.202.4.240
Last login: Thu Jun 16 13:56:16 2022 from ec2-18-206-107-26.compute-1.amazonaws.com

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[[ec2-user@ip-172-31-89-120 ~]$ whoami
ec2-user
[[ec2-user@ip-172-31-89-120 ~]$ ping google.com
PING google.com (142.250.31.139) 56(84) bytes of data.
64 bytes from bj-in-f139.1e100.net (142.250.31.139): icmp_seq=1 ttl=97 time=1.43 ms
64 bytes from bj-in-f139.1e100.net (142.250.31.139): icmp_seq=2 ttl=97 time=1.48 ms
64 bytes from bj-in-f139.1e100.net (142.250.31.139): icmp_seq=3 ttl=97 time=1.44 ms
```