AWS Certified AI Practitioner

~ Stephane Maarek

(PART - 3)

AWS Security Services

- IAM (Identity & Access Management):

↳ Root account created by default.

↳ Create one user per one person and assign them to groups.

↳ Groups only contain users not other groups.

↳ Users/groups can be assigned JSON documents called policies which define permissions.

↳ Use least previlige principle.

- Consists of
  - **Version:** policy language version, always include "2012-10-17"
  - **Id:** an identifier for the policy (optional)
  - **Statement:** one or more individual statements (required)
- Statements consists of
  - **Sid:** an identifier for the statement (optional)
  - **Effect:** whether the statement allows or denies access (Allow, Deny)
  - **Principal:** account/user/role to which this policy applied to
  - **Action:** list of actions this policy allows or denies
  - **Resource:** list of resources to which the actions applied to
  - **Condition:** conditions for when this policy is in effect (optional)

```
{
    "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/*"]
        }
    ]
}
```

↳ We will assign permissions to AWS Services with IAM Roles to act on our behalf.

- EC2 (Elastic Compute Cloud):

↳ Infrastructure as a Service

↳ It mainly consists of EC2, EBS, ELB and ASG.

↳ Choose OS, CPU, RAM, storage, n/w card, firewall and bootstrap script (EC2 UserData).

- AWS Lambda:

↳ These are the virtual functions which have short executions.

↳ They are run on-demand and can be scaled automatically.

↳ Pay per request and compute time.

↳ It is integrated with the whole AWS suite of services.

↳ They are event-driven which means functions are invoked by AWS when needed.

↳ They're integrated with many programming languages & monitored using AWS CloudWatch.

- Amazon Macie: It is a fully managed data security and data privacy service that uses ml and pattern matching to discover & protect your sensitive data in AWS. It helps identify and alert you to sensitive data, such as personally identifiable information (PII).

- AWS Config:

↳ helps with auditing & recording compliance of your AWS resources.

↳ helps record configurations and changes over time.

↳ then store the configuration data into S3 and receive alerts for any changes.

↳ It is a per-region service.

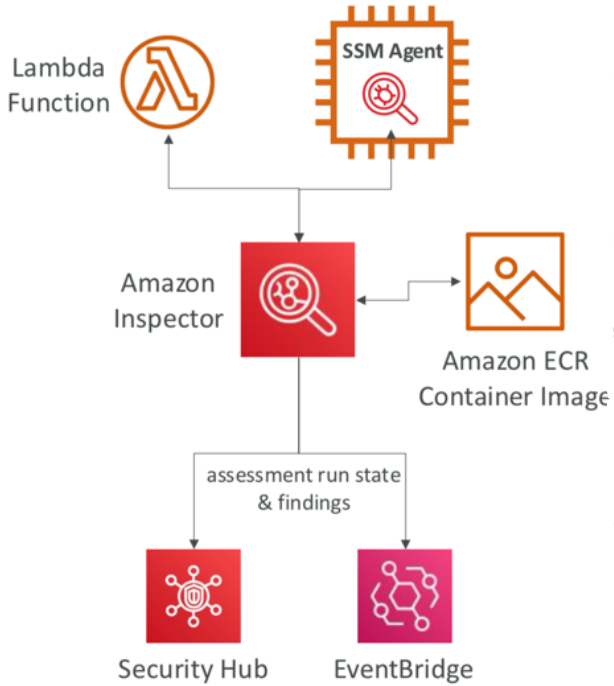
- Amazon Inspector:

↳ Automated security assessments

↳ It checks the EC2 instances against the unintended n/w accessibility and running OS for known vulnerabilities.

↳ Access container images as they're pushed to ECR.

↳ for lambda functions, it identifies code vulnerabilities and package dependencies as they're deployed.



↳ Reporting and integration with AWS Security Hub & send finding to the Amazon Event Bridge.

↳ A risk score is associated with all vulnerabilities for prioritization.

- AWS Artifact: Portal that provides customers with on-demand access to AWS compliance documentation and AWS Agreements. (Both artifact reports and agreements).

- AWS Audit Manager:

↳ It access risk and compliance of your AWS workloads.

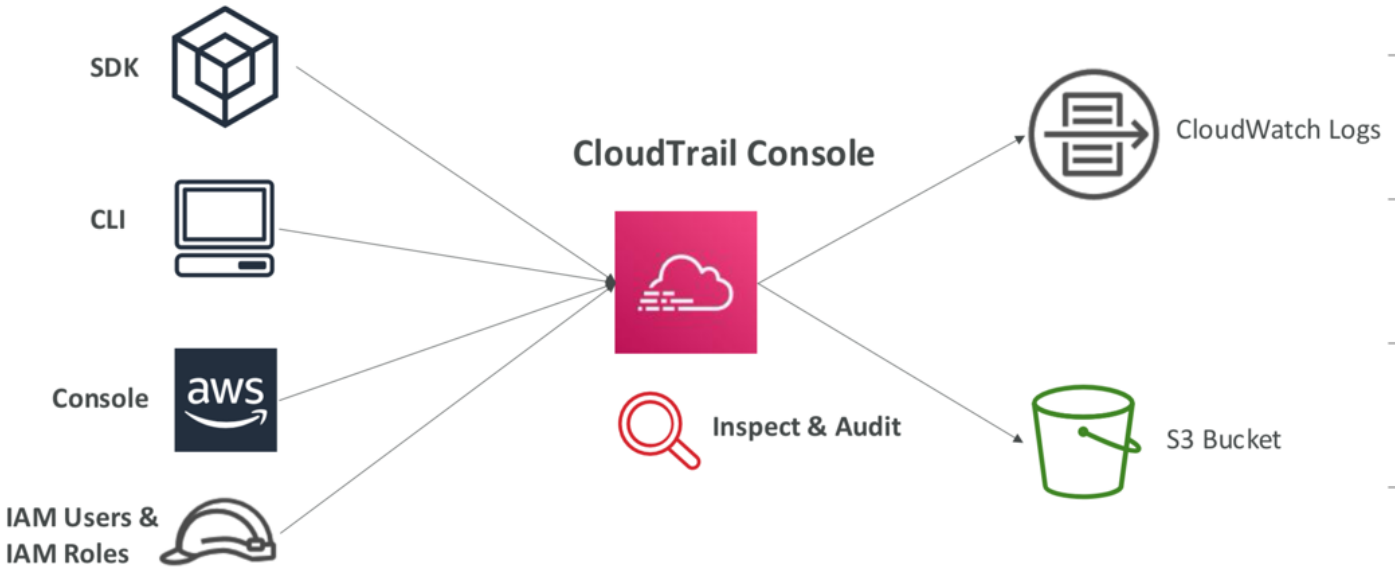
↳ Continuously audit AWS service usage and prepare audits.

↳ It generates reports of compliance alongside evidence folders.

- AWS CloudTrail:

↳ It provides governance, compliance & audit for our own account.

↳ Get a history of events/API calls made within your AWS account.



- AWS Trusted Advisor:

↳ It is a high level AWS account assessment that provides recommendations in 6 categories.

1. Cost Optimization
2. Performance
3. Security
4. Fault Tolerance
5. Service limits
6. Operational Excellence

- VPC (Virtual Private Cloud): It is a private n/w to deploy your resources.

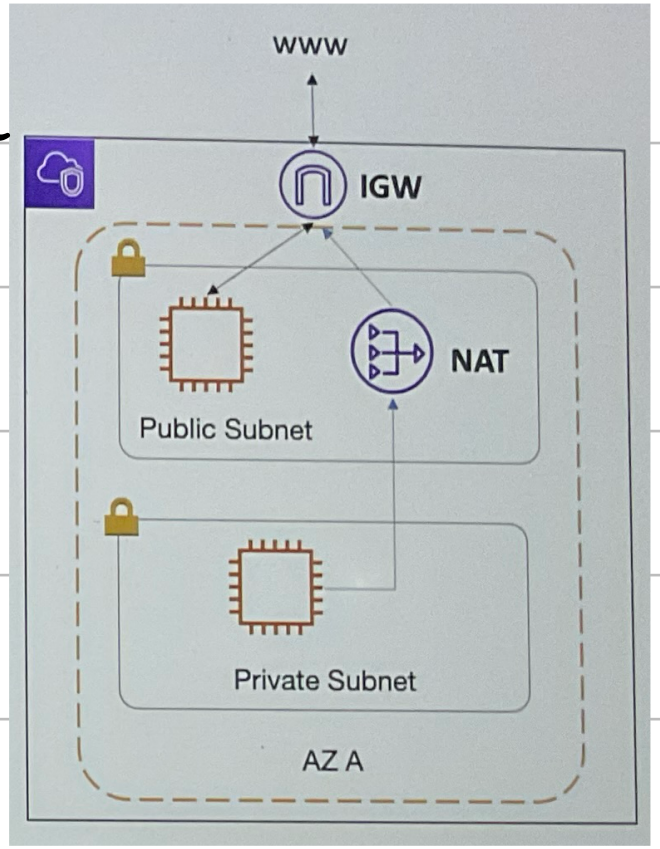
- Subnets: allow you to partition your n/w inside your VPC.

- Public Subnet: It is a subnet that is accessible from the internet.

- Private Subnet: Subnet that is not accessible in the internet.

- Internet Gateways: helps your VPC instances connect with the internet. The public subnets have a route to the internet gateway.

- NAT Gateways: It allow the instances in your Private Subnets to access the internet while remaining private.

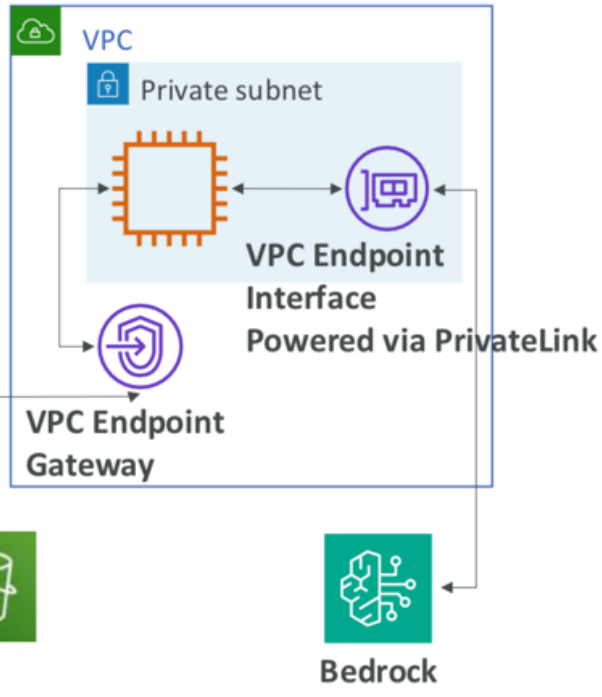


- VPC EndPoints and PrivateLink:

↳ AWS services are by default accessed over public internet

↳ Since the private subnets may not have internet access, we will use the VPC EndPoints.

↳ Using these EndPoints we can access AWS services privately without going over the public internet and this is powered by AWS PrivateLink.



↳ The S3 Gateway Endpoint is used to access Amazon S3 privately.

- **IAM Users –** mapped to a physical user, has a password for AWS Console
- **IAM Groups –** contains users only
- **IAM Policies –** JSON document that outlines permissions for users or groups
- **IAM Roles –** for EC2 instances or AWS services
- **EC2 Instance –** AMI (OS) + Instance Size (CPU + RAM) + Storage + security groups + EC2 User Data
- **AWS Lambda –** serverless, Function as a Service, seamless scaling
- **VPC Endpoint powered by AWS PrivateLink –** provide private access to AWS Services within VPC
- **S3 Gateway Endpoint:** access Amazon S3 privately

- **Macie –** find sensitive data (ex: PII data) in Amazon S3 buckets
- **Config –** track config changes and compliance against rules
- **Inspector –** find software vulnerabilities in EC2, ECR Images, and Lambda functions
- **CloudTrail –** track API calls made by users within account
- **Artifact –** get access to compliance reports such as PCI, ISO, etc…
- **Trusted Advisor –** to get insights, Support Plan adapted to your needs

AWS Services for Bedrock

- **IAM with Bedrock**
  - Implement identity verification and resource-level access control
  - Define roles and permissions to access Bedrock resources (e.g., data scientists
- **GuardRails for Bedrock**
  - Restrict specific topics in a GenAI application
  - Filter harmful content
  - Ensure compliance with safety policies by analyzing user inputs
- **CloudTrail with Bedrock:** Analyze API calls made to Amazon Bedrock
- **Config with Bedrock:** look at configuration changes within Bedrock
- **PrivateLink with Bedrock:** keep all API calls to Bedrock within the private VPC

Exam

Domain 1 : fundamentals of AI and ML (20%)

Domain 2 : fundamentals of Generative AI (24%)

Domain 3: Applications of foundation Models (28%)

Domain 4: Guidelines for Responsible AI (14%)

Domain 5: Security, Compliance, and Governance of AI solutions (14%)