Sprint 1 Presentation

Week 1-3

Introduction

Week 1

- Familiarise with AWS
- Familiarise with cloud
- Familiarise with AWS Services

Week 2

- Familiarise with Prowler, DJ Hammer & Scout Suite
- Research on other audit tools

Week 3

- Trying out AWS EC2 and Prowler

Cloud-Based Applications

- Fully deployed in the cloud & all parts of the application run in the cloud
- Have either been created in the cloud or have been migrated from an existing infrastructure to take advantage of the benefits of cloud computing
- Can be built on low-level infrastructure pieces
- Can use higher level services that provide abstraction from the management, architecting & scaling requirements of core infrastructure.

Main Cloud Computing Models

1. Infrastructure as a Service (IaaS)
    - Contains the basic building blocks for cloud IT
    - Typically provide access to networking features, computers (virtual or on dedicated hardware) & data storage space
    - Highest level of flexibility & management control over your IT resources
2. Platform as a Service (PaaS)
    - Remove the need for organisations to manage underlying infrastructure
    - Allows focus on deployment & management of applications
3. Software as a Service (SaaS)
    - Completed product that is run & managed by the service provider
    - Only need to think about how you will use that particular piece of software

EC2

- Amazon EC2 provides scalable computing capacity in the AWS cloud.
- Leveraging it enables organizations to develop and deploy applications faster, without needing to invest in hardware upfront.
- Users can launch virtual servers, configure security and networking, and manage cookies from an intuitive dashboard.

Use Cases

- Run cloud-native and enterprise applications
- Scale for High Performance Computing (HPC) applications
- Develop for Apple platforms
- Train and deploy ML applications

Why is AWS EC2 Important?

1. You don’t require any hardware units
2. Easily scalable (up or down)
3. You only pay for what you use
4. You have complete control
5. Highly secure
6. You can access your assets from anywhere in the world

Cloud Storage

- A cloud computing model that enables storing data & files on the internet through a cloud computing provider that you access either through the public internet or a dedicated private network connection.
- The provider securely stores, manages & maintains the storage servers, infrastructure & network to ensure you have access to the data when you need it at virtually unlimited scale, & with elastic capacity.
- With cloud storage you can:
    - Cost-effectively protect data in the cloud without sacrificing performance
    - Scale up your backup resources in minutes as data requirements change
    - Protect backups with a data center & network architecture built for security-sensitive organisations

Object Storage

- Data storage architecture for large stores of unstructured data
- Objects store data in the format it arrives in & makes it possible to customize metadata in way that make the data easier to access & analyse
- Objects kept in secure buckets that deliver virtually unlimited scalability Less costly to store large data volumes

File Storage

- Stores data in a hierarchical folder & file format
- A.k.a Network-Attached Storage (NAS) server with common file level protocols of Server Message Block (SMB) used in Windows instances & Network File System (NFS) found in Linux

Block Storage

- Enterprise applications like databases or enterprise resource planning (ERP) systems often require dedicated, low-latency storage for each host
- Analogous to direct-attached storage (DAS) or storage area network (SAN)
- Stores data in the form of blocks
    - Each block has its own unique identifier for quick storage & retrieval

Cloud Storage Use Cases

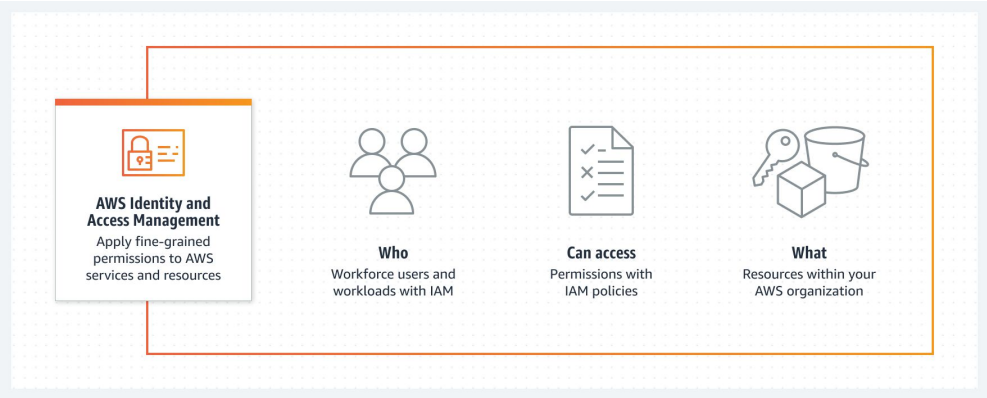
- Analytics & Data Lakes
  - Analytics demand large-scale, affordable, highly available & secure storage pools (i.e. data lakes)
  - Keep information in its native form
  - Cloud-based data lakes can sit at the center of multiple kinds of data warehousing & processing (inc. big data & analytical engines) to help you accomplish your next project in less time & with more targeted relevance
- Backup & Disaster Recovery
  - Critical for data protection & accessibility
  - Archival vaults can be created to help comply with legal or regulatory requirements
- Software test & Development
  - Often require separate, independent & duplicate storage environments to be built out, managed & decommissioned

Cloud Storage Use Cases

- Cloud Data Migration
  - Hybrid, edge & data movement services meet you where you are in the physical world to help ease your data transfer to the cloud
- Compliance
  - Designed to ensure that you can deploy & enforce comprehensive compliance controls on your data
  - Through a shared responsibility model, cloud vendors allow customers to manage risk effectively & efficiently in the IT environment
- Cloud-native Application Storage
  - Use technologies like containerisation & serverless to meet customer expectations in a fast-paced & flexible manner

AWS Identity & Access Management

- Can specify who or what can access services & resources in AWS
- Centrally manage fine-grained permissions
- Analyse access to refine permissions across AWS



Use Cases

1. Apply fine grained permissions & scale with attribute-based access control
2. Manage per-account access or scale access across AWS accounts & applications
3. Establish organisation-wide & preventive guardrails on AWS
4. Set, verify & right-size permissions toward least privilege

IAM Roles

- Used to grant temporary access to multiple identities (humans external to AWS accessing your services, IAM users or applications)
- Assume the role temporarily & any permissions policies attached to the role are by proxy applied to the identity assuming that role

Trust Policies VS Permission Policies

Trust Policy	Permission Policy
• Controls which identity can assume that role • Once a role is assumed by an identity, AWS issues it Temporary Security Credentials • Only works for a period of time • Once time has elapsed, the identity needs to re-authenticate & get new Temporary Security Credentials	• Defines the permissions that the role has which by proxy defines the permissions that the identity assuming that role will have

How IAM Policies Work

- Attached to identities (i.e. users, groups or roles)
- Attached to some AWS resources (resource based policies)
- JSON documents consisting of one or more statements that grant or deny access to AWS resources

Identity & Access Control

AWS offers you capabilities to define, enforce & manage user access policies across AWS services

These include:

1. AWS IAM
    - Define individual users with permissions across AWS resources AWS MFA for privileged accounts (inc. options for software & hardwarebased authenticators)
2. AWS Directory Service
    - Integrate & federate with corporate directories to reduce administrative overhead & improve end-user experience
3. AWS IAM Identity Center
    - Centrally manage workforce access to multiple AWS accounts & applications

Governance, Risk & Compliance

- A structured way to align IT with business goals while managing risks & meeting all industry & government regulations.
- Companies use GRC to achieve organisational goals reliably, remove uncertainty, & meet compliance requirements.
- Benefits:
    - Data-driven decision-making
    - Responsible operations
    - Improved cybersecurity

Prowler

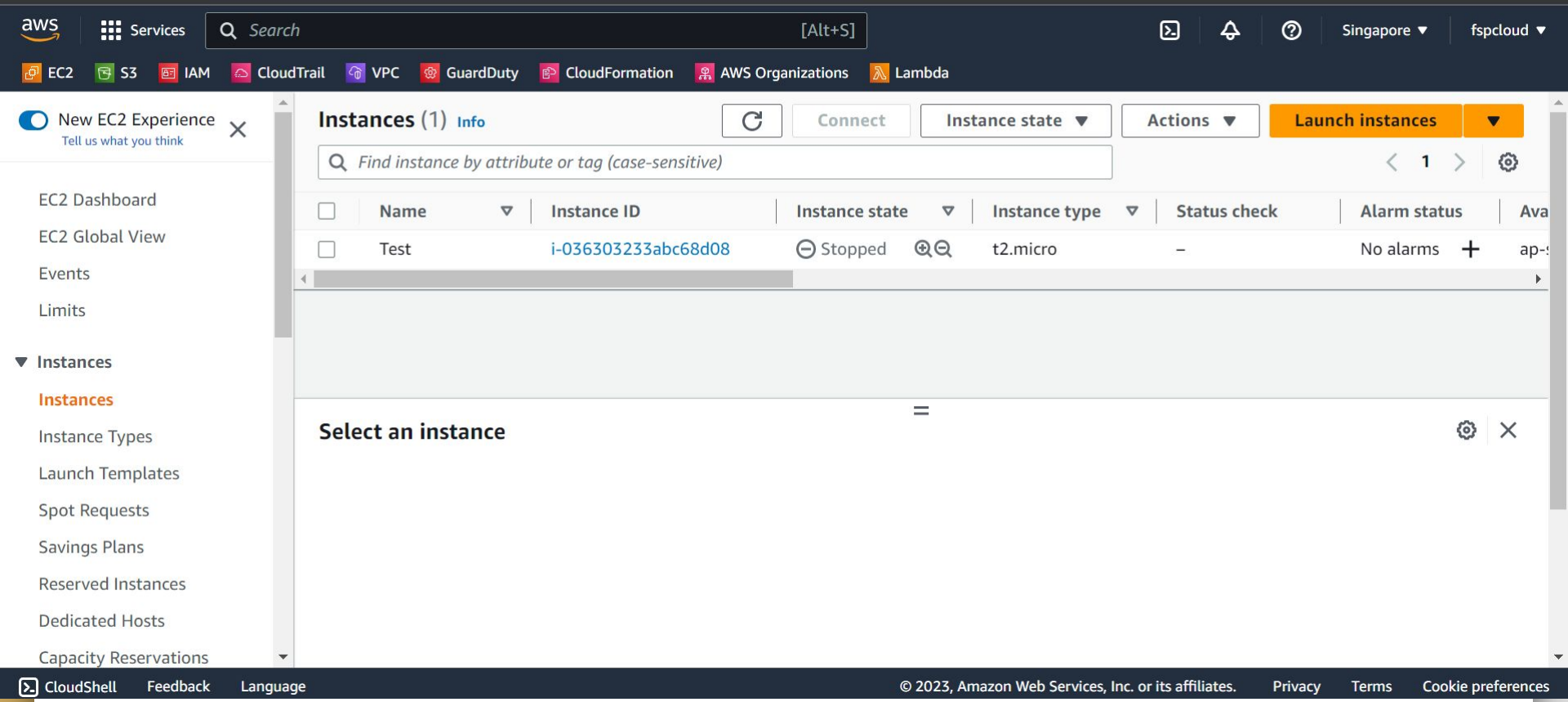
- Open Source Security Tool
- Works with AWS, Azure & Google Cloud security
- Used for best practices assessments, audits, incident response, continuous monitoring, hardening & forensics readiness
- Perform quick inventory check
    - Give console information about the number of each resource you have
    - In json/csv generated files, you will find information about what is the specific resource (region, aws service, resource type, resource id & ARN)

Scout Suite

- Enables security posture assessment of cloud environments
- Using the APIs exposed by cloud providers, Scout Suite gathers configuration data for manual inspection & highlights risk areas
- Presents a clear view of the attack surface automatically
- Provides a point-in-time security-oriented view of the cloud account it was run in
- Written in Python
    - 3.6
    - 3.7
    - 3.8

DJ Hammer

- A cloud security tool designed to keep your Amazon Web Services landscape safe
- It detects typical AWS services vulnerabilities on a regular basis and writes information about discovered vulnerabilities to DynamoDB tables.
- Dow Jones Hammer is written in Python, versions starting from 3.6 are supported;
- Identification lambdas are configured to use python3.6 runtime;
- Reporting and remediation engine runs on EC2 with the latest version of CentOS 7, using Python 3.6 installed from IUS Community Project.


aws
Services
Search
[Alt+S]
Singapore
fspcloud
EC2
S3
IAM
CloudTrail
VPC
GuardDuty
CloudFormation
AWS Organizations
Lambda
New EC2 Experience
Tell us what you think
EC2 Dashboard
EC2 Global View
Events
Limits
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Instances (1) Info
Connect
Instance state
Actions
Launch instances
Find instance by attribute or tag (case-sensitive)
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Test
i-036303233abc68d08
Stopped
t2.micro
–
No alarms
Select an instance
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Thank you !