



WHOAMI



HI, I'M MOHAMED EID

Passionate DevOps enthusiast with expertise in Linux system administration and automation. Proficient in Bash, Git, Ansible, Docker, AWS, and Terraform, I focus on streamlining processes and enhancing system reliability in cloud environments. Always eager to learn and share knowledge with others.

• •

• •



[in](#) [f](#) /mohamedeid404/

+



I'm Here

Table Of Content

CH-00 - IT & Cloud Fundamentals.....	8
➡ IT.....	8
● IT Fundamental:.....	8
➡ Cloud.....	11
● Physical Server (Powerful Computers):.....	11
● Data Centers:.....	12
● Cloud Types.....	14
● Shift from CAPEX to OPEX model :.....	15
● Cloud Services:.....	16
● Virtualizations:.....	17
● Web Application:.....	19
CH-01,02 - Stephane intro “Nothing important”.....	20
CH-03 - Getting started with AWS.....	20
➡ Region:.....	20
● دyi بناءا على الآتي Region بختار ال.....	21
➡ Availability Zones (AZ):.....	21
● ف دة بيضمنلك حاجتين من مميزات ال cloud :.....	22
➡ AWS Points of Presence (Edge Locations).....	23
CH-04 - IAM & AWS CLI.....	24
➡ IAM Introduction (Identity and Access Management): Users, Groups, Policies.....	24
➡ IAM Users, Groups Hands ON.....	25
➡ IAM Policies:.....	30
● Policy Structure:.....	30
➡ IAM Policies Hands On:.....	32
➡ IAM – Password Policy.....	42
● Passwords:.....	42
● Multi Factor Authentication - MFA.....	42
➡ IAM MFA Hands ON.....	43
● Passwords Policy:.....	43
● Assign MFA:.....	45



I'm Here

➡ AWS Access Keys, CLI and SDK:.....	46
● SDK (Software Development Kit):.....	47
➡ AWS CLI Hands On:.....	47
➡ AWS CloudShell:.....	50
➡ IAM Roles for AWS Services:.....	51
● Most Common Roles:.....	51
➡ IAM Roles Hands ON:.....	52
➡ IAM Security Tools, Hands On:.....	54
● IAM Credentials Report (account-level).....	54
● IAM Credentials Report Content.....	55
● IAM Access Advisor (user-level).....	55
➡ IAM Summary:.....	56
CH-05 - EC2 Fundamentals.....	57
➡ AWS Budget Setup:.....	57
➡ EC2 Basics:.....	62
● من خلالها تقدر : service عباره عن	62
● EC2 sizing & configuration options.....	62
● دة بيكون عباره عن : ال Script	63
➡ Create An EC2 Instance with EC2 User Data to have a website Hands On:.....	64
➡ EC2 Instances Types:.....	64
● m5.2xlarge.....	65
● مفهوم الأنواع دي على حسب غرضك: AWS هتلaci ان	65
● مقارنة بسيطة:.....	66
➡ Security Group & Classic Ports Overview.....	66
● Control the inbound & outbound traffic by:.....	67
● Important Example:.....	68
● Classic Ports:.....	69
➡ Security Groups Hands On:.....	69
➡ SSH Overview:.....	70
➡ How To SSH Using Linux Or Mac.....	70
➡ How To SSH Using Windows7.8:.....	72



I'm Here

➡ How To SSH Using Windows10:.....	73
➡ SSH Troubleshooting:.....	74
➡ EC2 Instance Connect (Easy way).....	74
➡ EC2 Instance Roles Demo:.....	76
➡ EC2 Instance Purchasing Options:.....	77
● On-Demand Instances :.....	77
● Reserved Instances & Convertible Reserved Instances (1&3 year):	
77	
➡ Spot Instances & Spot Fleet:.....	80
● How Spot Request Work :.....	81
● How to terminate spot instances?.....	81
● Spot Fleet:.....	82
➡ EC2 Instance launch types hands on:.....	83
CH-06 - EC2 - Solutions Architect Associate Level.....	84
➡ 001 Private vs Public vs Elastic IP:.....	84
➡ 002 Private vs Public vs Elastic IP Hands On.....	85
● Create Elastic IP:.....	85
● بتعاتك وبتسقاد الآتي : elastic ip بترتبط بال .. instance بعد ما كريت ال	85
➡ 003 EC2 Placement Groups.....	86
● Cluster.....	86
● Spread.....	86
● Partition.....	87
➡ 004 EC2 Placement Groups - Hands On.....	87
➡ 005 Elastic Network Interfaces (ENI) - Overview.....	88
● Network Cards / Interface.....	88
➡ 006 Elastic Network Interfaces (ENI) - Hands On.....	89
● Example: Initial Configuration.....	90
● How It Works Internally.....	91
➡ 008 EC2 Hibernate.....	92
● Use Cases:.....	93
● فيه شويه حاجات بتحكمك لو هستعمل ال Hyberenate :	93
➡ 009 EC2 Hibernate Hands On:.....	93



I'm Here

• الحاجات دي لازم تحصل :	94
• TEST.....	95
CH-07 - EC2 Instance Storage.....	96
→ 001 EBS Overview.....	96
• مميزاتها :	96
• Delete On Termination:.....	97
→ 002 EBS Hands On.....	100
→ 003 EBS Snapshots.....	103
• EBS Snapshots Features.....	104
→ 004 EBS Snapshots - Hands On.....	105
→ 005 AMI Overview (Amazon Machine Image).....	107
• أنواع ال AMI :	107
→ 006 AMI Hands On.....	108
→ 007 EC2 Instance Store.....	109
• Cons:.....	109
• Use Case:.....	109
→ 008 EBS Volume Types.....	110
• GP2/GP3 (SSD) - General Purpose.....	110
• io1/io2 (SSD).....	110
• st1 (HHD).....	110
• sc1 (HHD).....	110
• General Purpose SSD :	111
• Provisioned IOPS (PIOPS) SSD Use Cases.....	111
• Hard Disk Drives (HDD).....	112
• Solid state drive (SSD) volumes.....	113
• Hard disk drive (HDD) volumes.....	113
→ 009 EBS Multi-Attach.....	114
• Key points:.....	114
• Benefits:.....	114
→ 010 EBS Encryption.....	115
• هتحصل على الآتي : EBS Volume encrypted لو عملت	115
• EBS Encryption leverages keys from KMS (AES-256).....	115



I'm Here

● Encryption: encrypt an unencrypted EBS volume.....	115
→ 011 Amazon EFS (Elastic File System).....	117
● Key Points.....	117
● EFS – Performance & Storage Classes.....	118
● Storage Tier:.....	120
● Availability & Durability:.....	121
→ 012 Amazon EFS - Hands On.....	122
→ 013 EBS vs EFS:.....	126
● EBS.....	126
● EFS.....	126
→ 014 EBS & EFS - Section Cleanup.....	127
CH-08 - High Availability and Scalability ELB & ASG.....	128
→ 001 High Availability and Scalability.....	128
● Scalability:.....	128
● Availability:.....	129
→ 002 Elastic Load Balancing (ELB) Overview.....	129
● Key Diff Between AWS LB & Nginx LB.....	130
● Types of load balancer on AWS.....	130
● Load Balancer Security Groups.....	131
→ 003 Note About the 1-Classic Load Balancer (CLB).....	132
→ 004 2-Application Load Balancer (ALB).....	132
● Key Features.....	132
● Target Groups:.....	132
● Listeners and Rules:.....	133
● Health Check.....	133
● ‘X-Forwarded-For’ Header (How it works?):.....	135
→ 005 Application Load Balancer (ALB) - Hands On - Part 1.....	136
→ 006 Application Load Balancer (ALB) - Hands On - Part 2.....	137
● Tip1- Enter the instances through ALB only.....	137
● Tip2 - Modify the ALB Listeners & rules.....	138
→ 007 Network Load Balancer (NLB).....	140
● Key Features.....	140



I'm Here

● Network Load Balancer –Target Groups.....	141
➡ 008 Network Load Balancer (NLB) - Hands On.....	142
➡ 009 Gateway Load Balancer (GWLB).....	144
● Gateway Load Balancer –Target Groups.....	145
➡ 010 Elastic Load Balancer - Sticky Sessions.....	146
● عندنا بقاناً عين من ال cookies :.....	147
➡ 011 Elastic Load Balancer - Cross Zone Load Balancing.....	148
➡ 012 Elastic Load Balancer - SSL Certificates.....	149
● Load Balancer SSL Certificate (Secure Sockets Layer):.....	149
● Server Name Indication (SNI):.....	151
➡ 013 Elastic Load Balancer - SSL Certificates - Hands On.....	152
➡ 014 Elastic Load Balancer - Connection Draining.....	153
➡ 015 Auto Scaling Groups (ASG) Overview.....	154
● Overview:.....	154
● Auto Scaling Group Capacity:.....	155
● Create Launch Template:.....	155
➡ 016 Auto Scaling Groups Hands On.....	157
➡ 017 Auto Scaling Groups - Scaling Policies.....	160
● Dynamic Scaling Policy:.....	160
● Good Metrics to Scale On in AWS:.....	161
● Scaling cooldown:.....	162
● Predictive Scaling:.....	162
● Activity History Example :.....	162
➡ 018 Auto Scaling Groups - Scaling Policies Hands On.....	163
CH-09 - AWS Fundamentals RDS + Aurora + ElastiCache.....	169
➡ 001 Amazon RDS Overview (Relational Database Service).....	169
● Key Features.....	169
➡ 002 RDS Read Replicas vs Multi AZ.....	170
● Overview.....	170
● Connection string.....	171
● Replicas End point.....	171
● Cost.....	171



I'm Here

● RDS Multi AZ (Disaster Recovery).....	172
➡ 003 Amazon RDS Hands On.....	174
➡ 004 RDS Custom for Oracle and Microsoft SQL Server.....	181
● RDS vs. RDS Custom.....	181
● RDS: entire database and the OS to be managed by AWS.....	181
● RDS Custom: full admin access to the underlying OS and the database.....	181
➡ 005 Amazon Aurora.....	182
● Relational Databases:.....	182
● Overview:.....	182
● Key Features.....	182
1. High Performance:.....	182
2. High Availability and Durability:.....	183
3. Scalability:.....	184
4. Scalability:.....	184
5. Backup and Recovery:.....	184
6. Compatibility:.....	184
● What if the master database failed for RDS and Aurora:.....	185
● Aurora DB Cluster.....	185
● The diff between Aurora Server less and normal one.....	186
➡ 006 Amazon Aurora - Hands On.....	186
➡ 007 Amazon Aurora - Advanced Concepts.....	189
● Aurora Replicas - Auto Scaling.....	189
● Aurora – Custom Endpoints.....	190
● The diff between Aurora Server less and normal one.....	190
● Global Aurora.....	191
● Aurora Machine Learning.....	193
➡ 008 RDS & Aurora - Backup and Monitoring.....	194
● RDS Backup:.....	194
● Automated Backup.....	194
● Manual DB Snapshots.....	194
● Aurora Backup:.....	194



I'm Here

● Automated Backup.....	194
● Manual DB Snapshots.....	194
● RDS & Aurora Restore options.....	195
● Aurora Database Cloning.....	195
→ 009 RDS & Aurora Security.....	196
● Encryption at Rest.....	196
● Encryption in Transit.....	196
● IAM Database Authentication.....	196
● Security Groups.....	196
● SSH Access.....	196
● Audit logs.....	197
→ 010 RDS Proxy.....	197
● Use Case.....	197
● RDS Proxy Enhanced Security.....	198
→ 011 ElastiCache Overview.....	199
● Diff Between Cookie & Cache.....	199
● Amazon ElastiCache.....	200
● Amazon ElastiCache Engines.....	201



I'm Here

IT & Cloud Fundamentals



All From [Eisa Abo Sherif](#) & [Stephane Maarek](#)



• IT Fundamental:



- اي اجهزة احنا بنسخدمها اسمها Computing Device

- هتلaci في الاجهزه دي حاجات مشتركة كتير وهيا:

1. CPU (Central Processing Unit):

- وحدة المعالجة المركزية .. دا المخ اللي بي process كل حاجة

- بي كل ال instructions fetch , execute , decode process اللي جياله من programs

- الاداء بتاعه بيتقاس بعدد ال cores وال clock speed علاقه طردية

- جوا ال CPU حاجة اسمها Registers ودي عباره عن small fast storage

- بيستخدمها بديلة عن ال RAM لأنها اسرع منها .. بيستخدمها ف حالة انو عاوز ي quick access على حاجة.

- فى ال CPU الجديدة هتلaci small amount of high-speed memory تستخدم

- فال cashing علشان موضوع ال processing ميأخذش وقت اطول



I'm Here

- فى ال CPU الجديدة بيكون فيها Multi-core Processing ياعني تقدر ت perform multiple operations فى نفس الوقت
- سرعته بتتقاس بال GHz

2. GPU (Graphics Processing Unit):

- عباره عن processor مخصص انو ي graphic renders خاصه بالجرافيك زي ال images , animation , videos, processing task 3D environment

3. RAM (Random Access Memory):

- اسرع من ال SSD , HDD
- عباره عن temporary storage لـ data اللي بيستخدمها ال CPU وي process it .. بتخلی ال CPU ي Access الداتا وي procces it من خلالها زي انك ت run app او ت open file
- كل ما تكون ال RAM اكتر كل ما تكون قادر انك تعمل Multi tasking ياعني تفتح برامج وتعمل حاجات كتير فى نفس الوقت بدون ما الجهاز يهنج بتستخدم بردو فى ال buffer , cashing
- لو ال RAM مش كافية ممكن انك تأخذ من ال HDD او SSD جزا portion ك virtual memory
- سرعتها بتتقاس بال Giga byte

4. HDD & SSD

- بيخذنوا الداتا العاديـة وال SSD اسرع من ال SSD
- سرعتها بتتقاس بـ tera Gigabyte او



I'm Here

5. Network Cards / Interface



Connects the computing device to the Outside world. Can be wireless (WiFi) or wired (use Ethernet/LAN cables).

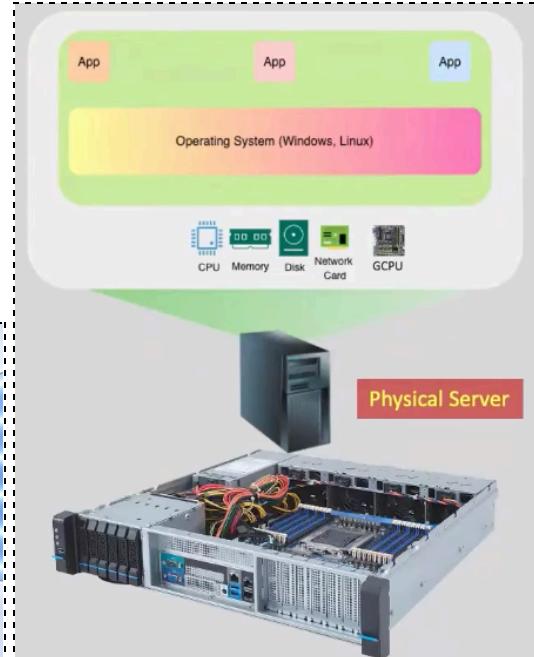
- عن طريقها بنوصل لل internet سواء wireless زى الاب كدا او لو كمبيوتر ممكن بكابل او ممكن ب وصلة تخلية يلقط وايفاي.
- سرعتها بتتقاس بال **Mbps or Gbps** .. ميجا او جيجا بايت / ثانية

اتكلمنا عن كل اللي فات دة لان دول نفس مكونات ال Servers اللي بتبقى موجودة فى ال

Data Centers

Cloud

• Physical Server (Powerful Computers):



I'm Here

- بيكون عبارة عن نفس المكونات بتاعة الكمبيوتر العادي ولكن اكتر بمراحل ومحظوظين في Racks زى اللي فى الصورة دي وال Racks دي فى اماكن اسمها Data Centers.
 - بين ال Operating System وال server hardware بيكون موجود ال Applications اللي بيوصل ال requests لل hardware علشان يتعلملها process ويرجع تاني ال Applications responds
-

• Data Centers:



- دي الاماكن المجهزة اللي بيكون فيها ال servers بتاعتتنا .. حماية وكاميرات وانظمة مراقبة وتكييفات وكل حاجة تحافظ على ان ال servers دي تفضل شغالة ومحدش يخترقها.
- هتلaci جوا يمكن شوارع ويمكن levels فوق بعض طوابق .. ف بيبقى عندك كميات رهيبة .. بتتقسم فى كابينات كدا اللي هيا بالطول دي اسمها racks بيكون جواها ال servers وعلى كل حاجة server بحيث نعرف ال stickers دة بتاع مين وتابع لاي



I'm Here

.. IP address وممكن يكون مكتوب عليه كمان ال business unit الارضيه حتى دي بتقى تحتها كابلات.

- كل ال servers دي بتقى معزولة عن بعضها .. يقدرو يتكلمو من خلال ال network لو انت سامح لهم او تحتاج دة.

- ممكن تاخد server او rack room كاملة .. كل حاجة متاحة على حسب احتياجاتك

• المكونات بالتفصيل :



- **Rack-Mountable Servers** : دي ال Physical servers وال

Racks دة نوع معين .. ال servers دي بنادها نحطها في ال Rack-Mountable

ال Racks دي من الخلف بيكون فيها ال storage وال network interface وال

power وكدا .. ال servers دي بقى اللي بيكون عليها ممكن تطبيقات عادي زي اوبر

او مثلا data bases .. ال Racks دي كل واحدة فيها تكون secured ومراقبة

والمبني كمان متراقب وكله تحت الكنترول 😊

• **Data Centers** : أنواع ال

- **On-Premises** : بيكون مملوك للهيئة او الشركة او الحكومة وهو اللي بيتحمل كل التكاليف

من الصفر .. building , network , storage , hardware , Virtualization , OS

, Data , App

- **On-Cloud** : عالكلود زي AWS , Azure ومن مميزاته ..



I'm Here

● Cloud Types

1. Public & Private Cloud

- زى AWS , Azure متاح للعامة Public

- ال Data centers باللى فيها بتاعتنا ومحدش بيوصلها غيرنا وده مهم فى ال Private

زى البنوك او كدا critical use case

2. Hybrid Cloud

- لو هتستخدم ال Private وال Public مع بعض ف دة اسمو Hybrid Cloud سواء ال private connectivity by the internet او هيئة حكومية مثل connection بينهم وبينهم وعندها بيانات عملاء ف دي هتخليها private وبقى البيانات دي عادي تكون عال public ف بتخليلها عال public ويبقى ده Hybrid

التحدي بيكون فى اننا نـ Authenticate users مابين ال private , Public التحدي بيكون فى اننا نـ

Cloud حاجة عال Access حاجة عال Public يحتاج بـ user يعني لو فيه

ف ازاي نخليه يقدر يعمل دة.

3. Multi Cloud

- انى اقسم ال work load بتاعي على كذا cloud provider

- لو عندنا تطبيقات خاصة بـ ال E-Commerce ف افضل استخدم AWS

- لو عندنا تطبيقات خاصة بـ Microsoft ف افضل Azure

- لو بنك ف افضل IBM

- لو Google ف AI/Machine Learning افضل

- لو عندي جزئية خاصة بال Virtualization ف هتلaci جزا خاص بال VMware على كل ال

Cloud Providers



I'm Here

ممكن تستخدم Private & Public & Multi Cloud على data مع بعض .. شوية Hybrid وشوية على Azure .. كدا دة اسمو AWS & Multi Cloud

- Shift from CAPEX to OPEX model :

- بوجود الـ Cloud اتحولنا من CAPEX إلى OPEX .. ياعني بدل ماانا هدفع واكلف واعمل Data Center واصرف عليه من الصفر .. لا انا بس هدفع تكاليف التشغيل فقط ودة اللي وفترتو الـ Cloud زي AWS , Azure cloud providers واي حاجة تانية بتكون من مسؤولية الـ Provider

- النفقات الرأسمالية (CAPEX) : ودة راس المال اللي بحتاجة علشان ابدا بيها المشروع او ابني بيها الـ data center

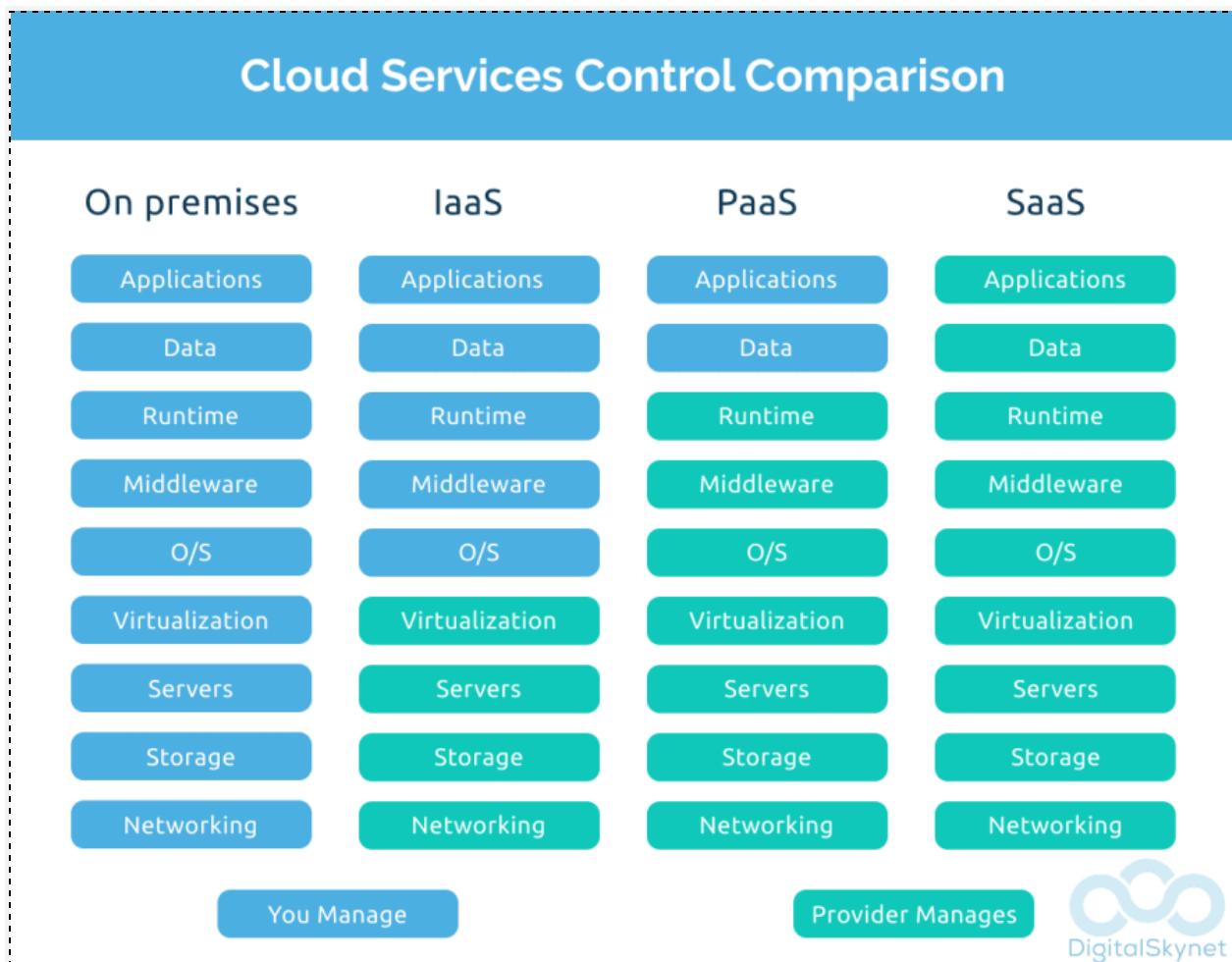
- النفقات التشغيلية (OPEX) : ودي هيا المصارييف data centers التشغيلية بعد ما بنيت الـ

- Consumption Based Model : دة ياعني هنشتغل بمبدأ Pay As You Go على قد استخدامك.



I'm Here

- **Cloud Services:**



- **On-Premises :**

- انت اللي شايل كل حاجة من البداية للنهاية.

- **Infrastructure as a service (IaaS)**

- بتاخد فقط ال Virtual Machines فى AWS .. والباقي من عند ال Providers

interpreter : هتشتغل python ولا java ولا بتستخدم انهي **Run Time** -

Message : ال اللي بين ال software زى OS وال Applications **Middleware** -

.brokers like RabbitMQ, Apache Kafka

AWS هي الرائدة فى الجزء دة -



I'm Here

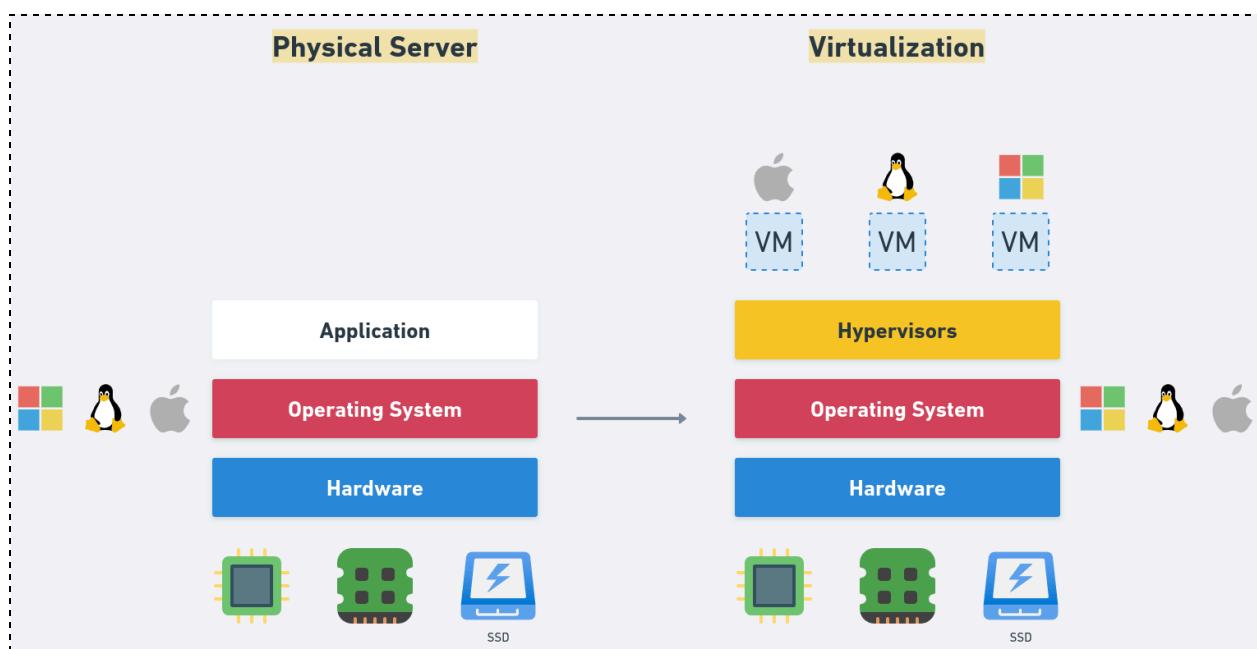
- **Platform as a service (PaaS)**

ف ال دة ال model customer بیأجر platform جاهزة بي run عليها ال app بتاعه.

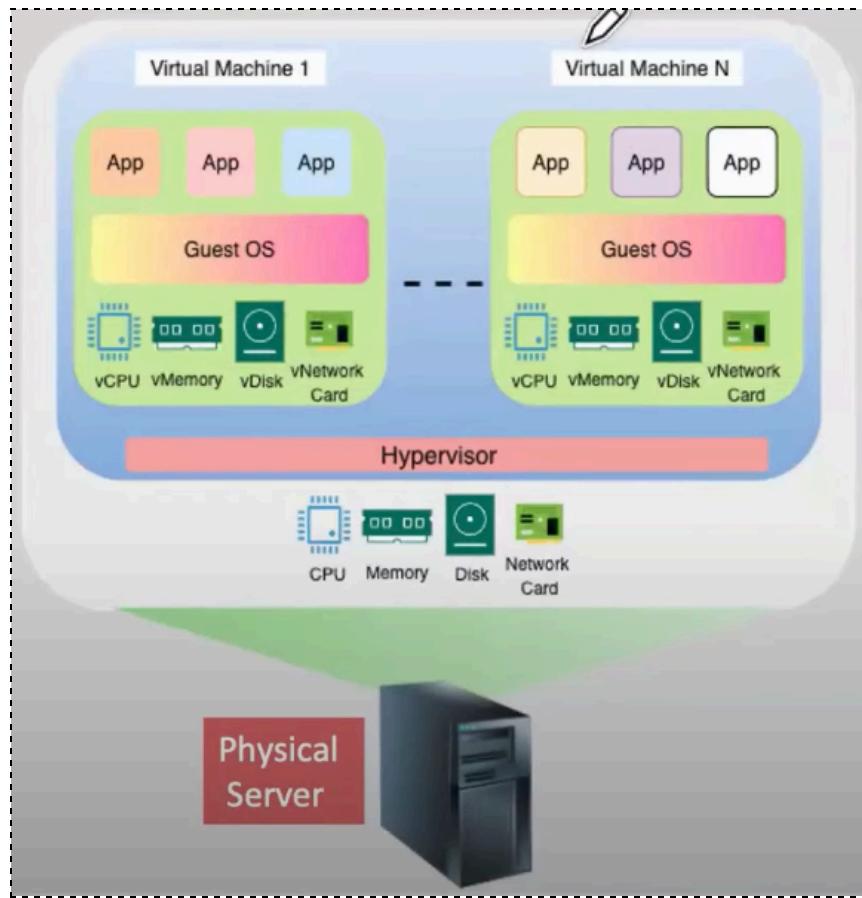
- **Software as a service (SaaS)**

ف ال دة ال hosted , managed by software customer جاهز cloud provider

- **Virtualizations:**



I'm Here

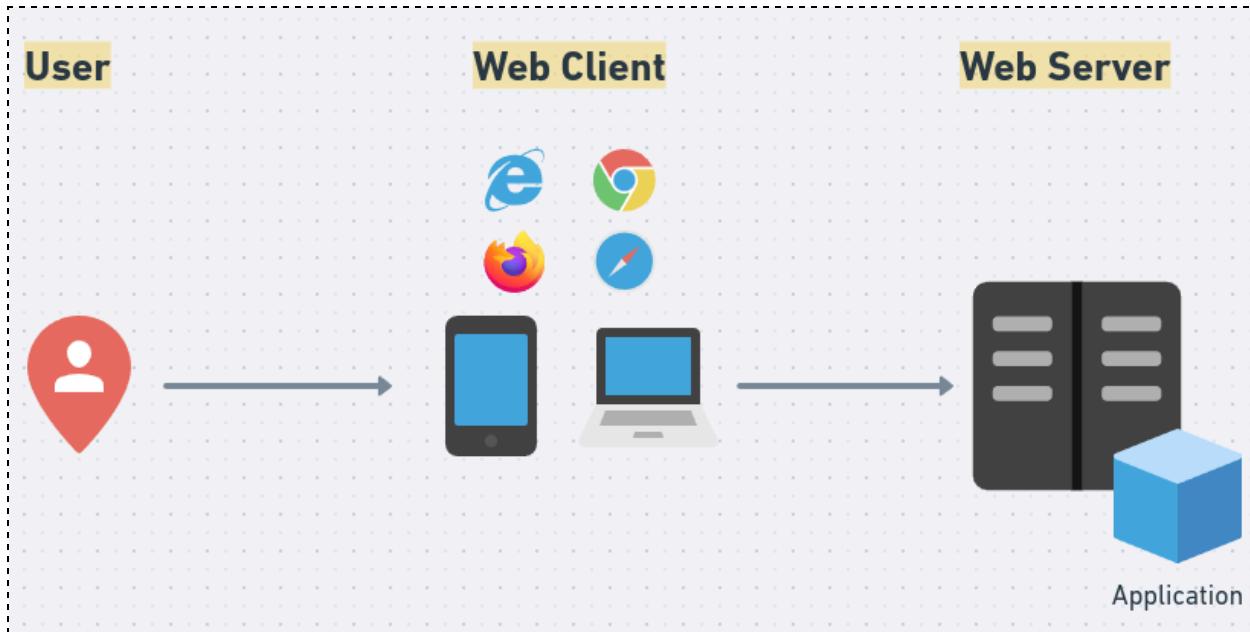


- اشتريت server .. كمبيوتر قوي جدا ومستغلتش امكانياته كلها يبقى كدا غلط
- ال Hypervisor عبارة عن Software .. من خلال ال Hypervisor اللي هو المحاكي او ال Emulator بنتشارك ال VM فى ال Virtual Machines اللي تحت VMware , Virtual box , HyperV ومن امثاله
- وانت بتكريت ال VM اللي فوق دي بتحددها ال Storage وال Ram وكل حاجة من ال hardware اللي تحتاجها لانك بتكون عارف ال VM دي هينزل عليها تطبيقات اية بالضبط وعارف هيا عاوزة متطلبات اية
- كل ال VM دي بتقى معزولة عن بعضها .. يقدرو يتكلمو من خلال ال network لو انت سامح لهم ب دة.



I'm Here

- **Web Application:**



- هي الاجهزة اللى ال user بيخش من خلالها عال web clients

- هو ال server اللى بيستضيف ال Application بتاعنا .. ياعني لو

ال server دة معانا ال ip بتاعه ودخلنا عليه هيدخلنا علطول عال Application

- اشهر تطبيقات web server ف ويندوز iis وف لينكس apache , nginx

- عشان تبع ملفاتك لـ server البعيد دة بتسخدم اي software من ال FTP زى

filezilla

- **After Access URL:**

- ال url بيتتحول لـ ip عن طريق ال DNS

- ال ip دة بيروح للسيرفر اللى هو ف الحالة دي ويب سيرفر ومن ال ip بيعرف انت عاوز

انهي صفحة ويب او موقع ياعني ويا بيكون فيه السورس كود بتاعها او بي generate

ده ويعرضها لك.



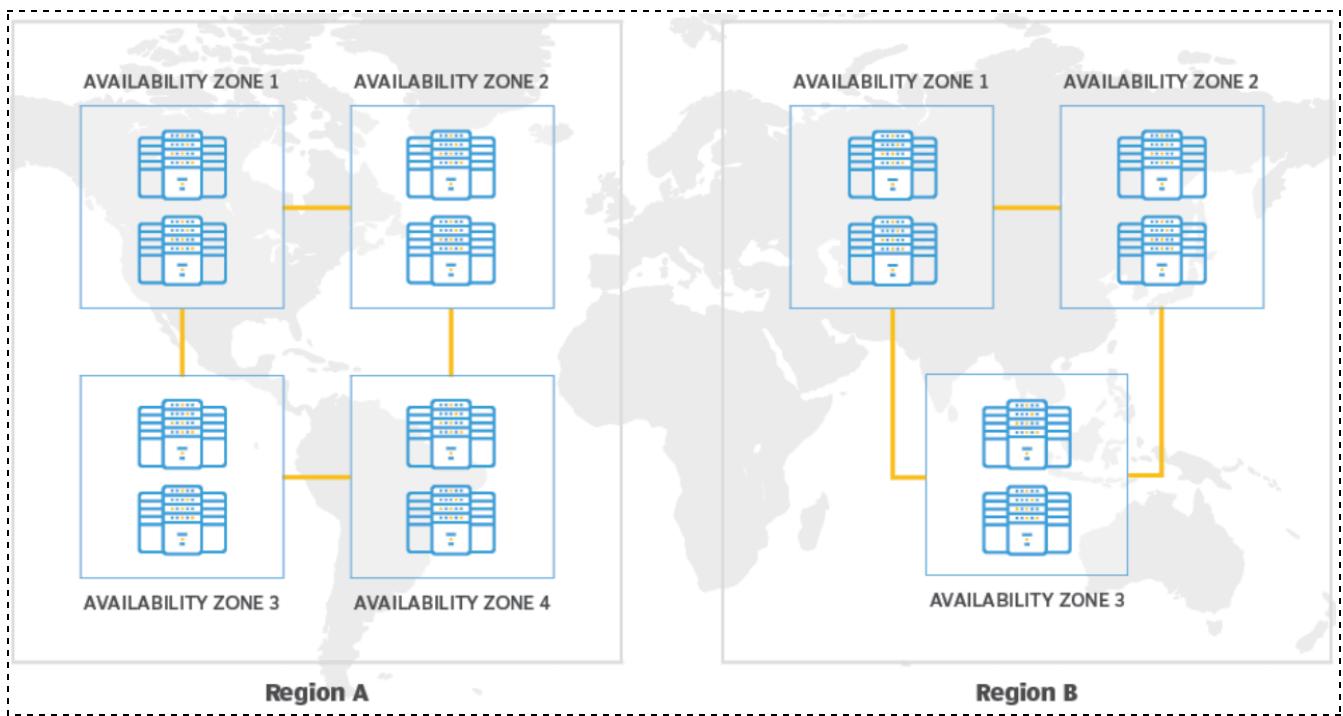
I'm Here

- **DNS & Hosts File:**

- ملف الهاوستس دة بيكون فيه الip بتاع الموقع بمعنى انا لو عندي موقع example.com ف بيكون في ملف الهاوستس دة لازم ليه ip معين بحيث مثلاً لو بنجت عليه هيرد عليا بالip دة او لو كتبتو لك url ف بيتحول عن طريق dns لنفس الip الموجود في ملف الهاوستس.

CH-03 - Getting started with AWS

➡ Region:



I'm Here

- منطقة جغرافية تكون جواها cluster of Availability Zones اللي بيكون جواها
- بتقى منتشرة فى العالم وكل region منفصلة عن الثانية وكل شوية بيظهر regions بتاعي applications اللي بـ deploy على data centers
- كل region بيقي ليها كود مثلا الكود بتاعها Sydney مثلا الكود بتاعها ap-southeast-2 جديدة بيحصل توسع يعني.

• بختار ال Region دي بناءا على الآتي:

• Latency

- لو عندي مثلا website و ال end user بتاعي اللي هيسخدم ال website من Europe ف latency sensitive applications or - Access end user زي ال video gaming or real time videos
- لو عندي مثلا website و هو بي Access ال website ف latency sensitive applications or - Access end user زي ال video gaming or real time videos تاخير عليه

• Services

- مش كل ال services فيها نفس ال regions ممكن تلقي service موجودة في region تانية مش موجودة وفي region تانية مش موجودة في region

• Cost

- مش كل ال services فيها نفس التكلفة ف كل ال regions .. تكلفة ال services بتختلف من region للتانية

• Compliance or Data Sovereignty (سيادة)

- ممكن دولة يكون ليها قوانين معينة تشترطبقاء ال data داخل حدود الدولة دي مينفعش تخرج براها.



I'm Here

➡ Availability Zones (AZ):

- عباره عن data centers او اكتر ومنفصلين عن بعضهم physically .. ومنفصلين وبعد عن بعض الى حد ما يكفي ان لو حصل كارثة زي مثلا زلزال او قطع تيار كهربى او كدا ال Availability Zones بتاعتي متتالش كلها .. اللي تقع الثانية تشيل مكانها وهكذا
- كل AZ ليها ال power,cooling and networking منفصلة.
- كل AZ تحتوي على عدد من ال Data Centers مش معروف
- بيكونو متوصلين ببعض بـ high bandwidth, ultra-low latency networking
- من 3 اقل حاجة ل 6 اقصى حاجة في كل region

• ف دة بيضمنك حاجتين من مميزات ال cloud :

● Disaster recovery:

- ان لو حصل failure ف ال services بتاعتي بقدر recover بشكل سريع و عن طريق ان بيكون عندي ال data center services دي في تاني ف automatic تانية AZ

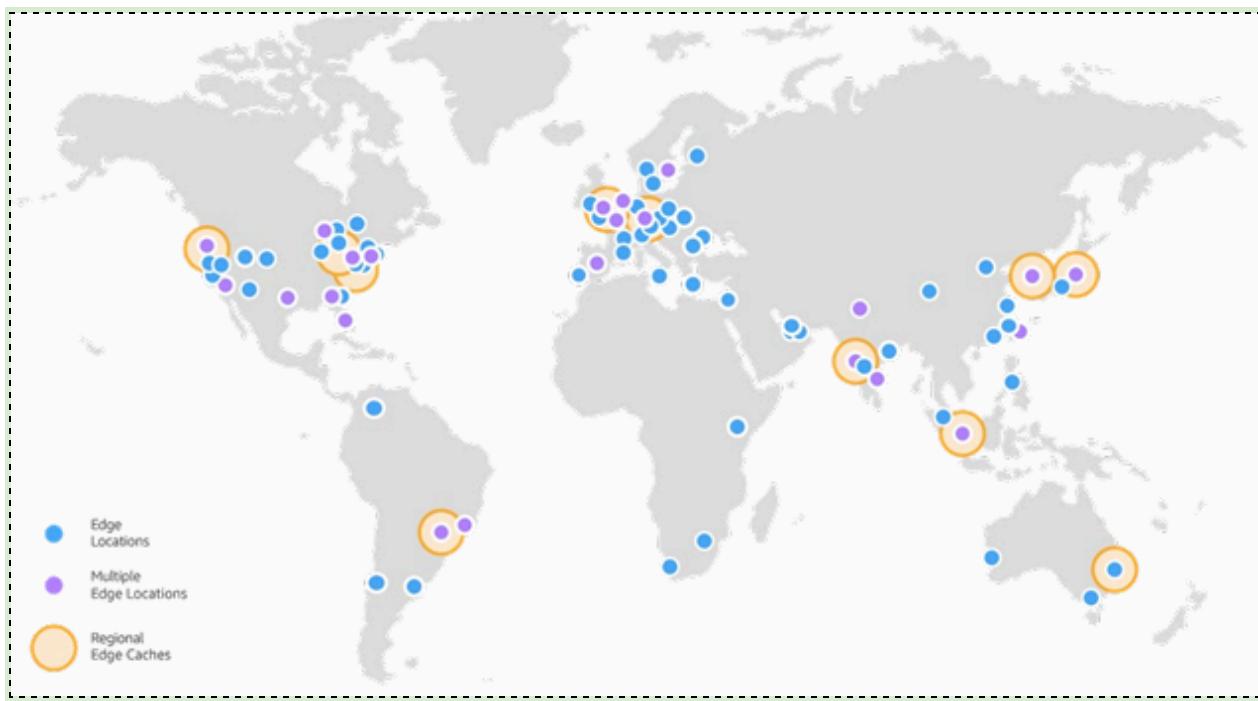
● Fault tolerance:

- ودي عباره عن ان لو عندي services ف مكان redundant زيها ف مكان تاني لو حصل مشكلة ف المكان الاولاني ال services اللي ف المكان الثاني بتاخذ مكانها من غير ما ال end user يحس



I'm Here

➡ AWS Points of Presence (Edge Locations)



- Amazon has 400+ Points of Presence (400+ Edge Locations & 10+ Regional Caches) in 90+ cities across 40+ countries.
 - Content is delivered to end users with lower latency.
-



I'm Here

CH-04 - IAM & AWS CLI

→ IAM Introduction (Identity and Access

Management): Users, Groups, Policies

عباره عن AWS موجودة فى Free Service نوعها -

ال services فى كل ال regions متاحة .. وفيه Global Services -

Services تانيه بتكون متاحة فى regions معينه بس عندك مثلا EC2 instance

لازم تحدد معاها ال Region علشان لو عملت Launch ل EC2 instance فى

معينه مش هتلقيها ف ال Region الثانية على عكس ال Region

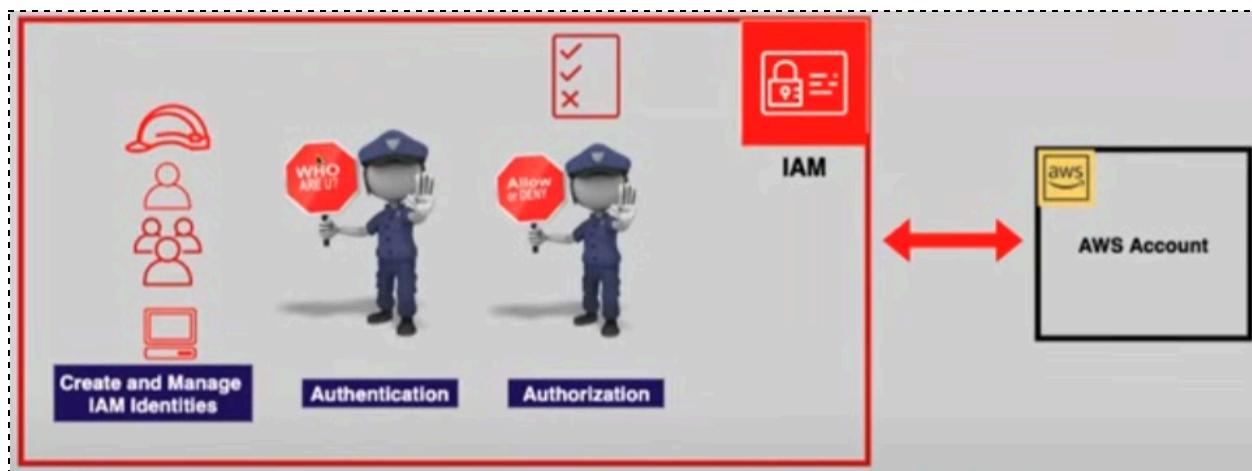
Services

بتمكنك من انك تكريت users & groups وتديمهم permissions وكدا -

انت بتحش بال Root User ولكن دة مش مفضل انك تستخدموه فى -

العادي يستخدم Admin Or Normal User

علشان تعرف ال Service دي متاحة عندك فى ال region ولا لا من [هنا](#) -



I'm Here

➡ IAM Users, Groups Hands ON.

Search >> IAM >> User Name (Stephan), Password >>
Permissions

Permissions options

- Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
- Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

i Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

Create group

► Set permissions boundary - *optional*

"نقدر تدخل ال user جروب انت عامله وال permissions فيه جاهزة او ت create"

"Attach Policy او ت Permissions ال Copy group"

"بما ان هنا مفيش Groups قديمة ف احنا هنكريت جروب جديد"



I'm Here

Create user group

Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

User group name
Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and '+,-,@,_' characters.

Permissions policies (1/884)

Filter by Type

Policy name	Type	Use...	Description
<input checked="" type="checkbox"/>  AdministratorAccess	AWS managed ...	None	Provides full access to AWS services

"في حالة بقى علنا Admin user وعازينو create group ف عملنا policy"

بتاعته خليناها Access يكون واحد كل ال Administrator Access عال

"Services

Permissions options

- Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
- Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1/1)

Group name	Users	Attached policies	Created
admin	0	AdministratorAccess	2023-10-24 (Now)



I'm Here

"كدا بقا الجروب جاهز .. ف ظهر لنا فى ال check groups عالجروب اللي لستة

عاملينه علشان نضيف ال user فيه."

"قدر وانت بتعمل ال user تضيف Tags ودي بتسهل عليه ت Access ال users مثلًا

".department, project, environment, or cost center : تقسمهم :

Search >> Users , User Groups

"هتلaci عندي بقا ال user وال permissions اللي واحدها اللي هيا بتاعة الجروب وهتلaci

ال Configurations اللي عندي وكل ال groups اللي انت عملتها وانت بت create

"user , group

AWS Account

Account ID

 219637129727

Account Alias

aws-stephane-v5 [Edit | Delete](#)

Sign-in URL for IAM users in this account

 <https://aws-stephane-v5.signin.aws.amazon.com/console>

"ال user اللي انت عملته بيكون ليه id و Account alias من خاللهم بتخشن بهم"

"password عالاكونت بجانب ال



I'm Here

Sign in

Root user
Account owner that performs tasks requiring unrestricted access. [Learn more](#)

IAM user
User within an account that performs daily tasks. [Learn more](#)

Account ID (12 digits) or account alias

Next

"بالنسبة لـ url دة من خلاة بيدخلك مباشر على ال user دة بتكون تحتاج ال password "id او ال alias بجانب ال

Amazon Web Services Sign-In

Sign in as IAM user

Account ID (12 digits) or account alias

IAM user name

Password

Remember this account

"دة بيكون شكل ال root اللي انت دخلت بيه فى البداية خالص .. Account ID فقط"



I'm Here

The screenshot shows the AWS IAM Dashboard. On the left, a sidebar titled "AWS Account" displays the Account ID (219637129727), Account Alias (aws-stephane-v5 with Edit | Delete link), and a Sign-in URL (https://aws-stephane-v5.signin.aws.amazon.com). The main content area has a dark header with "Account", "Organization", "Service Quotas", "Billing Dashboard", and "Security credentials". A "Sign out" button is located in the bottom right corner. The top navigation bar includes the AWS logo, Services, search, and global settings.

"دء بيكون شكل ال IAM User"

The screenshot shows the AWS Console Home. The top header displays the Account ID (219637129727) and IAM user (stephane). The main content area features a "Recently visited" section with a large cube icon and a message stating "No recently visited services". Below this, there's a link to explore commonly visited AWS services (IAM, EC2, S3, RDS, Lambda). The right sidebar is identical to the one in the IAM dashboard, with links for Account, Organization, Service Quotas, Billing Dashboard, and Security credentials, along with a "Sign out" button.



I'm Here

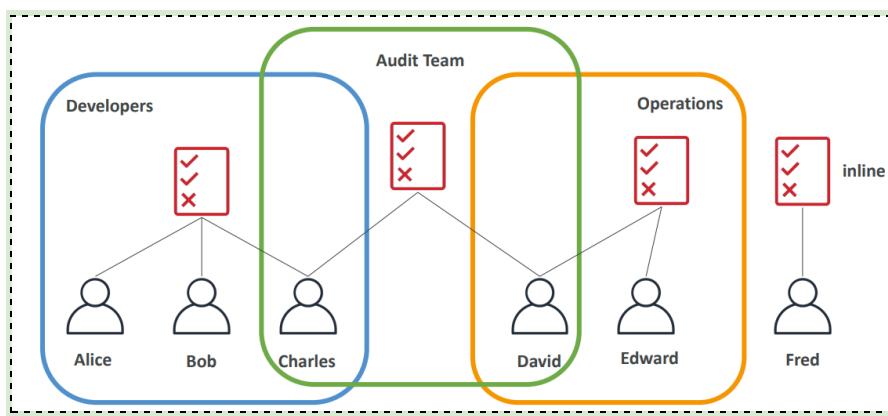
" ان حصلت مشكلة فى ال IAM Users Accounts هتهنلها من خلال ال Root الاصلي ..

إنما لو حصلت مشكلة فى ال Root Account مشكلة كبيرة وهتكلم ال ".Support

" من خلال ال Root user تقدر ت delete stephane user وميكونش ليه access على

"اي حاجة"

➡ IAM Policies:



عبارة عن User & Group Permissions لـ JSON Files -

ال Policy اللي واحدها الجروب بتطبق علي كل user فيه . -

• Policy Structure:

ب يكون عباره عن permissions define .. من خلالة بت JSON file و بت

ال resources allowed or denied هل actions specify معينه .. ال

ده بيكون من : Structure



I'm Here

```

{
  "Version": "2012-10-17",
  "Id": "S3-Account-Permissions",
  "Statement": [
    {
      "Sid": "1",
      "Effect": "Allow",
      "Principal": {
        "AWS": ["arn:aws:iam::123456789012:root"]
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": ["arn:aws:s3:::mybucket/*"]
    }
  ]
}

```

- Version :**

دة 17-10-2012 policy language version - دة حاليا ودة

- ID (Optional):**

عبارة عن identifier لـ policy -

- Statement:**

تحتوي على rule او اكثر ال Statement عبارة عن rule وتحتوي على -
كذا عنصر:

- **SID (Optional):**

عبارة عن identifier لـ Statement -

- **Effect:**

هل ال Allow or Deny دي Statement -

- **Action:**

ال account or user or which role ال policy الى ال يطبق عليه -



I'm Here

- **Resources:**

- ال Resources اللى ال Actions هتطبق عليها.

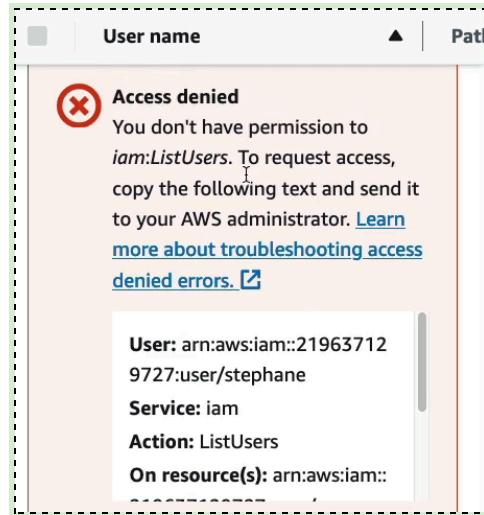
- **Condition(Optional):**

- شروط تفعيل ال policies دي.

➡IAM Policies Hands On:

"لو شيلت stephane من ال group admin permissions كدا هيفقد ال admin permissions اللي كان واحدها

لانها تبع الجروب.. ف مش هيقدر مثلا انو ي list users



Users >> Stephane >> Permissions



I'm Here

The screenshot shows the 'Permissions' tab of the AWS IAM user configuration page. At the top, there are tabs for 'Permissions', 'Groups', 'Tags (1)', 'Security credentials', and 'Access Advisor'. Below the tabs, the heading 'Permissions policies (0)' is displayed, followed by the sub-instruction: 'Permissions are defined by policies attached to the user directly or through groups.' A search bar labeled 'Search' is present. On the right, a context menu is open over a button labeled 'Add permissions' with the option 'by Type' selected. Other options in the menu include 'Create inline policy' and 'Types'. Below the menu, there are columns for 'Policy name' (with a search icon), 'Type', and 'Attached via ...'. A message 'No resources to display' is shown at the bottom.

"قدر من تاني تحط ال **اللى انت عاوزها** لل permissions "user stephane

The screenshot shows the 'Permissions options' dialog box. It contains three radio button options: 'Add user to group' (selected), 'Copy permissions', and 'Attach policies directly'. The 'Add user to group' option is described as adding the user to an existing group or creating a new one, with a recommendation to manage permissions by job function. The 'Copy permissions' option is described as copying all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user. The 'Attach policies directly' option is described as attaching a managed policy directly to a user, with a recommendation to attach policies to a group instead.

"قبل كدا دخلناه جروب وخد ال **permissions** بتاعته **اللى كانت** Administration

"read only policy .. ول يكن **permissions** **Attach policies** دلوقتى هن



I'm Here

Permissions policies (1132)				
Filter by Type				
	Search	All types		
			< 1 2 3 4 5 6 7 ... 57 >	⚙️
<input type="checkbox"/>	Policy name ↗	Type	Attached e...	▼
<input type="checkbox"/>	 AccessAnalyzerSer...	AWS managed	0	
<input type="checkbox"/>	 AdministratorAccess	AWS managed - job f...	1	
<input type="checkbox"/>	 AdministratorAcce...	AWS managed	0	
<input type="checkbox"/>	 AdministratorAcce...	AWS managed	0	
<input type="checkbox"/>	 AlexaForBusinessD...	AWS managed	0	

Permissions policies (1/1132)				
Filter by Type				
	Search	All types		
	iamre	All types	1 match	⚙️
<input checked="" type="checkbox"/>	Policy name ↗	Type	Attached e...	▼
<input checked="" type="checkbox"/>	 IAMReadOnlyAccess	AWS managed	0	

"بعد ما خد ال users list كدا يقدر ي list readonly permission staphane مثلًا.. لو
جيت ب الـ stephane واحد ت嘗لـ create group readonly permission مش هينفع."



I'm Here

<input type="checkbox"/>	Policy name	Type	Attached via
<input type="checkbox"/>	AdministratorAccess	AWS managed - job f...	Group admin
<input type="checkbox"/>	AlexaForBusinessD...	AWS managed	Group developers
<input type="checkbox"/>	IAMReadOnlyAccess	AWS managed	Directly

"ب يكون واصحلك انت واحد permissions اية ومن انهي groups بالضبط ولو directly ف دة اللى root مديهولك ال root مديي ل stephane وهو بيكرية".readonly permission

IAM >> Policies >> AdministratorAccess

The screenshot shows the AWS IAM Policies page. On the left, the navigation menu is visible with 'Policies' selected, indicated by a green checkmark. The main pane displays a list of policies. The 'AdministratorAccess' policy is highlighted with a green arrow pointing to its name in the list.

Policies (1130) <small>Info</small>					
A policy is an object in AWS that defines permissions.					
<input type="button"/> C	<input type="button"/> Actions	<input type="button"/> Delete	<input type="button"/> Create policy	Filter by Type	
<input type="text"/> Search		<input type="button"/> All types		<input type="button"/>	
< 1 2 3 4 5 6 7 ... 57 > <input type="button"/>					
	Policy name	Type	Use...	Des...	
<input type="radio"/>	AccessAnalyzerSer...	AWS managed	None	All	
<input type="radio"/>	AdministratorAccess	AWS managed ...	Permis...	Pro	
<input type="radio"/>	AdministratorAcce...	AWS managed	None	Gra	



I'm Here

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Summary

JSON

 Search

Allow (384 of 384 services)

Service	Access level	Resource
Access Analyzer	Full access	All resources
Account	Full access	All resources
Activate	Full access	All resources
Alexa for Business	Full access	All resources
AMP	Full access	All resources
Amplify	Full access	All resources

"لما تخش على ال policies وتخش على واحدة منهم ول يكن AdministratorAccess هنلاقي

كل ال services اللي ال policy دي تقدر تحكم فيهـم وكمان اية نوع ال access اللي واحدـاه

"Full Access هنا مثلا



I'm Here

Permissions defined in this policy [Info](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

[Copy](#) [Summary](#) [JSON](#)

```

1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Action": "*",
7              "Resource": "*"
8          }
9      ]
10 }

```

"لو دخلت على JSON هتلaci محتوي ال Policy خاص بال JSON File يعني لو
تانية زي ما هنشوف تحت هتلaci محتوي تاني خصوصا فال statements لأن كل policy بـ
" مختلفة rules

هنا يعني ال JSON File دة .. بن على كل ال Allow any action .. ودة
فعلا ال اللي بيأخذو ال access ".AdministratorAccess"

Policies (1130) [Info](#)

A policy is an object in AWS that defines permissions.

[Actions](#) [Delete](#) [Create policy](#)

Filter by Type

Policy name	Type	Used as	Description
IAMReadOnlyAccess	AWS managed	Permissions	Provides read only access



I'm Here

"لو دخلت مثل على policy تانية زي IAMReadOnly هتلaci و اخدة access على service واحدة"

The screenshot shows the 'Permissions defined in this policy' section of an IAM policy. It includes tabs for 'Summary' (selected) and 'JSON'. A search bar is present. The main area shows one service permission: 'Allow (1 of 384 services)' for the 'IAM' service with 'Full: List Limited: Read' access level and 'All resources' as the resource. A link 'Show remaining 383 services' is available.

"لو دخلت عال service دي هتو ضحلك اية بالظبط اللي اقدر أ read only عليه.. اية هيا ال API Calls اللي مسموح بيها"



I'm Here

Action	Resource
GetAccountSummary	All resources
GetLoginProfile	All resources
ListAccessKeys	All resources
ListAccountAliases	All resources
ListAttachedGroupPolicies	All resources
ListAttachedRolePolicies	All resources
ListAttachedUserPolicies	All resources
ListCloudFrontPublicKeys	All resources
ListEntitiesForPolicy	All resources
ListGroupPolicies	All resources
ListGroups	All resources

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

[Copy](#) [Summary](#) [JSON](#)

```

1  [
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Effect": "Allow",
6        "Action": [
7          "iam:GenerateCredentialReport",
8          "iam:GenerateServiceLastAccessedDetails",
9          "iam:Get*",
10         "iam>List*",
11         "iam:SimulateCustomPolicy",
12         "iam:SimulatePrincipalPolicy"
13       ],
14       "Resource": "*"
15     }
16   ]
17 ]
```

"هنا فال JSON File محتوي ال policy مختلف عن اللي فاتت read only policy وهذا."



I'm Here

"list" دى نفس الكلام على Get users , Get Groups .. مثلا野 card * "Get

يبقى الخلاصة : دة الترتيب 

IAM >> Policies >> One Of The Tolices >> services can access by the policy , json file content

IAM >> Policies >> Create Policy

Policies (1130) [Info](#)

A policy is an object in AWS that defines permissions.

[C](#) [Actions ▾](#) [Delete](#) [Create policy](#)

Filter by Type

[All types ▾](#)

ممكن انت ت Create ال policy الخاصة بيك .. هتلقي عندك visual editor or json

"editor



I'm Here

The image displays two screenshots of the AWS Policy Editor interface. The top screenshot shows the 'Select a service' section, which allows specifying what actions can be performed on specific resources in a service. It includes a dropdown menu labeled 'Choose a service' and a button to 'Add more permissions'. The bottom screenshot shows the 'IAM' section, which sets permissions for IAM. It includes a search bar for actions, a radio button for 'Effect' (set to 'Allow'), and buttons for 'Filter Actions', 'Manual actions | Add actions', and 'All IAM actions (iam:*)'.

"وبختار بقا ال service ثم ال actions وهكذا"

و بالنسبة لـ JSON .. نفس الكلام



I'm Here

```

1 {  

2     "Version": "2012-10-17",  

3     "Statement": [  

4         {  

5             "Sid": "Statement1",  

6             "Effect": "Allow",  

7             "Action": "☐",  

8             "Resource": "☐"  

9         }  

10    ]  

11 }

```

The screenshot shows the AWS IAM Policy editor interface. On the left, there's a code editor window displaying a JSON policy document. The policy contains one statement that allows access to a specific resource. On the right, there's a sidebar with options like 'Edit statement', 'Remove', 'Add actions', and a dropdown menu for 'Choose a service' which lists various AWS services.

"وبعدها بقا تحط لل policy name & description وهكذا"

➡ IAM – Password Policy

- **Passwords:**

IAM >> Account Setting >> Edit Password Policy

- تقدر تحدد لـ users الـ passwords بتاعتهم لازم يكون شكلها عامل ازاي
- تقدر تحدد المدة اللى لازم يغورو فيها الـ passwords دي
- تقدر تمنع انهم يعiendo استخدام passwords قديمة

- **Multi Factor Authentication - MFA**

عياره عن password معاك device محفوظ جوا



I'm Here

- تقدر تطبق ال Multi Factor Authentication عن طريق تطبيقات زي Google او من خلال Physical Devices او من خلال Authy او Authenticator

Virtual MFA device	Universal 2nd Factor (U2F) Security Key
 Google Authenticator (phone only)	 YubiKey by Yubico (3 rd party)
Support for multiple tokens on a single device.	Support for multiple root and IAM users using a single security key

Hardware Key Fob MFA Device	Hardware Key Fob MFA Device for AWS GovCloud (US)
 Provided by Gemalto (3 rd party)	 Provided by SurePassID (3 rd party)

→IAM MFA Hands ON

- **Passwords Policy:**

IAM>> Access Management >> Account Setting >> Password



I'm Here

Policy >> Edit

تقدر تستخدم ال IAM Default بالشكل دة

Password policy

IAM default

Default password requirements for IAM users.

Custom

Use a customized password policy.

Password minimum length

8 characters

Password strength

Include a minimum of three of the following mix of character types:

- Uppercase
- Lowercase
- Numbers
- Non-alphanumeric characters (! @ # \$ % ^ & * () _ + - = [] { } | ')

Other requirements

- Never expire password
- Must not be identical to your AWS account name or email address

أو ت انت ال Password Policy الخاصة بيك بحيث تستخدمها بعدين.



I'm Here

Password policy

IAM default
Default password requirements for IAM users.

Custom
Use a customized password policy.

Password minimum length.
Enforce a minimum length of characters.
 characters
Needs to be between 6 and 128.

Password strength

Require at least one uppercase letter from the Latin alphabet (A-Z)
 Require at least one lowercase letter from the Latin alphabet (a-z)
 Require at least one number
 Require at least one non-alphanumeric character (! @ # \$ % ^ & * () _ + - = [] 0 | ')

Other requirements

Turn on password expiration
 Password expiration requires administrator reset
 Allow users to change their own password
 Prevent password reuse

● Assign MFA:

Account Name >> Security Credentials

My security credentials (root user) Info

The root user has access to all AWS resources in this account, and we recommend following [best practices](#). To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

⚠ MFA not activated for root user
The root user for this account does not have multi-factor authentication (MFA) activated. Activate MFA to improve security for this account.

Assign MFA

Device name , Device Type بت ایل Assign MFA من خالل



I'm Here

ودي ال Authenticating Apps تقدر تستخدموها لو مش معاك device

Android	Twilio Authy Authenticator , Duo Mobile , LastPass Authenticator , Microsoft Authenticator , Google Authenticator , Symantec VIP
iOS	Twilio Authy Authenticator , Duo Mobile , LastPass Authenticator , Microsoft Authenticator , Google Authenticator , Symantec VIP

لو قفلت ال acc root وجيت تفتح تاني هيطلب منك MFA Code هتجبيه من خلال التطبيق او الجهاز ايا كان يعني .. لو التطبيق او الجهاز ضاعو هتبقي مشكلة كبيرة.

➡ AWS Access Keys, CLI and SDK:

- اتعاملنا مع AWS من خلال ال Management Console من خلال المتصفح يعني.. وعندك طريقتين كمان هما ال CLI وال SDK والاتنين علشان نشتغل منهم لازمنا Access Keys

Access keys			
Access key ID	Created	Last used	Status
AKIASK4E37PV4TU3RD6C	2020-05-25 15:13 UTC+0100	N/A	Active Make inactive X

ال Access Key بتاعك انت بس ميخرجش بره.



I'm Here

• **SDK (Software Development Kit):**

- عبارة عن مجموعة من الـ libraries & tools يقدرو يستخدموهم Developers اللى
- وهما بيكتبوا كود لـ Applications بتاعتهم بحيث يقدرو يخلو الـ Applications interact مع AWS Services
- **DevOps and CI/CD:** SDKs are used in continuous integration and continuous deployment (CI/CD) pipelines to automate the deployment and management of applications on AWS

مثال على استخدام SDK هو الـ CLI اللى هنستخدمه فى اتنان AWS كمان 

شوية .. دة مبني على AWS SDK For Python واسمو 3 boto3

➡AWS CLI Hands On:

Users >> Stephane >> Security Credentials >> Access Keys >>
Create Access Key



I'm Here

Access key best practices & alternatives Info

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Use case

Command Line Interface (CLI)

You plan to use this access key to enable the AWS CLI to access your AWS account.

Local code

You plan to use this access key to enable application code in a local development environment to access your AWS account.

Application running on an AWS compute service

You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

Third-party service

You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

Application running outside AWS

You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.

Create access key ×

✓ Success

This is the **only** time that the secret access keys can be viewed or downloaded. You cannot recover them later. However, you can create new access keys at any time.

Download .csv file

Access key ID	Secret access key
AKIA4OHDCKKLTZNZBRUT Copy	D32MzVn1lqqrPPYxvWAtvxoMltO3ft6l/Dyan6PF Hide

Close

بعد ما وصلت لـ Access Key ول يكن بعد ما اخترت CLI بتروح بقا على ال terminal

علشان تربط الاثنين بعض



I'm Here

```
~ ➔ aws configure
AWS Access Key ID [None]: AKIA40HDCKKLTNZBRUT
AWS Secret Access Key [None]: D32MzVn1IqqrPPYxvWAtvxoMlt03ft6I/Dyan6PF
Default region name [None]: eu-west-1
Default output format [None]:
~ ➔ aws iam list-users
```

```
{
  "Users": [
    {
      "Path": "/",
      "UserName": "stephane",
      "UserId": "AIDA40HDCKKLSE4HHDCOE",
      "Arn": "arn:aws:iam::855174697623:user/stephane",
      "CreateDate": "2020-05-27T16:28:16+00:00",
      "PasswordLastUsed": "2020-05-27T16:33:03+00:00"
    }
  ]
}
(END)
```

بت Configure .. وبالنسبة لـ Region بختار الاقرب ليك.

من خلال ال commands تقدر تعمل بقا كل اللي كنت بتعملو على aws management

console قبل كدا

لو شيلت ال user اللي هو stephane من جروب ال admins يعني مبقاش واحد اي 

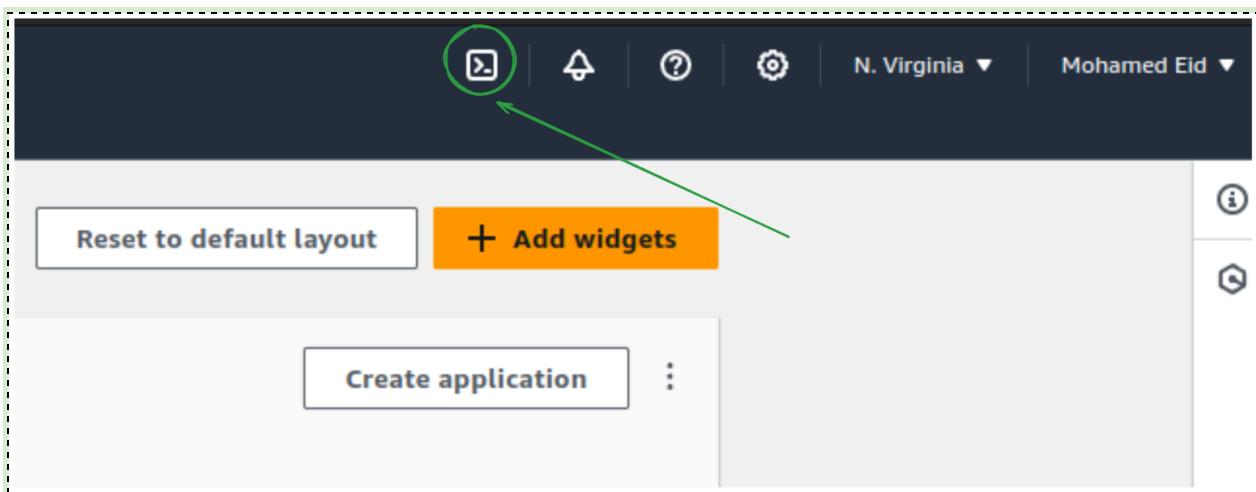
list the command terminal نفس ال وجيit فى ال permissions

users هتلافقى انو مديكش نتيجة وده حصل مباشره.



I'm Here

➡ AWS CloudShell:



```
aws Services ▾ Search for services, features, marketplace products, and docs [Option+S]
☒ AWS CloudShell
eu-central-1
Preparing your terminal...
[cloudshell-user@ip-10-0-184-1 ~]$ Try these commands to get started:
aws help or aws <command> help or aws <command> --cli-auto-prompt
[cloudshell-user@ip-10-0-184-1 ~]$ aws
```

A screenshot of the AWS CloudShell terminal window. The title bar says "AWS CloudShell" and "eu-central-1". The main area shows the AWS CLI preparing the terminal environment. It includes a search bar at the top and a command prompt at the bottom.

- Terminal عادي خالص على AWS وبيكون متاح فى بعض ال regions تقدر تشوفهم

من هنا

- repository عادي ياعني لو انشأت file هتلاقيه موجود متخزن وتقدر تعمله

terminal download وتعمل upload وهذا اكناك فاتح terminal عادي.

- terminal على جهازي افضل اكيد.



I'm Here

➡ IAM Roles for AWS Services:

- Role ياعني دور ك ترجمه حرفيه .. ياعني هديك permission تقوم ب دور معين وغالبا بيكون الموضوع دة لمدة قصيرة ..
- لو عملت access على user list ال EC2 instance وجيت ت ال attach role مش هتلقيها واحده ال permission دة ف بنروح ن iam list-users ليها تكون ليها policy allow read only وبالتالي تقدر ت list users .. ودي امتهن اكتر :

• Cross-Account Access

- شركة A عاوزه تدي Permission للأكونت بتاع شركة B إنو يقدر يستخدم الداتا اللي على ال S3 Bucket بتاع شركة A ف دة بيتم عن طريق ان شركة A تكريت role وتديها لاكونت شركة B .. ال role بتقى عباره عن policies ف بتحدد في ال انهى permission مسموح بيها.

• AWS Lambda Functions

- عاوزين نديها role دور ياعني تمكنا من انها يكون ليها ال Lambda function access DynamoDB tables اللي تخليها قادره ت perform operations مكنها انها permission service ادinyaها على some resources

• EC2 Instances and S3 Access

- عاوزين نخلي ال EC2 Instance اللي اسمها service قادره انها retrieve S3 Bucket ل configurations files & upload logs على تقدر تعمل دة



I'm Here

- **Most Common Roles:**

- EC2 Instance Roles
 - Lambda Function Roles
 - Roles for CloudFormation
-

➡ IAM Roles Hands ON:

Access Management >> Roles >> Create Role

Trusted entity type

AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

زي مانت شايف فيه كذا نوع ولكن هنشتغل حاليا على AWS Service



I'm Here

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case
EC2

Choose a use case for the specified service.

Use case

- EC2**
Allows EC2 instances to call AWS services on your behalf.
- EC2 Role for AWS Systems Manager**
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
- EC2 Spot Fleet Role**
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
- EC2 - Spot Fleet Auto Scaling**
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
- EC2 - Spot Fleet Tagging**
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
- EC2 - Spot Instances**
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.
- EC2 - Spot Fleet**
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.
- EC2 - Scheduled Instances**
Allows EC2 Scheduled Instances to manage instances on your behalf.

بعدها بتختار ال Service اللي عاوز تديها ال role

Permissions policies (1/882) Info

Choose one or more policies to attach to your new role.

Filter by Type			
<input type="text"/> IAMRe	<input type="button"/>	All types	1 match
<input checked="" type="checkbox"/> Policy name		Type	Description
<input checked="" type="checkbox"/> IAMReadOnlyAccess		AWS managed	Provides read only access to IAM via the ...

بعدها بت attach ال policy وليكن هندي ال .. كدا قادرة ت read EC2 IAMReadOnly

اي حاجة في IAM

بعدها بتحط ال role name , description وبكدا انت كريت ال role



I'm Here

Roles (3) <small>Info</small>			
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.			
<input type="button"/> C	Delete	Create role	
<input type="button"/>	Search		< 1 >
<input type="checkbox"/> Role name	▲	Trusted entities	Last activity
<input type="checkbox"/> AWS ServiceRoleForSupport		AWS Service: support (Service-Linked)	-
<input type="checkbox"/> AWS ServiceRoleForTrustedAdvisor		AWS Service: trustedadvisor (Service)	-
<input type="checkbox"/> DemoRoleForEC2		AWS Service: ec2	-

Permissions policies (1) <small>Info</small>			
You can attach up to 10 managed policies.			
<input type="button"/> C Simulate Remove Add permissions			
<input type="checkbox"/> Policy name	▲ Type	▼ Attached entities	▼
<input type="checkbox"/> IAMReadOnlyAccess	AWS managed	1	

ولو ضغطت عليها هتلaci ال permission اللي وآخذه اللي هو IAMReadOnly

➡ IAM Security Tools, Hands On:

- **IAM Credentials Report (account-level)**

عبارة عن report يتعلمك download من خلال الـ root يكون فيه معلومات عن كل الـ

users

Access Reports >> Credential Report



I'm Here

Credentials report of IAM users in this account Info

The credentials report lists all your IAM users in this account and the status of their various credentials. After a report is created, it is stored for up to four hours.

Credentials report

[Download credentials report](#)

No report created in the past 4 hours. A new report will be created.

● IAM Credentials Report Content

الاسم

نوع ال user

امتي اتكررت ال user

امتي اخر مرة ال password اتغير

هل فيه MFA ولا لا

امتي ال password هي expired وامتي المفروض هي تغير

A	B	C	D	E
1	user arn	user_creation_time	password_enabled	password_last_used
2	<root_account> arn:aws:iam::855174697623:root	2020-05-27T16:01:07+00:00	not_supported	2020-05-27T16:56:56+00:00
3	stephane arn:aws:iam::855174697623:user/stephane	2020-05-27T16:28:16+00:00	TRUE	2020-05-27T16:33:03+00:00
4				2020-05-27T16:33:03+00:00

F	G	H	I	J
1 password_last_changed	password_next_rotation	mfa_active	access_key_1_active	access_key_1_last_rotated
2 not_supported	not_supported	TRUE	FALSE	N/A
3 2020-05-27T16:28:17+00:00	N/A	FALSE	TRUE	2020-05-27T17:25:55+00:00
				N/A

● IAM Access Advisor (user-level)

بيوضلك اية ال services اللی ال user دة استخدمها وامتي استخدمها وكمان لما استخدمنا

كان واحد عليها permission اية .. زی تحت کدا واحد admin access



I'm Here

Access Management >> Users >> Access Advisor

Permissions Groups (1) Tags (2) Security credentials **Access Advisor**

Access Advisor shows the services that this user can access and when those services were last accessed. Review this data to remove unused permissions. [Learn More](#)

Allowed services (367)

IAM reports activity for services and management actions. [Learn more](#) about action last accessed information. To see actions, choose the appropriate service name from the list.

Service	Policies granting permissions	Last accessed
AWS Organizations	AdministratorAccess	Today
AWS Identity and Access Management	AdministratorAccess	Today
AWS Health APIs and Notifications	AdministratorAccess	Today
AWS User Notifications	AdministratorAccess	Today
Amazon EC2	AdministratorAccess	Today
AWS Resource Explorer	AdministratorAccess	Today

➡ IAM Summary:

- **Users:** mapped to a physical user, has a password for AWS Console
- **Groups:** contains users only
- **Policies:** JSON document that outlines permissions for users or groups
- **Roles:** for EC2 instances or AWS services
- **Security:** MFA + Password Policy
- **AWS CLI:** manage your AWS services using the command-line



I'm Here

- **AWS SDK:** manage your AWS services using a programming language
 - **Access Keys:** access AWS using the CLI or SDK
 - **Audit:** IAM Credential Reports & IAM Access Advisor
-

CH-05 - EC2 Fundamentals

➡AWS Budget Setup:

Your Name >> Billing And Cost Management

Billing and Cost Management home [Info](#) [Reset layout](#)

Cost summary [Info](#)

Month-to-date cost Access denied	Last month's cost for same time period Access denied
Total forecasted cost for current month Access denied	Last month's total cost Access denied

[View bill](#)

Cost monitor [Info](#)

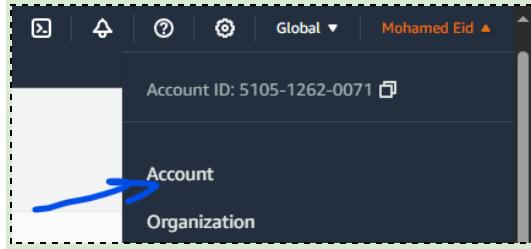
Budgets status Setup required No budget created	Cost anomalies status (MTD) Setup required No monitor created
---	---

هتلaciي انك معندكش Billing & Cost عال لانك فاتح من user عادي رغم
انك واحد واحد Administrator Access .. ف علشان نحل المشكلة دي لازم نفعل ال
root user دة من ال access



I'm Here

Open the root user >> Account



IAM user and role access to Billing information [Info](#) [Edit](#)

IAM user/role access to billing information

Deactivated

IAM user and role access to Billing information [Info](#) [Edit](#)

IAM user/role access to billing information

Activated

- وبعد activate ان ال user يقدر عادي تتحكم billing & cost access regular user فيهم من خلال ال

Billing and Cost Management home [Info](#) [Reset layout](#)

[Cost summary](#) [Info](#)

Month-to-date cost
\$0.00
↓ 0% compared to last month for same period

Total forecasted cost for current month
Access denied

Last month's cost for same time period
\$0.00
Dec 1 – 15, 2023

Last month's total cost
\$0.00

[View bill](#)

[Cost monitor](#) [Info](#)

Budgets status
Setup required
No budget created

Cost anomalies status (MTD)
Setup required
No monitor created

I'm Here

Billing And Cost Management >> Billing and Payments >> Bills >> Charges By services

<input type="checkbox"/> Elastic Compute Cloud		USD 0.00
<input checked="" type="checkbox"/> No Region		(USD 44.57)
<input type="checkbox"/> EU (Ireland)		USD 43.77
<input type="checkbox"/> Amazon Elastic Compute Cloud NatGateway		USD 39.43
\$0.048 per GB Data Processed by NAT Gateways	77.449 GB	USD 3.72
\$0.048 per NAT Gateway Hour	744 Hrs	USD 35.71
<input type="checkbox"/> EBS		USD 0.62
\$0.05 per GB-Month of snapshot data stored - EU (Ireland)	3.518 GB-Mo	USD 0.18
\$0.11 per GB-month of General Purpose SSD (gp2) provisioned storage	4 GB-Mo	USD 0.44
<input type="checkbox"/> Elastic IP Addresses		USD 3.72
\$0.00 per Elastic IP address not attached to a running instance for the month	1 Hrs	USD 0.00
\$0.005 per Elastic IP address not attached to a running instance per hour	743 Hrs	USD 3.72

- من خلالها تقدر تشفف كل ال Active Services وكل اشتغلت عليها

كلفتك فلوس قد اية

Billing And Cost Management >> Cost Analysis >> Free tier



I'm Here

AWS Free Tier (43) [Info](#)

Service	AWS Free Tier usage limit	Current usage	Forecasted usage	MTD actual usage
AWS Lambda	400000.0 seconds are always free per month as part of AWS Free Usage Tier (Global-Lambda-GB-Second)	400,000 seconds	826,667 seconds	<div style="width: 200px; height: 10px; background-color: red;"></div>
Amazon Simple Queue Service	1000000.0 Requests are always free per month as part of AWS Free Usage Tier (Global-Requests)	1,000,000 Requests	2,066,667 Requests	<div style="width: 200px; height: 10px; background-color: red;"></div>
AWS X-Ray	100000.0 Traces are always free per month as part of AWS Free Usage Tier (Global-XRay-TracesStored)	100,000 Traces	206,667 Traces	<div style="width: 200px; height: 10px; background-color: red;"></div>
AmazonCloudWatch	10.0 Alarms are always free per month as part of AWS Free Usage Tier (Global-CW:AlarmMonitorUsage)	10 Alarms	21 Alarms	<div style="width: 200px; height: 10px; background-color: red;"></div>
AWS Lambda	1000000.0 Request are always free per month as part of AWS Free Usage Tier (Global-Request)	646,310 Request	1,335,707 Request	<div style="width: 200px; height: 10px; background-color: blue;"></div>

- من خلالها تقدر تتبع استخدمك الحالي والمتوقع لو فاتح free tier acc

Billing And Cost Management >> Budget And Planning >> Budgets

Templates - new

Choose a template that best matches your use case.

Zero spend budget

Create a budget that notifies you once your spending exceeds \$0.01 which is above the AWS Free Tier limits.

Monthly cost budget

Create a monthly budget that notifies you if you exceed, or are forecasted to exceed, the budget amount.

Daily Savings Plans coverage budget

Create a coverage budget for your Savings Plans that notifies you when you fall below the defined target.

Daily reservation utilization budget

Create a utilization budget for your reservations that notifies you when you fall below the defined target.



I'm Here

⌚ Your budget My Zero-Spend Budget has been created successfully.

[Submit feedback](#)

Billing and Cost Management > Budgets > Overview

Overview Info

Budgets (1) <small>Info</small>								
		Download CSV		Actions		Create budget		
<input type="text"/> Find a budget		Type - Show all budgets		< 1 >				
<input type="checkbox"/>	Name	▲	Thresholds	▼	Budget	Amount u...	Forecaste...	Current vs. budgeted
<input type="checkbox"/>	My Zero-Spend Budget		\$1.00	-	-	-	0.0	

من خالها تقدر تكريت \$0.01 لو تعديت Budget setup ي notify you . alert .. ويكتب ال email بتابعك اللي هيعتاك عليه ال free tier account .

Zero spend budget
 Create a budget that notifies you once your spending exceeds \$0.01 which is above the AWS Free Tier limits.

Monthly cost budget
 Create a monthly budget that notifies you if you exceed, or are forecasted to exceed, the budget amount.

Daily Savings Plans coverage budget
 Create a coverage budget for your Savings Plans that notifies you when you fall below the defined target.

Daily reservation utilization budget
 Create a utilization budget for your reservations that notifies you when you fall below the defined target.

Monthly cost budget - Template

Budget name

Provide a descriptive name for this budget.

My Monthly Cost Budget (\$10)

Names must be between 1-100 characters.

Enter your budgeted amount (\$)

Last month's cost: \$94.85

10.00

Email recipients

Specify the email recipients you want to notify when the threshold has exceeded.

Separate email addresses using commas

بالنسبة لـ monthly بتحدله انت عاوز تدفع كام هنا \$10 خلال الشهر .



I'm Here

i You will be notified when 1) your **actual spend** reaches 85% 2) your **actual spend** reaches 100% 3) if your **forecasted spend** is expected to reach 100%.

هیعنی لك mail لو صرفت 85% من ال \$10 ولو وصلت 100% او لو المتوقع

%100 توصل

Overview Info

Budgets (2) <small>Info</small>						
		Thresholds	Budget	Amount u...	Forecaste...	Current vs. budgeted
<input type="checkbox"/>	Name	▲ Thresholds	\$10.00	-	-	0.0
<input type="checkbox"/>	My Monthly Cost Budget (\$10)	OK	\$10.00	-	-	0.0
<input type="checkbox"/>	My Zero-Spend Budget	⚠ Exceeded (1)	\$1.00	\$29.83	\$86.40	2982.6

- لما بتعدي ال budget بتتحول للشكل دا

➡ EC2 Basics:

- EC2 = Elastic Compute Cloud = Infrastructure as a Service

• عباره عن service من خللها تقدر :

- تاجر EC2 << virtual machines

- تخزن EBS << Virtual Drives على Data

- توزع ال load من خلل ELB machines

- ت Scale Services من خلل ASG << auto-scaling group



I'm Here

● EC2 sizing & configuration options

- Operating System (OS): Linux, Windows or Mac OS
 - How much compute power & cores (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 (configure at first launch): EC2 User Data
-

pass : عباره عن AWS mechanism فى من خلالة بـ **User Data** -

وهيابـتـ launch فى configurations or commands لـ EC2 Instance

الغالب بتكون فى شكل shell script

لما Run Commands process معناها انك تـ **Bootstrapping** -

الـ machine تـ run دة بي Script واحدة بس لـ machine الـ

start تـ

bootstrapping يبقى الـ User data بـ script فيه الـ بـتـاعـي الـى بـيـتـنـفـدـ من خـلـالـ الـ 

لـ machine start تـ



I'm Here

User data Info

```
#!/bin/bash
# Use this for your user data (script from top to bottom)
# install httpd (Linux 2 version)
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
echo "<h1>Hello World from $(hostname -f)</h1>" > /var/www/html/index.html
```

• ال Script دة بيكون عباره عن :

- Install updates , softwares
- Download something from the internet or any thing you can think of

كل ما كان ال Script اللي بيتنفذ اثناء ال boot time اكبر كل ما ال instance هتاخذ

وقت علي ما تـ launch

ال Script دة بيتنفذ من خلال ال root user يعني في ال script هتشتغل as sudo

- عندك انواع كتير من ال EC2 Instances دول امثله لهم.

- ال t2.micro اللي هنشتغل عليه وفي ال free tier بيتيحلك 750 hour / month



I'm Here

➡ Create An EC2 Instance with EC2 User Data to have a website Hands On:

هیكريت Instance زى ما عملنا فى ال و cloud practitioner user data علىها من خلال ال

لوا عملت Stop لى Instance و جيت شغلتها تانى هتلaci ال IPV4 اتغير ف خلي بالك.

➡ EC2 Instances Types:

- هتلaci كل الانواع وكل اللى محتاج تعرفه عنهم [هنا](#)

PAGE CONTENT

General Purpose

M7g M7i M7i-flex M7a Mac M6g M6i M6in M6a M5 M5n M5zn M5a

M4 T4g T3 T3a T2

Compute Optimized

Memory Optimized

Accelerated Computing

Storage Optimized

HPC Optimized

Instance Features

Measuring Instance Performance

[Amazon EC2 M5 instances](#) are the latest generation of General Purpose Instances powered by Intel Xeon® Platinum 8175M or 8259CL processors. These instances provide a balance of compute, memory, and network resources, and is a good choice for many applications.

Features:

- Up to 3.1 GHz Intel Xeon Scalable processor (Skylake 8175M or Cascade Lake 8259CL) with new Intel Advanced Vector Extension (AVX-512) instruction set
- New larger instance size, m5.2xlarge, offering 96 vCPUs and 384 GiB of memory
- Up to 25 Gbps network bandwidth using Enhanced Networking
- Requires HVM AMIs that include drivers for ENA and NVMe
- Powered by the [AWS Nitro System](#), a combination of dedicated hardware and lightweight hypervisor
- Instance storage offered via EBS or NVMe SSDs that are physically attached to the host server
- With M5d instances, local NVMe-based SSDs are physically connected to the host server and provide block-level storage that is coupled to the lifetime of the M5 instance
- New 8xlarge and 16xlarge sizes now available.

Instance Size	vCPU	Memory (GiB)	Instance Storage (GB)	Network Bandwidth (Gbps)***	EBS Bandwidth (Mbps)
m5.large	2	8	EBS-Only	Up to 10	Up to 4,750
m5.xlarge	4	16	EBS-Only	Up to 10	Up to 4,750

● m5.2xlarge

Class : تشير إلى ال m -



I'm Here

5 : تيشر إلى الـ AWS hardware بتطور الـ generation .. هتلaci m5 , m6 m7 generations جديدة ف هتلaci size 2xlarge : بتيسير إلى الـ size هتلaci عندك 4x , 8x , 12x و هكذا .

• هتلaci ان AWS مقساماك الأنواع دي على حسب غرضك :

General Purpose : مناسب لـ work loads زي الـ load balancers CPU , Memory , Networking و فيه balance code repository

General purpose النوع اللي هتستخدمه اللي هو T2 من الـ

Compute Optimized : بستخدمها لـ Applications اللي بحتاج media transcoding زي الـ performance processing

Memory Optimized : بستخدمها لـ Applications اللي بحتاج High Memory ف الـ performance

Storage Optimized : بستخدمها لـ Applications اللي بحتاج Storage ف الـ performance

Accelerated Computing : بستخدمها لو تحتاج اعمل machine learning او graphic workloads او complex calculations



I'm Here

مقارنة بسيطة:

Instance	vCPU	Mem (GiB)	Storage	Network Performance	EBS Bandwidth (Mbps)
t2.micro	1	1	EBS-Only	Low to Moderate	
t2.xlarge	4	16	EBS-Only	Moderate	
c5d.4xlarge	16	32	1 x 400 NVMe SSD	Up to 10 Gbps	4,750
r5.16xlarge	64	512	EBS Only	20 Gbps	13,600
m5.8xlarge	32	128	EBS Only	10 Gbps	6,800

t2.micro is part of the AWS free tier (up to 750 hours per month)

- ودة [Website](#) بقارن بين كل الانواع والاسعار

➡ Security Group & Classic Ports Overview

- أكنو Virtual Firewall يكون على ال EC2 instances بتاعتكم وببي control

- انت بتحدددها بتخليك تتحكم ف inbound and outbound traffic

- وهكذا protocols,ports and source/destination ip

- هتلaciي ان outbound traffic are allowed كل ال by default ياعني تقدر

- تكلم اي حد بره

- هتلaciي ان inbound traffic are denied كل ال by default وف الحالة دي

- بتحدد ازاي هتعامل مع ال inbound roles من خلال ال rules اللي بتحطها ول يكن

- مثلا:

● Example:

- حاطط rules بتسمح ب port 80 اللي جاي علي http traffic

- حاطط rules بتسمح ب port 443 اللي جاي علي https traffic

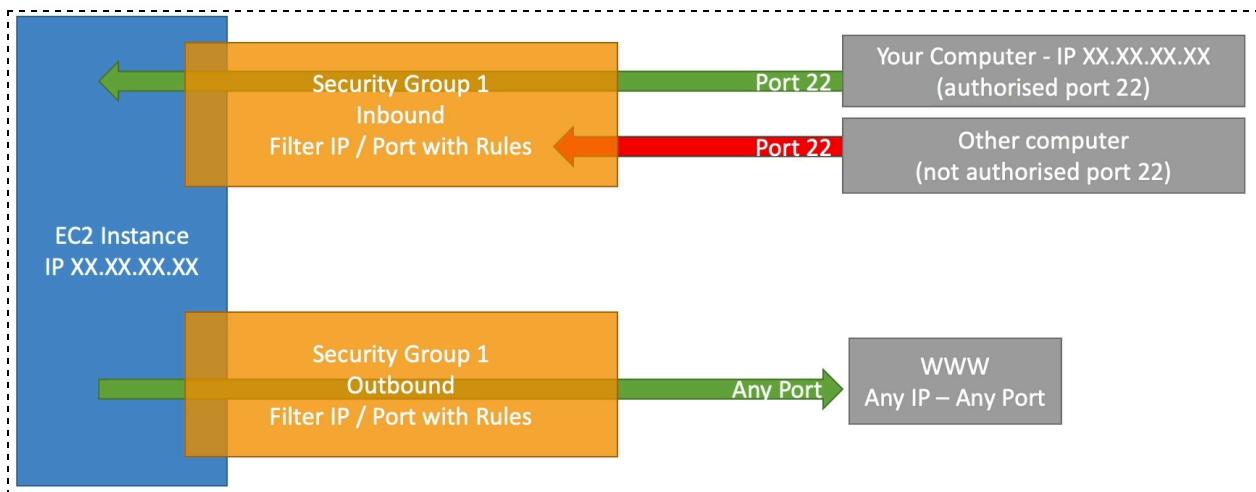


I'm Here

- حاطط rules بتسمح ب ssh traffic اللی جای علی port 22 من ip معین فقط وفى root user ip الغالب بيكون
- ممکن ت اکثر من define instance 1 ل Security Group
- ال EC2 instance level بتشتغل على ال Security Group مش على ال
- network access control , الی بيشتغل على ال subnet هو ال subnet level
- list

● Control the inbound & outbound traffic by:

- IPV4 - IPV6
- Ports
- Inbound & Outbound Network



يفضل فصل ال SSH فى Security group لوحدها.

لو بت Access ال App بتعاك وفيه time out او wait كتير ف 100% السبب ال

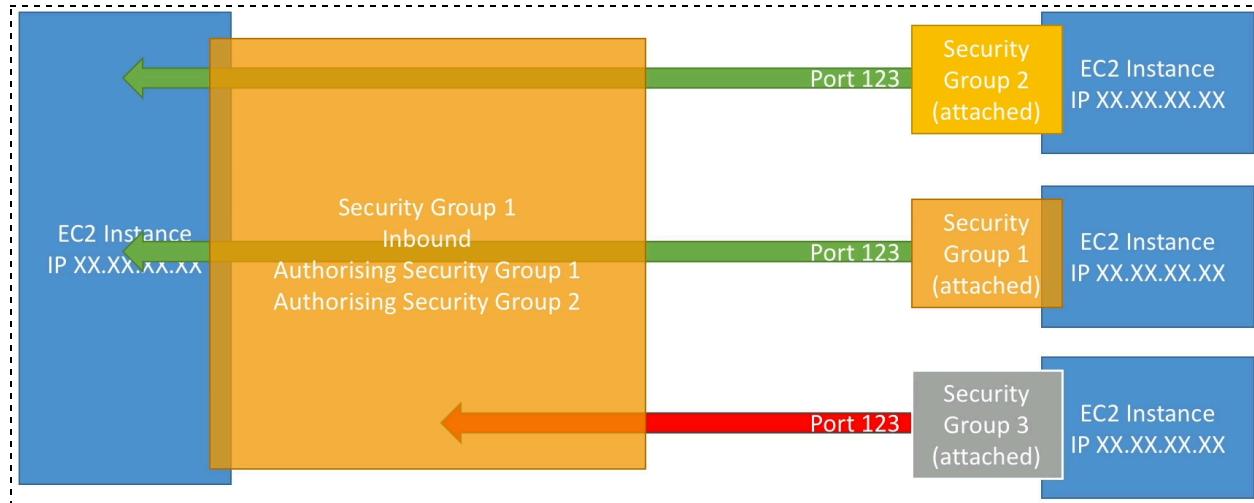
Security group

ولو Application or launching فغالبا دي مشكلة Connection Refused Error



I'm Here

- **Important Example:**



- فى ال Security Group اللي عالشمال انا سامح فيه بال inbound traffic من ال instances اللي على اليمين اللي هما 1.2 بالتالي اي Security Group جواهم هيبقى مسموح بال traffic اللي جاي منها على ال instance اللي عالشمال

انك تسمح بال inbound traffic اللي جاي من ال Security Group يعني عن انك تسمح بكل instance جواه مش هتفضل تكتب ip كل instance انت بتشوف مين ال security group اللي لامهم وتسمح بيها وخلاص .. ودة مناسب فال auto scaling علشان لو فيه بترزيد او بتنقص بردو اكيد مش هتفضل تعدل ال inbound rules عال Security Group اللي عالشمال

انك ت Authorized Security Group عند Security Group تاني بيتم من خلال ال ID بناءً.

- **Classic Ports:**

- 22 = SSH (Secure Shell) - log into a Linux instance



I'm Here

- 3389 = RDP (Remote Desktop Protocol) – log into a Windows 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
-

➡️Security Groups Hands On:

فى حالة الـ inbound traffic لو فتحت الـ Security Group اللي جاي على port 80 

تنقائي الـ outbound من 80 allowed هيكون

طبعاً دة على عكس الـ iptables مثلاً لازم تحط للاتين .rules



I'm Here

➡SSH Overview:

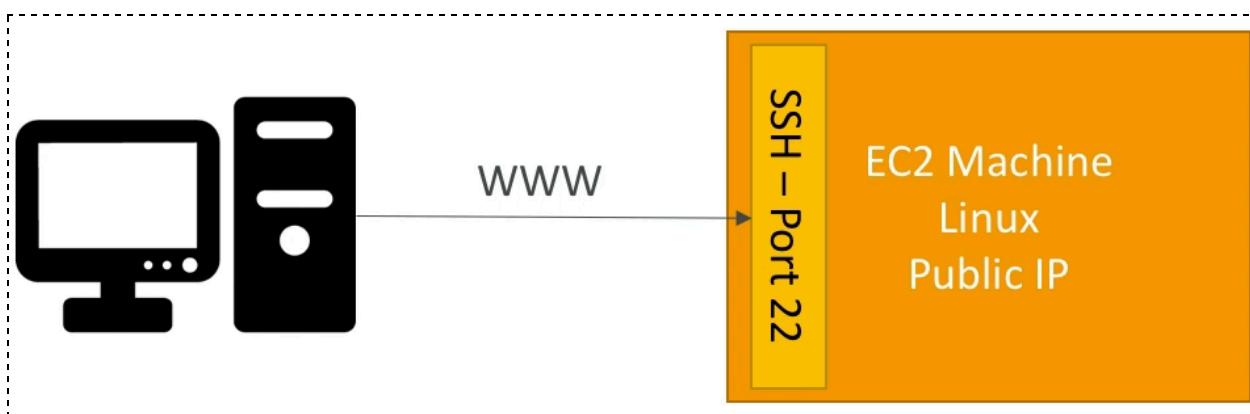


- اقل من windows 10 مينفعش معها ssh

- فى العموم windows لـ Putty

- هتتشرح قدام EC2 Instance Connect

➡How To SSH Using Linux Or Mac



I'm Here

- بتفتح ال Port 22 فى ال security group اللي بيحوي ال EC2 instance بتاعتك .. ولكن انت اكيد مش بتكون فاتح ال ssh عال public ipv4 instance لاي حد ي access ssh لازم يا تكون محدد ال ip اللي هي او عن طريق key access

```
Ssh -i key.pem ec2-user@ipv4
```

- دة ال user Ec2-user دة ال instance عال اللي معمول عال واللى لما تخش هتخشن بيه
- دة بتاع ال Ipv4 دة instance

```
~/aws-course ➔ ssh -i EC2Tutorial.pem ec2-user@3.250.26.200
@@@@@@@WARNING: UNPROTECTED PRIVATE KEY FILE! @@@@_
Permissions 0644 for 'EC2Tutorial.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
@@@@@@@WARNING: UNPROTECTED PRIVATE KEY FILE! @@@@_
Permissions 0644 for 'EC2Tutorial.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 "EC2Tutorial.pem": bad permissions
Received disconnect from 3.250.26.200 port 22:2: Too many authentication failures
Disconnected from 3.250.26.200 port 22
✖ ➔ ~/aws-course ➔ chmod 0400
```

- دة الحل بتاعه ف انك تدي الملف owner لل read permission فقط .

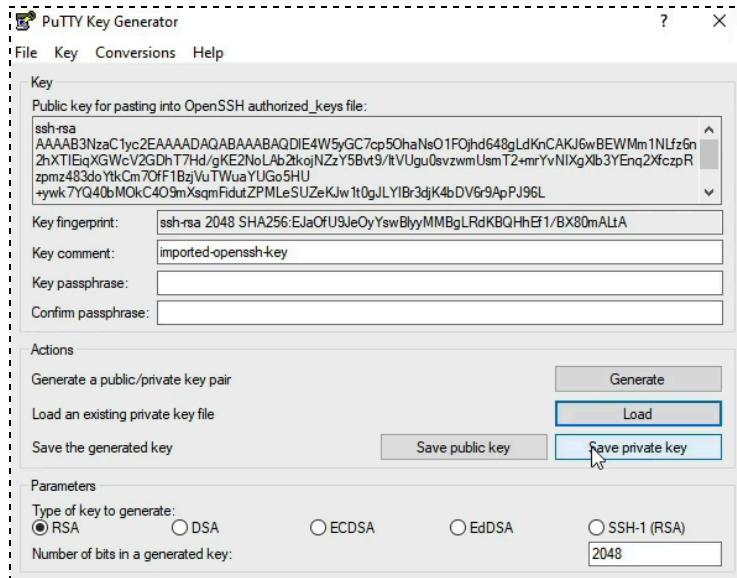


I'm Here

→How To SSH Using Windows7.8:

(1) هتحمل من جوجل putty

(2) بعد ما تسطبه هتلاقى عندك ليه جزأين puttygen خاص بال key وال ذات نفسه



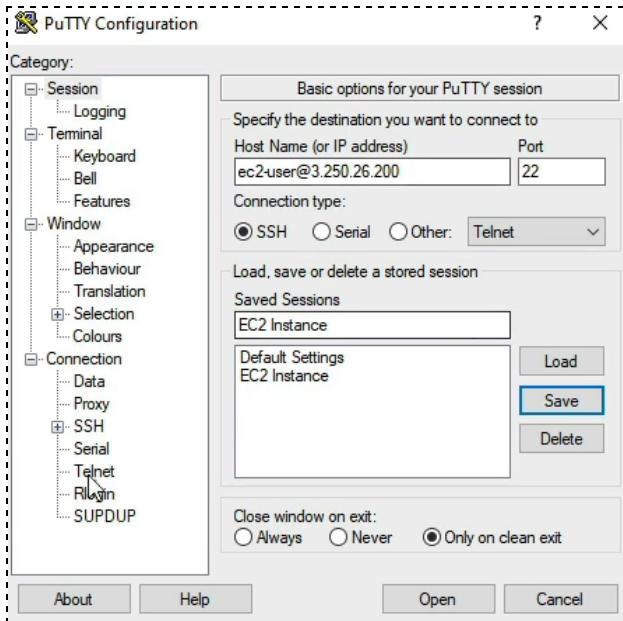
- هت اال load key.pem وتحوله ل key.ppk او لو حملته من الاول بصيغة ppk ف

تمام ياعني .. وت save private key

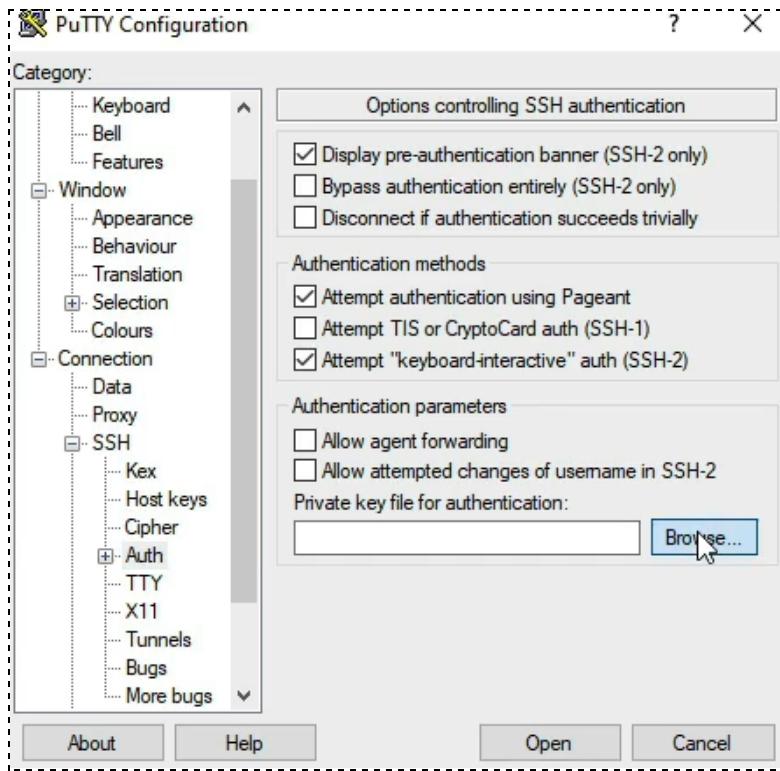
: (3) هتملي الداتا دي :



I'm Here



ppk وبعدين هت load auth الى هو (4)



بت save الى عملته دة فى الصفحة الاولى بحيث متعملش الخطوات دي كل ما تحتاج instance عال (5)



I'm Here

➡How To SSH Using Windows10:

- ممكن من خلال putty عادي

```
Ssh -i key.pem ec2-user@ipv4
```

- لو جالك error هيبقى نفس ال error اللي زى اللي فوق علشان owner ال file

وتحتغورو من خلال :

```
Right click on the file >> properties >> security >> Advanced >>  
Change >> choose your self.
```

```
PS C:\Users\stephanemaarek\Desktop> ssh -i .\EC2Tutorial.pem ec2-user@3.250.26.200  
The authenticity of host '3.250.26.200 (3.250.26.200)' can't be established.  
ECDSA key fingerprint is SHA256:INQMVOPtZV+fRKl+EeoRtTp+pWI4koar4F8a6QTmPgE.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '3.250.26.200' (ECDSA) to the list of known hosts.  
Last login: Mon May 16 17:28:25 2022 from bl14-117-32.dsl.telepac.pt  
  
_ _|_ _|_)  
_ | ( _| / Amazon Linux 2 AMI  
_ | \_ | _|  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-172-31-33-135 ~]$
```

➡SSH Troubleshooting:

- ملف كوييس اقرأه

➡EC2 Instance Connect (Easy way)



I'm Here

هیتم الموضوع من خلال ال browser بجرا ما بتضغط ال connect -
بتنفتح عال browser

Instances (1/1) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm st
My First Instance	i-034466697feb9ef80	Running	t2.micro	2/2 checks passed	No alarm

Connect to instance Info

Connect to your instance i-034466697feb9ef80 (My First Instance) using any of these options

EC2 Instance Connect Session Manager SSH client EC2 Serial Console

Instance ID: i-034466697feb9ef80 (My First Instance)

Public IP address: 3.250.26.200

User name: ec2-user

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Cancel Connect

Connect to instance | EC2 Manager X i-034466697feb9ef80 (My First Instance) +

Last login: Mon May 16 17:43:26 2022 from bl14-117-32.dsl.telepac.pt

Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/[ec2-user@ip-172-31-33-135 ~]\$

I'm Here



ممكن حتى لو فتحت ال ssh عال instance anywhere/ipv4 من معرفيش ت

anywhere/ipv6 في الحاله دي افتح connect

💡 Any timeout (not just for SSH) is related to security groups or a

Firewall

لو عملت Stop لـ Instance وجيـت شغلتها تاني ممكن تلاقي ال IPV4 اتغير ف خلي

بالـك.. يعني مش هتعرف تخـش لو محدد انك ت ssh بال ipv4 اللي اتغير

➡ EC2 Instance Roles Demo:

الـى عملـه انـو access الـ instance user list وحاـول يـ list الـ instance ولكن الـ instance readonly role attach لـ attach الـ role دـي .. فـ عملـنا lـ instance roles lـ attach lـ users list الـ

لـ ما تـيجـيـت role attach الـ instance attach علىـ ما تـسمـعـ عـالـ

مستـعـجـلـشـ.

الـ instance lـ linux installed CLI lـ instance lـ ما كـريـتـهاـ بـ



I'm Here

```
[ec2-user@ip-172-31-17-250 ~]$ aws --version
aws-cli/1.18.147 Python/2.7.18 Linux/4.14.225-169.362.amzn2.x86_64 botocore/1.18.6
[ec2-user@ip-172-31-17-250 ~]$ aws iam list-users
Unable to locate credentials. You can configure credentials by running "aws configure".
[ec2-user@ip-172-31-17-250 ~]$ aws configure
AWS Access Key ID [None]:
AWS Secret Access Key [None]:
Default region name [None]:
Default output format [None]: ^C
[ec2-user@ip-172-31-17-250 ~]$
```

- متعلش لـ credential configue اي حد لو دخل عال instances بالشكل دة يقدر retrieve key access ويخرب الدنيا

➡ EC2 Instance Purchasing Options:

• On-Demand Instances :

- ودي go as you like OS Linux , Windows بندفع بالثانية واي تاني
بالساعه .. وده اعلى سعر ال Options يعني لو تحتاج مثلا سيرفر اسبوع شهر
شهرين ثلاثة.

- مفيش فيها upfront payment دفع مقدم يعني.

ال usage : فى ال short-term usage اللى مش توقع ال load بتاعها.💡

• Reserved Instances & Convertible Reserved Instances

(1&3 year):

• Reserved Instances

- وهذا AWS Cost بتقل ال Configuration ثابتة لل بتاعتك زي ال Instances.type , region

- فيها upfront payment دفع مقدم .. ممكن متدفعش وممكن تدفع جزاً ممكن تدفع كل الحساب وطبعاً كل ما دفعت اكتر كل ما هتاخذ خصم اكتر.



I'm Here

- بيبقى فيها تقريبا 70% discount عن ال instances on demand

- دى فى ال market place لو مبقتش محتاجها

- سنة او 3 سنين مش سنة الي 3 سنين

ال usage : فى ال database steady state usage applications 

• Convertible Reserved Instances

- نوع من انواع ال Reserved Instances ميزته انك تقدر تغير ال

- EC2 instance type, instance family, OS, scope and tenancy

- بيبقى عليه discount يصل ل 66%

• Saving Plans (1&3 year):

- بيبقى فيها تقريبا 70% discount زى ال reserved

- بتلتزم فيها بالاستخدام مثلا (10 دولار/ساعة لمدة 1 أو 3 سنوات) ولو استخدامك زاد عن

اللى انت محددة هتدفع بال on-demand

- على M5 instance family & regionLocked لل us-east-1 يعني لو حدبت على

مش هتعرف تغيره

• Spot Instances:

- ودى سعرها بيكون مخفض لنسبة قد تصل ل 90% من سعر ال On-Demand

- ودى يعتبر اقل سعر ف ال instances options المتاحة. ف ال option دة انت

بتسخدم ال unused EC2 Instances بسعر مخفض لكن ممكن تخسر ال

instances spot instance تخطي ال max price بتابعك ف اي وقت لو سعر ال

.critical services customer وده طبعا مش مناسب لل

ال usage : مش مناسب لل critical jobs ومناسب للاتي :

Batch jobs , Data analysis , Image processing , Any distributed ,

workloads , Workloads with a flexible start and end time



I'm Here

- **Dedicated Hosts & Dedicated Instances:**

- الاتنين متقاربين ال hosts بتاخد full control وبيكون ليك physical server عال

- اما ال instances بيكون ليك control اقل ف بتختارها لما متكونش hardware

detailed hardware control

- علشان اللغبطة من الاسم Dedicated Host يعني السيرفر ملكك ..

hardware instances على ملكك يعني Instances

- الدفع بيكون حاجة من الاتنين :

- **On-demand**

- pay per second for active Dedicated Host

- **Reserved**

- 1 or 3 years (No Upfront, Partial Upfront, All Upfront)

Comparison Summary

Feature	Dedicated Hosts	Dedicated Instances
Control	Full control over instance placement on specific physical servers	AWS manages instance placement
Hardware Visibility	Full visibility into physical hardware (sockets, cores)	No visibility into physical hardware
Licensing	Ideal for BYOL scenarios requiring specific hardware licensing	Less suitable for complex licensing
Isolation	Dedicated hardware for a single customer	Dedicated hardware for a single customer
Management	Requires more management effort	Simpler, less management overhead
Billing	Billed per host	Billed per instance
Use Cases	Regulatory compliance, detailed hardware control, BYOL	Physical isolation without hardware control



I'm Here

● Capacity Reservation:

ال capacity هنا معناها عدد ال EC2 Instance من type معين في region او معينة AZ

وهذا AWS بتعملك on-demand EC2 Instance ل Reservation -

Capacity Availability zone معينه لمدة بيتم الاتفاق عليها.

مفيش time commitment مفاصيل في اي وقت براحتك

مفيش discount ولكن ممكن تدمجها مع ال reserved instances وال saving

حيث تأخذ خصم plans

هتحاسب اكنك instance شغالة او مش شغالة هتحاسب عليها.

ال Usage : ه تكون مناسبة لل short-term uninterrupted workloads في AZ معينة.

● Scheduled Instances:

ودي من اسمها تقدر من خلالها انك تشغل ال Instances بتاعتكم بجدولة يعني خلال عدد ساعات معينه مثل اف اليوم او الاسبوع او الشهر ودي بتكون لمدة سنة.

● Price Comparison - Example – m4.large – us-east-1

Price Type	Price (per hour)
On-Demand	\$0.10
Spot Instance (Spot Price)	\$0.038 - \$0.039 (up to 61% off)
Reserved Instance (1 year)	\$0.062 (No Upfront) - \$0.058 (All Upfront)
Reserved Instance (3 years)	\$0.043 (No Upfront) - \$0.037 (All Upfront)
EC2 Savings Plan (1 year)	\$0.062 (No Upfront) - \$0.058 (All Upfront)
Reserved Convertible Instance (1 year)	\$0.071 (No Upfront) - \$0.066 (All Upfront)
Dedicated Host	On-Demand Price
Dedicated Host Reservation	Up to 70% off
Capacity Reservations	On-Demand Price

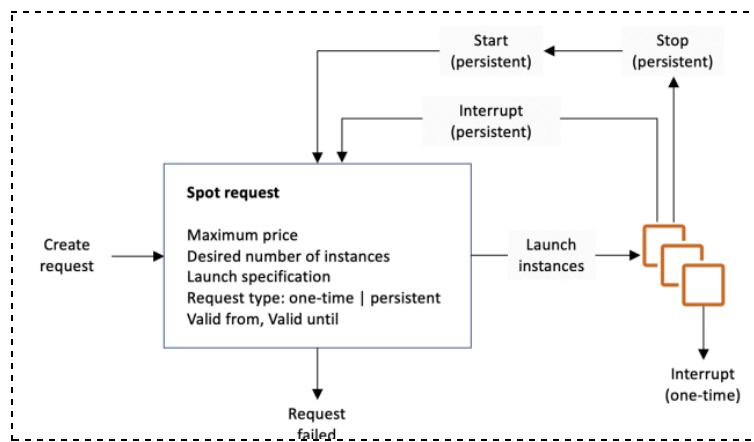


I'm Here

➡ Spot Instances & Spot Fleet:

- لو السعر تخطي السعر اقصي سعر انت هتدفعو قدامك دققيتين تقرر فيهم هل هتعمل stop او هتعمل لـ stop price .. لو هتعمل stop لما ال instance ينزل عن ال start تقدر تعملها max price من تاني.

● How Spot Request Work :



- بتحدد كام عدد ال instances وال max price اللي هتدفعو وال launch specifications

● How to terminate spot instances?

- عندك نوعين من ال request : request

● One-time request

- مجرد ما بتعمل ال request ال instances بت launch ولو حصلها interrupt مش هتقوم تاني الا لما انت تعمل request جديد دة مناسب لـ termination continuous او مش محتاجة one single run اللي يحتاج work loads execution



I'm Here

- Example

You have a data processing job that you run periodically. You submit a one-time Spot Instance request to complete this job. Once the job is finished, or if the instance is terminated, no further action is taken automatically.

● Persistent request

يبقى في النوع دة لو تحتاج ت ال instances terminate خالص لازم الاول توقف ال Persistent request -
حصلها launch او termination interrupt instance واحدة جديدة
كديل ودة مناسب لل work loads اللى بتحتاج continuous execution or high availability

- Example

You have a long-running data analysis application that needs to run continuously. You submit a persistent Spot Instance request for 3 instances. If any of these instances are interrupted, AWS will automatically attempt to launch new instances to maintain the count of 3.

يبقى في النوع دة لو تحتاج ت ال instances terminate خالص لازم الاول توقف ال 
لانك لو موقفتوش هيحصل لل instances relaunch بحيث يحافظ persistent request

على عددها اللي انت محددهوله.



I'm Here

- **Spot Fleet:**

لو عندك variable traffic وعاوز تهندل اللى web application : **Example** -
بيجييك خلال اليوم وتحافظ على انك تدفع اقل تكلفة وانو يكون available عططول هتعمل
الاتي :

- **Define Target Capacity :**

بت define عدد ال instances اللي عاوزها وال cpu وهكذا -

- **Choose the allocation strategy:**

- **Lowest price**

ودي لو محتاج اقل cost -

- **Diversified or Capacity Optimized**

لو محتاج Availability عالية وأنك تقلل the risk of interruption -

- **priceCapacityOptimized (recommended) :**

مิกس بين الاثنين lowest price و high capacity Available -

- **Choose instances types and AZs**

هت list ال AZs وال types اللي ال application بتاعك can run on it -

- **Mix Purchase Options**

- Optionally include a mix of Spot and On-Demand Instances to balance cost and availability.

- **Launch Spot Fleet**

➡EC2 Instance launch types hands on:

Instances >> spot request >> request spot instances

ممكن من هنا او وانت بت launch instance عادي هتلقي دي ..



I'm Here

▼ Advanced details [Info](#)

Purchasing option [Info](#)

Request Spot Instances

[Customize](#)

Request Spot Instances at the Spot price, capped at the On-Demand price

CH-06 - EC2 - Solutions

Architect Associate Level



I'm Here

→001 Private vs Public vs Elastic IP:

Instance: i-03977f3eb2e4e0d4d

Details	Security	Networking	Storage	Status checks	Monitoring	Tags
Instance summary Info						
Instance ID i-03977f3eb2e4e0d4d	Public IPv4 address 3.129.218.15 open address	Private IPv4 addresses 172.31.11.234				
Instance state Running	Public IPv4 DNS ec2-3-129-218-15.us-east-2.compute.amazonaws.com open address	Private IPv4 DNS ip-172-31-11-234.us-east-2.compute.internal				

الى instance انت بتاجرها بيكون لها public & private ip -

لما بت ssh عال instance بنسخدم ال public ip مينفعش ال private ip عال لاننا مش فى

ال same network

ال instance لو عملتها start دة بيتغير وبعدين stop دة بيتغير -

→002 Private vs Public vs Elastic IP Hands On

• Create Elastic IP:

Network & Security >> Elastic IPs >> Allocate Elastic IP Address

بيكون ليه تكلفة خاصه لواحدة بحوالى 0.005\$ في الساعه

Elastic IP addresses (1/1)		C	Actions ▲	Allocate Elastic IP address
<input type="text"/> Filter Elastic IP addresses				
Public IPv4 address: 18.216.64.85 X		Clear filters		
<input checked="" type="checkbox"/>	Name	Allocated IPv4 add...	Type	
<input checked="" type="checkbox"/>	-	18.216.64.85	Public IP	Instance ID: i-0d246d23ecd86955



I'm Here

• بعد ما كريت ال instance بتربطه بال elastic ip .. وبتستفاد الآتي :

- لو عملت stop لـ instance وبعدين start مش هيتغير وده بيغيفد فى حاجات كتير منها

ال DNS record مثلا

- بعد ما بتربطه .. تقدر ت ssh عليه .. بتلاقي ان ال public ipv4 , elastic ip بقو

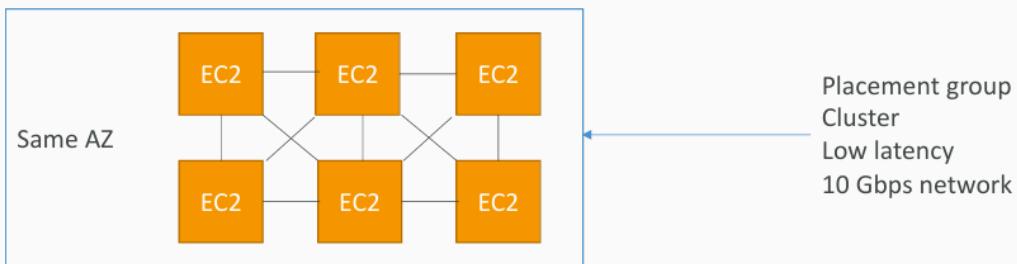
واحد .. هما نفس ال elastic

- تقدر بعد ما ربطته ب instance تشيله وتربطه بوحدة تانية



→003 EC2 Placement Groups

• Cluster

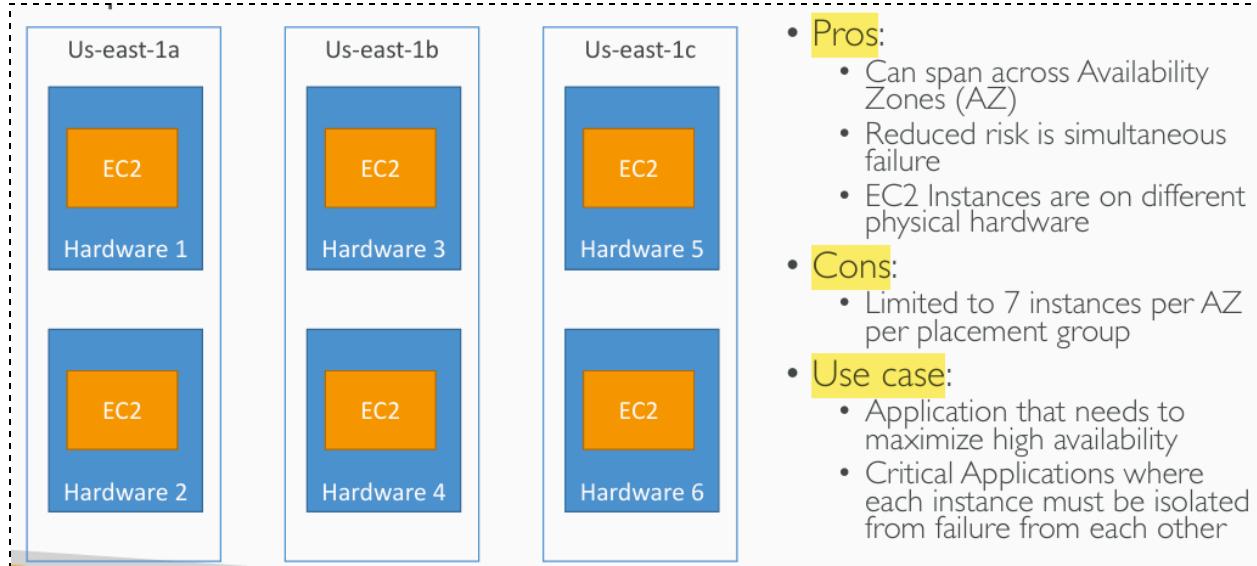


- **Pros:** Great network (10 Gbps bandwidth between instances with Enhanced Networking enabled - recommended)
- **Cons:** If the AZ fails, all instances fail at the same time
- **Use case:**
 - Big Data job that needs to complete fast
 - Application that needs extremely low latency and high network throughput

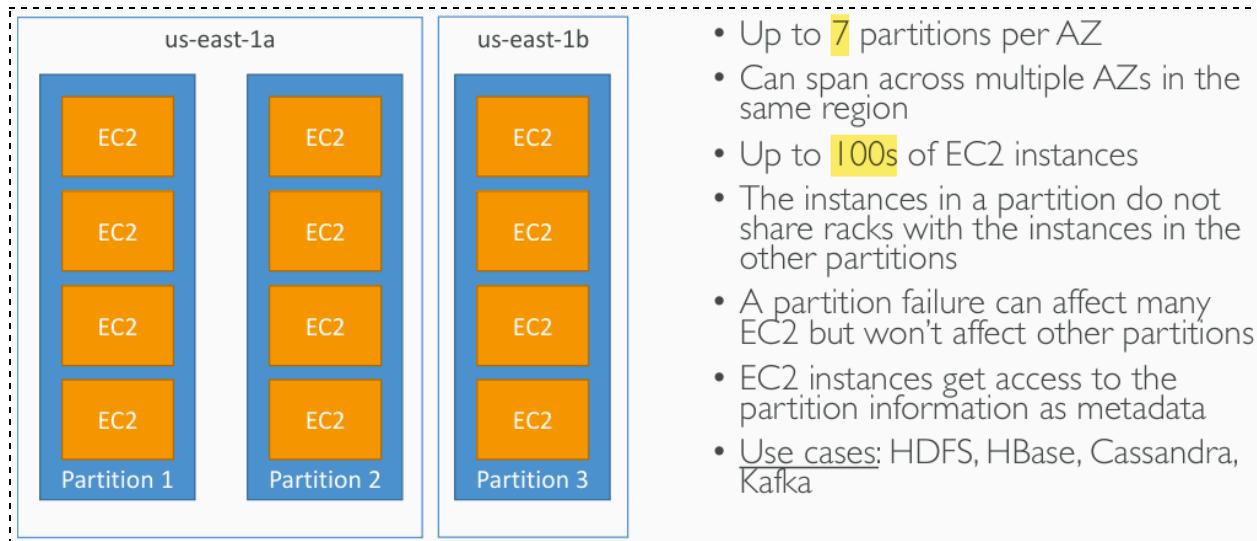


I'm Here

● Spread



● Partition



- highest networking performance >> **Cluster**
- maximum availability when there's an AZ failure >> **Spread**



I'm Here

→004 EC2 Placement Groups - Hands On

Network & Security >> Placement group >> Create Placement group >> name,type

- بعد ما بتكريت ال placement group بتروح تكريت ال instances اللي هتحطها

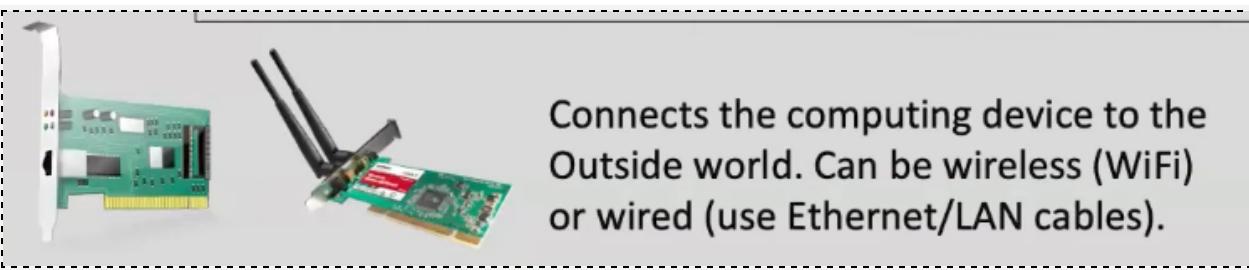
فيها

Instances >> Create Instance >> Advanced details >> Placement groups >> choose the placement group

→005 Elastic Network Interfaces (ENI) -

Overview

• Network Cards / Interface



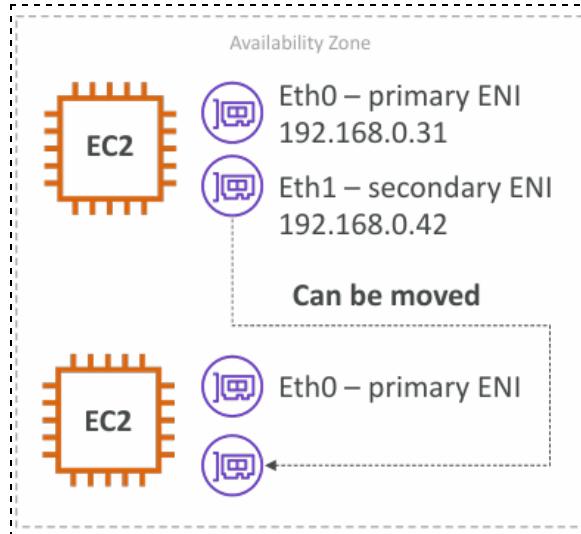
- عن طريقها بنوصل لل internet سواء wireless زى الاب كدا او لو كمبيوتر ممكن

بکابل او ممكن ب وصلة تخلية يلقط وايفاي.. فى الحالة بتاعتنا ال instance بتوصل

للانترنت من خلالة.



I'm Here



virtual network card عن عباره : ENI -

- ENI Have :

- Primary private IPv4, one or more secondary IPv4
 - One Elastic IP (IPv4) per private IPv4
 - One Public IPv4
 - One or more security groups
 - A MAC address

عبارة عن interface virtual instance attach لـ بتأتى بعمليات تكريرها وتعلمتها

- انت اول مبت launch ال EC2 Instance بتاعتک بتاخد private ip جوا ال

اللى انت حددت انها تكون فيها **subntet**

- جوا ال EC2 Instance هتلaci option من خالله تقدر تحدد هل هتدى ال EC2

و لا Instance public ip

- ال ENI زري مقولنا بيتعملها attach عال EC2 Instance ف بتكون جزا من ال

دي .. ف ساعتها ال EC2 Instance ه يكون ليها 2 ip ال

الى هو ال primary وال secondary بناءً على ENI

- ممكن تشيلها من instance و attach it لواحدة تانية

- محكمة بال AZ اللي هيا فيها



I'm Here

→006 Elastic Network Interfaces (ENI) - Hands

On

هنعمل 2 instances كل واحدة هتلaci عندها network interface بيكون ليها id instance id دي مربوطة بانهie network interface وهكذا متوضح ال

Network & Security >> Network Interface

Network interfaces (2) <small>Info</small>					
<input type="text"/> Filter network interfaces					
Name	Network interface ID	Subnet ID	VPC ID	Availability Zone	
-	eni-0479b24bf2debda40	subnet-444bf62f	vpc-6047d20b	us-east-2a	
-	eni-00f63c73c7d0187fc	subnet-444bf62f	vpc-6047d20b	us-east-2a	

Network interfaces (2) <small>Info</small>					
<input type="text"/> Filter network interfaces					
Description	Instance ID	Status	Public IPv4 address	Primary private IPv4 address	
-	i-0575f9fde3525b143	In-use	3.143.214.169	172.31.7.169	
-	i-0145a88f58ba656db	In-use	18.189.185.151	172.31.13.28	

بمجرد ما تكريت action هتعدددها ومن action تقدر ت attach network interface على instance دي لاي من الاثنين ف هتروج عليها هتلaci علىها network interface ال ال network interface ال الجديدة والاصلية



I'm Here

Network interfaces (2)

Interface ID	Description	Public IPv4 address	Private IPv4 address	Private IPv4 DNS	IPv6
eni-00f63c73c7...	-	18.189.185.151	172.31.13.28	ip-172-31-13-28.us...	-
eni-021963833f...	DemoENI	-	172.31.10.247	ip-172-31-10-247.us...	-

وتقرب بعد كذا تنقلها من واحده للثانوية

● Example: Initial Configuration

● Instance A:

- Attached ENI: **eni-12345678**
- Private IP: **10.0.0.5**
- Elastic IP: **54.123.45.67**

● Instance B:

- No ENI initially attached

● User Connection:

- Users connect to the application using the Elastic IP
54.123.45.67

● How It Works Internally

● Before Failover:

- Users access the application on Instance A via Elastic IP **54.123.45.67**.



I'm Here

- The traffic is routed through the Elastic IP to the private IP **10.0.0.5** of Instance A.

- **During Failover:**

- You detach the ENI from Instance A.
- The ENI retains its IP configuration.

- **After Failover:**

- You attach the ENI to Instance B.
- Instance B now uses the same IP configuration.
- Users access the application on Instance B via Elastic IP **54.123.45.67**.
- The traffic is routed through the Elastic IP to the private IP **10.0.0.5** of Instance B.

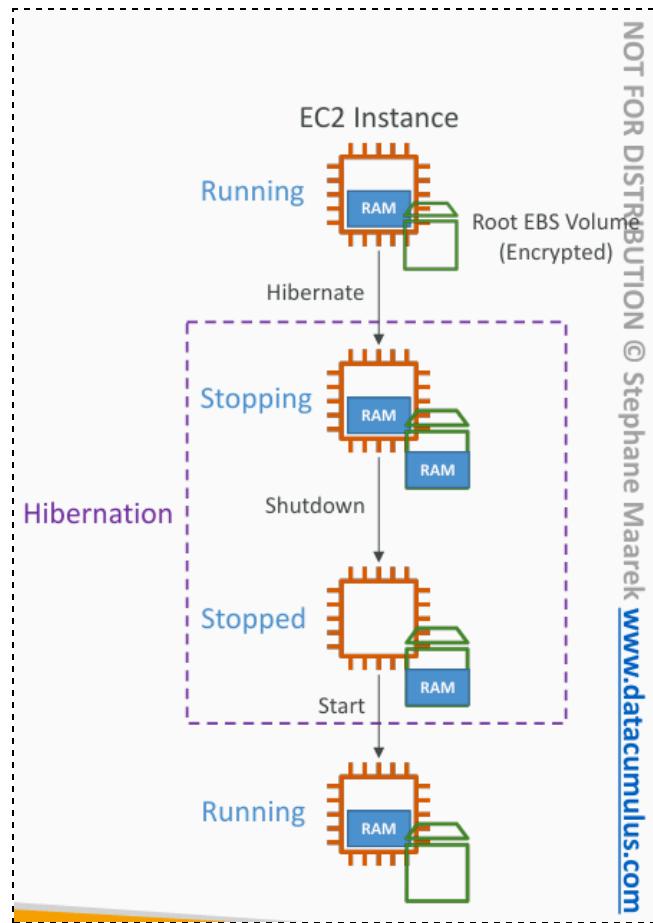
يبقى انت رابط ال ENI عال instance A لو بعمل صيانة مثلاً لـ app اللي عليها وعاوز انقل على instance B على ENI بنقل ال instance B ولما ال user ي ال .instance b هينقلو لل private ip الخاص ب Elastic ip



I'm Here

→008 EC2 Hibernate

- sleep ال instance computer بتعمل لـ اكناك بتاعك instance اكناك بتعمل لـ
- فـى الطبيعى لو انت قفلت الكمبيوتر بتاعك shutdown وفتحته من تانى بي boot from
- وبـىيـتـى يـشـغـلـ البرـامـجـ منـ تـانـىـ وـبـقـتـحـ الـ filesـ منـ تـانـىـ وهـكـذاـ scratchـ
- انما لو عملـتـهـ Sleepـ الحـوارـاتـ دـىـ كـلـهاـ الـىـ بـتـكـونـ مـوـجـودـةـ فـىـ الـ RAMـ بـتـخـزـنـ فـىـ
- الـ SSDـ اوـ فـىـ الـ HDDـ عـلـىـ حـسـبـ اـنـتـ عـاـمـلـ الـ OSـ بـتـاعـكـ عـلـىـ مـيـنـ فـيـهـمـ وـلـمـ تـشـغـلـهـ
- منـ تـانـىـ وـبـقـتـحـ الـ dataـ دـىـ بـتـرـجـعـ مـنـ تـانـىـ مـنـ الـ RAMـ لـ SSD or HDDـ لـ



- دـةـ نفسـ الـىـ بـيـحـصـلـ عـلـىـ instanceـ بـنـفـعـ لـيـهـاـ الـ Hibernـateـ modeـ وـاحـناـ
- بنـكريـتـهـاـ فـ لـمـ بـنـعـمـلـ لـيـهـاـ Hibernـateـ dataـ بـتـخـذـنـ الـ dataـ الـىـ كـانـتـ فـىـ الـ RAMـ عـنـدـهـاـ



I'm Here

فی ال EBS root volume لحد ما تقوم من جديد وترجع تاني ال data دی لـ RAM ب بتاعتها تاني.

● Use Cases:

- لو process بتاخذ وقت طويـل ومـش عـاوزـها تـفـصـل او لو فيه services شـغـالـة عـالـةـ

from scratch وبـتـاخـذ وقت طـويـل عـلـى ما تـفـتح ومـش عـاوزـها تـفـتح instance

• **فـيـه شـوـيـه حاجـات بـتـحـكـمـك لو هـتـسـتـعـلـم ال Hyber~nate**

- Supported Instance **Families** – C3, C4, C5, I3, M3, M4, R3, R4, T2, T3, ...
- **Instance RAM Size** – must be less than 150 GB.
- **Instance Size** – not supported for bare metal instances.
- **AMI** – Amazon Linux 2, Linux AMI, Ubuntu, RHEL, CentOS & Windows...
- **Root Volume** – must be EBS, encrypted, not instance store, and large
- Available for **On-Demand, Reserved and Spot Instances**



An instance can NOT be hibernated more than **60 days**

→009 EC2 Hibernate Hands On:

Create EC2 Instance >> Advanced Details >> Hibernate Behavior



I'm Here

Stop - Hibernate behavior Info

Select

Select

Enable

Disable

• الحاجات دي لازم تحصل :

لازم يكون ال root volume علية مساحة كافية تكفي ال RAM Content اللي instance start ت من جديد.. هنا عندنا ال 1 هي تخزن عليه لحد ما ال instance ف كدا دة مناسب.

EBS root volume 8GiB وال GiB Memory

▼ Storage (volumes) Info

EBS Volumes

Volume 1 (AMI Root) (Custom)

Storage type Info	Device name - required Info	Snapshot Info
EBS	/dev/xvda	snap-00022cfee7f3b9690

Size (GiB) Info	Volume type Info	IOPS Info
8	gp2	100 / 3000

Delete on termination Info	Encrypted Info	KMS key Info
Yes	Yes	(default) aws/ebs Key ID: 6e839668-f27c-4cd1-b6...

▼ Instance type Info

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory
On-Demand Linux pricing: 0.0126 USD per Hour
On-Demand Windows pricing: 0.0172 USD per Hour

Free tier eligible

Compare instance types

لازم يكون ال root volume encrypted



I'm Here

• TEST

علشان نشوف الدنيا دي شغالة ولا اية هنستخدم اسمو command uptime بيعرفنا ال
دي بقالها قد اية شغالة instance.

```
[ec2-user@ip-172-31-14-73 ~]$ uptime  
23:34:14 up 1 min, 1 user, load average: 0.30, 0.12, 0.04  
[ec2-user@ip-172-31-14-73 ~]$ uptime
```

ظاهر لنا دلوقتي بقالها شغالة لمدة دقيقة .. ف انت لو مش مفعل ال Hibernate و عملتها
stop & start المفروض لو جيت تنفذ نفس ال command يظهر لك 0 ولكن بما انك
مفعل ال Hibernate ف هتلاقي العداد دة متصرفش وكمل تاني ودة معناه ان الداتا دي
اللى كانت عال RAM انتقلت عال EBS root volume لحد ما ال instance تقوم
من جديد ورجعتله تاني وكملت.

EC2 > Instances > i-034480cbc82cd80ca

Instance summary for i-034480cbc82cd80ca [Info](#)

Updated less than a minute ago

Instance ID	Public IPv4 address	Private IPv4 address
i-034480cbc82cd80ca	3.142.166.248 open address	172.31.14.73
Instance state	Public IPv4 DNS	Private IPv4 DNS
Pending	ec2-3-142-166-248.us-east-2.compute.amazonaws.com open address	ip-172-31-14-73.us-east-2.compute.internal
Instance type	Elastic IP addresses	VPC ID
t2.micro	-	vpc-6047d20b
AWS Compute Optimizer finding	IAM Role	Subnet ID
Opt-in to AWS Compute Optimizer for recommendations. Learn more	-	subnet-444bf62f

```
[ec2-user@ip-172-31-14-73 ~]$ uptime  
23:35:57 up 2 min, 1 user, load average: 0.23, 0.12, 0.05  
[ec2-user@ip-172-31-14-73 ~]$
```



I'm Here

CH-07 - EC2 Instance Storage

→001 EBS Overview

- عباره عن instance attach لـ Virtual hard drive بتعمله بتاعتك، اكناك عندك كمبيوتر ومعاك هارد خارجي بتوصله بيـه وبحفظ عليه الداتا بتاعتك.

• مميزاتها :

- **Persistent Storage**: الداتا هفضل موجودة حتى لو عملت stop او restart لـ instance بتاعتك .. لو مسحت الـ EBS volume هتلقي ان الـ instance موجودة ممكن بعد كدا تعملها instance attach لـ instance تانية.

- **Different Types**: فيه انواع كتير منها على حسب الغرض من استخدامك تحتاج اية بالضبط (general-purpose, high-performance, or cost-effective) (.storage)

- **Backup and Restore**: تقدر تأخذ snapshots (backup) لـ EBS (snapshots (backup)) بتـ الـ volumes دي بحيث تقدر تـ restore الـ volumes

- **Resize and Change**: تقدر تـ resize ، change الـ EBS volumes دي من غير ما تفقد الـ data بتاعتك

متقدرش تـ attach الـ EBS Volume دي لاكثر من instance الا فى حالة معينه  .
هنعرفها بعدين.

الـ EBS Volume محكمة بالـ AZ اللي هيا فيها بمعني .. الـ EBS Volume انت بتكريتها وتعملها عالـ instance والـ instance تكون موجودة ول يكن فـ AZ1 فـ AZ2

لو انت فـ AZ1 تانية مش هتشوف الـ EBS Volume اللي فـ AZ1



I'm Here

EBS root volume الاساسية واي واحدة تانية انت بتكريتها بتقى بيبقى عندك

اضافيه volume

• Delete On Termination:

The screenshot shows the 'Configure storage' section of the AWS Lambda function configuration. It displays a single volume entry: 1x 8 GiB gp3 Root volume (Not encrypted). Below this, there is a button labeled 'Add new volume'.

- وانت بتكريت ال instance بتاعتك كنت بتخصص root volume بعدد giga معينه

.. ف انت لو عملت delete لـ root volume بتاعتك ال EC2 instance

هيتمسح باللي فيه وده ال default behavior

- علشان اغير ال root volume default behavior دة وميتمسحش ال default behavior لو جيت اعمل

check بشيل ال instance delete من هنا

The screenshot shows the 'Delete On Termination' configuration settings. It lists two options: 'By default Root EBS is deleted' and 'By default Other Attached EBS is not deleted'. Below this, a table lists a single volume entry:

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination
Root	/dev/xvda	snap-09f18f682fd23a1b1	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>

- ف ال screen اللي فى الصفحة اللي فاتت هتلاحظ انك ممكن تـ add new volume

.. يقصد EBS volume ياعني او انت تكريتها بعدين مش لازم وانت بت configure

ال instance وبعد دة تـ attach EBS volume دي لـ instance عادى .. ف

بکدا بقت ال instance بتاعتك عندها 2 .. الاولى root volume والثانية

ال instance EBS Volume اللي انت كريته .. وزي مقولنا قبل كدا لو مسحت ال

دي ال EBS Volume مش بتتمسح

- او وانت بتكريت ال EBS Volume تخـش على Advanced وبعدين تخـلي delete

root volume علشان ال EBS متمسحش وكذلك لـ on termination = no



I'm Here

تقدر تخلی ببردو ليه instance **delete on termination = no** علشان لما ال

تتمسح ال root volume دة يفضل موجود



I'm Here

▼ Configure storage [Info](#)

[Advanced](#)

1x GiB gp3 Root volume (Not encrypted)

1x GiB gp2 EBS volume (Not encrypted) [Remove](#)

 Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage [X](#)

[Add new volume](#)

▼ Storage (volumes) [Info](#)

[Simple](#)

EBS Volumes

[Hide details](#)

▶ Volume 1 (AMI Root) (8 GiB, EBS, General purpose SSD (gp3))

▼ Volume 2 (Custom) [Remove](#)

Storage type [Info](#)

EBS

Device name - required [Info](#)

/dev/sdb

Snapshot [Info](#)

Select

Size (GiB) [Info](#)

5

Volume type [Info](#)

gp2

IOPS [Info](#)

100 / 3000

Delete on termination [Info](#)

No

Encrypted [Info](#)

Not encrypted

KMS key [Info](#)

Select

KMS keys are only applicable when encryption is set on this volume.



I'm Here

→002 EBS Hands On

لو حددت ال instance من تحت هتعرف اية ال volumes اللى مرتبطة بيها سواء

EBS root او EBS اضافي

The screenshot shows the AWS CloudWatch Metrics interface. At the top, there's a search bar and a dropdown menu for 'Metric type'. Below that is a table with columns: Metric name, Namespace, Unit, and Last value. The table contains data for several metrics, including 'Latency' and 'Throughput' for different stages of the Lambda function.

Metric name	Namespace	Unit	Last value
Latency	aws.lambda.metric	Microseconds	1000000000000000000
Throughput	aws.lambda.metric	Bytes	1000000000000000000
Latency	aws.lambda.metric	Microseconds	1000000000000000000
Throughput	aws.lambda.metric	Bytes	1000000000000000000
Latency	aws.lambda.metric	Microseconds	1000000000000000000
Throughput	aws.lambda.metric	Bytes	1000000000000000000

لو ضغطت عال volume دة هيدخلك عالصفحة دي .. هتلaci معلومات عنه ومرتبط

باني create volume instance و هكذا ومن هنا تقدر ت .. او من هنا

Elastic Block Store (EBS) >> Volumes



I'm Here

Volumes (1/1)

Volume ID: vol-0ec2ac1777f918db3

Details Status checks Monitoring Tags

Volume ID	Size	Type	Volume status
vol-0ec2ac1777f918db3	8 GiB	gp2	Okay
Volume state	IOPS	Throughput	Encryption
In-use	100	-	Not encrypted

بعد ما بتكريت ال EBS volume بتاخذ وقت على ما تكون Available ف لازم دي instance علشان تقدر تعملها attach على Available تكون



I'm Here

Volumes (1/2)

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created
-	vol-0ec2ac1777f918db3	gp2	8 GiB	100	-	snap-00022cf...	2022/05/16 17:11 GMT+1
<input checked="" type="checkbox"/>	vol-07547a181f5ae63fc	gp2	2 GiB	100	-	-	2022/05/16 18:59 GMT+1

Volume ID: vol-07547a181f5ae63fc

Details | Status checks | Monitoring | Tags

Details

Volume ID vol-07547a181f5ae63fc	Size 2 GiB	Type gp2	Volume status Okay
Volume state Creating	IOPS 100	Throughput -	Encryption Not encrypted

Details

Volume ID vol-07547a181f5ae63fc	Size 2 GiB	Type gp2	Volume status Okay
Volume state Available	IOPS 100	Throughput -	Encryption Not encrypted

بعد ما عملت attach لو رجعت لـ instance ودخلت على ال storage هتلaci ان
ال Attached EBS Volume بالشكل دا

Block devices

Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encryp...
vol-0ec2ac1777f918db3	/dev/xvda	8	Attached	Mon May 16 2022 17:11:03...	No
vol-07547a181f5ae63fc	/dev/sdf	2	Attached	Mon May 16 2022 18:59:56...	No

لو عملت terminate لـ instance هتلaci ان ال root volume اتسخ اما ال
EBS volume by default لسة موجود .. دة بناءا على انك معملتش check على



I'm Here

ال CCP1 وانت بتكريته زي ما وضحتنا قبل كدا في ال delete on termination

ودة بيكون متوضح على اليمين من نفس الاسكرين اللي فاتت

Instance: i-034466697feb9ef80 (My First Instance)				
Block devices				
Attachment status	Attachment time	Encrypted	KMS key ID	Delete on termination
Attached	Mon May 16 2022 17:11:03...	No	-	Yes
Attached	Mon May 16 2022 18:59:56...	No	-	No

➡003 EBS Snapshots



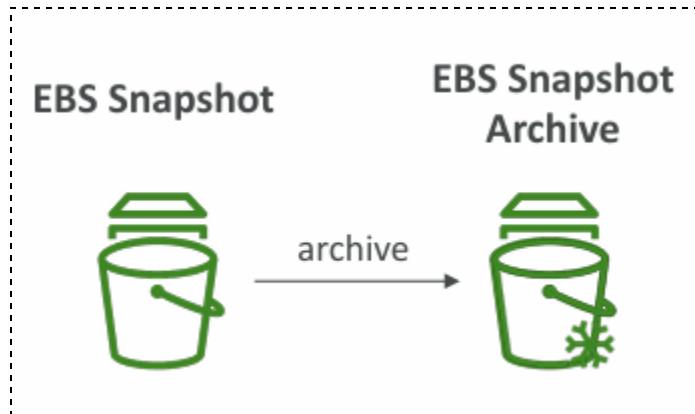
ول يكن انت تحتاج تأخذ backup من AZ1 ل AZ2 .. زي مقولنا مينفعش ال EBS1 تعملها attach ل instance في AZ2 تانية .. وبالتالي الحل هنا انك بتاخذ snapshot لـ EBS1 لـ instance volume لـ AZ2 فال snapshot restore عامل snapshot لـ EBS2 volume عال data اللي فال دى... ف كدا كل ال .EBS2 volume هترووح عال



I'm Here

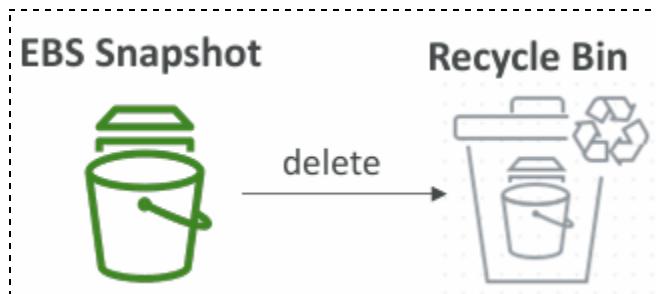
• EBS Snapshots Features

• EBS Snapshot Archive



- ممکن ت ال snapshot move ال "Archive tier" دی ل ودة بیکون ارخص بنسبة 75% ولكن بتستyi حوالی 24:72 ساعة لحد ما ترجع ال snapshot دی.

• Recycle Bin for EBS Snapshots



- بت recycle bin علشان لو مسحت snapshot بالغلط هتلaciها فی ال setup rules وبتفضل جوا لمدة سنة

• Fast Snapshot Restore (FSR)

- لو هتکریت من ال snapshot instance وعاوزها فی اسرع وقت ممکن ف دة انسب نوع ليك.



I'm Here

→004 EBS Snapshots - Hands On

عشان تكريت snapshot

Elastic Block Store (EBS) >> Volumes

Volumes (1/1)					Actions		Create volume
<input type="button" value="Filter volumes"/>					Actions		
Name	Volume ID	Type	Size		Modify volume	Create snapshot	Create snapshot lifecycle policy
-	vol-066e0164889e6ed9f	gp2	2 GiB		<input type="button" value="Modify volume"/>	<input type="button" value="Create snapshot"/>	<input type="button" value="Create snapshot lifecycle policy"/>

هتلقيها هنا ..

Elastic Block Store (EBS) >> Snapshots

Snapshots (1)							Actions		Create snapshot
<input type="button" value="Owned by me"/>							Actions		
Name	Snapshot ID	Size	Description	Storage...	Snapshot status		Actions	Create snapshot	
-	snap-0c379c9b4dcbfedf	2 GiB	DemoSnapshot	Standard	<input checked="" type="checkbox"/> Completed		<input type="button" value="Recycle Bin"/>	<input type="button" value="Actions"/>	

عشان ت copy snapshot ال region دى ل AZ

و عشان create volume دة ممكن تخليه فى اي volume منها..

Snapshots (1/1)							Actions		Create snapshot
<input type="button" value="Owned by me"/>							Actions		
Name	Snapshot ID	Size	Description		Create volume from snapshot	Create image from snapshot	Copy snapshot	Modify permissions	
-	snap-0c379c9b4dcbfedf	2 GiB	DemoSnapshot		<input type="button" value="Create volume from snapshot"/>	<input type="button" value="Create image from snapshot"/>	<input type="button" value="Copy snapshot"/>	<input type="button" value="Modify permissions"/>	



I'm Here

جوا ال snapshots هتلaci ال recycle bin اللى اتكلمنا عنها منها بتحدد عدد الايام

اللى تقدر فيها تسترجع ال snapshots الممسوحة

Snapshots (1)

Owned by me

Filter snapshots by attributes and tags

Name	Snapshot ID	Size	Description	Storage...	Snapshot status
-	snap-0c379c9b4dcbfedf	2 GiB	DemoSnapshot	Standard	Completed

Create snapshot

Recycle Bin

Resources

Retention rules

Recycle Bin > Resources

Resources (1/1) Info

EBS Snapshots

Name	Resource ID	Bin entry date	Bin exit date
-	snap-05fafc7f99b3e758e	Tue Apr 05 2022 23:34:00...	Wed Apr 06 2022 23:34:0...

Recover

من هنا تقدر ت archive زى ما شرحنا

Snapshots (1/1)

Owned by me

Filter snapshots by attributes and tags

Name	Snapshot ID	Size	Description
-	snap-0c379c9b4dcbfedf	2 GiB	DemoSnapshot

Actions ▲ Create snapshot

- Create volume from snapshot
- Create image from snapshot
- Copy snapshot
- Modify permissions
- Manage fast snapshot restore
- Archive snapshot** (highlighted)
- Restore snapshot from archive
- Change restore period
- Delete snapshot
- Manage tags

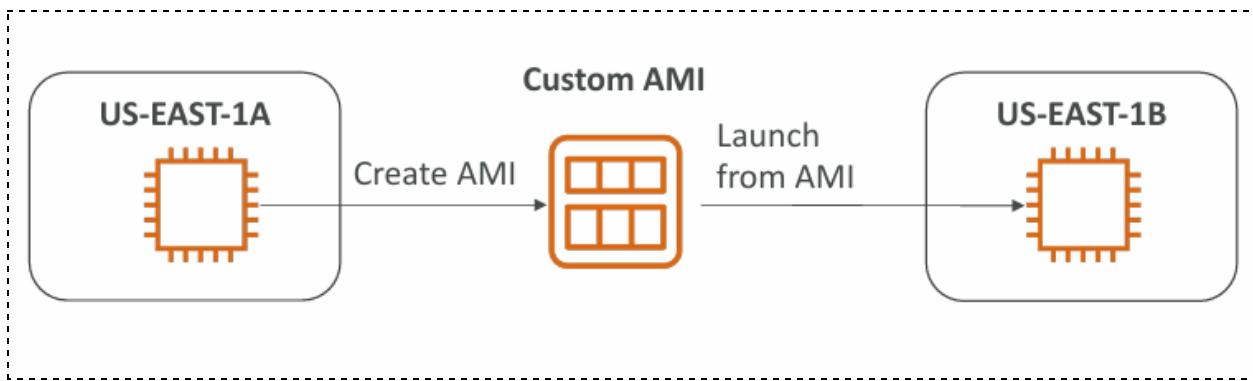
Snapshot ID: snap-0c379c9b4dcbfedf

Details	Permissions	Storage tier	Tags
Snapshot ID snap-0c379c9b4dcbfedf		Storage tier Standard	Archive completed on -
Volume ID vol-066e0164889e6ed9f		Tiering status -	Temporary restore expires on -
		Last tier change started on -	Tier change progress -



I'm Here

→005 AMI Overview (Amazon Machine Image)



- ودي عباره عن Instance يعني عباره عن Pre Configured Instances
جاهزة معملوها كل ال configuration اللي كنا بنعملها ف اول محاضرة
وبعملها Save as AMI image وفيما بعد لو عاوز اعمل نفس ال task بختار ال
Configuration دي علطول مش هفضل كل شوية اعمل نفس ال image

• أنواع ال AMI :

• Public AMI:

- ناس عملتها ومشير لها Public وتقدر انت تستخدمها علطول

• Private AMI (Yours):

- بتاعتكم انت اللي عاملها

• AWS Market Place AMI:

- ممكن يكون حد عامل Image معينه وبيبيعها مثلاً.



I'm Here

→006 AMI Hands On

The screenshot shows the AWS EC2 Instances page. A context menu is open over an instance named "My First Instance". The menu includes options like "Launch instances", "Launch instance from template", "Migrate a server", "Connect", "Stop instance", "Start instance", "Reboot instance", "Hibernate instance", "Terminate instance", "Instance settings", "Networking", "Security", and "Image and templates". A sub-menu under "Image and templates" shows "Create image".

بمجرد ما بتعمل ال instance image تقدر تعمل image بالشكل دة و هتلaciي ال هنا

تقدر ت launch instance الجديدة هتلaciيها بالظبط زي القديمة

كل ال configuration بتاعتها

Images >> AMIs

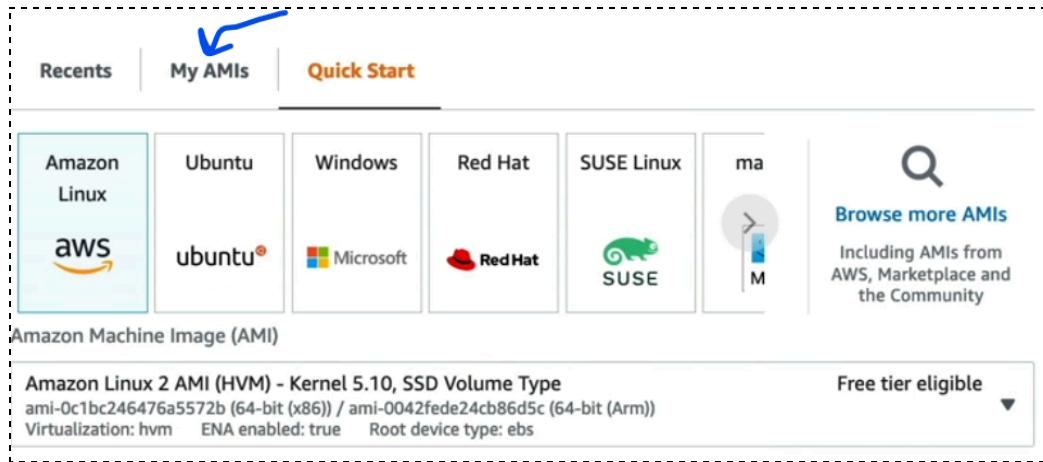
The screenshot shows the AWS AMIs page. A list of available AMIs is displayed, with one entry selected: "ami-019206cd8b19c8ffa" with the name "DemolImage" and source "783768293452/DemoImage".

او تقدر من ت launch instance ال AMI دي بالAMI دى وانت بتعمل ال

بالشكل العادي وبدل ما تختار AWS linux هتختر My AMI image وتختر ال



I'm Here



➡007 EC2 Instance Store

- احنا قولنا ان ال EBS volume بيفي عباره عن Virtual hard drive بتعمله instance attach لـ performance . هي كويسيـة ولكن ال instance attach شوية .. ف لو محتاج حاجة بـ Performance اعلى بيفي ال EC2 Instance Store

- **Cons:**

- فيها عيب وهو انك لو عملت instance store لـ terminate instance store على عكس ال EBS Volume لما كنت بتمسح ال instance store موجودة وكتـت تقدر ت delete it تانية إلا بـقا لو كنت عاملها on termination

- **Use Case:**

- Short term storage : Buffer, Cache, Temporary Data

 بيفي لو محتاج Short long storage دي تمام .. لو محتاج Long term storage

EBS افضل.



I'm Here

→008 EBS Volume Types

- **GP2/GP3 (SSD) - General Purpose**

- دة general-purpose ssd volume تقدر تستخدمه لل balance وتكلفته قليلة فيه
- بين ال performance , price ودة الى غالبا هنستخدمه واحنا بنجرب لانه بيستخدم فى boot volumes, Virtual desktops, Development and test environments

- **io1/io2 (SSD)**

- دة low latency و high-performance ssd volume تقدر تستخدمه لو تحتاج high throughput و
- يعني هينقل داتا بشكل اسرع : **high throughput**

- **st1 (HHD)**

- دة HHD volume تقدر تستخدمه لو عاوز low cost و high throughput ومش فارقالك ال لأن هنا ال latency تكون عالية شوية

- **sc1 (HHD)**

- زيرو زي الى قبله دة ولكن هنا لو انت مش بت access الداتا بتعاتك كل شوية يعني كل فتره بت access الداتا يبقي دة انساب نوع ليك واكيد سعرو اقل من اللى فوقه دة.

- بيتم تصنيف ال EBS Volumes على حسب ال size , throughput , IOPS

- **IOPS** : Operation Per Second



I'm Here

- **General Purpose SSD :**

- 1 GiB - 16 TiB
- System boot volumes, Virtual desktops, Development and test environments

- **Gp3:**

- Baseline of 3,000 IOPS and throughput of 125 MiB/s
 - **Can increase IOPS up to 16,000 and throughput up to 1000 MiB/s independently**

- **Gp2:**

- Small gp2 volumes can burst IOPS to 3,000
 - Size of the volume and IOPS are linked, max IOPS is 16,000
 - 3 IOPS per GB, means at 5,334 GB we are at the max IOPS

اقدر اتحكم فى ال IOPS منفصلين فى Gp3 على عكس ال Gp2 

- **Provisioned IOPS (PIOPS) SSD Use Cases**

- Critical business applications with sustained IOPS performance
- Or applications that need more than 16,000 IOPS
- Great for databases workloads (sensitive to storage perf and consistency)
- **io1 (4 GiB - 16 TiB)**
 - Max PIOPS: 64,000 for Nitro EC2 instances & 32,000 for other
 - **Can increase PIOPS independently from storage size**



I'm Here

- **io2 Block Express (4 GiB – 64 TiB):**
 - Sub-millisecond latency
 - Max PIOPS: 256,000 with an IOPS:GiB ratio of 1,000:1
- **Supports EBS Multi-attach**

- **Hard Disk Drives (HDD)**

- Cannot be a boot volume
- 125 GiB to 16 TiB
- **Throughput Optimized HDD (st1)**
 - Big Data, Data Warehouses, Log Processing
 - Max throughput 500 MiB/s – max IOPS 500
- **Cold HDD (sc1):**
 - For data that is infrequently accessed
 - Scenarios where lowest cost is important
 - Max throughput 250 MiB/s – max IOPS 250

IOPS 16000 بيقى gp2, gp3 لو محتاج اقل من

و io1 لحد 64000 واكتر من كدا لحد 250000 بيقى

مش محتاج تعرف كل ال details دي هتلaci كل التفاصيل دي [هنا](#)



I'm Here

● Solid state drive (SSD) volumes

	General Purpose SSD volumes		Provisioned IOPS SSD volumes	
Volume type	gp3	gp2	io2 Block Express ³	io1
Durability	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)		99.999% durability (0.001% annual failure rate)	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)
Use cases	<ul style="list-style-type: none"> Transactional workloads Virtual desktops Medium-sized, single-instance databases Low-latency interactive applications Boot volumes Development and test environments 		Workloads that require: <ul style="list-style-type: none"> Sub-millisecond latency Sustained IOPS performance More than 64,000 IOPS or 1,000 MiB/s of throughput 	<ul style="list-style-type: none"> Workloads that require sustained IOPS performance or more than 16,000 IOPS I/O-intensive database workloads
Volume size	1 GiB - 16 TiB		4 GiB - 64 TiB ⁴	4 GiB - 16 TiB
Max IOPS per volume	16,000 (64 KiB I/O)	16,000 (16 KiB I/O)	256,000 (16 KiB I/O) ⁵	64,000 (16 KiB I/O)
Max throughput per volume	1,000 MiB/s	250 MiB/s ¹	4,000 MiB/s	1,000 MiB/s ²
Amazon EBS Multi-attach	Not supported		Supported	
NVMe reservations	Not supported		Supported	Not supported
Boot volume	Supported			

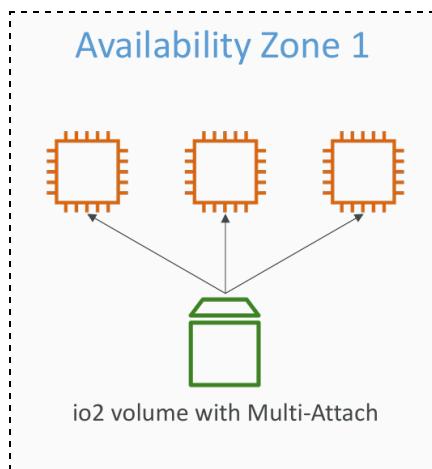
● Hard disk drive (HDD) volumes

	Throughput Optimized HDD volumes	Cold HDD volumes
Volume type	st1	sc1
Durability	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)	
Use cases	<ul style="list-style-type: none"> Big data Data warehouses Log processing 	<ul style="list-style-type: none"> Throughput-oriented storage for data that is infrequently accessed Scenarios where the lowest storage cost is important
Volume size	125 GiB - 16 TiB	
Max IOPS per volume (1 MiB I/O)	500	250
Max throughput per volume	500 MiB/s	250 MiB/s
Amazon EBS Multi-attach	Not supported	
Boot volume	Not supported	



I'm Here

→009 EBS Multi-Attach



EBS Multi-Attach is a feature of Amazon EBS that **allows you to attach a single Provisioned IOPS SSD (io1 or io2) volume to multiple EC2 instances in the same Availability Zone**. Here's an overview of EBS Multi-Attach:

- **Key points:**

io1/io2 متحدة فقط لنوع

- تقدر تربط ال EBS Volume دة بعدد 16 instances فى Nitro-based EC2 instances
- نفس الوقت
- لازم ال instances تكون فى نفس ال AZ
- تستخد فى applications ودى clustered Linux applications
- across multiple servers

- Requires a cluster-aware file system (not standard file systems like ext4 or XFS).

- **Benefits:**

- High availability : لو fail instance حصلها الباقي بيشتغل
- بتمكناك ت build clustered applications



I'm Here

➡010 EBS Encryption

• لو عملت EBS Volume encrypted : هتحصل على الآتي :

- كل ال data اللي فى ال EBS Volume دي بتكون encrypted
- ال data اللي بتروح و نتيجي بين ال EBS Volume وال instances بتكون encrypted
- كل ال instances وال snapshots اللي هتعمل من ال snapshots دي بتكون encrypted
- ال latency بيسبب طفيف جدا مش هتحس بيها

• EBS Encryption leverages keys from KMS (AES-256)

- KMS stands for AWS Key Management Service.
 - AES stands for Advanced Encryption Standard, a widely used encryption algorithm, 256 refers to the key size in bits.
- يبقى ال encryption بيتمن من خلال AWS KMS والنوع ال default اللي بيتم -
استخدامه هو (AES-256)

• Encryption: encrypt an unencrypted EBS volume

- Create an EBS snapshot of the volume
- Encrypt the EBS snapshot (using copy)
- Create new EBS volume from the snapshot (the volume will also be encrypted)



I'm Here

- Now you can attach the encrypted volume to the original instance

ياعني كان عندنا unencrypted EBS volume وكنا عازين نخليه encrypted

Snapshots (1/1)

Name	Snapshot ID	Size	Description
-	snap-065047d562375dad5	1 GiB	-

Actions

- Create volume from snapshot
- Create image from snapshot
- Copy snapshot**
- Modify permissions

New snapshot settings

Description
A description for the snapshot copy.
[Copied snap-065047d562375dad5 from eu-west-1]
255 characters maximum.

Destination Region
The Region in which to create the snapshot copy.
eu-west-1

Encryption Info
Use Amazon EBS encryption as an encryption solution for your EBS resources.
 Encrypt this snapshot

KMS key Info
(default) aws/ebs

KMS key description
 Default key that protects my EBS volumes when no other key is defined

Snapshots (1/2)

Name	Snapshot ID	Size	Description
-	snap-0278ddf9af9548627	1 GiB	[Copied snap-065047d562375dad5]

Actions

- Create volume from snapshot
- Create image from snapshot
- Copy snapshot

هتلacihe already encrypted بما انه معمول من



I'm Here

Encryption Info

Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.

Encrypt this volume

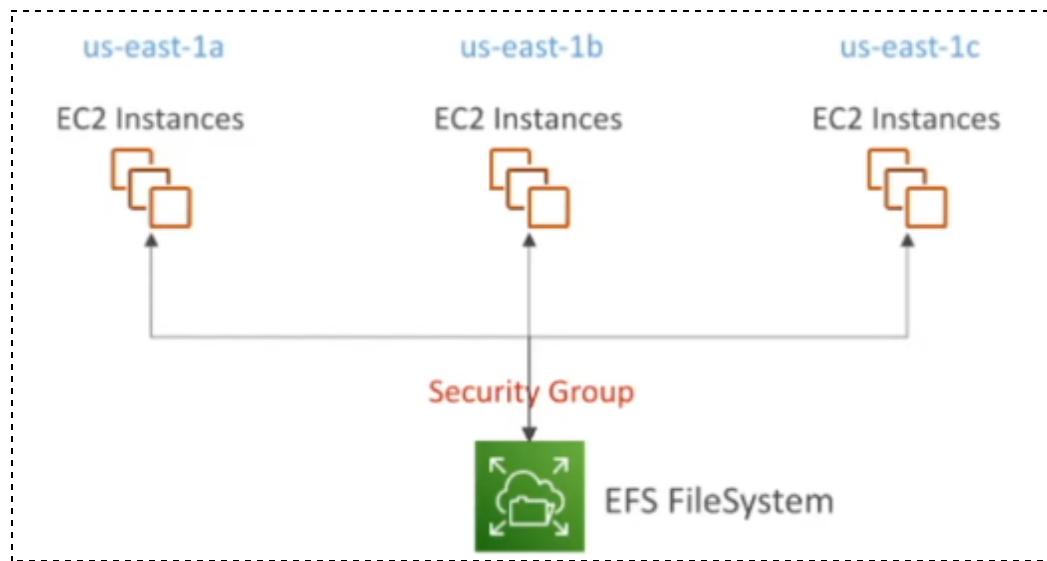
- أما لو بتعمل EBS Volume من جديد ف ممكن تخليه encrypted direct

Encryption Info

Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.

Encrypt this volume

→011 Amazon EFS (Elastic File System)



- إل storage EFS كان أما هنا عباره عن

- بتدفع عال storage اللي بتسخدمها فقط



I'm Here

- **Key Points**

- **Use Cases: Content management, web serving, data sharing, Wordpress**

- **Uses NFSv4.1 (Network file system) protocol**

- ودة استخدامه انو بيمكنك من انك ت access files over the internet سواء هت عليها read or write

- **Uses security group to control access to EFS**

- اللي داخل واللى خارج من ال file system دة بنعرف نتحكم فيه

- **Compatible with Linux based AMI (not Windows)**

- شغالة مع فقط Linux

- **Encryption at rest using KMS**

- الداتا اللي عال file system دة بتكون encrypted AWS KMS اللي هيا Key Management Service

- **POSIX file system (~Linux) that has a standard file API**

- بتشغل اكناها POSIX عادي زي بتاع linux دة يعني انها بتتبع ال Standards اللي هيا بتصرف بالطريقة العادية زي ما كنت فى لينكس بنفس طريقة ال file handling commands وال ياعني تقدر تستخدم معاها ls , mv , cp وهكذا



I'm Here

- File system scales automatically, pay-per-use, no capacity planning!

- ال EFS بت grow .. ياعني هت write data هتلقيها بت grow , shrink هتمسح

"pay for what you use .. ياعني هتلقيها بت shrink data

- EFS – Performance & Storage Classes

- وانت بت Create ال EFS هتلافي عندك:

- Performance Mode:

- General Purpose (default): latency-sensitive use cases (web server, CMS, etc...)

- ودة بيكون حاجة balanced كدا من جميع النواحي

- Max I/O: higher latency, throughput, highly parallel (big data, media processing)

- دة لو تحتاج high throughput بيكون اغلي شوية أكيد .. هتفهم معنى ال throughput دلوقتي

- Throughput Mode:

- Bursting : 1 TB = 50MiB/s + burst of up to 100MiB/s

- عباره عن Traffic عالي فجأة عال EFS ف هل عاوز ال EFS يهندل ال traffic اللي حصل دة ولا انفجار Bursting

- Provisioned : set your throughput regardless of storage size, ex: 1 GiB/s for 1 TB storage

- بتهيئها .. ياعني بتحدد انت عاوز ال throughput بتاعك يكون قد اية وليكن مثلا 1 GB/sec



I'm Here

- **Elastic** : automatically scales throughput up or down based on your workloads

وحة بيـ Scale Automatic مع الـ work load اللـى جـاي وبيعمل -

وـدة بيـون مفضـل فـي الـ up and down unpredictable workloads

يبي مثلا لو عندك بيتبعدt ول يكن 1 GB عال file system دة وفجاة بقو 20 GB ف دة (انفجار) .. اما لو انت عارف ال throughput rate ف خليك provision .. أما لو عاوز الموضوع dynamic ف خليك elastic وكلو بحسابه 😊.

- **Storage Tier:**

- هنعمل اية في ال file system دة بعد فتره معينه .. في عندك فيها 3 option 3
بن manage بيها ال lifecycle بتاعه ال file system من خلالها تقدر تحدد

- Frequently Accessed:

- مُصمم لـ active data workloads الـ data access اللي بيحصلها باستمرار

- **Infrequently Accessed(EFS IA):** cost to retrieve files, lower price to store.

- مناسبة لو ال data بنا عتنا مش بيحصلها access كتير .. بتكون هنا التكلفة أقل ولكن فيه تكلفة على استرجاع الملفات

- **Archive:** rarely accessed data (few times each year), 50% cheaper

- "ارخص منهم" options اللّى فوق وطبعاً اقل لك عدد مرات من الـ 2 access بيحصلها لو الـ data



I'm Here

Lifecycle management

Automatically save money as access patterns change by moving files into the Infrequent Access (IA) or Archive storage class. [Learn more](#)

Transition into Infrequent Access (IA)

Transition files to IA based on the time since they were last accessed in Standard storage.

30 day(s) since last access

Transition into Archive

Transition files to Archive based on the time since they were last accessed in Standard storage.

90 day(s) since last access

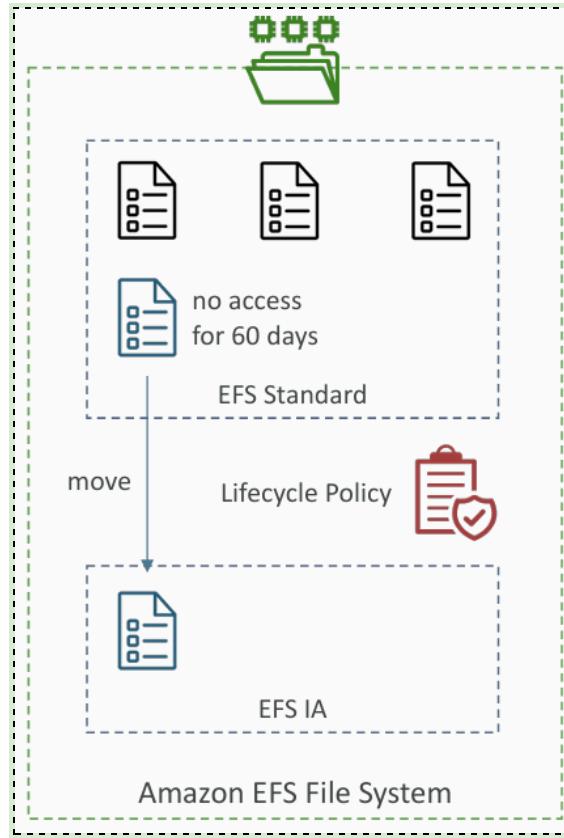
Transition into Standard

Transition files back to Standard storage based on when they are first accessed in IA or Archive storage.

None

عشنان ت move ال data between storage tiers بتعنك دي بيتم دة من خلال 

انك بت set lifecycle polices تحققلك دة.



• Availability & Durability:

- **Regional:** Multi-AZ, great for prod

- متاح ف اكتر من AZ .. ياعني لو واحدة وقعت ال EFS file system دة يفضل شغال

"اغلي .. مناسب لل production environment"



I'm Here

- **One Zone:** One AZ, great for dev, backup enabled by default, compatible with IA (EFS One Zone-IA)

يشتغل ف zone واحدة فقط .. وده مناسب اكتر لـ development or backup or "testing

File system type

Choose to either store data across multiple Availability Zones or within a single Availability Zone. [Learn more](#)

Regional
Offers the highest levels of availability and durability by storing file system data across multiple Availability Zones within an AWS Region.

One Zone
Provides continuous availability to data within a single Availability Zone within an AWS Region.

→012 Amazon EFS - Hands On

على EFS setting اللي عاوزها بناء على اللي اشرح فوق
وختار security group ولو معملتش security group مخصص لـ EFS
وارجع اختياره وبعدها تكريت ال instances وترتبط ال instances بال EFS

Network settings [Info](#)

VPC - required [Info](#)

vpc-0799daa55c9fb6493 (default) [Edit](#)

172.31.0.0/16

Subnet [Info](#)

No preference

[Create new subnet](#)

subnet-0b033c07c2fcf2d1b

VPC: vpc-0799daa55c9fb6493 Owner: 510512620071 Availability Zone: us-east-1d
IP addresses available: 4091 CIDR: 172.31.32.0/20

subnet-0a3d455d7730cdc92

VPC: vpc-0799daa55c9fb6493 Owner: 510512620071 Availability Zone: us-east-1a
IP addresses available: 4091 CIDR: 172.31.0.0/20

subnet-017c65ab00faaf2af

VPC: vpc-0799daa55c9fb6493 Owner: 510512620071 Availability Zone: us-east-1c
IP addresses available: 4091 CIDR: 172.31.16.0/20

subnet-0d0cb74f90357682b

VPC: vpc-0799daa55c9fb6493 Owner: 510512620071 Availability Zone: us-east-1b
IP addresses available: 4091 CIDR: 172.31.80.0/20



I'm Here

" هكريت مثلا instance A مجرد اسم اول واحده يعني .. من ال network setting هختار لها subnet طب انهي subnet setting هختار لها us-east-1b instance B وهكذا us-east-1a instance A "

"دي كدا وانت بتكريرت ال EFS بتختار ال subnet وال security group وكمان "

Mount targets

A mount target provides an NFSv4 endpoint at which you can mount an Amazon EFS file system. We recommend creating one mount target per Availability Zone. [Learn more](#)

Availability zone	Subnet ID	IP address	Security groups
us-east-1a	subnet-0a3d455d7730cdc92	Automatic	Choose security groups sg-0cb83134332e4b1c2 X default
us-east-1b	subnet-0d0cb74f90357682b	Automatic	Choose security groups sg-0cb83134332e4b1c2 X default
us-east-1c	subnet-017c65ab00faaf2af	Automatic	Choose security groups sg-0cb83134332e4b1c2 X default
us-east-1d	subnet-0b035c07c2cf2d1b	Automatic	Choose security groups sg-0cb83134332e4b1c2 X default
us-east-1f	subnet-09a2ba7c68db5b25e	Automatic	Choose security groups sg-0cb83134332e4b1c2 X default

بتختار نفس ال file system لـ instances لـ file system لـ instances لـ file system

mount point و بتختار نفس ال system



I'm Here

File systems

EFS FSx

Shared file system 1

File system Info
fs-03ad3ad91588ea5e7
Availability: Regional

Mount point Info
/mnt/efs/fs1

Add shared file system **Create new shared file system**

4 remaining (Up to 5 file systems maximum)

Automatically create and attach security groups
To enable access to the file system, the required security groups will be automatically created and attached to this instance and the selected file system. To manually manage the security groups, clear the checkbox. [Learn more](#).

Automatically mount shared file system by attaching required user data script
Automatically mount your file system by updating your user data to install efs-utils. If you would like to manually mount your file system, clear the checkbox.

تلقائي بيتعمل security groups عال instances اللي بتحتوي عال AZs اللي بتاعتك اللي

مرتبطة ب واحد .. ياعني ال 3 instances اللي عملناهم دلوقتي كل واحدة كانت

في AZ مختلفه ف لو دخلت على ال EFS هتلقي ان فيه بالإضافة لل security group اللي

عملناه فيه اتعملت ال security groups by default security groups اللي اتعملت

تلقائي دي ولو دخلت عال inbound rules دي هتلقي انها في ال security groups بتسمح



I'm Here

ب بـ protocol NFS الى اتكلمنا عنـه قبل كـذا.

Availability zone	Mount ID	Subnet ID	target state	IP address	Network interface ID	Security groups
eu-west-1a	fsmt-095ef9845742400c7	subnet-09b25e9baf4dae1d7	Available	172.31.24.238	eni-01d64b8447127d289	sg-0e949281 1e288e9e0 (efs-sg-1), sg-01357c51 28cce2851 (efs-sg-2), sg-0600b2c4 30ec51f45 (efs-demo)
eu-west-1b	fsmt-0887a085cec67f874	subnet-069b03c0b1a519b91	Available	172.31.45.40	eni-0a1559b3f69e200c1	sg-0e949281 1e288e9e0 (efs-sg-1), sg-01357c51 28cce2851 (efs-sg-2), sg-0600b2c4 30ec51f45 (efs-demo)

Security Groups (1/1) Info C Actions Export security groups to CSV Create security group

Filter security groups

Name	Security group ID	Security group name	VPC ID	Description
sg-01357c5128cce2851	efs-sg-2	vpc-0a40b157dcd7c81f1	Created by th	

Details Inbound rules Outbound rules Tags

You can now check network connectivity with Reachability Analyzer Run Reachability Analyzer

Inbound rules (1/1) C Manage tags Edit inbound rules

version	Type	Protocol	Port range	Source
	NFS	TCP	2049	sg-0521b4deede655e...

لو روحـت بـقا دخلـت عـلـى اول mount point file فى الـ instances فى الـ file system

و سـجـلت خـروـج و دـخـلـت عـالـ instance التـانـيـة او التـالـيـه و دـخـلـت عـلـى نفسـ الـ

mount point هـتـلاـقـي نفسـ الـ file هـنـاك .. فـ الـ 3 مشـتـرـكـين فى نفسـ الـ mount point

على نفسـ الـ file system رغمـ انـهـم فى different AZs



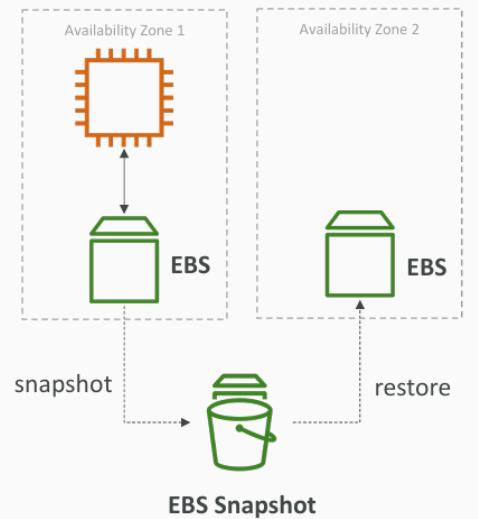
I'm Here

→013 EBS vs EFS:

- إتكلمنا ف كل دة قبل كدا دة بس ملخص سريع.

● EBS

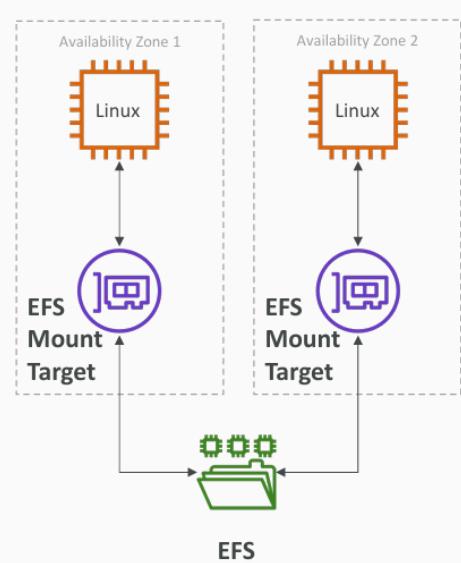
- EBS volumes...
 - one instance (except multi-attach io1/io2)
 - are locked at the Availability Zone (AZ) level
 - gp2: IO increases if the disk size increases
 - gp3 & io1: can increase IO independently
- To migrate an EBS volume across AZ
 - Take a snapshot
 - Restore the snapshot to another AZ
 - EBS backups use IO and you shouldn't run them while your application is handling a lot of traffic
- Root EBS Volumes of instances get terminated by default if the EC2 instance gets terminated. (you can disable that)



I'm Here

• EFS

- Mounting 100s of instances across AZ
- EFS share website files (WordPress)
- Only for Linux Instances (POSIX)
- EFS has a higher price point than EBS
- Can leverage Storage Tiers for cost savings
- Remember: EFS vs EBS vs Instance Store



➡014 EBS & EFS - Section Cleanup

- هتمسح كل حاجة كدا كدا انت المفروض ..,instances,volumes,snapshots .

بتمسح اول باول علشان التكفله.



I'm Here

CH-08 - High Availability and Scalability ELB & ASG

→001 High Availability and Scalability

- **Scalability:**

- قدرة ال system على انو يهندل ال increased load الى جايده عن طريق

: adding resources وعندك منها نوعين



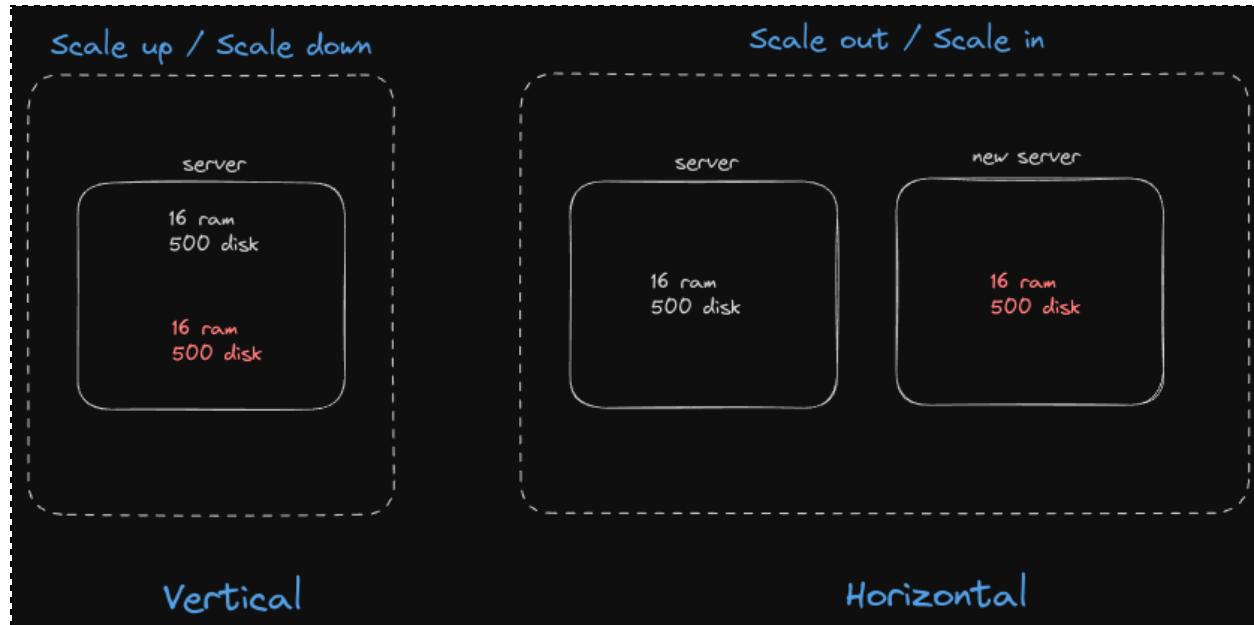
I'm Here

- **Vertical Scaling (Scaling Up/down):**

Machine على نفس ال power CPU, RAM - اضافة

- **Horizontal Scaling (Scaling Out/in)**

Machines اضافة زيادة -



- **Availability:**

قدرة ال system على انو يفضل up and running وده بيتم عن طريق انو يكون ليه

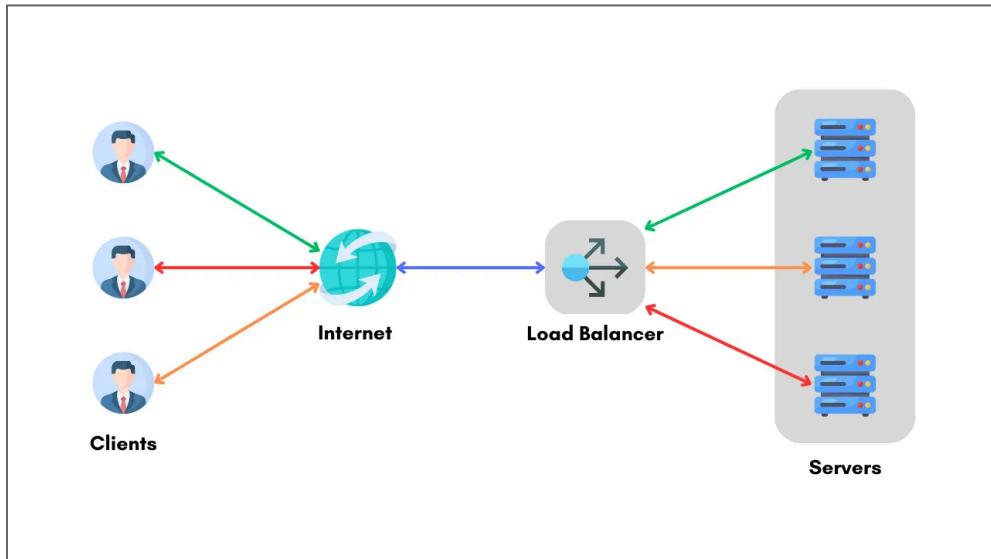
.redundancy, failover mechanisms, and reliable infrastructure

موجود ف كذا AZs مثلا علشان لو instance وقعت الثانيه تشتعل وهكذا.



I'm Here

→002 Elastic Load Balancing (ELB) Overview



: عباره عن server او مجموعة من ال servers وظيفتها انها -
توزيع ال load او ال traffic اللى جايلها على مجموعة من ال back end servers .. موضوع ال AWS load balancing دة downstream instances
بنسميهم اسمها service Elastic Load Balancer بتقدمه لك



I'm Here

- **Key Diff Between AWS LB & Nginx LB**

Key Differences

1. Management and Maintenance:

- **NGINX:** Requires manual setup, configuration, and maintenance.
- **ELB:** Fully managed by AWS, reducing operational overhead.

2. Scalability:

- **NGINX:** Manual scaling and configuration required.
- **ELB:** Automatically scales to handle traffic fluctuations.

3. Availability and Redundancy:

- **NGINX:** Requires additional setup for high availability and failover.
- **ELB:** Built-in high availability and fault tolerance.

4. Customization and Control:

- **NGINX:** Greater control and customization options.
- **ELB:** Limited to AWS-provided configurations but sufficient for most use cases.

5. Cost:

- **NGINX:** Potentially lower costs but higher management overhead.
- **ELB:** Pay-as-you-go pricing, potentially higher costs but lower management overhead.

- **Types of load balancer on AWS**

- **Classic Load Balancer (v1 - old generation) – 2009 – CLB**
 - **Support Protocols:** HTTP, HTTPS, TCP, SSL
- **Application Load Balancer (v2 - new generation) – 2016 – ALB**
 - **Support Protocols:** HTTP, HTTPS, WebSocket
- **Network Load Balancer (v2 - new generation) – 2017 – NLB**
 - **Support Protocols:** TCP, TLS (secure TCP), UDP



I'm Here

● Gateway Load Balancer – 2020 – GWLB

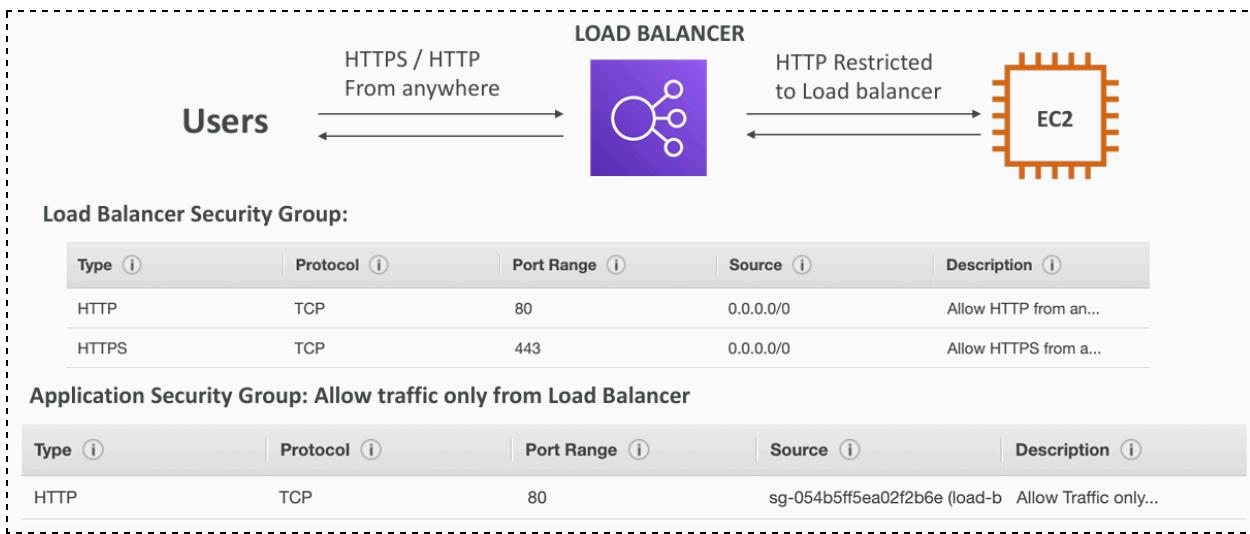
- Operates at layer 3 (Network layer) – IP Protocol
- هنتكلم عن كل نوع بالتفصيل تحت.

انك تستخدم ال Recommended new generations ببقي فيهم features اكتر. 

 Some load balancers can be setup as internal (private) or external (public) ELBs

● Load Balancer Security Groups

من ال user لـ load balancer بال security group بتسمح فى ال load balancer بال requests anywhere اللي جاي من requests أما من ال instances لـ load balancer اللي جاي من requests ف بتسمح فقط بال requests عن طريق ال load balancer وده بيحصل عن طريق انك بتحدد فى ال security group بتعالى instance هو ال source group بتعالى load balancer



I'm Here

→003 Note About the 1-Classic Load Balancer (CLB)

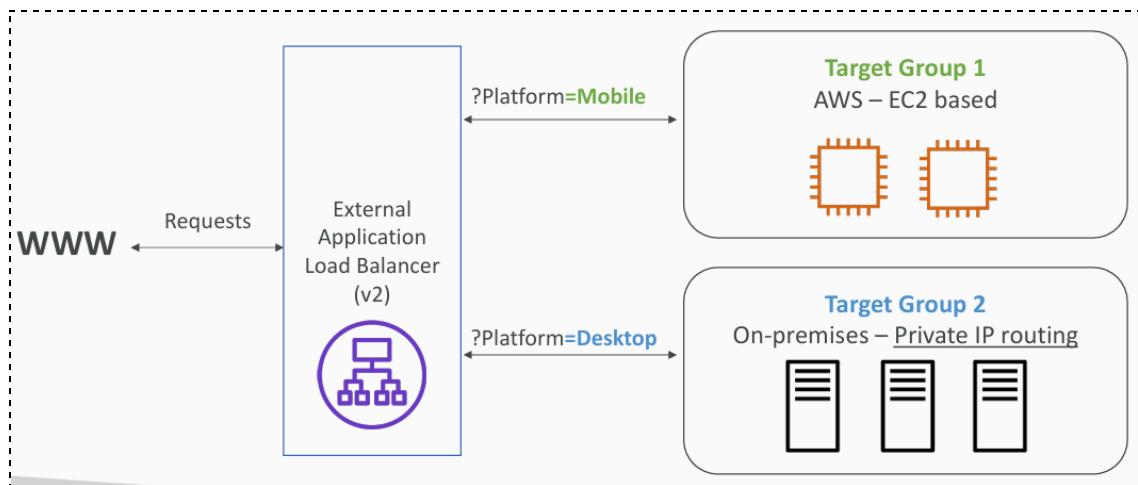
- The Classic Load Balancer is deprecated at AWS and will soon not be available in the AWS Console.
- The exam also has removed any references to it, so we will not cover it in depth in the course, nor the hands-on.

→004 2-Application Load Balancer (ALB)

• Key Features

بیشتعل ف 7 rules و بیندل ال traffic الی جای علیه بناءا على -
specifications كثیره
SSL/TLS Termination -

• Target Groups:



عبارة عن load balancer تكون خلف ال Backend Component -
اي حاجة من دول :



I'm Here

- **EC2 instances** (can be managed by an Auto Scaling Group) – HTTP
- **ECS tasks** (managed by ECS itself) – HTTP
- **Lambda functions** – HTTP request is translated into a JSON event
- **IP Addresses** – must be private IPs – must be private IPs

 ALB can route to **multiple target groups**

 Health checks are at the target **group level**

- **Listeners and Rules:**

ال **Listener Rules** دی عباره عن ان ازاي ال load balancer هيتعامل مع ال
اللى جايه من ال user ويعملها routing على ال Target groups وده بيعتمد
على بعض ال : conditions

- **Route based on URL PATH**

If the URL path is `/images/*`, >> route traffic to **Target Group 1**.

If the URL path is `/videos/*`, >> route traffic to **Target Group 2**.

- **Route Based on Host Name**

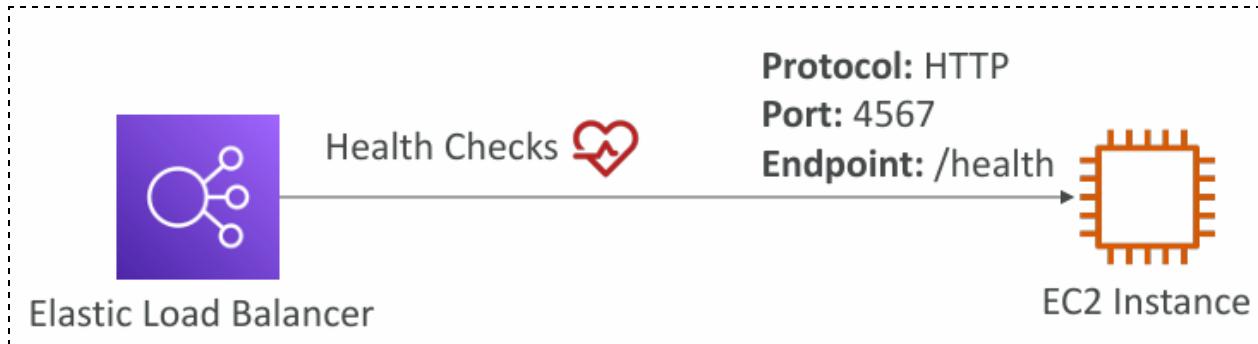
If the hostname is `api.example.com`,>>route traffic to **Target Group 1**.

If the hostname is `www.example.com`,>>route traffic to **Target Group 2**.



I'm Here

• Health Check



- عباره عن process ال load balancer بيعملها بانتظام علشان يتتأكد ان ال requests قادره انها ت respond اللـى هو باعدها ولا لا.
- سواء بتسخدم load balancer software او aws load balancer على سيرفرك زي nginx فانت بت configure ال health options الخاصة بال check.
- لما بتكرريت health check configuration بتقدر انك تعمل Targets group والخطوة الجايـة هيتووضح ياعني اية Health Check اكتر.

• Health Check Configuration:

- Configuration:
 - Target Type: EC2 instances
 - Health Check Protocol: TCP
 - Protocol: HTTP
 - Path: /healthcheck
 - Port: 80
 - Interval: 30 seconds
 - Timeout: 5 seconds
 - Healthy Threshold: 2



I'm Here

- **Unhealthy Threshold: 2**

- فـ المثال دة ال load balancer هيبيعت كل 30 ث لـ request

http://<target-ip>:80/healthcheck

- لو الـ request respond 200 ok فـ خلال 5 ث ..

It is considered **healthy**.

- لو الـ request fails فـ خلال 5 ث أو .. response with error

It is considered **unhealthy**.

- health checks fail فـ 2 حصله Target: لو الـ Unhealthy Threshold

.. متابعين ..

It will be marked as **unhealthy** and **stops receiving traffic**.

- health checks 2 success فـ Target: Healthy Threshold لو الـ

متتابعين .. وبلاش 1 دة مش مؤشر قوي ان ال instance تستحمل ولاا

it is marked as **healthy** and **starts receiving traffic again**.



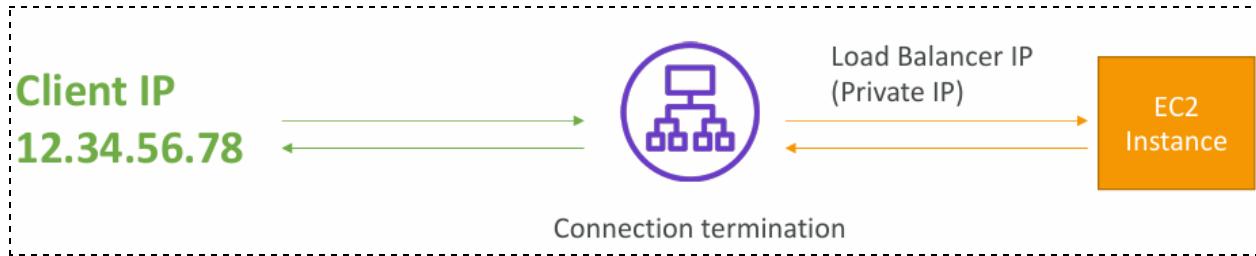
if the health check found the instance not working it will be

terminated then replaced



Health Checks support the TCP, HTTP and HTTPS Protocols.

● ‘X-Forwarded-For’ Header (How it works?):



I'm Here

- اـلـ client لما بيعمل request بيروح لل <> Application Load Balancer
- اـلـ ALP دة بيـشـتـغـلـ فـ 7 layer وبيـهـنـدـ الـ HTTP , HTTPS Traffic
- اـلـ ALP بيـضـيـفـ لـ X-Forwarded-For Header request الـ forward
- اـلـ ALP بيـهـنـدـ الـ targets بعد ما انـضـافـلـةـ الـ Header

```
GET / HTTP/1.1
Host: www.example.com
X-Forwarded-For: 192.0.2.1
```

- دا كـدا شـكـلـ الـ request الـ targets بعد ما انـضـافـلـةـ الـ Header

 الفـائـدةـ مـنـ الـمـوـضـوـعـ دـةـ إـنـ الـ backend target يـبـ

Can identify the original client's IP address for logging, analytics, and security purposes,
Helps in tracing the request path through multiple proxies.

→005 Application Load Balancer (ALB) - Hands

On - Part 1

هـتـكـرـيـتـ 2 instances http والـ SG بتـاعـهـمـ هـتـسـمـحـ فيهـ انـ الـ connections any where وـهـتـكـرـيـتـ الـ load balancer وـهـتـسـمـحـ الـ تـيـجيـ عنـ طـرـيـقـ any where وـهـتـكـرـيـتـ الـ load balancer any where منـ http والـىـ خـارـجـةـ منهـ برـدو connection الـىـ دـاخـلـلـهـ انـهاـ تكونـ any where والـىـ خـارـجـةـ منهـ برـدو ec2 instances قادرـ الـ load balancer يـسـتـلمـ ويـوزـعـ عـالـ all all وـبـالـتـالـيـ كـداـ قـادـرـ الـ loadbalancer DNS اوـ الـ ip addresses instances بتـاعـ

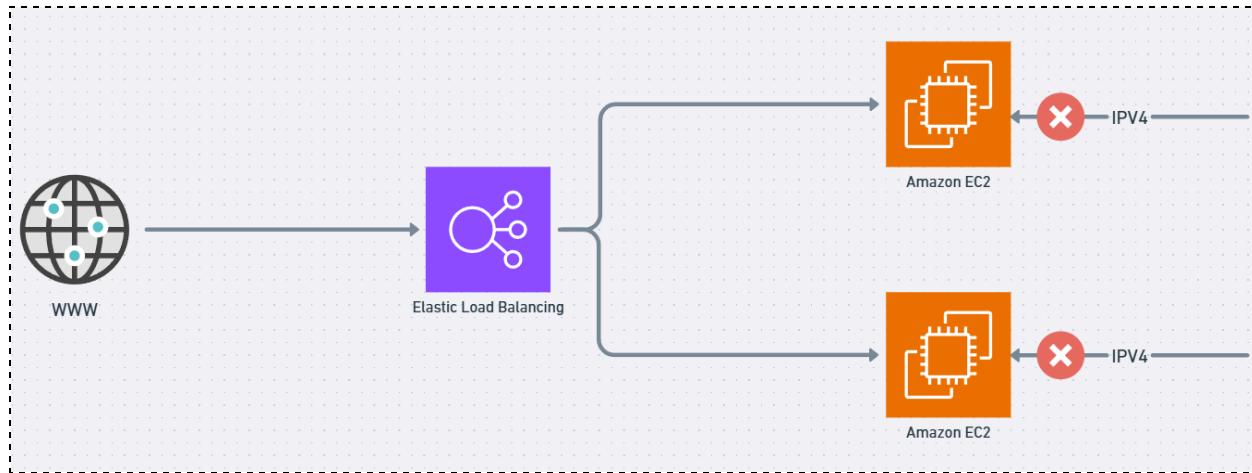


I'm Here

→006 Application Load Balancer (ALB) - Hands

On - Part 2

- Tip1- Enter the instances through ALB only



لما اشتغلنا فى Part 1 كنا نقدر ن access ال EC2 Instances سواء من ال IPv4 بتاعهم او تخش عال Load Balancer DNS وهو بيوز عك عليهم .. ف احنا عاوزين نقول جزأيه ان حد يقدر يخشن عال EC2 Instances direct من خال ال load balancer

دة هيتم عن طريق ال security group قولنا انها اكناها عباره عن firewall بت security group inbound , outbound traffic control

Edit inbound rules

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules	Type	Protocol	Port range	Source	Description - optional
sgr-0a481cf93629863c8	SSH	TCP	22	Custom	
sgr-0d3e6dcdd8ab1b41a	SSH	TCP	22	Custom	
-	HTTP	TCP	80	Custom	

Security Groups dropdown:

- demo-sg-load-balancer... | sg-06e7d5c80e3c17dcc
- Q load X

Add rule



I'm

بنّاع ال instances ون allow فى ال inbound rules يجليك فقط من

ال load balancer بنّاع ال Security group

دلوقي لو جيت ت timeout من خلال ال IPv4 هت instances Access معاك.

● Tip2 - Modify the ALP Listeners & rules

Go to ALP >> Listeners >> HTTP-80 >> Listeners rules >> add rules

Add condition Rule limits

Rule condition types

Route traffic based on the condition type of each request. Each rule can include one of each of the following conditions: host-header, path, http-request-method and source-ip. Each rule can include one or more of each of the following conditions: http-header and query-string.

Source IP	Include one of each
Host header	
Path	Paths are not supported.
HTTP request method	
Source IP	Include one or more of each
HTTP header	this rule.
Query string	

Cancel Confirm

تقىر تحط عدد ال rules اللي انت عاوزها وكل rule بال condition بنّاعها .. وبعدين

بتحدد ال action اللي هيحصل بناءا عال condition دة

هنا احنا هنعمل action معين يحصل لو ال user دخل عال path دة

Path

Define the path. For example: /item/*. Case sensitive.

is /error

Maximum 128 characters. Allowed characters are a-z, A-Z, 0-9; the following special characters: _-.~/~"@:@; & (using &); and wildcards (*) and (?).



I'm Here

Actions

Action types

Forward to target groups Redirect to URL Return fixed response

Return fixed response Info

Use fixed-response actions to drop client requests and return a custom HTTP response. When a fixed-response action is taken, the action and the URL of the redirect target are recorded in the access logs.

Response code
The type of message you want to send.
404

Content type - optional
The format of your message.
text/plain

Response body - optional
Enter your response message.
Not found, custom error!

1024 character maximum

هتلaci عنده حاجة اسمها priority معناها الأولوية .. فايدتها أننا لو عندنا rule 100

مثلاً الـ rule اللي الأولوية بتاعتتها على هي اللي هتنفذ

Rule: DemoRule

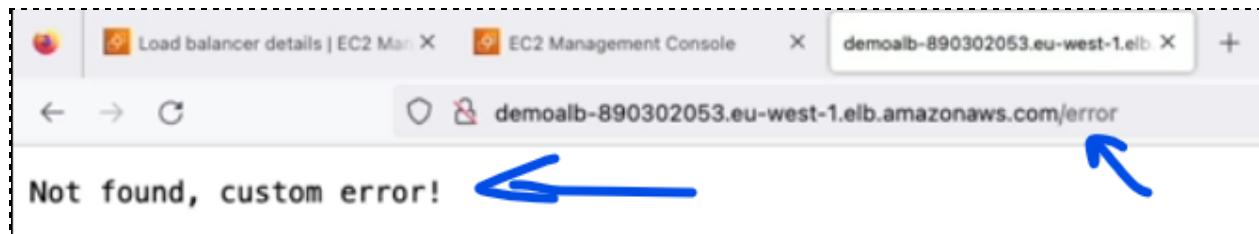
Priority

Rule priority controls the evaluation order of a rule within the listener's set of rules. You can leave gaps in priority numbers.

5

1 - 50000

ودي كانت النتيجة



I'm Here

→007 Network Load Balancer (NLB)

• Key Features

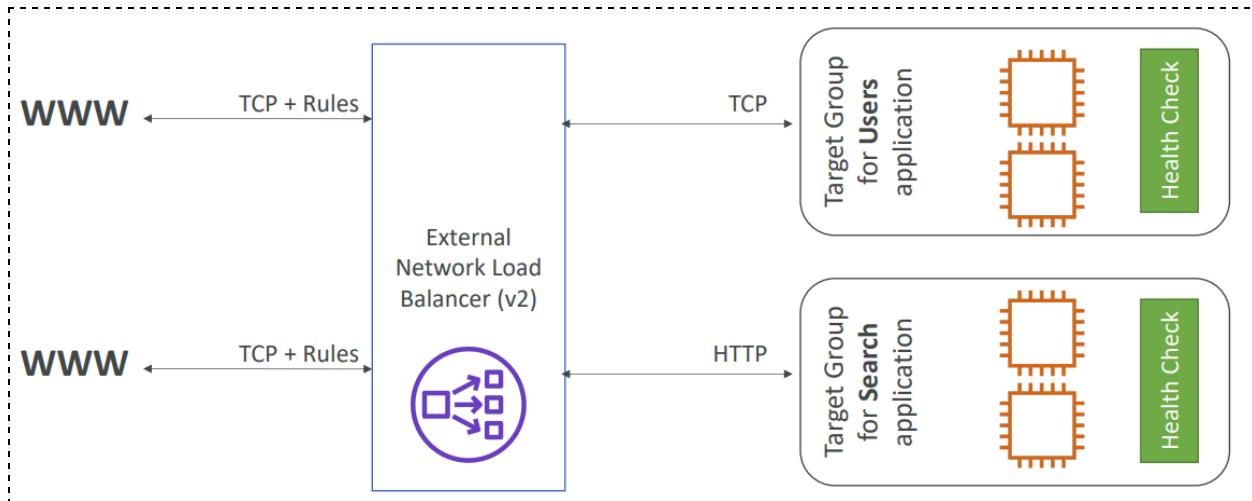
- بيشتغل في Layer 4 وبـ TCP & UDP traffic
- بيهدل الـ real-time .. وده بيخلية مناسب اكتر لـ high volume of connections
- .gaming, media streaming, or financial services
- الـ latency هنا ms 400 ms مقارنه بالـ ALP اللي كان ms 100

NLB has one static IP per AZ, and supports assigning Elastic IP

(helpful for whitelisting specific IP)

مizza ان ال NLP ليه Static IP بتخليك تستخدمها بشكل كويis ف مثلا لو عندك data base او اي backend services وعاوز تخليها ت Accept ال Traffic اللي جاي عليها only او اي Traffic اللي جاي من الـ Static IP ف بتروح فالـ firewall بتاعها ت allow Traffic اللي جاي من الـ IP دة وبس كدا ضمنت ان مفيش اي Traffic هيجيلك غير منه فقط.. نفس الكلام وانت بت assign ال Static IP عال DNS . مفيش تغيير ف ال IP دة كويis.

- مش متاح ف ال free tier

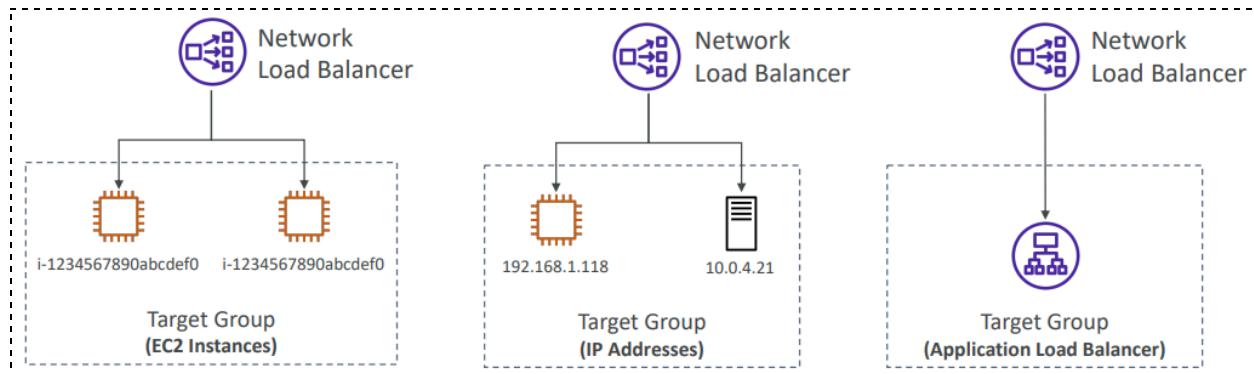


I'm Here

● Network Load Balancer –Target Groups

- نفس اللى قولناه فوق ممكن تكون IP Addresses او EC2 instances وهذا الزيادة ممكن

يكون ALP



● IP Addresses

- فى حالة لو ال ip addresses كان لازم تكون target group

● NLP With ALP As a target group

- ال scenario دة بيحصل لما اكونحتاج ال TCP/UDP traffic يهندل ال NLP العالى اللى

جايلى ويكون فيه low latency وال ALP يديني اوبشنز كتيره علشان ي Handle

HTTP/HTTPS traffic



I'm Here

→008 Network Load Balancer (NLB) - Hands On

- Create >> NLP SG , Instances SG , Instances with user data , target group (wait for the instances to be healthy) , NLP

1. Instances SG >>

عندنا 2 instances وانت بتكرريلهم هتروح الاول تكريت SG تسمح فيه بال

user data من NLP SG وتحط فى ال inbound الكود بتاعك اللي هيعرفك انت

بتاكسس انهى instance

The screenshot shows the AWS NLB configuration interface. At the top, there's a dashed box labeled "Inbound rules Info". Inside, a rule is defined for "sgr-0223613f79833d56d" with "HTTP" as the type, "TCP" as the protocol, port range 80, and a "Custom" source. A tooltip "sg-08a015347b89ee1d7" is shown over the source field. Below this is an "Add rule" button and a "Save rules" button at the bottom right. An arrow points from the text "NLP SG" to the "Save rules" button. At the bottom, there's a dashed box labeled "Outbound rules Info" with a single rule for "sg-0b80cfec4638e17955" allowing "All traffic" on all ports to "0.0.0.0/0". A warning message at the bottom states: "⚠ Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.".

2. NLP SG

دي ال inbound , outbound الخاصة بيه

The screenshot shows the AWS NLB configuration interface. At the top, there's a dashed box labeled "Inbound rules Info". Inside, a rule is defined for "sgr-0f61ea07040ed8237" with "HTTP" as the type, "TCP" as the protocol, port range 80, and a "Custom" source. A tooltip "0.0.0.0/0" is shown over the source field. Below this is an "Add rule" button and a "Save rules" button at the bottom right. A warning message at the bottom states: "⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.".



I'm Here

Outbound rules Info

Security group rule ID	Type	Protocol	Port range	Destination	Description - optional
sgr-0b5fa02d0ae166fc9	All traffic	All	All	Custom	0.0.0.0/0

Add rule

⚠️ Rules with destination of 0.0.0.0/0 or ::/0 allow your Instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.

3. NLP

هتختار ال instances target جروب الى هتوزع عليه

Listeners and routing Info

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

Listener TCP:80

Protocol	Port	Default action
TCP	: 80	Forward to Select a target group

[Create target group](#)

Instances TG

زي مقولنا تستني ال instances healthy ان ال target group توضحلك ان .. لان

فی البداية بتكون unhealthy cause of bootstrapping

Targets

Registered targets (2)						
Filter targets						
Instance ID	Name	Port	Zone	Health status	Health status details	Launch time
I-0713330ed80bec881	machine1	80	us-east-1b	Healthy		July 31, 2024, 23:40 (...
I-0e67f8d946fb67ab	machine1	80	us-east-1b	Healthy		July 31, 2024, 23:40 (...

Anomaly mitigation: Not applicable

لو عملت stop ل instance وروحت عال target group هتلقيها بالشكل دة انها في

ال stopped state

Targets

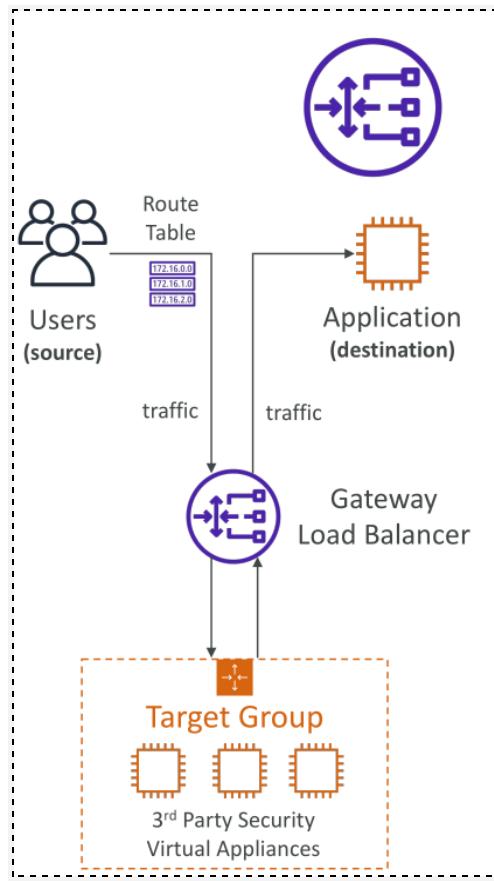
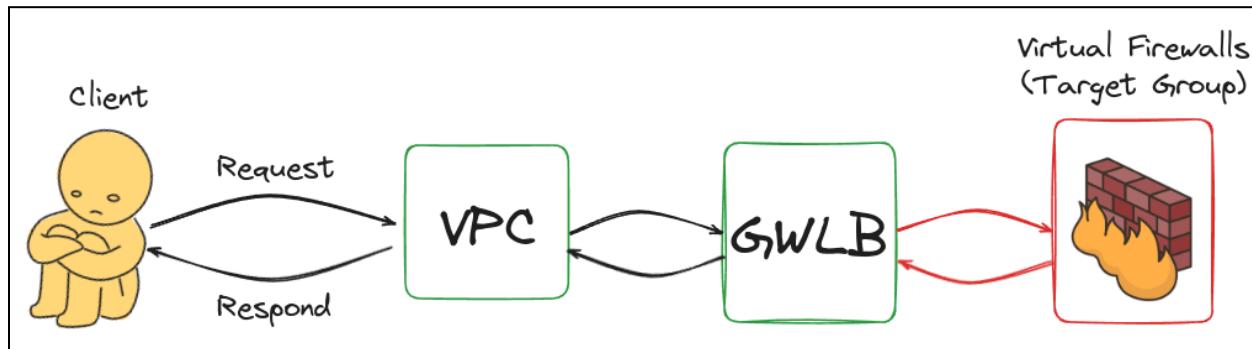
Registered targets (2) Info							
<small>Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.</small>							
Filter targets							
Instance ID	Name	Port	Zone	Health status	Health status details	Launch...	Anomaly detection result
I-0c53c2832c982065d	Machine1	80	us-east-1b	Unused	Target is in the stopped state	August 1, ...	Normal
I-01d07075fb54e4973	Machine1	80	us-east-1b	Healthy	-	August 1, ...	Normal

Anomaly mitigation: Not applicable

I'm Here



➡009 Gateway Load Balancer (GWLB)



• النوع ثالث من أنواع ال load balancers .. محتاجين نعرف عنها هنا طريقة عملها :

- سيكون فيه Traffic داخل عال AWS infrastructure

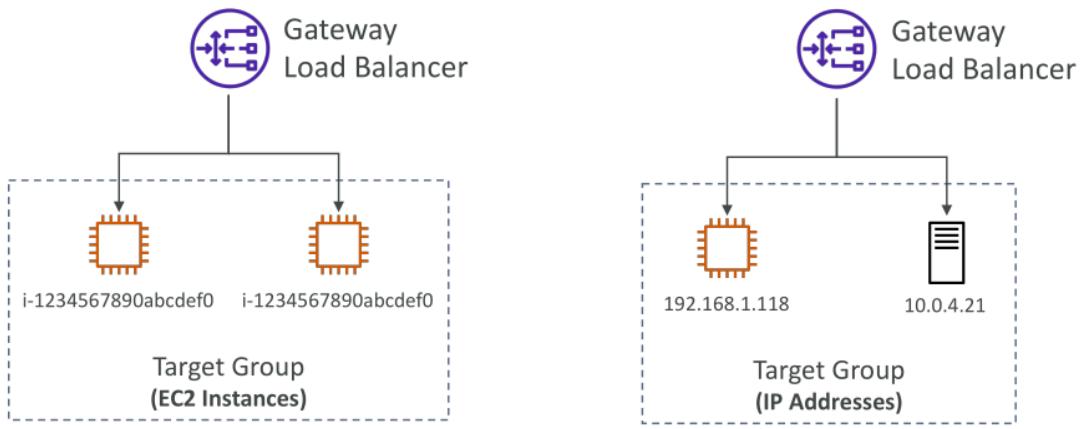


I'm Here

- الـ GWLB بتسلم الـ Traffic دة وتعمله route على firewall instance او اكتر من واحد بيكونو داخل target group
 - يتم فلترة الـ Traffic دة من خلال الـ firewall ويبيشوف مين هيتعملو accept ومين reject
 - AWS infrastructure accepted Traffic route لـ GWLB وبترجعه للـ firewall بـHands on ولكن بعدين لأن الموضوع معقد شوية.

● Gateway Load Balancer –Target Groups

- EC2 instances
- IP Addresses – must be private IPs



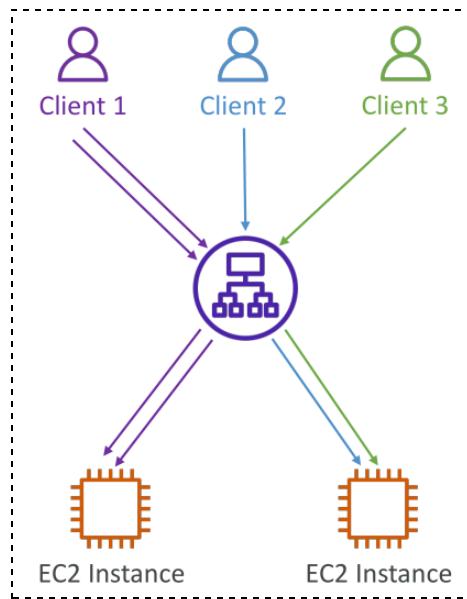
- نفس اللي قولناه فوق ممكن تكون EC2 instances او Private IP Addresses



I'm Here

→010 Elastic Load Balancer - Sticky Sessions

- Overview:



- فى الطبيعى ال classic , network , application load balancer بيوzu عو ال traffic عال instance الاولى ثم الثانية ثم الثالثه وهكذا .. فى الحالة دي لو استخدمت ال sticky sessions الللى هيتم ان ال client لو بعث 2 request لل load balancer هيدى على نفس instance مش هيزعuo

- Cycle Scenario:

- ال user بيعت لل load balancer request ف يتحولو على اي server فال session ID generate session ID على هيئة cookie ويبيتها لل browser دة بيكون unique لل user حتى ال load balancer من خلال ال session ID الموجود فى ال cookie بيعرف هيدى ال same requests على انهي server



I'm Here

• عندها بقا نوعين من ال cookies :

1. Application-based Cookies

- ال user لما بييعدت request لال server وال server يgenerate cookie with session id .
الموضوع مستمر ان ال user دة بال session id بتاعة مرتبط ب specific server .
عليه ودة مش هيتغير .

- طب اية بيحصل لما بمسح browser cookies ؟ اللي بيحصل ان ال session دى خلاص
انقللت ف هترجع بقا من تاني تبعت request وسيرفر جديد تحول عليه دا بمزاج ال load balancer
بناءا عال load وال server هي generate cookie & session id .
وتبدا من جديد حتى تلاقي ان ال account عمل sign out من الموقع اللي بتسخدمه او ان ال themes
بتاعة المتصفح اتمسحت او ال shop cart فضيit وهكذا

2. Duration-based Cookies

- لمدة معينة انت بتحدها ول يكن مثلا لمرة 30 دقيقة ال user هيفضل يستخدم نفس ال instance
مش هتجدد وهيفضل يتحول على نفس ال

هتلaci حتي في ال requests , responses فى جزا ال network & cookies .
في ال browser بتتهي امتى وهكذا .

Hello World from ip-172-31-7-176.eu-central-1.compute.internal

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Headers	Cookies	Request	Response	Cache	Timings	Stack Trace
304	GET	domain--	/	BrowserTab	html	cached	72 B		Filter Cookies					
404	GET	domain--	favicon.ico	FaviconLoad	html	cached	196 B		Response Cookies					

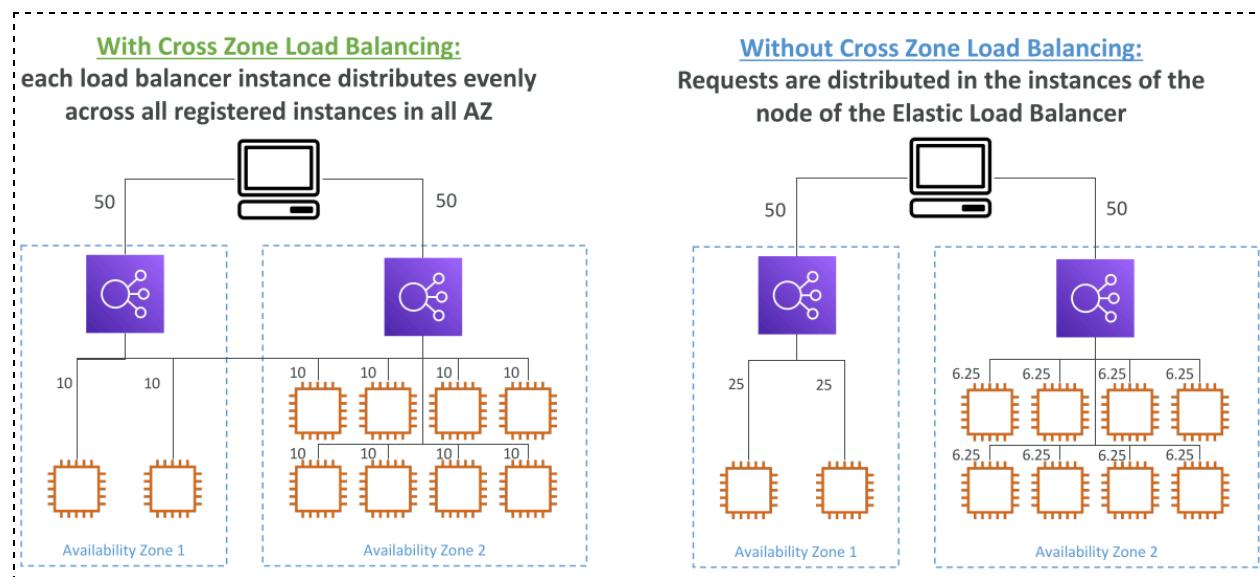
AWSALB:
expires: "2021-07-08T08:22:17.000Z"
path: "/"
value: "LMS8AbvN8fJxPcPGu8kG3alvOoDSMSkqQnGAM8nVHFTf1akppnX2s40WXJwMg0STQJMeiimfS7zvCMDFgciv+psAjmXXDg0N7XA4eSkFSAiW3B"
AWSALBCORE:
expires: "2021-07-08T08:22:17.000Z"
path: "/"
sameSite: "None"
value: "LMS8AbvN8fJxPcPGu8kG3alvOoDSMSkqQnGAM8nVHFTf1akppnX2s40WXJwMg0STQJMeiimfS7zvCMDFgciv+psAjmXXDg0N7XA4eSkFSAiW3B"
AWSALBCLONE:
value: "A02fRk/gsmH277N9183wz774Rf0d4ZRTDz0hf8Cteiqj+4+p37f8sq4KPA/2QoUQjMfPnIN794Z2DOLnpWefFOXO4M-Q2hICQ5EhW33y40"
AWSALBCORE:
value: "A02fRk/gsmH277N9183wz774Rf0d4ZRTDz0hf8Cteiqj+4+p37f8sq4KPA/2QoUQjMfPnIN794Z2DOLnpWefFOXO4M-Q2hICQ5EhW33y40"

I'm Here



→011 Elastic Load Balancer - Cross Zone Load

Balancing



ال Traffic اللي جاي لو انت مفعمل ال Cross zone LB فى الحالة دي هيتوزع عال 10

بالتساوي اما لو مش مفعله ف ال traffic اللي جاي على AZ معينه هيقسم عال instance

الى جواها فقط ومش هيخرج براها.

بنستخدمه علشان الدنيا تمشي بالتساوي وعلشان مفيش instance تقع مننا.

بتلاقيه ALB فى حالة ال enabled by default

classic , NLB فى حالة ال disable by default

بالنسبة للدفع لو متفعل هتدفع فقط فى ال NLB

تقدر بعد ما تخشن عال load balancer تعرف هو enable ولا disable من هنا



I'm Here

Attributes	Tags
TP/2	WAF fail open
1	Off
op invalid header fields	X-Forward-For header
f	Append
cess logs	Cross-zone load balancing
f	On

ومن تقدّر تخلّيه enable or disable edit

Target selection configuration

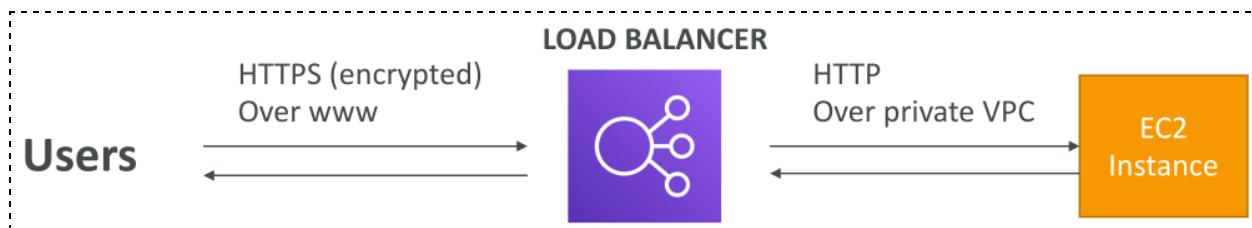
Cross-zone load balancing

By default, each Gateway Load Balancer Elastic Network Interface (ENI) only distributes traffic across the registered targets in its Availability Zone. If you enable cross-zone load balancing, each load balancer node distributes traffic across the registered targets in all enabled Availability Zones.

i Regional data transfer charges may apply when cross-zone load balancing is turned on. [Learn more](#) 

→012 Elastic Load Balancer - SSL Certificates

- Load Balancer SSL Certificate (Secure Sockets Layer):



- بنستخدمها علشان نEncrypt , protect connection ال user بين ال load وال

balancer

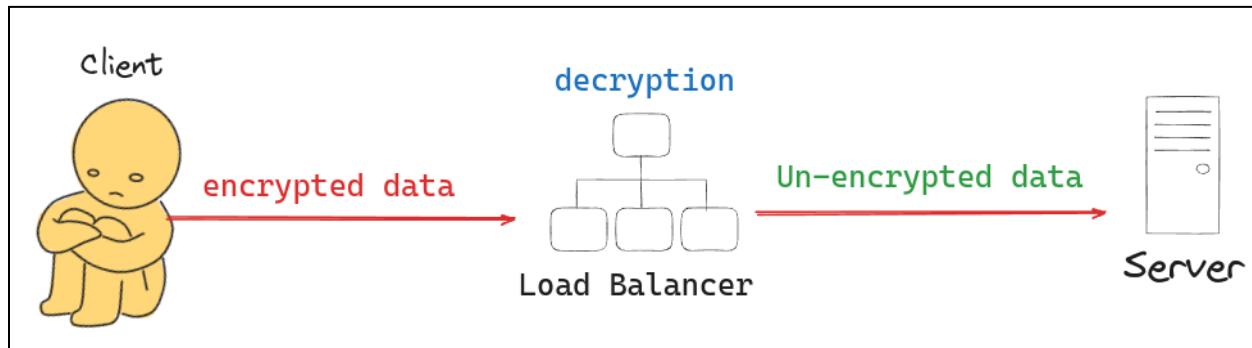


I'm Here

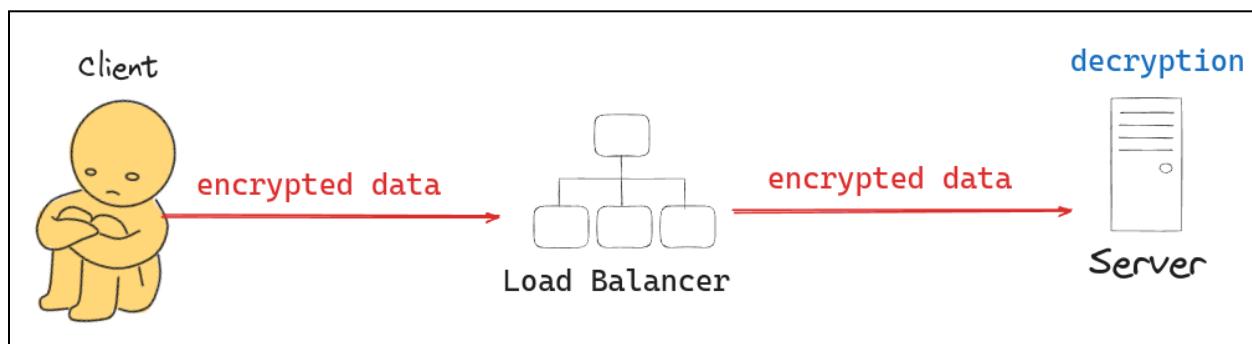
الـ SSL : هو بیـنـاـت secure internet connection الـ SSL اـلـيـدـاـت older protocol

- الـ **TLS** : الأحدث و more secure حالياً مستخدم أكثر ولكن شائع اننا بنقول عليه SSL

- **SSL Termination:**



- الـ SSL/TLS traffic بيجي من الـ user معموله encrypt فالـ load balancer بيعملو وده فايدته انو decrypt وبيبعث الـ unencrypted data لـ backend servers دى لـ SSL بيخفف الحمل عالـ backend servers انو ميعملش decrypt وكمان بتكون تحتاج Certificate واحدة بس عالـ back end server مش لكلـ load balancer.



- SSL Passthrough:

الـ SSL/TLS traffic بيجي من الـ user وبيفضل كدا لحد ما يوصل للـ backend servers .. ودة فايدته ان انت حفت End-to-End Encryption على طول المسار الـ .data protected



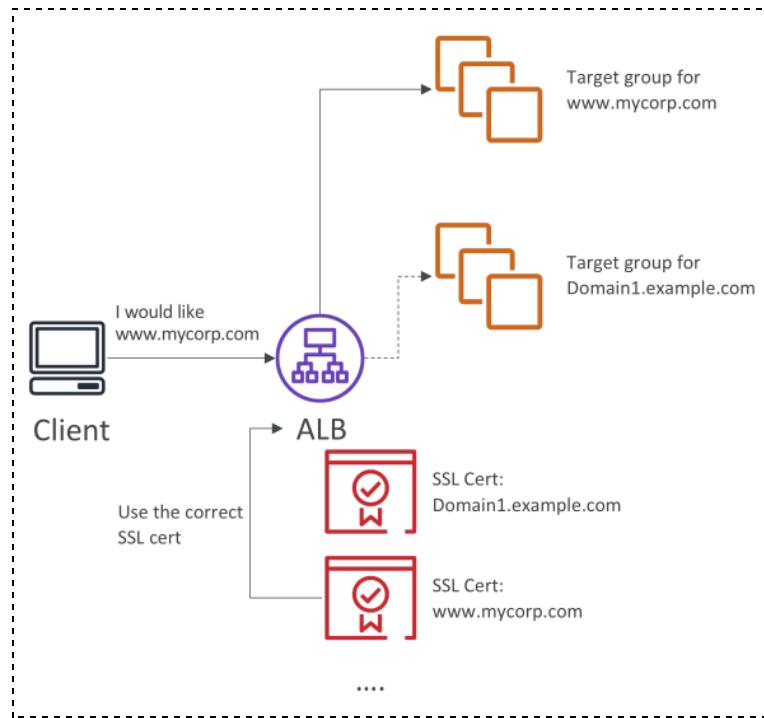
I'm Here

- **AWS Certificate Manager (ACM):**

عبارة عن AWS Service بـ simplify provisioning, managing, and deploying SSL/TLS certificates for use

او ممكن انت بتاعتك certificate details manual upload ال

- **Server Name Indication (SNI):**



لو عندي server واحد فقط وعليه كذا website mycorp.com وليكن website Domain1.example.com وهكذا .. وكل website ليه load balancer ف ازاي ال certificate هيعرف ان ال certificate balancer الفانية تبع الموقع الفلاني؟

- ال client بيبدأ SSL/TLS handshake اللي يكون فيه host name اللي عاوز يوصله وضمن ال SNI Field client hello message
- ال load balancer بيستلم ال SNI Field من خلال ال client hello message
- بيروح ال load balancer عال domain names اللي معمولها configure عنه ويعرف ال certificate اللي تبع انهي موقع (host name) ويوصل ال client فيه



I'm Here

4. بمجرد ما يعرف ال load balancer data بياخد بقا ال ssl termination or ssl passthrough ويعتها لل backend servers

- Only works for ALB & NLB (newer generation), CloudFront, Does not work for CLB (older gen).
-

→013 Elastic Load Balancer - SSL Certificates -

Hands On

The screenshot shows the AWS Lambda console with the 'Listeners' tab selected. The 'Listeners (1)' section displays a single listener configuration for port 80. The 'Add listener' button is highlighted with a red arrow. The table below shows the listener details:

Protocol:Port	ARN	Security policy	Default SSL cert	Default routing rule
TCP:80	ARN	Not Applicable	Not Applicable	Forward to demo-tg-nlb

بخش عال listeners ALB , NLB بتعاك سواء load balancer و بتخشد

في حالة NLB هنختار TLS بدل ما كنا بنختار TCP

Listener details Info

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

Protocol	Port	Default action
TLS	: 443 1-65535	Info Forward to demo-tg-nlb Target type: Instance, IPv4 Create target group

وفي حالة ال ALB بدل HTTPS هنختار HTTP



I'm Here

Listener details

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

Protocol	Port
HTTPS ▾	: 443
	1-65535

→014 Elastic Load Balancer - Connection

Draining

- محتاج مثلا تعمل APP update لـ old instances بتاعك وال عاوز تغيرها مثلا ف لـ ما تغيرها ال Load Balancer هيوقف اي connections بين ال user & instances ولكن باستخدام ال Connection Draining حصلها instance حتى لو ال connection او حصل فيها اي مشكلة خلتها Unhealthy connection مفتوح لمدة معينة stop time out انت بتحدها اسمها

- يبقي ال connection ول يكن هيفضل لمدة 5 دقايق 300 ث شغال لحد ما ال instance تتبدل وال الجديدة تروح عليها connections

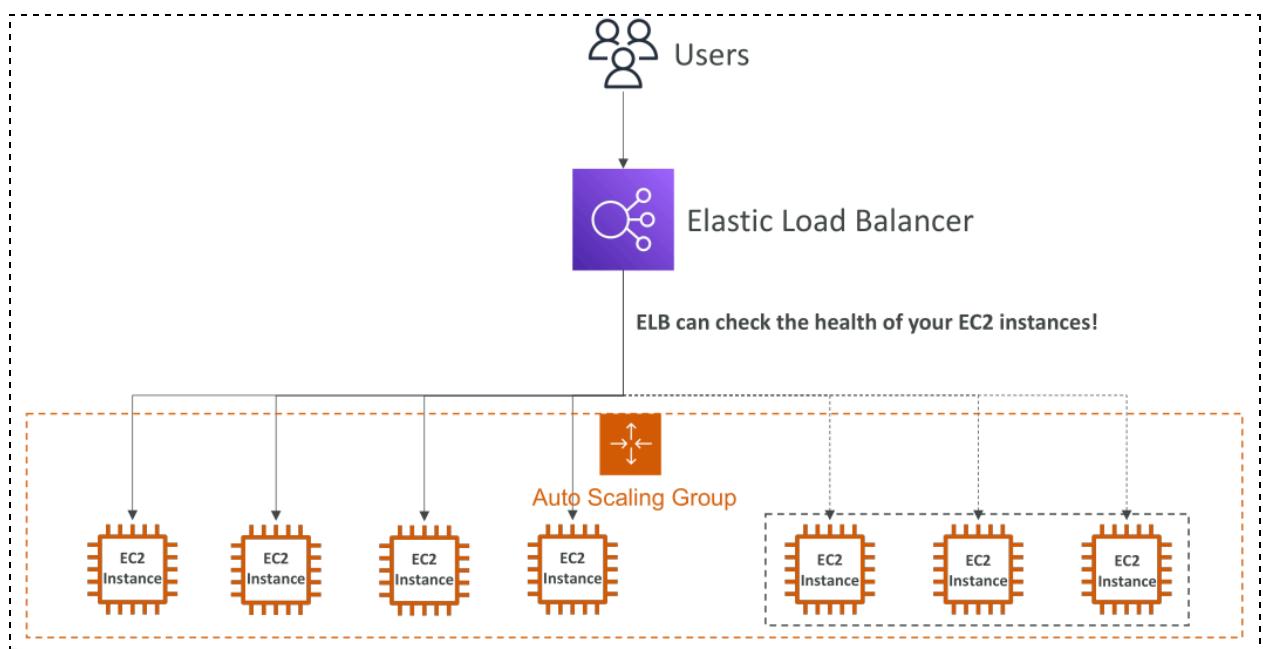
- ال Time out بتحدهه فى ال ELB Elastic Load Balancer ايا كان نوعه وبيكون من 1 .. 3600 ث .. على حسب نوع ال requests بتاعتك بقا لو هيا بتأخذ وقت كبير بتكبر المدة لو بتأخذ وقت صغير بتصغر المدة على حسب ال app ونوعيه ال requests



I'm Here

→015 Auto Scaling Groups (ASG) Overview

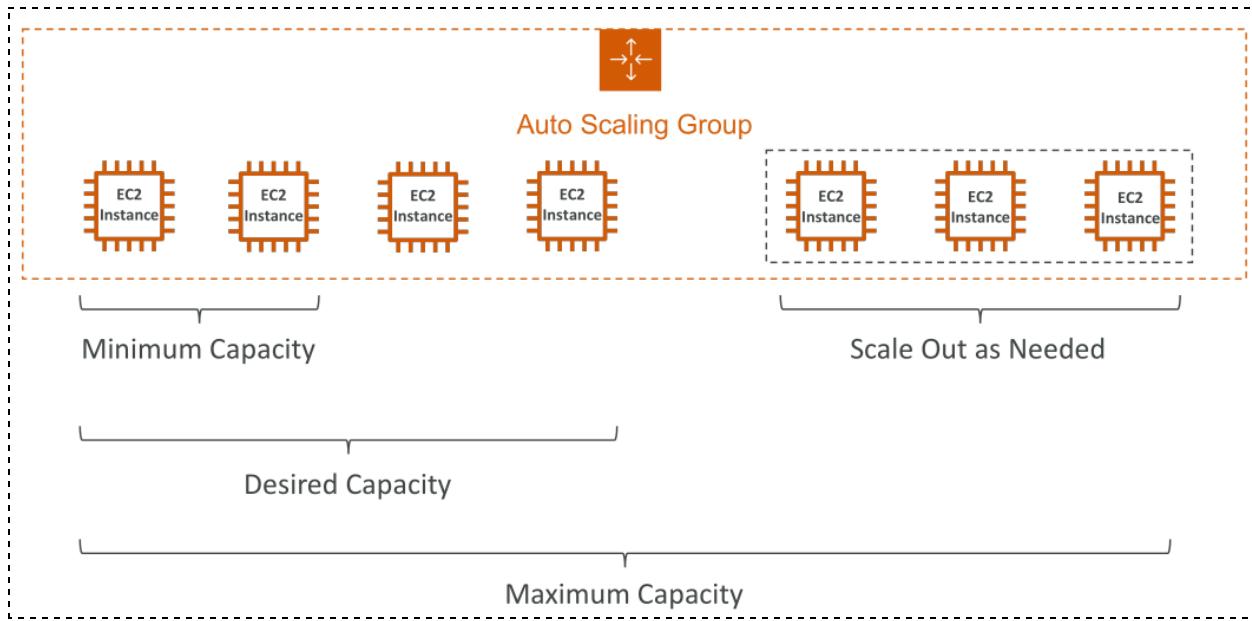
- **Overview:**



عباره عن **Free AWS feature** وظيفتها انها تحافظ على application بتاعك انو يكون Available من خالل انها بتزود وتتنقص على حسب ال EC2 Instances اللي بيعته ال load balancer عالجروب دة -
لو فيه traffic عالي بت scale out Automatic ولو فيه traffic قليل بترجع تاني تعمل instances علشان تقلل التكلفة لان التكلفة اكيد زادت بما انك زودت scale in Automatic -



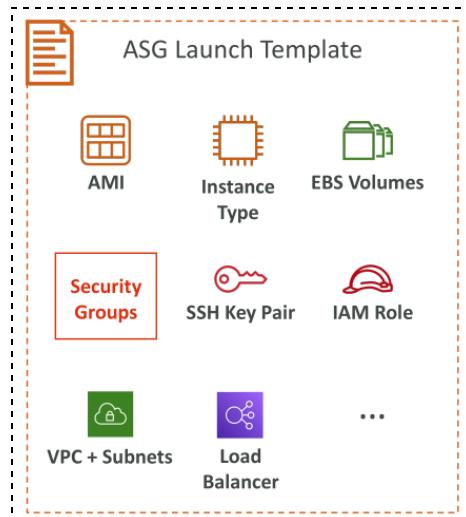
I'm Here



- **Auto Scaling Group Capacity:**

- أقل عدد Instances أنا عاوزها تكون موجودة .1
 - أكبر عدد Instances أنا عاوزاني اوصله .2
 - العدد المتوسط اللي أنا عاوزة .3
- ممكن أتحكم في عدد ال instances ازود او انقص بناء على ال cloud watch alarm
- متلا جالى alarm ان فيه استهلاك عالي فال CPU ف نزود EC2 Instances وهكذا

- **Create Launch Template:**



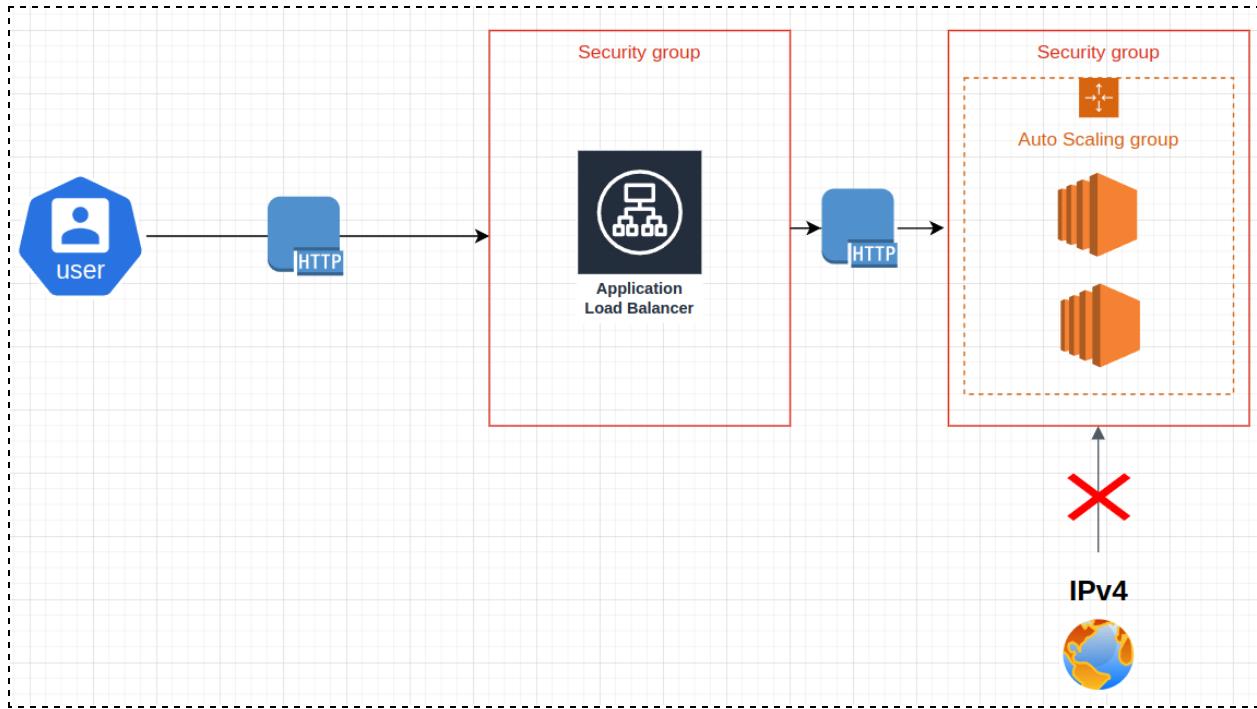
I'm Here

- شوية parameters بتعملها set بحيث اي EC2 Instance هتكريتها هتقوم بالparameters دي .. يا عين لما يحتاج يـ Scale out هيأخذ نفس ال Parameters ..
مثلا عملت set لـ EC2 Instance معنـي كـ ان اي Subnet من ال Zone = 1A وهـذا = 1A



I'm Here

→016 Auto Scaling Groups Hands On



أول حاجة هتعملها ال **instance** علشان اي **Launch template** تقوم بنفس ال
configurations

ASG >> Launch Template

Launch template [Info](#) [Switch to launch configuration](#)

Launch template
Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

Select a launch template

[Create a launch template](#)

هتختار مثلا 3 AZ 3 علشان هنقوم حوالي 3 instances



I'm Here

Network Info

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC

Choose the VPC that defines the virtual network for your Auto Scaling group.

vpc-0799daa55c9fb6493
 172.31.0.0/16 Default

▼

↻

[Create a VPC](#)

Availability Zones and subnets

Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets

▼

↻

us-east-1a | subnet-0a3d455d7730cdc92 X
 172.31.0.0/20 Default

us-east-1b | subnet-0d0cb74f903557682b X
 172.31.80.0/20 Default

us-east-1c | subnet-017c65ab00faaf2af X
 172.31.16.0/20 Default

[Create a subnet](#)

وبعدين نربطه بال ASG دة



I'm Here

Load balancing Info

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

No load balancer

Traffic to your Auto Scaling group will not be fronted by a load balancer.

Attach to an existing load balancer

Choose from your existing load balancers.

Attach to a new load balancer

Quickly create a basic load balancer to attach to your Auto Scaling group.

Attach to an existing load balancer

Select the load balancers that you want to attach to your Auto Scaling group.

Choose from your load balancer target groups

This option allows you to attach Application, Network, or Gateway Load Balancers.

Choose from Classic Load Balancers

Existing load balancer target groups

Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.

Select target groups



تزويد ال desired instance ولين ل 2 بدل 1 تلاقي فال instance واحدة بتقوم تروح عال ASG
تلاقي نفس الكلام ان فيه واحدة بتقوم تروح عال target groups بعدها تلاقيها بتوصل وبقت
load balancer علشان ال unhealthy ثم بقت healthy تيجي تأكسس ال unhealthy
بدل ما كان بيوجهك على واحدة بدأ يبدل عالاتنين وهكذا

ظهرلي مشكلة وهي اني لما جيت اعمل ال load balancer حددت 2 zone بس ولكن ال
load balancer لما جت تقوم قامت ف 1c وانا كنت محدد 1a & 1b ف روحت عال instance
target .. ولقيتها بدل ما كانت واقفة في ال instances بدت تقوم وفي ال balancer
group كذلك



I'm Here

Targets **Monitoring** **Health checks** **Attributes** **Tags**

Registered targets (2) Info

Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.

<input type="checkbox"/>	Instance ID	Name	Port	Zone	Health status	Health status details	Launch...
<input type="checkbox"/>	I-0e653d10d1436eda1		80	us-east-1c	Unused	Target is in an Availability Zone that is not enabled for the load balancer	August 1, ...
<input type="checkbox"/>	I-0af8ee8d7b4b06632		80	us-east-1a	Healthy	-	August 1, ...

Instances (2) Info

Find Instance by attribute or tag (case-sensitive)

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>		I-0e653d10d1436eda1	Running	t2.micro	Initializing	View alarms +	us-east-1c
<input type="checkbox"/>		I-0af8ee8d7b4b06632	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a

Targets **Monitoring** **Health checks** **Attributes** **Tags**

Registered targets (2) Info

Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.

<input type="checkbox"/>	Instance ID	Name	Port	Zone	Health status	Health status details	Launch...
<input type="checkbox"/>	I-0e653d10d1436eda1		80	us-east-1c	Initial	Target registration is in progress	August 1, ...
<input type="checkbox"/>	I-0af8ee8d7b4b06632		80	us-east-1a	Healthy	-	August 1, ...

ALB مربوط بال TG و TG مربوط بال ASG

→017 Auto Scaling Groups - Scaling Policies

- **Dynamic Scaling Policy:**

- **Target Tracking Scaling:**

مثلاً أحذلو ان أخرك ف استهلاك الـ CPU انو يكون 60% زيادة عن كدا زودلي -

وطبعاً هيلترم بال maximum .. instances اللي احنا حددهنا فوق



I'm Here

- **Simple/Step Scaling:**

- لو فيه cloud watch alarm معين نفذ كذا .. لو مثلا عندي alarm ان ال cpu usage بقى فوق ال 70% ف في الحالة دي زودلي EC2 instances ول يكن زود 2 ولو اقل من 70% قلل 1 وهكذا

- **Scheduled Scaling:**

- بنعمل دة لو فيه event ف وقت معين بيكون فيه traffic عالي .. رأس السنة مثلا عيد الأم يوم الجمعة كدا ياعني .. فالاوقات دي فيه traffic اعلى من الطبيعي ف زودلي EC2 instances ولما الايام دي تنتهي ارجع لل الطبيعي.

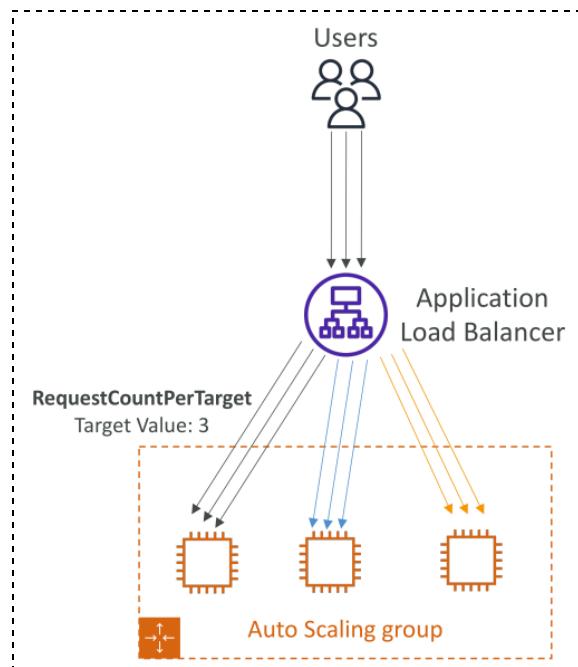
- **Good Metrics to Scale On in AWS:**

- حاجات ممكن ت Scale in/out بناءا عليها:

- **CPU Utilization:**

- **Request Count Per Target:**

- بناءا على عدد ال instances اللى جايhe عال requests بتاعتي هنا مثلا 3



I'm Here

- **Average Network In / Out:**

- Measures the average network traffic in and out of your instances.

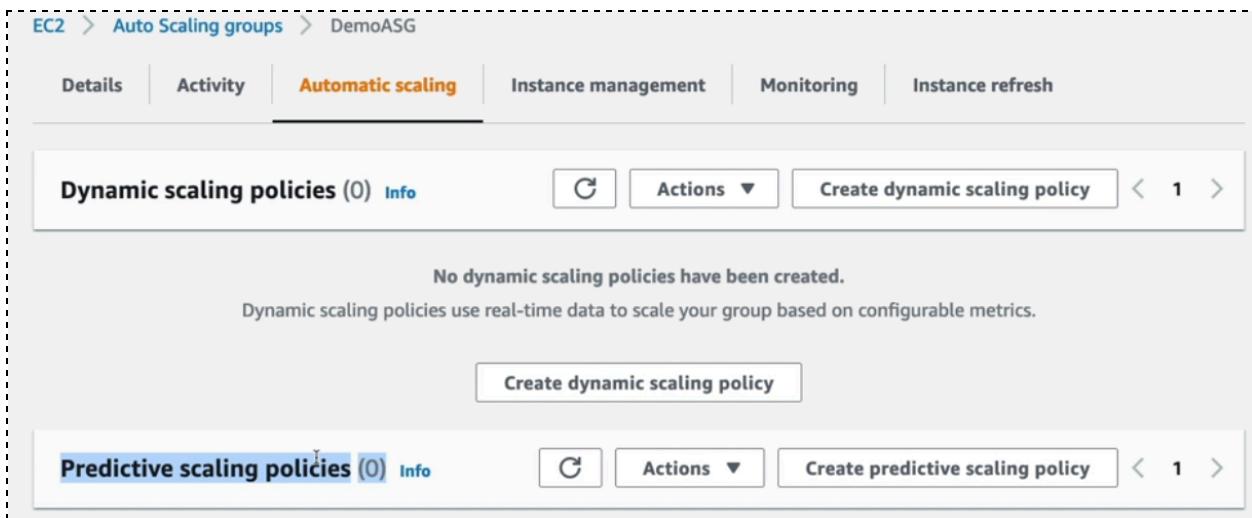
- **Custom Metrics:**

- ای specific metrics انت عاوزها و بتدخلها عال cloud watch وتسخدمها.

- **Scaling cooldown:**

- فتره فى خلالها ال ASG مبيقومش باي scaling actions تخص ال in/out سواء بحيث ي تكون by default rapid scaling وميكونش فيه stabilize excessive costs دة هيكلفك كتير rapid scaling معملتوش ال

- **Predictive Scaling:**



- عباره عن feature موجودة فى ال ASG بتحل ال traffic data اللى حصلت قبل كدا وبناء علىها بتعرف امتى ال traffic بيكون عالي وامتي اقل وكدا وبناءا عليه بت scale فى اي عطلة او مناسبة او كدا

- بنسخدمها لان من غيرها ال ASG ممكن متشغلش بكفاءة ممكنا يكون فيه مثلا lag time على ما ال instances تقوم اما لما بنسخدمها بت schedules scaling actions مقدما

- **Activity History Example :**

- 1. كنت محدد ف ال instance desired capacity = 1 ف هتلقيه زود من 0 إلى 1



I'm Here

كنت محدد الـ target tracking = 50% زاد عن 50% زود 1 instance لان زي مقولنا معنى الـ target tracking (ان آخرك ف استهلاك الـ CPU يكون 50% زيادة عن كدا زودلي EC2 instances .. وطبعا هيلترم بال اللي احنا حددناه فوق)

3. بعد ما زود instance وبقي عندنا 2 لقي ان فيه ضعف جاي تاني عال CPU وبيزيد عن 50%
تاني وبالتالي زود واحدة كمان ووصلنا لـ 3 اللي هو ال maximum

Activity history (3)			
Status	Description	Cause	Start time
Success ful	3 Launching a new EC2 instance: i-09f0a15800773c69f	At 2024-05-12T23:08:21Z a monitor alarm TargetTracking-CloudKode-ASG-AlarmHigh-cf4fd480-114d-4011-a374-8e2e709032fa in state ALARM triggered policy Target Tracking Policy changing the desired capacity from 2 to 3. At 2024-05-12T23:08:25Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 2 to 3.	2024 May 13, 01:08:27 AM +02:00
Success ful	2 Launching a new EC2 instance: i-0bb0b0f24bcefe6a2	At 2024-05-12T23:06:21Z a monitor alarm TargetTracking-CloudKode-ASG-AlarmHigh-cf4fd480-114d-4011-a374-8e2e709032fa in state ALARM triggered policy Target Tracking Policy changing the desired capacity from 1 to 2. At 2024-05-12T23:06:27Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 1 to 2.	2024 May 13, 01:06:30 AM +02:00
Success ful	1 Launching a new EC2 instance: i-0331d8fd086b43c89	At 2024-05-12T22:39:57Z a user request created an AutoScalingGroup changing the desired capacity from 0 to 1. At 2024-05-12T22:39:58Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 0 to 1.	2024 May 13, 12:40:00 AM +02:00

→018 Auto Scaling Groups - Scaling Policies

Hands On

ال setup بتاع ال predictive scaling بسيط بتحدد بس ال metrics وخلاص



I'm Here

Turn on scaling Info

Scale based on forecast
If switched off, predictive scaling will only forecast capacity and not take any scaling action. Only one predictive scaling policy can have scaling turned on at a given time.

Metrics and target utilization Info

Metrics
There are two metrics for predictive scaling. One metric tells the policy about the load your application has been under. The other metric and the target utilization determine the overall average utilization to target.

CPU utilization
Uses the total CPU to create the load forecast and the average CPU to define your target util...

Target utilization
The average CPU utilization rate to target in the forecast period.

50 % per instance
Must be greater than 0.

بالنسبة لل cloud watch alarm Dynamic scaling policy بتحدد بقا نوعها ولو فيه

وهكذا بردو setup بسيط

هنا هنكريت cpu 40% target tracking scaling بناءا عال

- خلي بالك بقا انك تغير ال desired , maximum capacity وكدا لان دلوقتي لما

تشتغل وال cpu يزيد عن 40% ف لازم تكون سامح ب دة قبل كدا

في ال ASG

Create dynamic scaling policy

Policy type

Scaling policy name

Metric type

Target value

Instances need
 seconds warm up before including in metric

Disable scale in to create only a scale-out policy



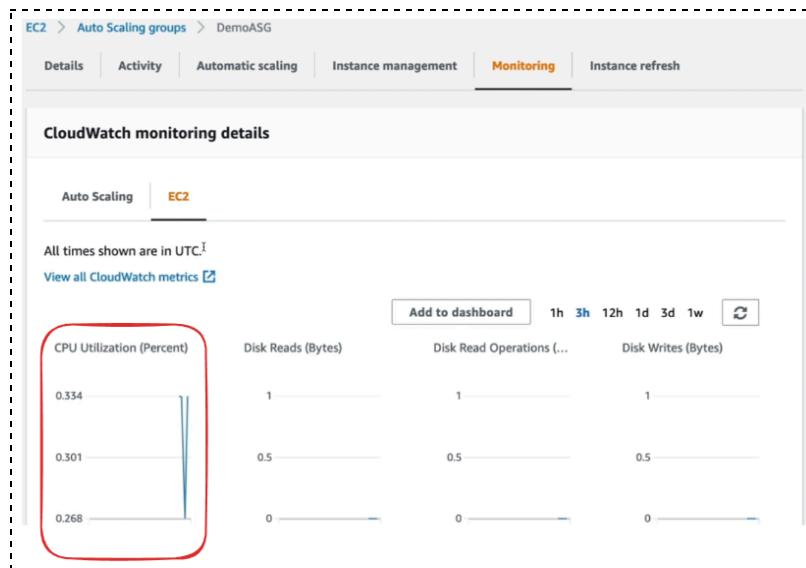
I'm Here

تقدر ت connect عال instance من خلال AWS command عادي وبدها دول بحيث

ت stress ال cpu انو يرفع عن 40%

```
sudo amazon-linux-extras install epel -y  
sudo yum install stress -y  
stress -c 4
```

زي مانت شايف فى ال monitoring ال cpu utilization رفع .. وبالتالي هي scale out على حسب الضغط وعلى حسب ال maximum capacity ب 1 او 2 instances



ولو روحت عال cloud watch alarm هتلaci فعلا ان فيه alarm جايلك من target policy اللي احنا كريتناها الأول لما بداننا خالص ان ال cpu اقل من 28 ف تمام هنكريت واحدة ودي البداية والثاني alarm high بيوصلوك ان ال cpu زاد عن 40% ف instance kada هنخش ف instances اكتر



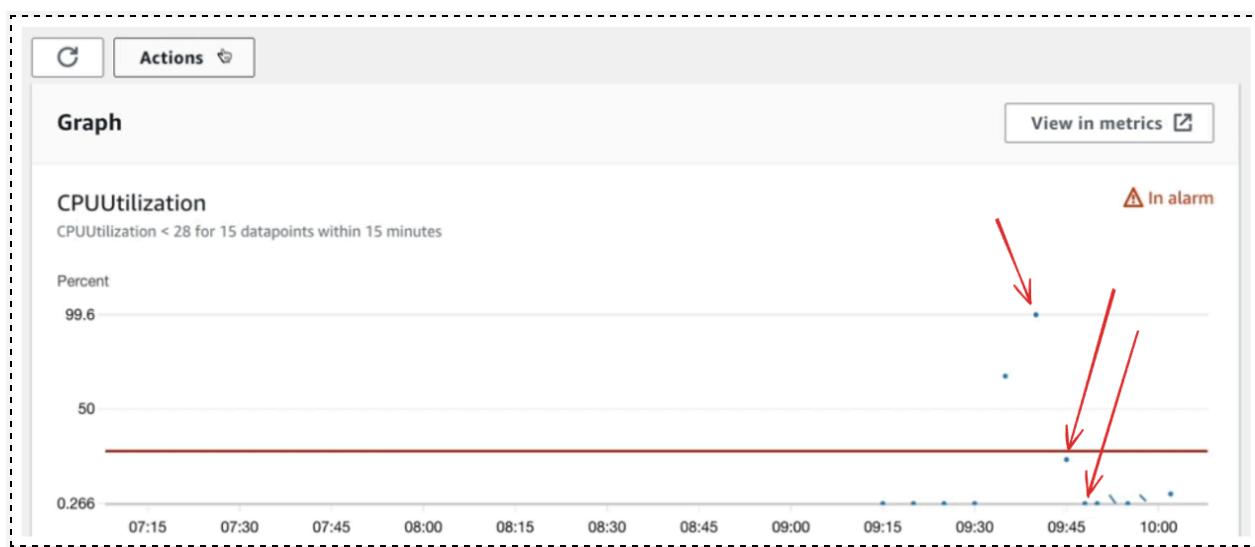
I'm Here

The screenshot shows the AWS CloudWatch Alarms page. On the left, a sidebar lists various services: Dashboards, Alarms (highlighted with a red arrow), Logs, Metrics, Events, ServiceLens, Container Insights, and others. The main area displays two alarms:

- TargetTracking-DemoASG-AlarmLow-**: State: OK, Last state update: 2021-07-01 11:41:44, Condition: CPUUtilization < 28 for 15 datapoints within 15 minutes.
- TargetTracking-DemoASG-AlarmHigh-**: State: In alarm, Last state update: 2021-07-01 11:41:14, Condition: CPUUtilization > 40 for 3 datapoints within 3 minutes.

لما تيجي ترجع لل connection بينك وبين ال instance هتلقيها معلقه علشان استهلاك ال cpu العالي ف روح عال instances dashboard يبقي كدا ال cpu هيرجع لل 0

هتلaci بقا graph لى حصل فى ال cloud watch .. طلع ثم نزل تاني لما عملنا reboot



ال ip بتتغير سواء v4 or v6 ثابت بتخشن خلل على instances



I'm Here

Question 3:

Elastic Load Balancers provide a

- static IPv4 we can use in our application

- static DNS name we can use in our application

- static IPv6 we can use in our application

Question 11:

For compliance purposes, you would like to expose a fixed static IP address to your end-users so that they can write firewall rules that will be stable and approved by regulators. What type of Elastic Load Balancer would you choose?

- Application Load Balancer with an Elastic IP attached to it

- Network Load Balancer

- Classic Load Balancer

مش هيحصل حاجة لأنو على 3
desired = 3

Question 16:

You have an application hosted on a set of EC2 instances managed by an Auto Scaling Group that you configured both desired and maximum capacity to 3. Also, you have created a CloudWatch Alarm that is configured to scale out your ASG when CPU Utilization reaches 60%. Your application suddenly received huge traffic and is now running at 80% CPU Utilization. What will happen?

- Nothing

- The desired capacity will go up to 4 and the maximum capacity will stay at 3

- The desired capacity will go up to 4 and the maximum capacity will stay at 4



I'm Here

Question 20:

You have an ASG and a Network Load Balancer. The application on your ASG supports the HTTP protocol and is integrated with the Load Balancer health checks. You are currently using the TCP health checks. You would like to migrate to using HTTP health checks, what do you do?

- Migrate to an Application Load Balancer

- Migrate the health check to HTTP

Submit

Question 21:

You have a website hosted in EC2 instances in an Auto Scaling Group fronted by an Application Load Balancer. Currently, the website is served over HTTP, and you have been tasked to configure it to use HTTPS. You have created a certificate in ACM and attached it to the Application Load Balancer. What can you do to force users to access the website using HTTPS instead of HTTP?

- Send an email to all customers to use HTTPS instead of HTTP

- Configure the Application Load Balancer to redirect HTTP to HTTPS

- Configure the DNS record to redirect HTTP to HTTPS



I'm Here

CH-09 - AWS Fundamentals

RDS + Aurora + ElastiCache

→001 Amazon RDS Overview (Relational Database Service)

عبارة عن service بتقديمها AWS بتسهيلك ال setup, operation, and scaling of relational databases in the cloud

- **Key Features**

- **Supports multiple database engines**, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle, and Microsoft SQL Server.
- **Automates tasks** such as hardware provisioning, database setup, patching, and backups.
- Provides **easy scaling** of database instance types and storage, Supports read replicas for read-heavy applications.
- **High Availability and Durability**: Multi-AZ (Availability Zone) deployments for automated failover and redundancy.
- **Automated backups** and **point-in-time recovery** options.



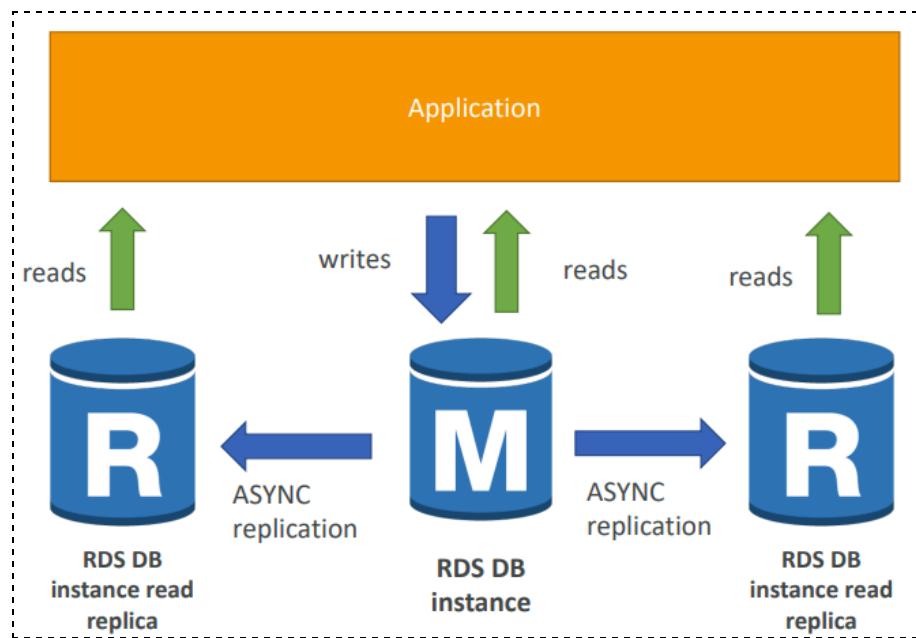
I'm Here

- Amazon CloudWatch integration for monitoring database performance and setting alarms.
- Pay-as-you-go pricing model.

BUT you can't SSH into your instances 

→002 RDS Read Replicas vs Multi AZ

• Overview



- Replicas : نسخ متماثلة
- ASYNC = asynchronous غير متزامن
- SYNC = Synchronization متزامن



I'm Here

- عباره عن بديل من ال database الاساسية بيحصل عليها read Replicas مش زى الاساسية بنسخدمها بحيث نوزع عليها حمل ال read بحيث نخف عن الاساسية.

- لو عندك web app عنده primary database بتهنل ال read , write operations وال app بي grow وبيجيلو heavy traffic ودة بيسبب performance issues علشان نحل المشكلة دي بنكريت primary database من ال Read Replicas تاخد انها primary database instance وتخف الضغط عال read traffic

- ال data عال replicas بتكون eventually consistent متسقة في النهاية معناها ان بيكون فيه delay ف ان ال replicas تاخد نفس ال recent data changes عال primary database

- ليك لحد 15 replicas فى ال AZ or Cross AZ or Cross Region

• Connection string

- عندك اسمه connection string parameter بحيث ان ال replicas الللى جاي ميروحش عال primary database ولكن يروح عال read traffic end point

• Replicas End point

- ال end point معناها .. انت لما بتعمل replicas بيكون ل كل واحده منها & end point دول ال port

- تقدر تحول ت replicas دى ل standalone database انها تكون read & write يحصل عليها primary

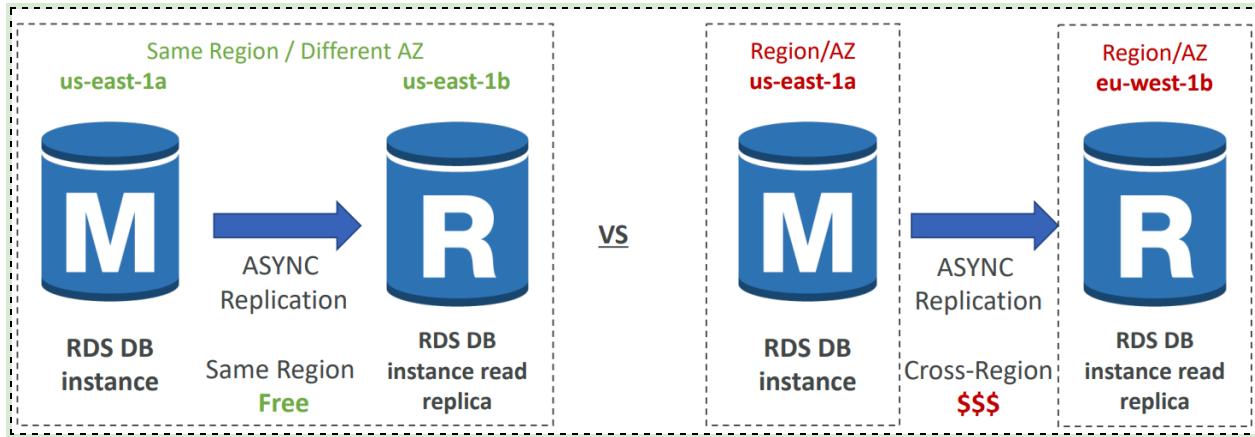
• Cost

💡 نقل ال data فى الطبيعي من AZ الى AZ تانية بيندفع عليه cost أما فى حالة ال

replicas عندك حالتين

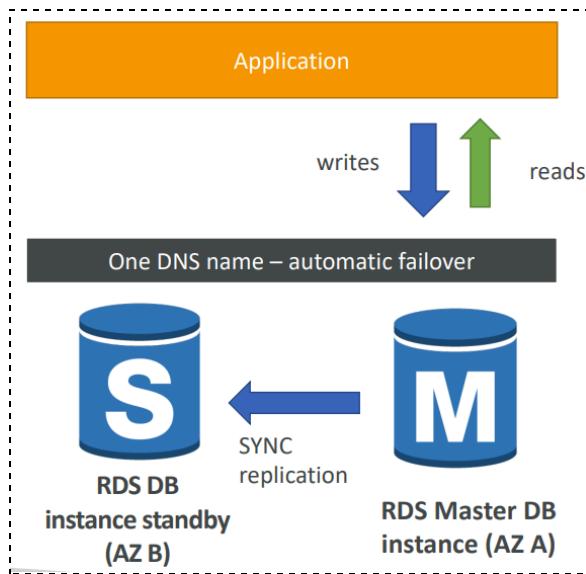


I'm Here



- لو هتكريت replicas فى نفس ال Region مش هتدفع
- لو هتكريت replicas فى مختلفة Regions هتدفع

• RDS Multi AZ (Disaster Recovery)



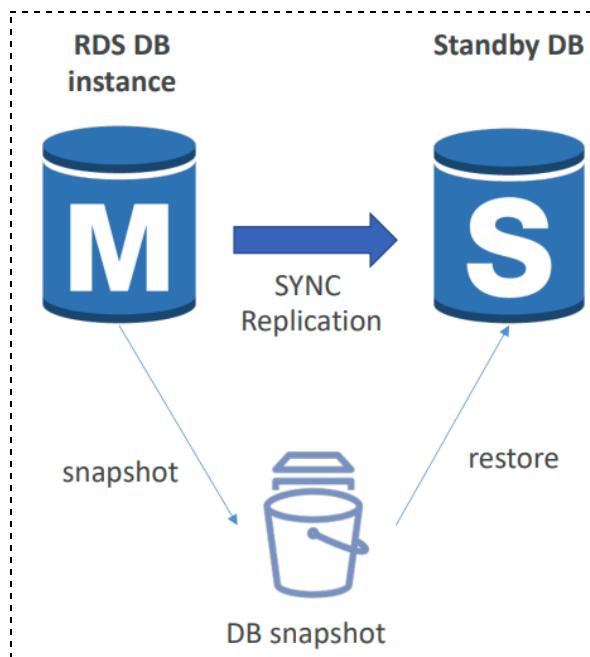
- لو عندك e-commerce application with critical data base علشان تضمن نفسك
- فى حالة لو ال database دي حصلها مشكلة بت ال deploy ال دى فى
- DB instance Standby بحيث لو واحدة وقعت الثانية تستلم مكانها.. بتسمى **AZ**
- الاتنين بيكونو مرتبطين بنفس ال **DNS Name** ف دة شئ كويس وبدون اي تدخل manual
- منك الموضوع هيتم من غير ماتحس.
- ال **setup as multi az** هيا كمان بيتعملها



I'm Here

- علشان تخلي ال RDS multi AZ

- فقط بت enable ال database و بت modify ال database ولكن اللي بيحصل في الخلفية يكون بالشكل دة



- بيتأخد snapshot من ال primary database وبعدين بيحصل restore ليها ف AZ مختلفة وبيحصل بعدها synchronization بينهم.



I'm Here

→003 Amazon RDS Hands On

هل تحتاج تحط كل ال configuration ولا تحتاج حاجة فى السريع

Choose a database creation method [Info](#)

Standard create
You set all of the configuration options, including ones for availability, security, backups, and maintenance.

Easy create
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

ال engines المتاحة

Engine options

Engine type [Info](#)

<input type="radio"/> Aurora (MySQL Compatible) 	<input type="radio"/> Aurora (PostgreSQL Compatible)
<input checked="" type="radio"/> MySQL 	<input type="radio"/> MariaDB
<input type="radio"/> PostgreSQL 	<input type="radio"/> Oracle
<input type="radio"/> Microsoft SQL Server 	<input type="radio"/> IBM Db2

امكانيات ال data base instance اللى هتقوم عليها ال



I'm Here

DB instance size

Production

db.r6g.xlarge

4 vCPUs

32 GiB RAM

500 GiB

1.017 USD/hour

Dev/Test

db.r6g.large

2 vCPUs

16 GiB RAM

100 GiB

0.231 USD/hour

Free tier

db.t3.micro

2 vCPUs

1 GiB RAM

20 GiB

0.020 USD/hour

1 primary & 2 standby **or** 1 primary & 1 standby **or** 1 primary only

Availability and durability

Deployment options [Info](#)

The deployment options below are limited to those supported by the engine you selected above.

Multi-AZ DB Cluster

Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.

Multi-AZ DB instance

Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.

Single DB Instance

Creates a single DB instance with no standby DB instances.

الى تحتاجها نوعها اية وحجمها .. storage suitable for free tier

Storage

Storage type [Info](#)

Provisioned IOPS SSD (io2) storage volumes are now available.

General Purpose SSD (gp3)

Performance scales independently from storage

Allocated storage [Info](#)

20

GiB

Minimum: 20 GiB. Maximum: 65,536 GiB

ⓘ After you modify the storage for a DB instance, the status of the DB instance will be in storage-optimization. Your instance will remain available as the storage-optimization operation completes. [Learn more](#)

علشان ميكونش فيه تكلفه اختار النوع دة لازم db.t2.micro حتى لو ظهر لك تكلفه تحت ف

عادي لازم بس تختار النوع دة



I'm Here

Instance configuration

The DB instance configuration options below are limited to those supported by the engine that you selected above.

DB Instance class [Info](#)

▼ Hide filters

Show instance classes that support Amazon RDS Optimized Writes [Info](#)

Amazon RDS Optimized Writes improves write throughput by up to 2x at no additional cost.

Include previous generation classes

Standard classes (includes m classes)

Memory optimized classes (includes r and x classes)

Burstable classes (includes t classes)

db.t3.micro

2 vCPUs 1 GiB RAM Network: 2,085 Mbps



Estimated Monthly costs

DB Instance 12.41 USD

Storage 2.30 USD

Total 14.71 USD

This billing estimate is based on on-demand usage as described in [Amazon RDS Pricing](#). Estimate does not include costs for backup storage, IOs (if applicable), or data transfer.

Estimate your monthly costs for the DB Instance using the [AWS Simple Monthly Calculator](#).

ان ربطةها ب instance network configuration هنلافي ال موجودة مش تحتاج تعمل

الامور تمام security groups linked



I'm Here

Connectivity Info



Compute resource

Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

Don't connect to an EC2 compute resource

Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

Connect to an EC2 compute resource

Set up a connection to an EC2 compute resource for this database.

EC2 instance Info

Choose the EC2 instance to add as the compute resource for this database. A VPC security group is added to this EC2 instance. A VPC security group is also added to the database with an inbound rule that allows the EC2 instance to access the database.

Choose an EC2 instance



لو دخلت عال security جروب دة هتلaci فى ال inbound rules بتاعته ال income مش من anywhere ف هنعدل دة



I'm Here

Endpoint & port

- Endpoint: database-1.cjoue2og2lw.us-east-1.rds.amazonaws.com
- Port: 3306

Networking

- Availability Zone: us-east-1f
- VPC: vpc-0799daa55c9fb6493
- Subnet group: default-vpc-0799daa55c9fb6493
- Subnets:
 - subnet-0b033c07c2fc2d1b
 - subnet-a3d455d7730cd92
 - subnet-017c65ab0faaf2af
 - subnet-0ddcb74f90357682b
 - subnet-08f797a262b242263
 - subnet-09a2ba7c68db5b25e

Security

- VPC security groups: demo-database-vpc (sg-0864f2ab32b4f4091) (Active)
- Publicly accessible: Yes
- Certificate authority: Info rds-ca-rsa2048-g1
- Certificate authority date: May 26, 2061, 02:34 (UTC+03:00)
- DB instance certificate expiration date: August 02, 2025, 03:40 (UTC+03:00)

Inbound rules (1)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sgr-0adb080ce6778c56b	IPv4	MySQL/Aurora	TCP	3306	156.211.40.141/32	-

Inbound rules

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-0adb080ce6778c56b	MySQL/Aurora	TCP	3306	Anywhere-IPv4	0.0.0.0/0

Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Add rule Cancel Preview changes Save rules

بعد ما بتكريت ال database بيكون ليها ال endpoint اللي اتكلمنا عنها من خلالها هتنصل عليها ودة هيكون باستخدام slectron GUI عباره عن سهله ف جوجل هتلقيه

slectron-1.38.0.tar.gz	99.4 MB
slectron-1.38.0.tar.xz	67.2 MB
slectron-1.38.0.x86_64.rpm	67.7 MB
slectron-Setup-1.38.0.exe	146 MB
slectron-Setup-1.38.0.exe.blockmap	157 KB
slectron_1.38.0_amd64.deb	67.6 MB



I'm Here

```
Sudo -i dpkg sqlectron_1.38.0_amd64.deb  
sudo apt remove sqlectron
```

بعد ما تفتحه هت test وبس

بالنسبة لل database/configration initial database/keyspace وانت بتعمل
database او configuration tab ترجع تشووفه من ال configuration او تقدر بعد ما عملتها ترجع تشووفه من ال

Server Information

Connection Test
Successfully connected

Name	Database Type		
RDS-Demo	MySQL		
Server Address			
database-1.cjuoe2og2iwn.us-east-	3306		
Domain	Unix socket path		
User	Password	Initial Database/Keyspace	Initial Schema
admin	*****	mydb	Schema
URI			
mysql://admin:*****@database-1.cjuoe2og2iwn.us-east-1.rds.amazonaws.com/mydb			
Make the password visible in order to change the database credentials through the URI format.			
SSH Tunnel			
Filter			
→ Test Cancel Save			



I'm Here

بعد ما ت save خش ب connect وتقدر بقا تعدل عليها ب SQL عادي.

The screenshot shows the MySQL Workbench interface. On the left, there's a sidebar with a search bar and a tree view of databases: 'information_schema', 'mydb' (selected), 'mysql', 'performance_schema', and 'sys'. The main area is titled 'mydb #1' and contains a single table named '1'. At the bottom right, there are 'Execute' and 'Discard' buttons.

من setting create replica وال action تقدر ت بسيطة.

The screenshot shows the AWS RDS 'Databases' page with one database listed: 'database-1'. The 'Actions' dropdown menu is open, showing various options: 'Create database', 'Quick Actions - New', 'Convert to Multi-AZ deployment', 'Stop temporarily', 'Reboot', 'Delete', 'Set up EC2 connection', 'Set up Lambda connection', and 'Create read replica'.

من action هتلaci كل ال options اللي ممكن تحتاجها

The screenshot shows the AWS RDS 'Databases' page with one database listed: 'database-1'. The 'Actions' dropdown menu is open, showing many more options than in the previous screenshot, including: 'Set up EC2 connection', 'Set up Lambda connection', 'Create read replica', 'Create Aurora read replica', 'Create Blue/Green Deployment - new', 'Promote', 'Take snapshot', 'Restore to point in time', 'Migrate snapshot', 'Create zero-ETL Integration', and 'Create RDS Proxy'. The 'Create database' option is highlighted in orange.

بعد ما تخلص امسحها ولو كنت مفعول ال **Deletion protection** ارجع الغيها.



I'm Here

→004 RDS Custom for Oracle and Microsoft

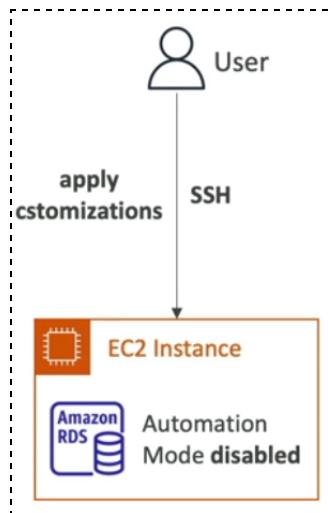
SQL Server

- **RDS vs. RDS Custom**

- **RDS:** entire database and the OS to be managed by AWS

الـ entire database & OS - كل حاجة managed By AWS

- **RDS Custom:** full admin access to the underlying OS and the database



من خلال RDS Custom تقدر يكون ليك full access على database & OS وال Automation mode ومتناش تفقل على instance



I'm Here

→005 Amazon Aurora



- **Relational Databases:**

من اسمها فيه علاقه بين ال tables جوا نفس ال database وال schema fixed

اللغة اللي ب query بسأل بيها عن ال data بتاعتي اسمها SQL Structured Query

Language

عكسها ال non-relational database

- **Overview:**

عبارة عن relational database service وmanaged by AWS ومصممه علشان

توفر لك compatible و high performance, high availability, and scalability

مع MySQL & PostgreSQL

- **Key Features**

1. High Performance:

- **Optimized Storage:** Aurora uses a distributed, fault-tolerant, self-healing storage system that automatically grows in increments of 10 GB, up to 128 TB per database instance.



I'm Here

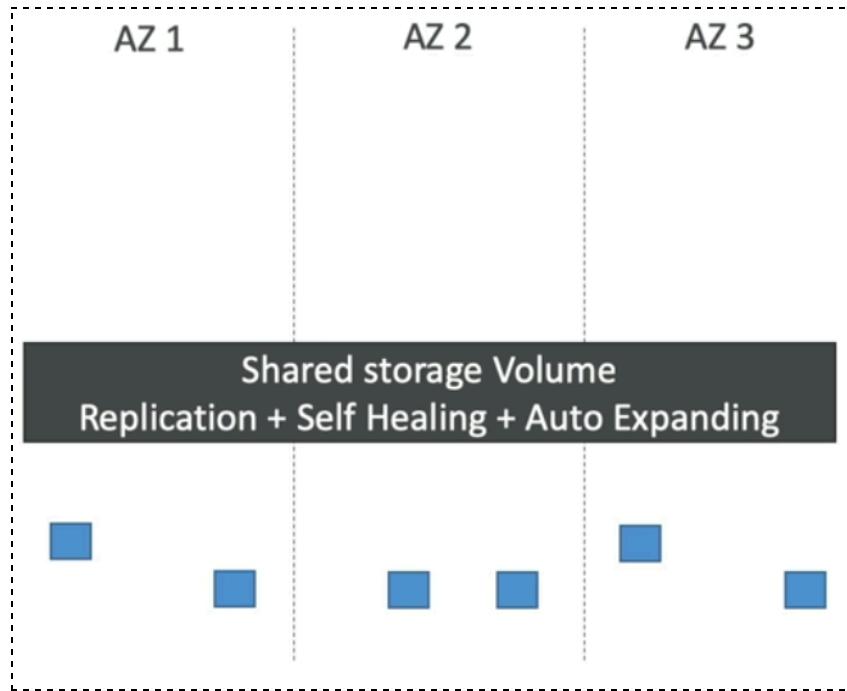
Shared storage Volume
Auto Expanding from 10G to 128 TB

ال Self healing ياعني لو فيه مشكلة حصلت فى الداتا corrupted تلفت هيا هتصلحها من نفسها .. عندك نسخ منها فى اماكن تانية ف بتاخذ منهم تحط مكان اللي تلف مش بتختروع جديد.

- **Low Latency:** It provides low-latency reads and writes, with the ability to deliver up to five times the throughput of standard MySQL and three times the throughput of standard PostgreSQL databases.

2. High Availability and Durability:

- **Fault-Tolerant Storage:** Data is replicated across six copies across three Availability Zones (AZs), ensuring data durability and high availability.



لو عملت write ل some data على 3 AZ..يبقى ال RDS multi AZ aurora

- **Automatic Failover:** Aurora automatically detects and handles instance failures, with failover typically completing within 30 seconds.
- **Multi-AZ Deployment:** Supports Multi-AZ deployments for automatic failover and increased availability.



I'm Here

3. Scalability:

- **Aurora Replicas:** Supports up to 15 low-latency read replicas, allowing you to scale read operations.

- متاح ليك 15 replicas خلال ال AZs بجانب ال Main database

- **Aurora Serverless:** Automatically scales the database capacity up or down based on application needs, allowing you to pay only for the resources you use.

4. Scalability:

- **Encryption:** Data is encrypted at rest using AWS Key Management Service (KMS) and in transit using SSL.
- **Network Isolation:** Integration with Amazon VPC allows you to isolate your database within a virtual network.
- **IAM Integration:** Allows fine-grained access control and authentication using AWS Identity and Access Management (IAM).

5. Backup and Recovery:

- **Automated Backups:** Continuous backups to Amazon S3 with point-in-time recovery.
- **Snapshot Backups:** Manual snapshots can be taken and restored as needed.

6. Compatibility:

- **MySQL-Compatible:** Aurora MySQL is compatible with MySQL 5.6, 5.7, and 8.0, allowing you to use existing MySQL tools and applications.
- **PostgreSQL-Compatible:** Aurora PostgreSQL is compatible with PostgreSQL 9.6, 10.x, 11.x, and 12.x, providing similar compatibility benefits.

- أغلبي حوالي 20% من ال RDS الباقين.. ولكن هي more efficient



I'm Here

- **What if the master database failed for RDS and Aurora:**

- **Aurora**

كدا كدا عندك 15 replicas متاحين اي واحدة منهم تقدر ت promote to be the master -
ودة بيحصل automatic فى خلال 30 ث

- **Amazon RDS**

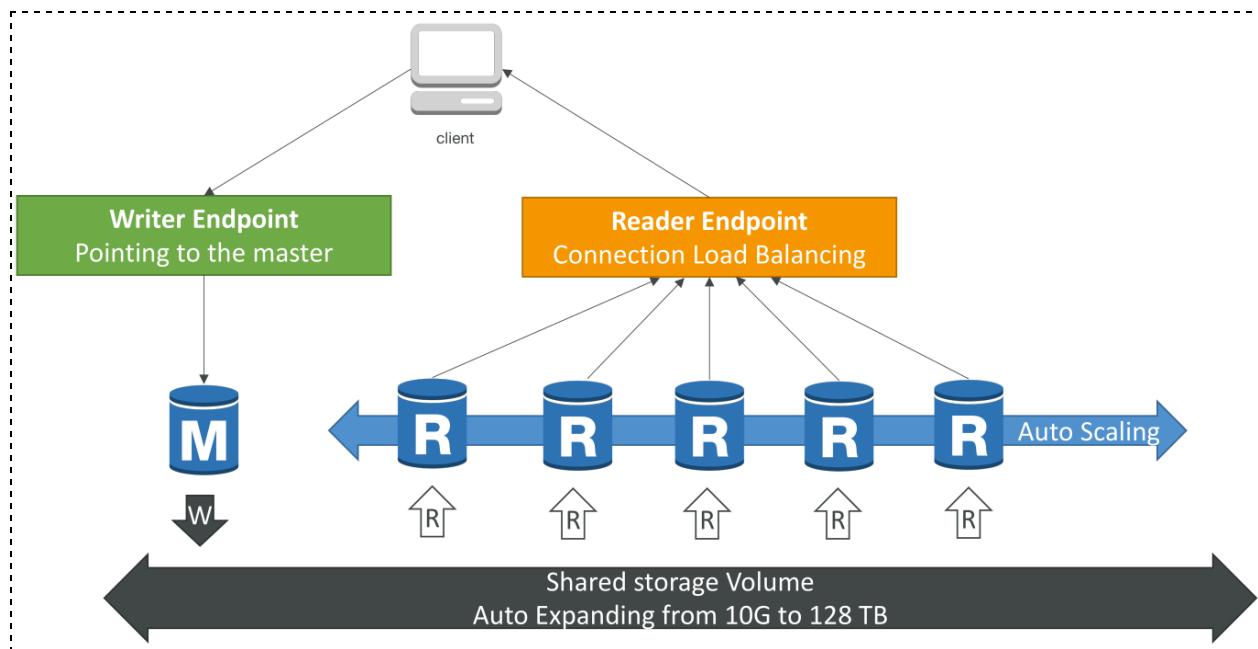
- **Have RDS Multi AZ**

لو عندك زي ما شرحنا هيكون عندك بجانب ال master standby instance هتلaci هتاخد الدور لو ال master failed -

- **Don't Have RDS Multi AZ**

لو معنكش بقا ال Down time هيطول على مات restore بقا من خلال backup ولا تشفف المشكلة فين وتصلّحها -

- **Aurora DB Cluster**



ال master DB بتقى مرتبطة ب writer endpoint عباره عن DNS name حتى لو ال client مشكله ال بتوجه عال writer endpoint دي وبتوجهه عال master اللي حصلها انها تبقى ال master instance -



I'm Here

- قولنا ان يكون عندنا 15 replicas ف صعب عليك ت track ال 15 replicas خصوصها انهم يعملون auto scaling

- **The diff between Aurora Server less and normal one**

- **Server less**

- مناسبة اكتر لل pay as you go unpredictable workloads ونظام الدفع

→006 Amazon Aurora - Hands On

. هيكون مكلف ال دة hands on .

يعتبر كل ال configuration اتكلمنا فيها.

بعد ما كريتناها .. هتلقيها بالشكل دة

- ال Region Cluster اللي بيوضح لك انت ف انهي

- read & write ودة ال main data base اللي بيحصل عليه Writer instance

عادي وبيكون عدده 1 فقط

- Reader Instance ودة بيحصل عليه read فقط وبيبقى فيه لحد 15

Databases							<input checked="" type="checkbox"/> Group resources		Modify	Actions ▾	Restore from S3	Create database
							<input type="text"/> Filter by databases					
DB identifier		Role	Engine	Region & AZ		Size						
•	database-2	Regional cluster	Aurora MySQL	eu-central-1	2 inst							
	database-2-instance-1	Writer instance	Aurora MySQL	eu-central-1b	db.t3.							
	database-2-instance-1-eu-central-1a	Reader instance	Aurora MySQL	eu-central-1a	db.t3.							



I'm Here

بعد ما ت ال select هتلaci ال endpoints الخاصة بال Regional Cluster وكم تحد اي instance لوحدها و هيظهر لك بردو ال ports وال writer وكدا..

Endpoint name	Status	Type	Port
database-2.cluster-ro-c2wzuhjkj1v.eu-central-1.rds.amazonaws.com	Available	Reader instance	3306
database-2.cluster-c2wzuhjkj1v.eu-central-1.rds.amazonaws.com	Available	Writer instance	3306

عندك Actions كتير تقدر تعملها

Reader instance = replica

- تزود reader instance فى نفس AZ مختلفه فى نفس AZ

- تزود replica فى Region مختلفة

- حصل مشكلة فى main مختلفات restore to point in time

- تضيف Auto scaling ل Replica



I'm Here

دلوقي هنضيف Replica to Auto Scaling Group

بنكريت policy وظيفتها ان معناها لو ال CPU Utilization زاد عن حد معين ول يكن 50% او

عدد ال connection زاد عن رقم كذا عال Replicas اللى already موجودة .. كريتلي

اكثر replica

Policy details

Policy name
A name for the policy used to identify it in the console, CLI, API, notifications, and events.

Policy name must be 1 to 256 characters.

IAM role
The following service-linked role is used by Aurora Auto Scaling.
 AWSServiceRoleForApplicationAutoScaling_RDSCluster

Target metric
Only one Aurora Auto Scaling policy is allowed for one metric.
 Average CPU utilization of Aurora Replicas [View metric](#) 
 Average connections of Aurora Replicas [View metric](#) 

Target value
Specify the desired value for the selected metric. Aurora Replicas will be added or removed to keep the metric close to the specified value.
 50 %

[► Additional configuration](#)

وبتحدد عدد ال Maximum Replicas Number

Cluster capacity details
Configure the minimum and maximum number of Aurora Replicas you want Aurora Auto Scaling to maintain.

Minimum capacity
Specify the minimum number of Aurora Replicas to maintain.
 1 Aurora Replicas

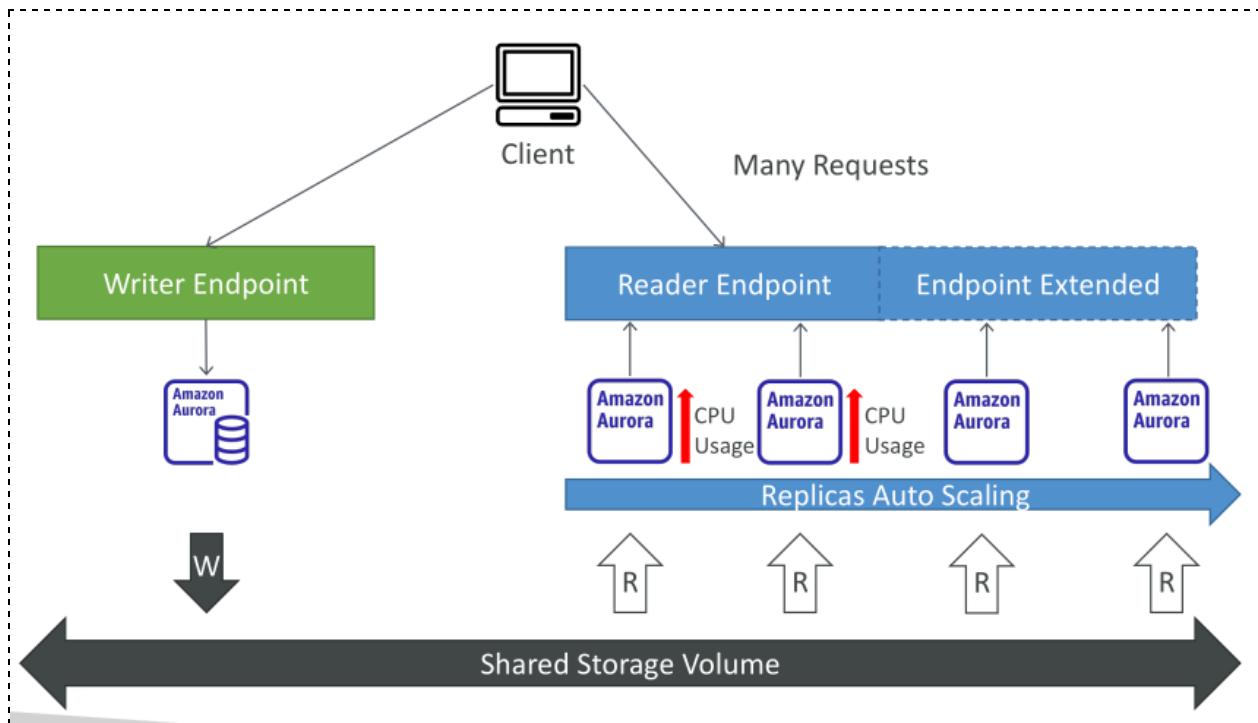
Maximum capacity
Specify the maximum number of Aurora Replicas to maintain. Up to 15 Aurora Replicas are supported.
 15 Aurora Replicas



I'm Here

→007 Amazon Aurora - Advanced Concepts

- Aurora Replicas - Auto Scaling

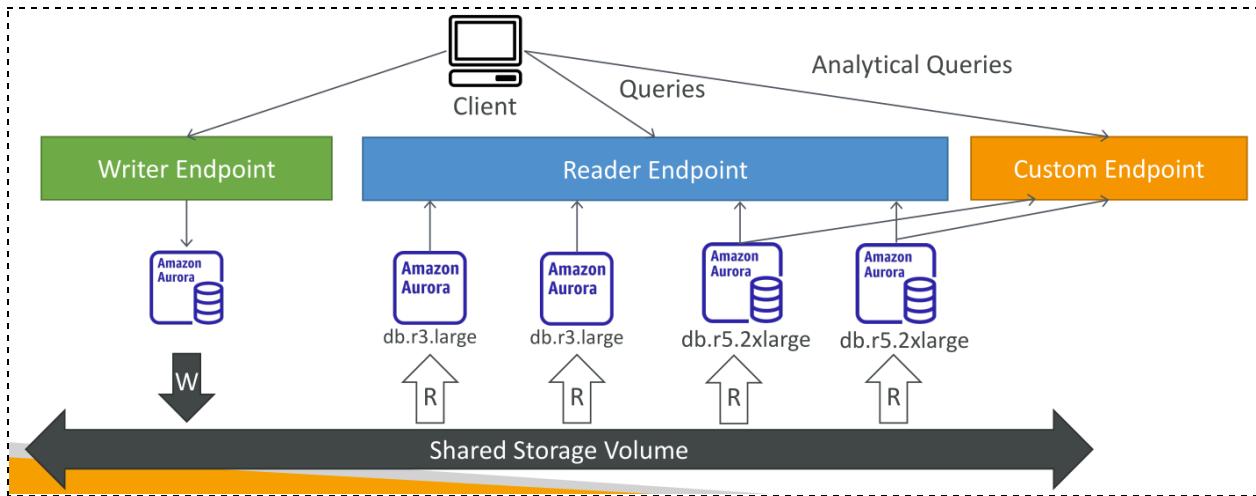


بعد ما ال reader auto scaling يزيد ال CPU utilization وال replicas بتزيد ب CPU utilization . هيا كمان بت extend endpoint .



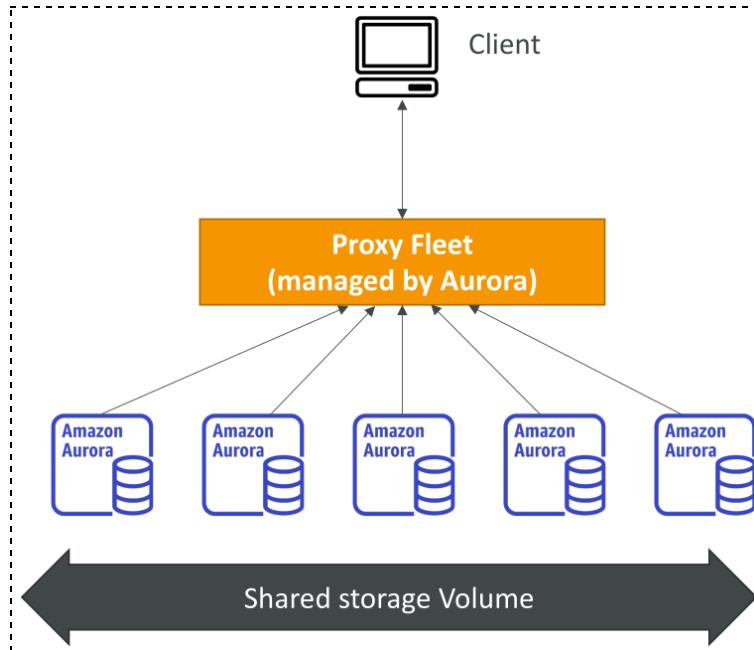
I'm Here

● Aurora – Custom Endpoints



بنكريت ال custom endpoint علشان نوزع traffic معين على instance معينه .. بمعنى
انك مثلًا عاوز ال Analytical queries traffic يروح على Reader Endpoint تستحمل الشغل دة
 تكون أقوى من ال Reader & custom replicas isolation بين ال endpoint

● The diff between Aurora Server less and normal one



مناسبة اكتر لـ unpredictable workloads او ال infrequent access ونظام الدفع
 capacity planning pay as you go



I'm Here

- ال data bases جاهزة بال usage بناءا عال auto scaling
 - يبقى ال client connect ل proxy fleet وده managed by Aurora وبيتوز عه
 - اللي بيكونو مخطوطين في instances auto scaling على حسب بقا ال usage
 - بتزيد او بتقل instances.

● Global Aurora

DB identifier	Role	Engine
database-2	Regional cluster	Aurora MySQL 5.7
database-2-instance-1	Writer instance	Aurora MySQL 5.7
database-2-instance-1-eu-central-1a	Reader instance	Aurora MySQL 5.7

- من Action زى مشوفنا تقدر كمان تضيف AWS Region بس لازم تكون مختار compatible instance نوع Global database feature Version مع ال Global database feature
 - استخدامها : بيكون عندك ال main + reader replicas ولكن primary region فى ال
 - انت مثلًا تحتاج serve عملاء اوربيين مختلفين عاوز يبقى عندك replicas فى region
 - تانية بحيث يكون الموضوع اسرع ف وبالتالي بت add region .. يبقى انت كنت فى ول يكن us-east-1 (N. Virginia) region

eu-west-1 (Ireland) to serve European users with low-latency read access and to have a disaster recovery solution.

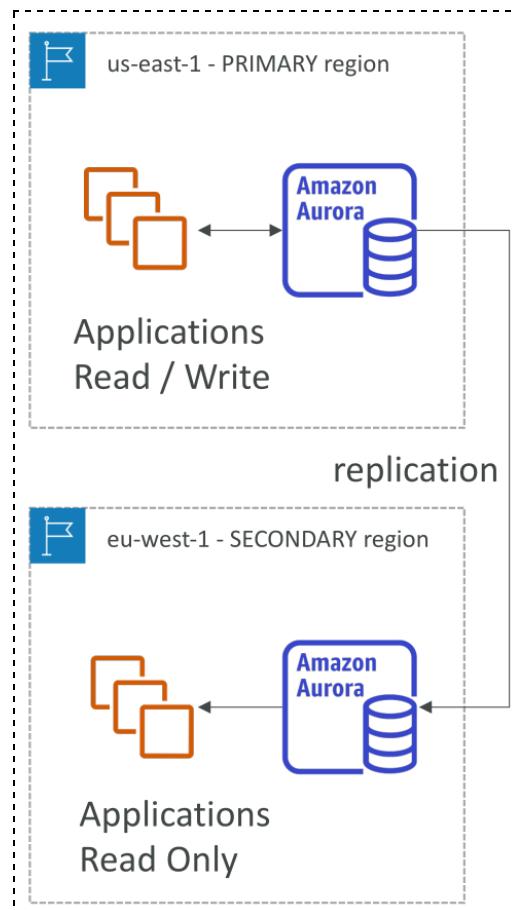


I'm Here

- Aurora Global Database (recommended):

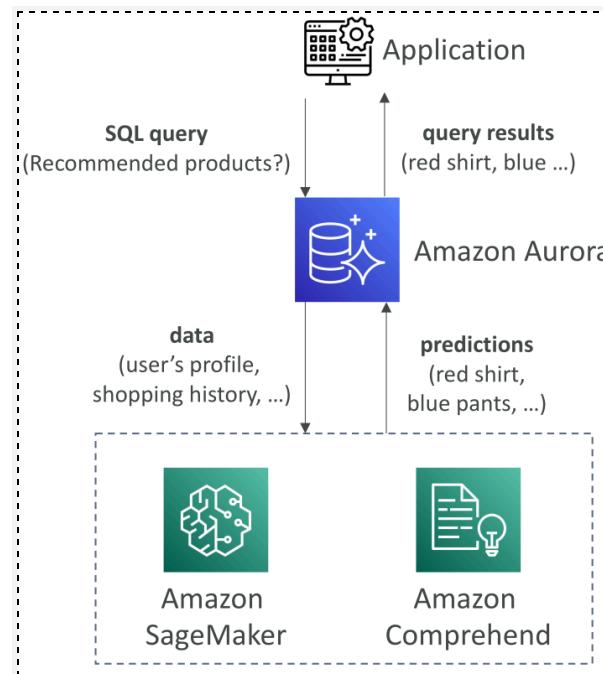
- دة اللي تقدر يكون عندك:

1. Primary region >> read & write
 2. Up to 5 secondary (read-only) regions, replication lag is less than 1 second
 3. Up to 16 Read Replicas per secondary region
- الـ main 1 + ياعني توtal 16 .. ف عندك بردو في replicas 16 regions الـ 5 الاضافيـه اللي تقدر تضيفهم كل واحدة يكون فيها
- Promoting another region (for disaster recovery) has an RTO of < 1 minute
 - Typical cross-region replication takes less than 1 second



I'm Here

• Aurora Machine Learning



عباره عن AWS Machine Learning Services و Aurora integration بين -
عندك مثلًا Aurora معينه ف تقدر انت من خلال simple SQL Services متصله ب ML Services -
ف recommended products application run it Query ول يكن مثلاً ايه ال shopping history زي ال database Aurora بما انها تتبع شوية داتا لـ ML services وهكذا وتشتغل ال profile ، shopping history دي عالداتا دي وتعرف ايه ال query results .. وتتبع ال recommended products دي لـ Aurora اللي APP هتبتعتها لـ .



I'm Here

→008 RDS & Aurora - Backup and Monitoring

● RDS Backup:

● Automated Backup

- بيحصل backup كل 5 دقايق بيتجدد ياعني لو عملت restore ل any point in time بتحصل على نسخة اخر 5 دقايق .. وال backups دي بتفضل من 0 : 35 يوم

● Manual DB Snapshots

- دي بتعملها manual والفرق بينها وبين ال automated ان دي بتفضل موجودة لحد ما انت تمسحها الثانية اخرها 35 يوم

لو مش عاوز costs عالية .. لو بتشغل مثلا على database ساعتين فقط في الشهر ..
بدل ما تشغل ال Automated Backup وبعد عليك كل ساعة ال data بتاعة ال backup
دي موجودة فيها .. خد افضل snapshot بعد ما تخلص ساعتين الشغل دول وابقي اعملها
دة ارخص بكثير.. لأنك حتى لو عامل stop لل data base بعد ما تخلص الساعتين restore
شغل ف انت هتدفع عليها حتى لو واقفة.

● Aurora Backup:

● Automated Backup

- بيحصل من 1 : 35 يوم ومتقدرش توقف ال backup دي اقل حاجة هتفضل ال data يوم .. ولليك point in time recovery في اي وقت خلال المدة دي.

● Manual DB Snapshots

- زيها زي اللي فوق .. بتعملها manual وبتخليها موجودة زي مانت عاوز وتمسحها وقت ما تعوز.



I'm Here

• RDS & Aurora Restore options

لما بت restore ال backup new فبتعمل snapshots من سواء . -

database بيهـا .

تقدر ت restore database من S3 ودي عباره عن service بنخزن بيهـا ال objects . -

AWS Cloud هنتكلم عنها بالتفصيل قدام .

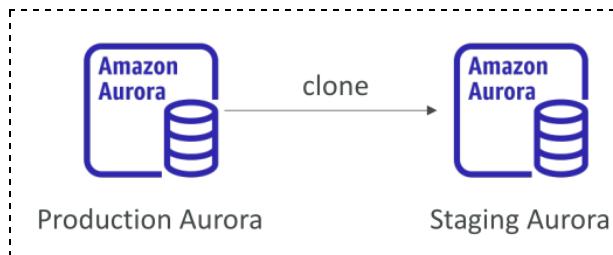
• Restoring MySQL RDS database from S3

- Create a backup of your on-premises database
- Store it on Amazon S3 (object storage)
- Restore the backup file onto a new RDS instance running MySQL

• Restoring MySQL Aurora cluster from S3

- Create a backup of your on-premises database using Percona XtraBackup
- Store the backup file on Amazon S3
- Restore the backup file onto a new Aurora cluster running MySQL

• Aurora Database Cloning



بت clone بتنسخ ال main database اللـى عـال production لو محتاج تعمل test عليها . -

ف حاجة معينـه عـشان متضرـهـاش هـيـا .. ف بـتـعـمـلـ الـ testـ بـتـاعـكـ عـالـ clonedـ databaseـ .

ودة اسرع من انك تاخـدـ snapshotـ وـتـ restoreـ itـ بـتـ copy-on-writeـ protocolـ اسمـهـ . -



I'm Here

→009 RDS & Aurora Security

• Encryption at Rest

لما بت enable ال Automatic Encryption ف كل ال RDS or Aurora لـ database instance, automated encrypted backups, read replicas, and snapshots . المتخرنة بتكون دة بيشمل ال encryption على database enable مش معمولها encryption enable مينفعش ت restore as new encrypted instance snapshot بتاخد وتعملها

• Encryption in Transit

.support encryption in transit using SSL/TLS بي RDS & Aurora بت configure database connection to use SSL/TLS بحيث تضمن ان ال app encrypted اللي بتتنقل بينك وبين ال data

• IAM Database Authentication

ممكن ت create IAM Policies تسمح لك باى access ال RDS & Aurora ممكن تستخدم IAM Tokens بدلا من ال data base passwords -
- IAM authentication relies on temporary authentication tokens generated by AWS. These tokens are valid for 15 minutes and can be used in place of a password when connecting to the database.

• Security Groups

- تقدر ت control the network access to your database من خلال انك تقدر تحكم ف مين ي give ال database access ممكن ip معين او ports معينه ..

• SSH Access

- متقدرش ت ssh عال databases دي لأنها managed serves by AWS ولكن ممكن من خلال RDS Custom اللي اتكلمنا عليها قبل كدا.

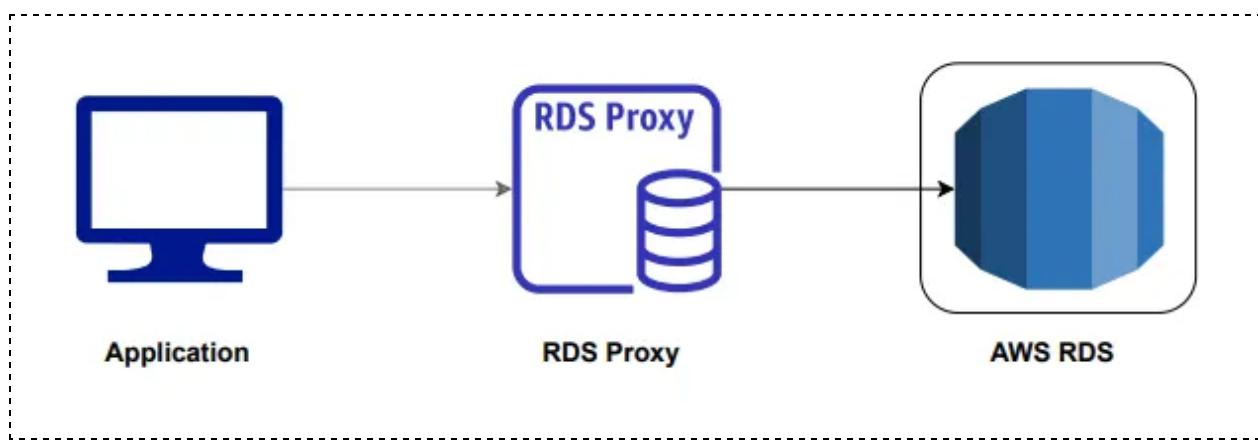


I'm Here

• Audit logs

- فيها كل حاجة حصلت على ال data bases وكل ال queries ولكن مش بتفضل موجودة لوقت طويل .. ف علشان كدا تقدر تتبع ال audit logs دي لـ cloud watch علشان تحفظها هناك.

→010 RDS Proxy



application باختصار عباره عن وسيط بين ال client & Server فى حالتنا ال - database server

• Use Case

طب هو وسيط بين ال client , database فى الحالة دي ليه محتاجينه طالما احنا نقدر ن فى عدنا ؟ connect directly to the database e-commerce app مثلا واثناء ال sale days فيه ضغط كبير و connections كتيرة رايحة عال database ممكن يوقعها ف علشان كدا بنستخدم ال RDS Proxy بحيث يخف الضغط عنها وهو بيكون عباره عن scale up and down multi AZs وبي بناءا على حجم ال standby database بسرعه سواء ل direct the connections وبي connection replica



I'm Here

- Supports RDS (MySQL, PostgreSQL, MariaDB, MS SQL Server) and Aurora (MySQL, PostgreSQL)

• RDS Proxy Enhanced Security

- لو عندك web app وعاوز ي connect to a RDS

• Without RDS Proxy

- فى الغالب بت save the user name & password فى ال app code وده خطر.

• With RDS Proxy

- تقدر تستخدم IAM roles فى انك تتحكم ف who can connect to the database او بي AWS Secrets Manager من ال database credentials retrieve

- ف ب كدا مش محتاج تحط ال password فى ال application Update it automatically

- عباره عن service بي تخذن فيها ال sensitive database passwords زى ال informations AWS Secrets Manager

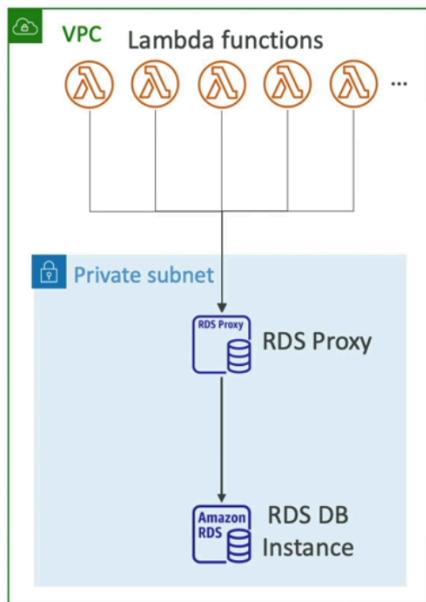
.. public access فقط من خلال ال VPC مش من ال RDS Proxy 

ياعني ال resources فقط اللي جوا ال VPC تقدر تأكسسه غير كدا لا

- من اكتر ال services اللي بتسخدم RDS Proxy هي Lambda function وهنتكلم عنها بالتفصيل بعدين ..



I'm Here



→011 ElastiCache Overview

- **Diff Between Cookie & Cache**

- **Cookie**

غرضها انها تخزن ال data اللي ليها علاقه بال user login session وال preferences -
بتاعته شوية داتا بسيطة ياعني .. وبتتخزن عند ال user's browser وزي ما شرحنا قبل كدا
بتتبعت في ال requests اللي بين ال server وال user .. وال cookie دي ال
بتاعها بنعملو set من خلال ال server ولو انتهي او عملت مسح لل expiration date
اللى فى ال browser مثلًا تلاقي ان ال login sessions عملت log out وكمان
زي ما بيحصل ..

- Cookies are sent with every HTTP request to the server.



I'm Here

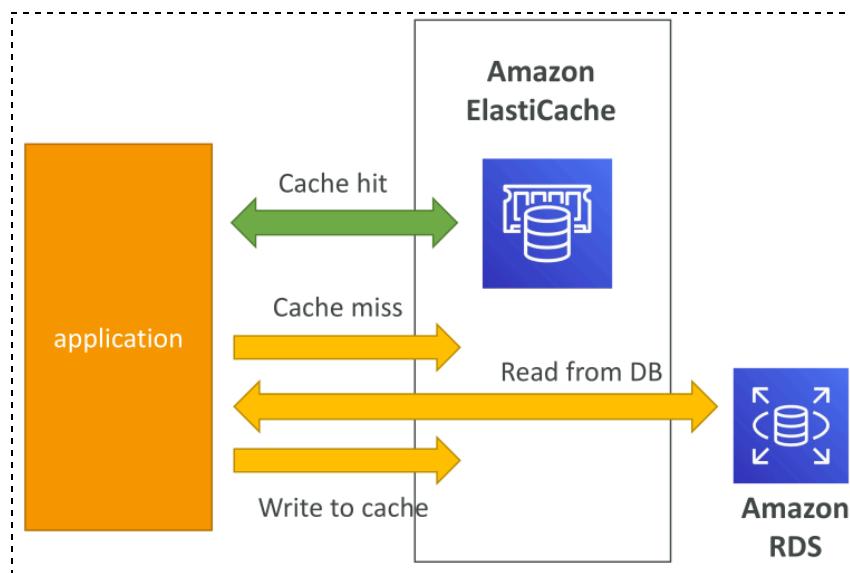
• Cookie

- اکبر شویة من اللى فاتت عباره عن web resources عال load times غرضها تقليل ال HTML او ال bandwidth وتقليل ال database files .. عباره عن زى server pages, images, CSS stylesheets, JavaScript files, and other user's computer by the locally ... multimedia content website لو جيت تزور نفس ال page او ال browser ويحصلها access ليها بردو set at the server cache headers الكلام دة اتعمله expiration date

- Cached resources are accessed locally by the browser without additional HTTP requests to the server.

• Amazon ElastiCache

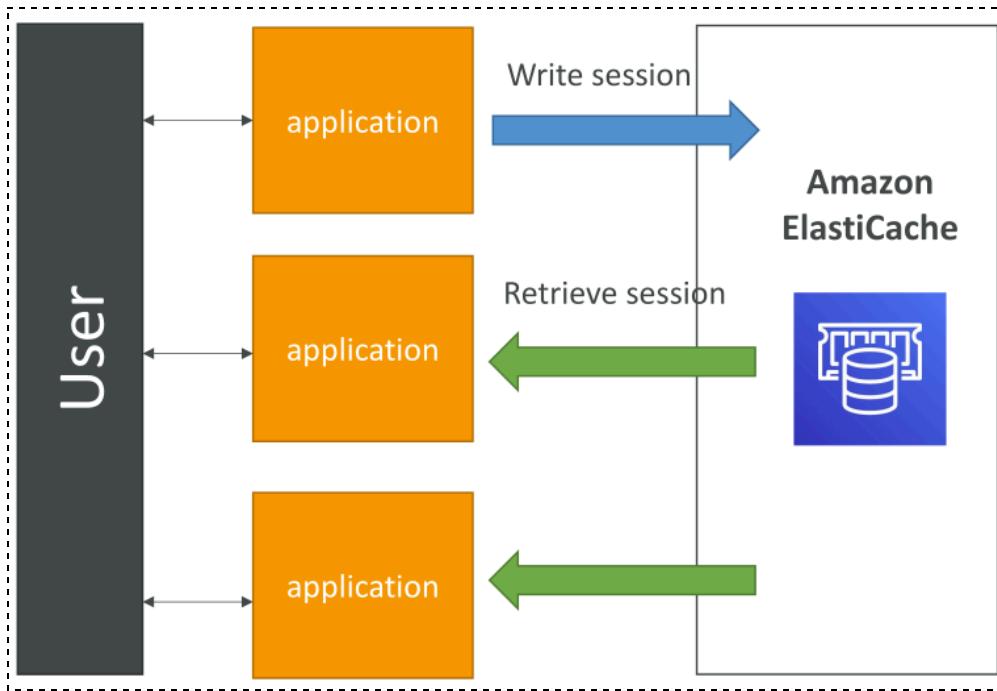
عباره عن Managed Service By AWS -



- لو ال queries already عمل application لوال ElasticCache query موجودة في ال Cache Hit AWS ElastiCache ف دة إسمه ومتخزنة في ال caches AWS ElastiCache ف هيروح ال App يجيها لو ال DataBase من ال



I'm Here



مثال کمان : ال user هي login ف اي واحد من ال Apps بتوعك فال App هي ال redirecting .. ف لو ال user دة حصلو ElasticCache Session data لاي instance تانية شايله ال App بتاعك ف ال instance دي بت retrive علطول ال user logged in ElasticCache ف بيفضل ال session data دی من ال user_logged_in ي دة كدا اسمه ان ال Application بتاعك log in again Stateless

- **Amazon ElastiCache Engines**

Follow



I'm Here