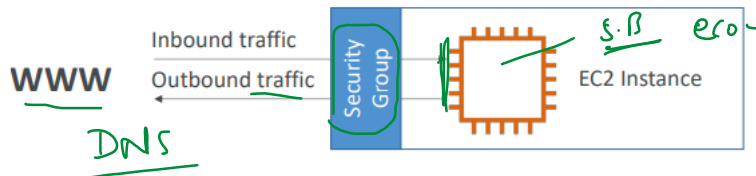


EC2- Security Groups

07:55 PM

Introduction to Security Groups

- Security Groups are the fundamental of network security in AWS
- They control how traffic is allowed into or out of our EC2 Instances.



- Security groups only contain allow rules } deny
- Security groups rules can reference by IP or by security group

Security Groups Deeper Dive

- Security groups are acting as a "firewall" on EC2 instances

They regulate:

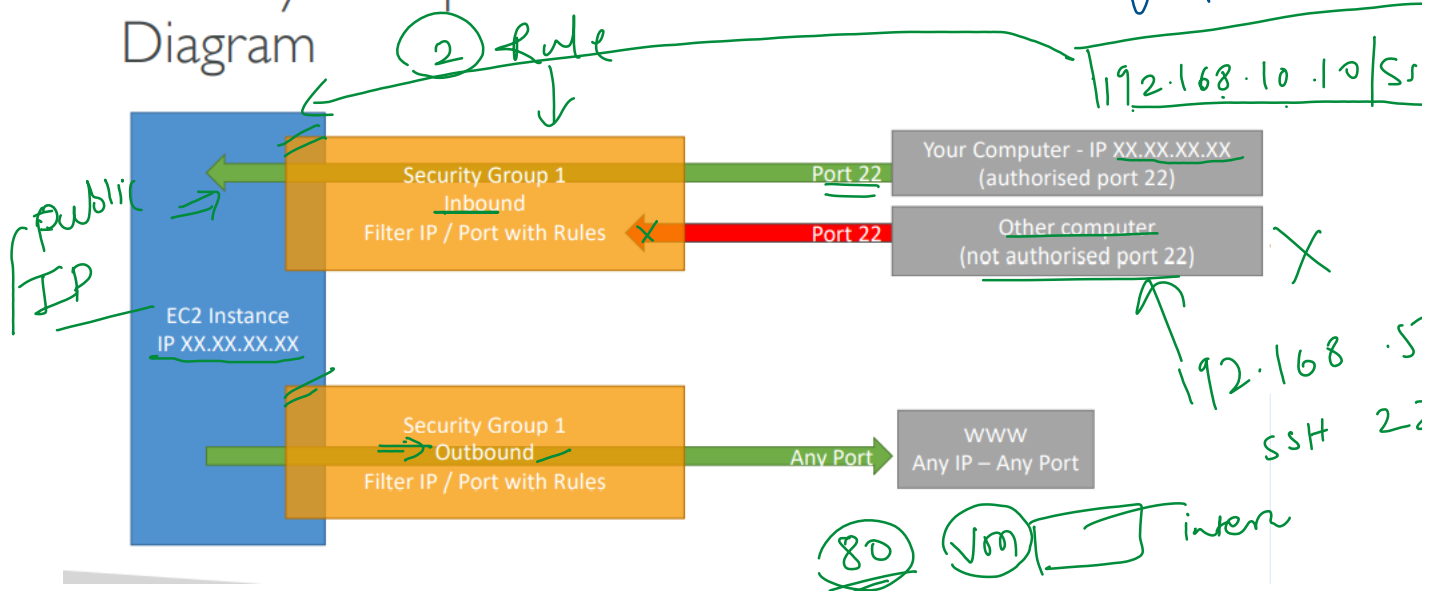
- Access to Ports
- Authorised IP ranges – IPv4 and IPv6
- Control of inbound network (from other to the instance)
- Control of outbound network (from the instance to other)

rules

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	test http page
SSH	TCP	22	122.149.196.85/32	
Custom TCP Rule	TCP	4567	0.0.0.0/0	java app

Handwritten notes: ID.VM 32, 8.8.8.8/

Security Groups Diagram



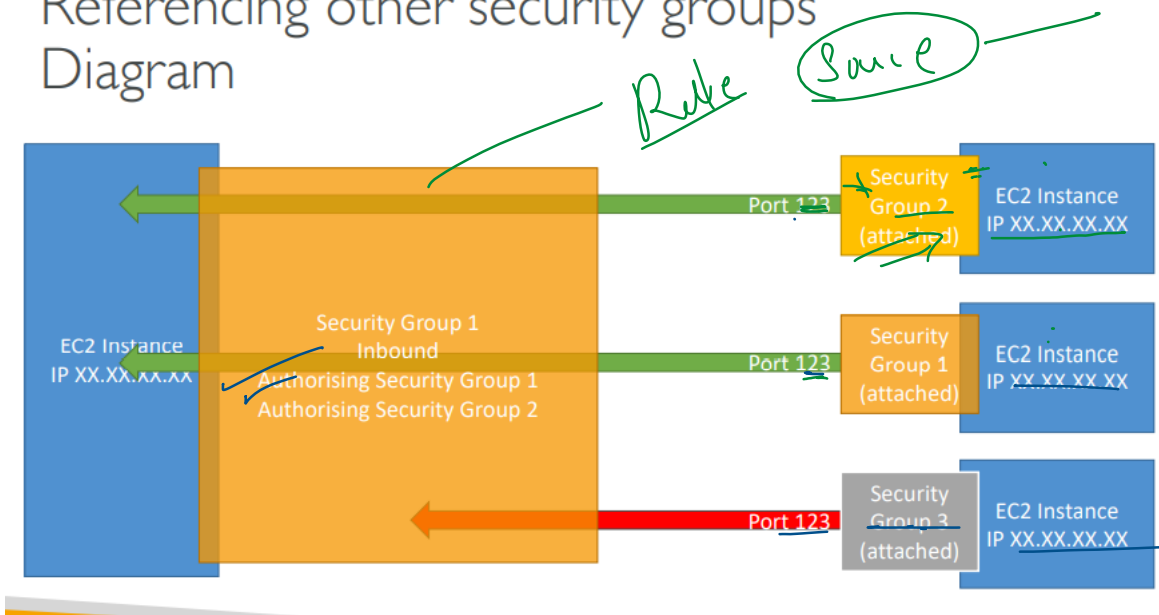
Security Groups

Good to know

- Can be attached to multiple instances
- Locked down to a region / VPC combination
- Does live "outside" the EC2 – if traffic is blocked the EC2 instance won't see it
- It's good to maintain one separate security group for SSH access
- If your application is not accessible (time out), then it's a security group issue
- If your application gives a "connection refused" error, then it's an application error or it's not launched
- All inbound traffic is **blocked** by default
- All outbound traffic is **authorised** by default

Referencing other security groups

Diagram



Classic 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

SSH Summary Table

SSH

Putty

EC2 Instance Connect

browser

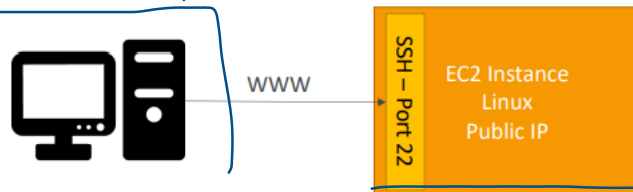
Mac	✓
Linux	✓
Windows < 10	
Windows >= 10	✓



How to SSH into your EC2 Instance

Linux / Mac OS X

- We'll learn how to SSH into your EC2 instance using Linux / Mac
- SSH is one of the most important function. It allows you to control a remote machine, all using the command line.



X
browser - Lin
still SSH 2

- We will see how we can configure OpenSSH ~/.ssh/config to facilitate the SSH into our EC2 instances

How to SSH into your EC2 Instance

Windows

- We'll learn how to SSH into your EC2 instance using Windows
- SSH is one of the most important function. It allows you to control a remote machine, all using the command line.



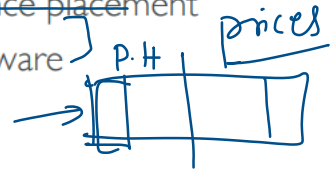
- We will configure all the required parameters necessary for doing SSH on Windows using the free tool Putty

EC2 Instances Purchasing Options

- **On-Demand Instances:** short workload, predictable pricing]
- **Reserved:** (MINIMUM 1 year)
 - **Reserved Instances:** long workloads
 - **Convertible Reserved Instances:** long workloads with flexible instances
 - **Scheduled Reserved Instances:** example - every Thursday between 3 and 6 pm]

12000
100 \$/m
70% 30 \$/m
\$1800
[Len]
2

- **Spot Instances:** short workloads, cheap, can lose instances (less reliable) ←
- **Dedicated Hosts:** book an entire physical server, control instance placement
- **Dedicated Instances:** no other customers will share your hardware



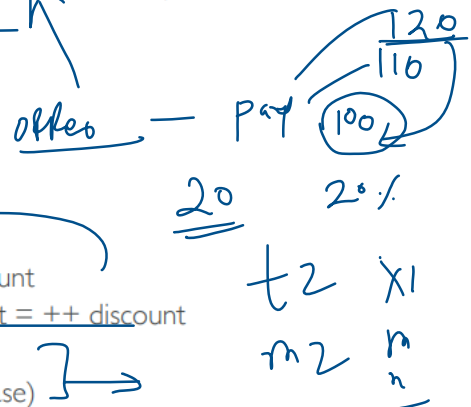
✓ EC2 On Demand

- Pay for what you use:
 - Linux or Windows - billing per second, after the first minute
 - All other operating systems - billing per hour
- Has the highest cost but no upfront payment
- No long-term commitment → 1 / AWS

- Recommended for **short-term** and **un-interrupted workloads**, where you can't predict how the application will behave

✓ EC2 Reserved Instances

- Up to 72% discount compared to On-demand
- Reservation period: 1 year = + discount | 3 years = +++ discount
- Purchasing options: no upfront | partial upfront = + | All upfront = ++ discount
- Reserve a specific instance type
- Recommended for steady-state usage applications (think database)



• Convertible Reserved Instance

- can change the EC2 instance type
- Up to 66% discount

• Scheduled Reserved Instances

- launch within time window you reserve
- When you require a fraction of day / week / month
- Commitment for 1 year only

note: the % discounts are different from the video as AWS change them over time – the exact numbers are not needed for the exam. This is just for illustrative purposes

EC2 Spot Instances

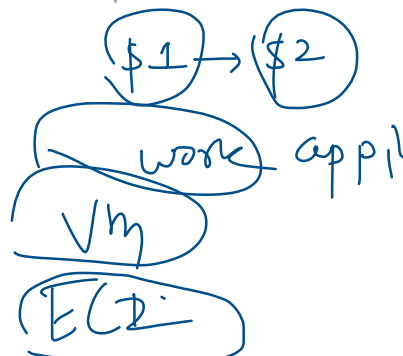


- Can get a **discount of up to 90%** compared to On-demand
- Instances that you can **lose** at any point of time if your max price is less than the current spot price
- The **MOST** cost-efficient instances in AWS

• Useful for workloads that are resilient to failure

- Batch jobs
- Data analysis
- Image processing
- Any **distributed** workloads
- Workloads with a flexible start and end time

• Not suitable for critical jobs or databases



EC2 Dedicated Hosts

Local policy

- An Amazon EC2 Dedicated Host is a physical server with EC2 instance capacity fully dedicated to your use. Dedicated Hosts can help you address compliance requirements and reduce costs by allowing you to use your existing server-bound software licenses.

- Allocated for your account for a 3-year period reservation
- More expensive (

- Useful for software that have complicated licensing model (BYOL – Bring Your Own License)
- Or for companies that have strong regulatory or compliance needs

shared
H/W
Defect-
S.I.
PCI,
h.

EC2 Dedicated Instances

- Instances running on hardware that's dedicated to you
- May share hardware with other instances in same account
- No control over instance placement (can move hardware after Stop / Start)

Characteristic	Dedicated Instances	Dedicated Hosts
Enables the use of dedicated physical servers	x	x
Per instance billing (subject to a \$2 per region fee)	x	
Per host billing		x
Visibility of sockets, cores, host ID		x
Affinity between a host and instance		x
Targeted instance placement		x
Automatic instance placement	x	x
Add capacity using an allocation request		x

Which purchasing option is right for me?




- **On demand:** coming and staying in resort whenever we like, we pay the full price
- **Reserved:** like planning ahead and if we plan to stay for a long time, we may get a good discount.
- **Spot instances:** the hotel allows people to bid for the empty rooms and the highest bidder keeps the rooms. You can get kicked out at any time
- **Dedicated Hosts:** We book an entire building of the resort

Price Comparison

Example – m4.large – us-east-1

Price Type	Price (per hour)
On-demand	\$0.10
Spot Instance (Spot Price)	\$0.032 - \$0.045 (up to 90% off)



Spot Block (1 to 6 hours)	Spot Price
Reserved Instance (12 months) – no upfront	\$0.062
Reserved Instance (12 months) – all upfront	\$0.058
Reserved Instance (36 months) – no upfront	\$0.043
Reserved Convertible Instance (12 months) – no upfront	\$0.071
Reserved Scheduled Instance (recurring schedule on 12 months term)	\$0.090 – \$0.095 (5%-10% off)
Dedicated Host	On-demand price
Dedicated Host Reservation	Up to 70% off

Handwritten notes on the right side of the table:

- A bracket groups the first five rows.
- Next to the "Reserved **Scheduled** Instance" row, there is a handwritten "10%".
- Next to the "Dedicated Host" row, there is a handwritten "3\$".