📘 AWS Certified Solutions Architect – Associate (SAA-C03)

Rafat Ashraf K.

✅ 1. EC2 (Elastic Compute Cloud)

- عبارة عن: سيرفر افتراضي (Virtual Machine) بتشغله على السحابة.
- بتتحكم في: نظام التشغيل – نوع الجهاز – المساحة – البروسيسور – الرام.
- حالات الاستخدام: استضافة مواقع – تطبيقات – قواعد بيانات.
- مميزاته:
  - بتدفع على قد الاستخدام.(Pay-as-you-go)
  - تقدر تعمل (**Auto Scaling**يزود/يقلل السيرفرات حسب الضغط.)
  - تقدر تحطه ورا **Load Balancer**علشان توزع الضغط.
- أنواعه:
  - **On-Demand:**استخدام مؤقت – تدفع بالساعات.
  - **Reserved:**حجز لفترة طويلة – أرخص في السعر.
  - **Spot Instances:**سعر قليل – بس ممكن تتقفل في أي وقت.

✅ 2. S3 (Simple Storage Service)

- عبارة عن: تخزين ملفات.(Images, Videos, Backups)
- مفيهوش حد أقصى للحجم أو عدد الملفات.
- الملفات بتتحفظ في حاجة اسمها **Buckets.**
- مميزاته:
  - تخزين دائم وداعم للتكرار والنسخ الاحتياطي.
  - صلاحيات على مستوى الملف أو الـ.Bucket (Public/Private)
  - يدعم (**Versioning**تحتفظ بكل نسخة من الملف.)
  - يدعم التشفير.(Encryption at rest and in transit)
- استخداماته:
  - استضافة صور/ميديا.
  - Backup.
  - استضافة.Static Websites

🔶 Enable versioning on the S3 bucket

- بيخلي الـ S3 يحتفظ بكل نسخة من الملف حتى لو اتعدلت أو اتمسحت.
- تقدر ترجع لأي نسخة قديمة بسهولة لو حصل حذف أو تعديل غلط.
- بيقلل خطر فقدان البيانات بشكل كبير.

🔷 Enable MFA Delete on the S3 bucket

- خاصية بتطلب تأكيد إضافي (MFA) قبل ما تسمح بحذف نسخة أو تغيير في إعدادات الـ bucket.
- بتضيف طبقة أمان زيادة عشان تمنع الحذف الغلط أو غير المصرح بيه.
- مفيدة جدًا لحماية البيانات الحساسة من الحذف بدون قصد.

✅ 3. Amazon Athena

هي خدمة من AWS بتخليك تعمل **SQL Queries مباشرةً على الملفات اللي في S3** ، من غير ما ترفعها أو تنقلها لأي قاعدة بيانات.

✅ مميزاتها:

- **من غير سيرفرات** → (Serverless)مش بتدير حاجة.
- بتشتغل على ملفات زي **JSON** :، **CSV**، **Parquet**، **إلخ**.
- بتدفع بس لما تعمل. 💰 Query
- مثالية لو البيانات موجودة في S3 وانت عايز تحللها بسرعة.

✅ 4. Amazon QuickSight:

- أداة **Visualizations** و) **Dashboards** زي Power BI أو.(Tableau
- بتستخدمها لعرض وتحليل البيانات بشكل تفاعلي.
- بتدعم مصادر كتير زي:
  - S3
  - RDS
  - Athena
  - Redshift
- تقدر تتحكم في **الصلاحيات** :مين يشوف إيه.

✅ 5. AWS Glue:

- خدمة **ETL** (Extract, Transform, Load).
- بتستخدمها عشان:
  - تجهز الداتا
  - تعمل لها تنظيف وتنظيم
  - وتحولها لشكل مناسب للتحليل.
- مش بتعمل Visualizations ، هي بس تجهيز للبيانات.

✅ 6. IAM (Identity and Access Management)

- لإدارة **المستخدمين** والصلاحيات في حساب AWS.
- بتقدر تنشئ:
  - **Users:** لكل شخص.
  - **Groups:** لمجموعة ناس.
  - **Roles:** للـ services علشان تاخد صلاحيات معينة.
  - **Policies:** ملفات JSON فيها الصلاحيات.
- مميزاته:
  - تقدر تتحكم مين يشوف إيه ويعمل إيه.
  - يشتغل مع (**MFA** تحقق بخطوتين.)
  - Shared Responsibility Model: انت مسؤول عن الـ Access.

✅ 7. AWS Secrets Manager

خدمة من AWS لتخزين وإدارة البيانات الحساسة زي الباسوردات و API Keys.

🔐بيعمل ايه؟

- بيخزّن الـ secrets بشكل مشفّر
- بيمنعك تكتب الباسورد في الكود
- بيغير الباسوردات أوتوماتيك (Automatic Rotation)
- بيراقب مين استخدم الـ secret وامتى (Monitoring)

✅ 8. RDS (Relational Database Service)

- عبارة عن: قواعد بيانات (Managed بتتظبط أوتوماتيك.)
- أنواعها: MySQL – PostgreSQL – MariaDB – Oracle – SQL Server.
- مميزاته:
  - AWSبتدير الصيانة – النسخ الاحتياطي – الحماية.
  - High Availabilityلو فعلت **Multi-AZ**.
  - Auto Scalingللمساحة.
- استخدامه:
  - قواعد بيانات المواقع والتطبيقات اللي محتاجة علاقات.(Relational)

✅ 9. VPC (Virtual Private Cloud)

- شبكة خاصة بتبنيها جوا AWS.
- بتحدد فيها:
  - **Subnets**: عامة أو خاصة.
  - **IP Range**.
  - **Route Tables**.
  - **Gateways** (Internet Gateway / NAT).
- هدفها:
  - تتحكم في مين يدخل على إيه.
  - بتعمل بيها بيئة أمان معزولة للخدمات بتاعتك.

✅ 10. Gateway VPC Endpoint

ده نوع من أنواع VPC Endpoints بيسمح للـ EC2 أو أي خدمة جوه (VPC إنها **توصل لخدمة AWS زي S3 أو DynamoDBمن غير ما تحتاج إنترنت**.

✅ 11. AWS Network Firewall

- **جدار ناري (Firewall)** خاص بـVPC
- بيعمل **فحص وتصفية للترافيك** (Traffic inspection & filtering)
- تقدر تكتب **قواعد لحظر أو السماح للترافيك** (rules)
- بيشتغل على **Inbound**و**Outbound**
- مناسب لحماية الشبكة زي الـ firewalls التقليدية

✅ 12. Amazon GuardDuty

- خدمة مراقبة أمنية (Threat Detection)
- تكتشف تهديدات أو نشاطات غريبة (مثل محاولات اختراق)
- مش بتحظر الترافيك، بس **بتنبهك**
- بيستخدم الذكاء الاصطناعي لتحليل الـ logs والأنشطة
- مناسب لمراقبة الحسابات و VPCs و IAM بشكل ذكي

✅ 13. Lambda

- خدمة = Serverless تشغل كود من غير ما تحتاج سيرفر.
- تكتب كود بلغة.(Python – Node.js – Java – Go)
- يتنفذ لما يحصل (Event زي رفع ملف على S3 أو.(API call
- مميزاته:
  - بتدفع بس وقت تنفيذ الكود.
  - مفيش سيرفر تشغله أو توقفه.
  - بيتكامل مع باقي خدمات.(AWS (S3 – DynamoDB – SNS

✅ 14. CloudFront

- = CDNشبكة توصيل محتوى.
- بتسحب الصور/الملفات من S3 أو سيرفرك، وتعرضها من أقرب موقع للزائر.
- يقلل وقت التحميل ويحمي من الهجمات.(DDoS)
- يدعم HTTPS و Caching وSigned URLs.

✅ 15. Route 53

- خدمة DNS من AWS.
- تربط اسم الدومين بالخدمة – S3 – Load Balancer – EC2) إلخ.)
- مميزاته:
  - Fast & Reliable.
  - يدعم) Health Checks يعرف لو سيرفرك وقع.)
  - Routing Policies:
    - Simple
    - Weighted
    - Latency-based
    - Failover

✅ 16. CloudWatch

- أداة للمراقبة والـ Logging.
- تتابع الأداء، وتصدر تنبيهات.
- تقدر تراقب:
  - EC2 usage
  - Lambda execution
  - S3 operations
- تقدر تعمل Dashboards و Alarms و Logs Filters.

✅ 17. Auto Scaling

- تزود أو تقلل عدد الـ EC2 instances حسب الضغط.
- بيشتغل مع Load Balancer.
- بتحط) Rules لو الـ CPU زاد عن ٨٠٪ ← زوّد سيرفر.)

✅ 18. Elastic Load Balancer (ELB)

- بيوزّع الترافيك بين أكتر من EC2.
- الأنواع:
  - **Application ELB**لـ(HTTP/HTTPS)
  - **Network ELB**أداء عالي للـ(TCP)
  - **Gateway ELB**للـ(third-party appliances)

✅ 19. Gateway Load Balancer (GWLB)

هو نوع من الـ Load Balancer بيستخدم علشان تمرّر الترافيك من خلال أدوات الأمان (زي الفايروول) من غير ما تغيّر الترافيك.

بيخلي أي ترافيك يروح الأول على الفايروول (أو أي أداة تفتيش)، و بعد يوصّله للسيرفرات بتاعتك .

بيستخدم لما تحب :

- تعمل فحص للترافيك (Packet Inspection)
- تدخل فايروول خارجي
- تزود أمان الشبكة من غير تعقيد

✅ 20. EBS (Elastic Block Store)

- تخزين مرتبط بـ EC2.
- بيشتغل زي الهارد ديسك.
- مميزات:
  - Snapshot Backup.
  - Encrypted.
  - تقدر توصله لأكتر من) EC2 بـ خاصية.(Multi-Attach

✅ 21. EFS (Elastic File System)

- تخزين ملفات مش مرتبط بجهاز معين.
- = Shared File System كذا EC2 يقدروا يقروا/يكتبوا عليه في نفس الوقت.
- مناسب للـ Big Data و Multi-Server Apps.

✅ 22. NFS (Network File System)

- بروتوكول مشاركة ملفات (يعني وسيلة إنك تخلي ملفاتك متاحة لأجهزة تانية).
- بيشتغل جوه الشبكة المحلية.(LAN)
- أي جهاز ممكن يعمل **mount**للـ NFS share ويشوف الملفات كأنها على جهازه.

💡مثال شائع:

عندك سيرفر ملفات في الشركة، وباقي الموظفين بيشوفوا الفولدر ده من أجهزتهم.

✅ 23. Amazon FSx for Windows File Server

- خدمة تخزين ملفات مخصصة لويندوز بتدعم بروتوكول SMB (نظام الملفات الشبكي لويندوز).
- بتديك تخزين ملفات سريع، آمن، وموثوق زي ما الشركات محتاجة.
- بتدعم Multi-AZ يعني توافر عالي، لو حصل مشكلة في منطقة بيشتغل تلقائي في التانية.
- بتحافظ على صلاحيات الملفات وأمانها زي نظام ويندوز الأصلي.

✅ 24. DynamoDB

- قاعدة بيانات NoSQL سريعة جدًا.
- مناسبة للجداول اللي مفيهاش علاقات.
- Auto Scaling – Backup – TTL – Streams.

✅ 25. SQS (Simple Queue Service)

خدمة **صف رسائل (Queue)**
بتحط فيها الرسائل، وكل رسالة بتتقرا **مرة واحدة بس** من مستهلك واحد.(Consumer)

✅مميزاته:

- Decoupling ممتاز) بتفصل بين الـ Producer و الـ(Consumer
- بيساعد في التعامل مع الرسائل لما الـ Consumer مش جاهز فورًا
- قابل للتوسع(Scalable)
- رسائل بتقعد في الـ Queue لحد ما حد يسحبها

✅ 26. SNS (Simple Notification Service)

خدمة **Publish/Subscribe**
يعني تقدر تبعت رسالة واحدة، وتتوزع على أكتر من جهة في نفس الوقت.

✅ مميزاته:

- كل اللي عامل Subscribe للـ Topic هيوصله الرسالة
- ممكن تبعت الرسالة لـ:

  HTTP endpoint , Email , Lambda , SQS
- إرسال إشعارات أو رسائل لموبايل/إيميل.Services/
- تشتغل مع Lambda أو.SQS
- مثال: رفع صورة على SNS ← S3 تبعت تنبيه.

✅ 27. CloudFormation

- خدمة بتخليك تبني البنية التحتية ككود.(Infrastructure as Code)
- تكتب ملف YAML/JSON فيه تفاصيل السيرفرات والشبكات... إلخ.
- تقدر تعمل Deploy لنفس البنية في كذا مكان.

✅ 28. Elastic Beanstalk

- Platform-as-a-Service.
- بترفع التطبيق بتاعك وهو يجهزلك السيرفرات تلقائي.
- يدعم.NET – Ruby – Node.js – PHP – Python – Java :

✅ 29. API Gateway

- خدمة لإنشاء وإدارة) APIs واجهات برمجية.(
- تشتغل مع Lambda أو أي سيرفر.
- تقدر تعمل بها REST API أو.WebSocket API
- مميزاتها:
  -) Rate Limitingتمنع الترافيك الزايد.(
  -) Authorizationتكامل مع IAM و.(Cognito
  - Loggingمع.CloudWatch

✅ 30. Step Functions

- خدمة بتربط بين أكتر من خدمة AWS على شكل **Workflow.**
- تقدر ترتب العمليات واحدة ورا التانية) مثلاً.(Lambda → SNS → DynamoDB :
- بتشتغل بلغة.JSON
- فيها Error Handling و.Retry

✅ 31. Kinesis

- خدمة لتجميع البيانات اللحظية.(Real-time Data Streaming)
- معمول لتحليل البيانات باستخدام SQL جوهKinesis
- مفيدة لـ:
  - تتبع.Logs
  - تحليل Clicks في المواقع.
  - بيانات إنترنت الأشياء.(IoT)
- الأنواع:
  - Kinesis Data Streams.
  - Kinesis Firehose (للتوصيل مع S3 أو.(Redshift
  - Kinesis Analytics.

✅ 32. CloudTrail

- خدمة لتسجيل كل العمليات اللي بتحصل في حساب AWS بتاعك.
- مثال: مين حذف – EC2 مين عدل – Policy إلخ.
- تحفظ اللوجات في S3 وتقدر تبعتهم لـ.CloudWatch

✅ 33. Global Accelerator

- خدمة بتزود سرعة وأداء التطبيقات عالمياً.
- بتستخدم شبكة AWS الداخلية لتقليل الـ.Latency
- بيفيدك لو عندك زباين في كذا دولة وعايزهم يوصلوا للخدمة بسرعة.

✅ 34. CodePipeline / CodeBuild / CodeDeploy

🔷 CodePipeline:

- بتدير عملية نشر الكود من A-Z (CI/CD).
- تربط بين GitHub أو CodeCommit مع مراحل Build و Deploy.

🔷 CodeBuild:

- خدمة لتجميع وبناء الكود (Compile – Test – Package).

🔷 CodeDeploy:

- خدمة لنشر الكود على EC2 أو Lambda أو ECS.

✅ 35. Trusted Advisor

- أداة بتراجع حسابك وتنصحك بـ:
  - الأمان.
  - الأداء.
  - التوفير المالي.
- بتقولك مثلاً: عندك EC2 مش شغال بس بتدفعله ← احذفه.

✅ 36. AWS Config

- خدمة بتتبع التغييرات اللي بتحصل في الـ Resources بتاعتك.
- مثال: مين غيّر Security Group ؟ إمتى؟.
- بتساعد في الـ Auditing والـ Compliance.

مميزاته:

- بيشتغل أوتوماتيك من غير تدخل يدوي.
- تقدر تعمل Rules مخصصة حسب احتياجك.
- بيخزن Snapshot للحالة الحالية والإعدادات.

✅ 36. Amazon Inspector

عبارة عن: خدمة فحص أمني للثغرات (Vulnerability Scanning) في EC2 والحاويات.

بتتحكم في: فحص النظام – البحث عن ثغرات – تقييم درجة الخطورة.

حالات الاستخدام:

- تقييم أمان السيرفرات والتطبيقات.
- اكتشاف الثغرات قبل ما يتم استغلالها.
- أوتوماتيك ويشتغل دورياً.
- بيطلع تقارير أمنية واضحة.

✅ 37. S3 Access Logs + EventBridge

عبارة عن:

- **S3 Access Logs** : بتسجل كل العمليات اللي حصلت على الملفات (مين دخل – منين – إمتى).
- **EventBridge** : بيستقبل أحداث معينة من AWS ويقدر يشغل أكشن بناءً عليها

حالات الاستخدام:

- معرفة تفاصيل الوصول للملفات.
- تشغيل أكشن معين لو حصل حدث معين (زي رفع ملف جديد).
- بيعطيك بيانات دقيقة عن عمليات الوصول.
- EventBridge مرن في الربط مع خدمات تانية.

عيوبه:

- مش بيراقب تغييرات الإعدادات (زي تعديل الـ policy أو الـ ACLs).
- محتاج تدمجه مع خدمة تانية لو عايز تراقب الإعدادات نفسها.

✅ 38. ElastiCache

- خدمة لتخزين البيانات في الذاكرة.(In-Memory Cache)
- تدعم:
  - **Redis**
  - **Memcached**
- بتحسّن السرعة بدل ما تقرأ من قواعد البيانات كل مرة.

✅ 39. Snowball / Snowmobile

- لنقل البيانات الضخمة جدًا من وإلى AWS.

🟤 Snowball:

- جهاز فعلي AWS تبعتهولك، تنقل عليه البيانات، وترجعه لهم.

🟤 Snowmobile:

- شاحنة ضخمة فيها Data Center كامل – لو عندك بيتابايتات بيانات.

✅ 40. Shield / WAF

🟣 AWS Shield:

- خدمة لحماية التطبيقات من هجمات DDoS.
- فيها نوعين Standard: (مجاني) و Advanced (مدفوع).

🟣 WAF (Web Application Firewall):

- تقدر تمنع هجمات XSS – SQL Injection.
- بتحط Rules على CloudFront أو ALB أو API Gateway.

✅ 41. AWS Organizations & Consolidated Billing

- تقدر تجمع أكتر من حساب AWS تحت إدارة واحدة.
  - تقسيم الحسابات (مثلاً: Dev – Prod – Billing).
  - مشاركة موارد.
  - فلترة الصلاحيات (Service Control Policies).
  - توحيد الفواتير وتوفير فلوس.

✅ 42. AWS Fargate

- خدمة managed بتشغل الحاويات (containers) من غير ما تحتاج تدير سيرفرات أو بنية تحتية.
- انت بس بتحدد الحاويات بتاعتك (Docker containers)، وFargate بيتكفل بالباقي (تشغيل، توسيع، صيانة).
- بيسهل عليك التركيز على تطوير التطبيقات بدل إدارة السيرفرات.
- بيدعم التكامل مع Amazon ECS و EKS.
- مناسب لو عايز حل بسيط، سريع، وبدون تعقيد في إدارة السيرفرات.

🔷 Amazon Rekognition

- بتحلل صور وفيديوهات، تكشف محتوى غير لائق بسهولة، مناسب للصور وتوفر مجهود تطوير قليل.

🔶 Amazon Comprehend

- بتحلل نصوص تكشف محتوى غير لائق بسهولة وتوفر مجهود تطوير قليل.

✅ DynamoDB Point-In-Time Recovery (PITR)

- ترجع جدول DynamoDB لأي وقت خلال آخر ٣٥ يوم
- استرجاع بدقة لحد الثواني
- بتحمي من فقد أو فساد البيانات بسبب أخطاء بشرية أو تطبيقية
- استرجاع سريع برضه بيحقق RTO قصير (زي ساعة)
- مدفوعة وأرخص من النسخ الاحتياطية اليدوية الكتير
- مش بديل عن النسخ الاحتياطية طويلة الأمد

✅ Requester Pays feature

- اللي بيحمّل البيانات هو اللي بيدفع تكلفة التحميل والطلبات.
- صاحب الـ bucket بيدفع التخزين بس.
- لازم الـ requester يحدد إنه هيدفع.(request-payer)

✅ Read Replica

هي نسخة طبق الأصل من قاعدة البيانات بتتحدث أوتوماتيك من الـ **Primary DB**، لكنها **للقراءة فقط** مش للكتابة

- تقلل الضغط على القاعدة الأساسية.
- تستخدمها للاستعلامات والتقارير الثقيلة.
- تتزامن مع القاعدة الأساسية باستمرار.

✅ 31. Savings Plans vs Reserved vs Spot (طرق الدفع)

النوع	السعر	الاستخدام	المرونة
On-Demand	غالي	مرن	عالي جدًا
Reserved	أرخص	ثابت لفترة (1-3 سنين)	قليل
Spot Instances	أرخص جدًا	لو شغلك مؤقت	ممكن يتقفل فجأة
Savings Plan	أرخص من On-Demand	مرن	بتلتزم بعدد ساعات معين شهريًا

✅مقارنات AWS بين الخدمات القريبة من بعض (جدول + أمثلة)

🔴الطبقة الأولى – مقارنات لازم تتحفظ ومتكررة

EC2 vs Lambda ◆

المقارنة	EC2 (Elastic Compute Cloud)	Lambda (Serverless)
نوع التشغيل	سيرفر دايم شغال	كود يتنفذ عند الطلب فقط
الإدارة	انت تدير السيرفر (OS, Patch, إلخ)	AWS تدير كل حاجة
الدفع	بتدفع بالساعات أو بالثواني	بتدفع لكل تنفيذ (بالـ ms)
حالات الاستخدام	مواقع تقيلة، قواعد بيانات، API	Tasks صغيرة، Serverless API، Events
المرونة	لازم تتابع وتظبط السيرفرات	أوتوماتيك 100%

S3 vs EBS vs EFS ◆

المقارنة	S3	EBS	EFS
النوع	Object Storage	Block Storage	File Storage
مربوط بـ؟	خدمة مستقلة	مربوط بـ EC2 فقط	ممكن توصله لأكتر من EC2
الاستخدام	صور، فيديوهات، نسخ احتياطي	هارد ديسك لـ EC2	مشاركة ملفات بين سيرفرات
الأداء	أسرع في القراءة الكبيرة	أسرع في القراءة/الكتابة الفورية	جيد للملفات المشتركة

RDS vs DynamoDB ◆

المقارنة	RDS (Relational DB)	DynamoDB (NoSQL DB)
نوع البيانات	جداول مترابطة – Structured	جداول بسيطة – Key/Value
اللغة	SQL	NoSQL (API-based)
الأداء	جيد – يعتمد على النوع	سريع جدًا
المرونة	لازم تحدد نوع DB ومساحة	Scalable أوتوماتيك
الاستخدام	مشاريع ERP، تطبيقات تقليدية	تطبيقات موبايل، Realtime، IoT

SQS vs SNS ◆

المقارنة	SQS (Simple Queue Service)	SNS (Simple Notification Service)
نوع الخدمة	Queue (صف انتظار)	Pub/Sub (إشعارات)
طريقة العمل	المستلم يسحب الرسائل	ترسل لكل المشتركين مرة واحدة
مثال	نظام طلبات – كل طلب يتنفذ لوحده	تنبيه لكل العملاء برسالة واحدة

Load Balancer vs Route 53 🔷

المقارنة	Elastic Load Balancer (ELB)	Route 53 (DNS)
الشغل بتاعه؟	توزيع الترافيك بين السيرفرات	توجيه الترافيك حسب اسم الدومين
نوع التوزيع	داخلي داخل Region	عالمي DNS Resolution
السيناريو المناسب	عندك أكتر من EC2	عندك أكتر من Region أو خدمة

CloudTrail vs CloudWatch 🔷

المقارنة	CloudTrail	CloudWatch
الوظيفة	يسجل كل العمليات اللي بتحصل	يراقب الأداء + Logs + Alarms
يراقب إيه؟	مين عمل إيه – API Calls	Usage – Errors – Metrics
يشتغل مع؟	كل AWS Services	EC2 – Lambda – RDS – وغيرهم

Security Group vs NACL 🔷

المقارنة	Security Group	NACL (Network ACL)
يطبق على؟	Instance (زي EC2 مثلًا)	كامل Subnet
الحالة الافتراضية	كل حاجة مقفولة	Incoming مقفول، Outgoing مفتوح
نوع القواعد	Stateful (يعرف الاتصال رايح/راجع)	Stateless
الأفضل في؟	أمان الخدمة نفسها	التحكم في الشبكة الأكبر

🔷 IAM Users vs Groups vs Roles vs Policies

العنصر	وظيفته	بيتستخدم في؟
IAM User	مستخدم حقيقي ليه Username/Password	دخول مباشر على AWS
Group	مجموعة مستخدمين	تسهّل إدارة الصلاحيات لمجموعة مع بعض
Role	هوية مؤقتة بتاخدها Service أو User	لما Lambda أو EC2 يحتاجوا صلاحيات مؤقتة
Policy	ملف JSON فيه صلاحيات	بيتطبّق على Users أو Roles أو Groups

> ✅ مثال:
> لو Lambda محتاجة توصل لـ S3 → تعمل Role وتديها صلاحية S3 → تربطها بـ Lambda.

🔍 الفرق بين NFS و Amazon EFS:

المقارنة	NFS (القديم)	Amazon EFS (Cloud version)
المكان	On-premises (في شبكة داخلية)	AWS Cloud
التحكم	إنت بتديره بنفسك	AWS بتديرهولك (Fully managed)
التوسع	ثابت – لازم تزود المساحة يدويًا	بيكبر تلقائي حسب الحاجة (Auto-scaling)
المرونة	بيشتغل على سيرفر واحد غالبًا	بيشتغل على أكتر من EC2 في أكتر من AZ
الحماية	مسؤوليتك	AWS بتوفرلك Encryption + IAM + Security
الأداء	بيعتمد على الشبكة بتاعتك	High throughput حسب نوع EFS (Standard/One Zone)

✅ من الاخر : لو بتستخدم AWS وعايز شيرد ستورج بين أكتر من — EC2 استخدم EFS
لو عندك شبكة محلية وجواها سيرفرات — استخدم NFS

🟡 الطبقة التانية – مفيدة جدًا للفهم والمراجعة

🔷 CloudFront vs S3 Static Hosting

المقارنة	CloudFront	S3 Static Website Hosting
السرعة	أعلى جدًا – CDN عالمي	عادي – من Region واحدة فقط
الحماية	أكتر – يدعم WAF و SSL	بسيط – أقل في الحماية
التكلفة	أغلى شوية	أرخص
المناسب لمين؟	مواقع فيها زوار من بلاد مختلفة	مواقع داخلية أو صغيرة

CloudFront vs Global Accelerator 🔷

المقارنة	CloudFront (CDN)	Global Accelerator
شغلها إيه؟	توصيل ملفات ثابتة بسرعة	تحسين الاتصال بالتطبيقات بالكامل
يشتغل مع؟	HTML – صور – مواقع – S3	Load Balancer – EC2 – ALB
البروتوكولات	HTTP / HTTPS	TCP / UDP
أفضل في؟	Static Content	تحسين الأداء العالمي

Auto Scaling vs Elastic Load Balancer 🔷

المقارنة	Auto Scaling	Elastic Load Balancer (ELB)
الوظيفة	يزود أو يقلل عدد EC2 تلقائيًا	يوزع الترافيك على كل EC2
التريجر	Based on Metrics (CPU, Traffic)	كل Request يدخل يتوزع تلقائي
الاستخدام	مرونة تلقائية	أداء متوازن بين السيرفرات

VPC vs Subnet 🔷

المقارنة	VPC (Virtual Private Cloud)	Subnet
مستوى الشبكة	شبكة كاملة	جزء من الشبكة (Public أو Private)
التحكم	فيه Gateways وRouting	تحكم بالـ Access على مستوى صغير
الاستخدام	تبني الشبكة الخاصة بيك	تقسم الشبكة لخدمات مختلفة داخل VPC

Reserved vs On-Demand vs Spot vs Savings Plan 🔷

النوع	الوصف	أرخص؟	مناسب لإيه؟
On-Demand	تشتري وقت الاستخدام فقط	❌	تجارب – شغل مؤقت
Reserved	تحجز لـ 1 أو 3 سنين مقدما	✅✅	سيرفر شغال طول الوقت
Spot	أسعار منخفضة – ممكن تتقفل فجأة	✅✅✅	Tasks مؤقتة مش مهمة أوي
Savings Plan	خصم مقابل التزام بوقت استخدام شهري	✅✅	شغل ثابت ومرن

🟢 الطبقة التالتة – توضيح أكتر وتوسيع للمعلومة

🔷 Kinesis vs SQS

المقارنة	Kinesis	SQS (Simple Queue)
النوع	Data Streaming (Realtime)	Queueing System
التخزين	يحتفظ بالبيانات لفترة قصيرة	يمسك الرسائل لحد ما تتسحب
الأداء	أسرع – بيانات كتير مرة واحدة	أبطأ – رسالة واحدة كل مرة
الاستخدام	تحليل لحظي – Logs – IoT	تنفيذ طلبات واحد ورا التاني

🔷 Elastic Beanstalk vs EC2

المقارنة	Elastic Beanstalk	EC2 فقط
مين بيدير البنية؟	AWS أوتوماتيك	إنت تدير كل حاجة
مناسب لمين؟	مطور عايز يركّز في الكود بس	مهندس بيحب يتحكم في كل حاجة
السيناريو	مشروع صغير/متوسط بسرعة	تحكم كامل – مشروع ضخم أو خاص جدًا

🔷 Security Group vs IAM Policy

المقارنة	Security Group	IAM Policy
يشتغل على إيه؟	يراقب الترافيك داخل الشبكة	يحدد مين يقدر يستخدم الخدمات
النوع	Network-level Security	Service-level Access
مثال	يمنع Port 22 عن EC2	يمنع مستخدم من حذف S3 Bucket

🔷 Kinesis vs Kafka (لو حبيت تعرف برّه AWS)

المقارنة	Kinesis (AWS)	Apache Kafka
الخدمة	Managed – AWS تديرها	لازم تديرها بنفسك
الأداء	جيد جدًا	أعلى أداء وأكثر تحكم
سهولة الاستخدام	أسهل وأسلس	معقدة شوية

🔷 SNS vs EventBridge

المقارنة	SNS (Simple Notification Service)	EventBridge (سابقًا CloudWatch Events)
نوع الاتصال	Pub/Sub بسيط	Event-driven Architecture متطور
مصدر الرسائل	Services – Users	Services – Custom Events – External SaaS
التوصيل	لكل المشتركين	توصيل مخصص حسب Rules

🔷 CloudWatch Logs vs CloudTrail Logs

المقارنة	CloudWatch Logs	CloudTrail Logs
يرصد إيه؟	أداء السيرفر – التطبيق – Lambda	كل API Calls – مين عمل إيه
المصدر	Logs من الخدمات	سجلات النظام نفسه
الاستخدام	ترصد أخطاء التطبيقات	تحقق من العمليات اللي اتعملت

🔷 Athena & Glue & QuickSight

الميزة	QuickSight	Glue	Athena
نوع الخدمة	Visualization	تجهيز بيانات / ETL	استعلام بيانات / Querying
بيشتغل على إيه؟	RDS, S3, Athena, Redshift	S3, RDS, JDBC	S3 (مع Glue Tables)
بيطلع Dashboards؟	✅ أه	❌ لأ	❌ لأ
سهل في استخدام الواجهات؟	✅ واجهة رسومية	❌ كله Configs و Jobs	❌ كله SQL
مناسب للتحليل التفاعلي؟	✅	❌	❌
مناسب للإدارة والمستخدمين؟	✅ (Users & Groups)	❌	❌

💡 الخلاصة:

- لو عايز **تحليل بصري (Dashboards)** → استخدم **QuickSight**
- لو عايز **تحضير البيانات** → استخدم **Glue**
- لو عايز **تشغل SQL على داتا في S3** → استخدم **Athena**

شوية نوتس يساعدو في الامتحان و حل الاسئله :

🧠 لو شفت الجملة دي في الامتحان... تفكر فورًا في:

الجملة في السؤال	الحل المتوقع أو الخدمة المناسبة
"The system must continue working if one AZ fails"	Use Multi-AZ, Load Balancer, RDS Multi-AZ
"Users complain about slow website from abroad"	Use CloudFront + Route 53 + S3 Static Site
"Need to isolate environments for dev/test/prod"	Use AWS Organizations, SCPs, and separate accounts
"Temporary credentials for EC2 to access S3"	Use IAM Role assigned to EC2
"Auto update infrastructure with code"	Use CloudFormation / CDK
"Limit cost overuse"	Budgets / Cost Explorer / Billing Alarms
"Encrypt data at rest and in transit"	Use KMS + HTTPS/SSL
"Connect on-prem to AWS"	VPN or Direct Connect
"Track configuration changes"	AWS Config

🎯 أهم Use Cases تحطها في دماغك:

- Lambda + API Gateway → REST APIs من غير سيرفر
- CloudFront + S3 → Web Hosting سريع وآمن
- EC2 + ALB + Auto Scaling → Web App بـ Load Balancing
- RDS Multi-AZ + Read Replica → High Availability + Performance
- VPC Peering / Transit Gateway → ربط VPCs ببعض
- S3 Lifecycle Rules → نقل البيانات من Standard لـ Glacier تلقائيًا
- CloudTrail + CloudWatch → Logging + Monitoring
- IAM Policy + SCP + MFA → Access Control

💡 أهم الكلمات المفتاحية في الأسئلة ومعناها الحقيقي:

الكلمة المفتاحية	معناها فعلياً تختار إيه أو تفكر في إيه؟
High availability	Use multiple AZs, Load Balancer, Auto Scaling
Scalable / Scale automatically	Auto Scaling Group, DynamoDB (On-Demand), Lambda
Decoupled Architecture	SQS – SNS – EventBridge
Cost-effective / Cheapest	Spot Instances – S3 Glacier – On-Demand Lambda
Fault tolerant	Multi-AZ Deployment / Load Balancer
Durable storage	S3 Standard, S3 One Zone-IA, EBS snapshots
Low latency	CloudFront – Global Accelerator – Edge Locations
Data analytics	Athena – Redshift – QuickSight
Real-time streaming	Kinesis Data Streams / Firehose
Serverless	Lambda – DynamoDB – API Gateway – S3 – Step Functions
Stateless / Ephemeral compute	Lambda – Fargate – Spot EC2
Long-term archival	S3 Glacier – Glacier Deep Archive
Temporary storage	Instance Store – /tmp on Lambda
Compliance / Audit Logs	CloudTrail – Config – CloudWatch Logs
Secure access to AWS services	IAM Roles – IAM Policies – KMS – SCP
Secure user access	IAM Users – MFA – Cognito
Web Application Security	WAF – Shield – CloudFront
Hybrid architecture	VPN – Direct Connect – Storage Gateway
Data Migration	Snowball – DMS – SCP – S3 Transfer Acceleration
Web hosting	S3 Static Website – Route 53 – CloudFront – ACM
Resilient Architecture	Multi-AZ – Load Balancer – ASG – Retry Logic
Configuration drift detection	AWS Config
Infrastructure as Code	CloudFormation – CDK
Monitoring	CloudWatch – Logs – Metrics – Alarms
Centralized access management	IAM Identity Center (SSO سابقًا) – Organizations – SCP
Temporary credentials	STS – IAM Role – AssumeRole