TECH Startup

Career Simulation 3
Eddie Leach
IAM Users and Permissions, Create EC2, Create S3, Knowledge Check

As the Cloud Solution Architect for TECH-Start's infrastructure migration initiative, my primary goal was to design and implement a scalable, secure, and cost-effective cloud environment using AWS Free Tier services. This project involved provisioning core resources to support the company's diverse team, including EC2 instances for application hosting and S3 storage for data access and collaboration. I established IAM users with role-based access controls aligned to each team's responsibilities, ensuring that developers, data scientists, and marketing personnel have appropriate permissions. Through the creation of these services and configurations, I've laid the groundwork for a cloud-native environment that supports TECH-Start's continued growth while adhering to AWS best practices in security and cost management.

Task 1: Create Multiple User Accounts to define IAM concepts.

Users (4) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Search

User name	Path	Groups	Last activity	MFA	Password age
admin-user	/	0	4 hours ago	Passke...	4 hours
datascientist-user	/	1	-	-	22 hours
developer-user	/	1	-	-	22 hours
marketing-user	/	1	-	-	22 hours

Task 2: Set permissions on User Accounts.

Data Scientist Permissions

datascientist-user Info

Summary

ARN
arn:aws:iam::727646475213:user/datascientist-u

Created
April 24, 2025, 00:27 (UTC-05:00)

Permissions | Groups (1) | Tags (1) | Secu

Permissions policies (3)

Permissions are defined by policies attached to the u

Search

Policy name
AmazonEC2FullAccess
AmazonS3FullAccess
IAMUserChangePassword

Developer Permissions

developer-user Info

Summary

ARN
arn:aws:iam::727646475213:user/developer-

Created
April 24, 2025, 00:11 (UTC-05:00)

Permissions | Groups (1) | Tags (1) | S

Permissions policies (2)

Permissions are defined by policies attached to th

Search

Policy name
AmazonEC2FullAccess
IAMUserChangePassword

Marketing Permissions

marketing-user Info

Summary

ARN
arn:aws:iam::727646475213:user/marketing

Created
April 24, 2025, 00:31 (UTC-05:00)

Permissions | Groups (1) | Tags (1)

Permissions policies (2)

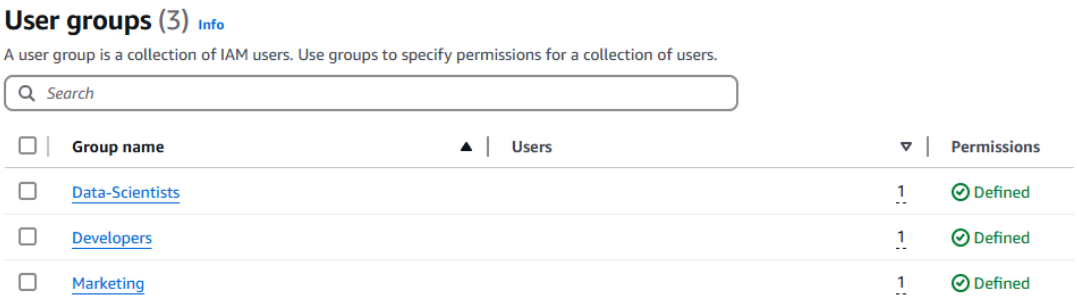
Permissions are defined by policies attached to t

Search

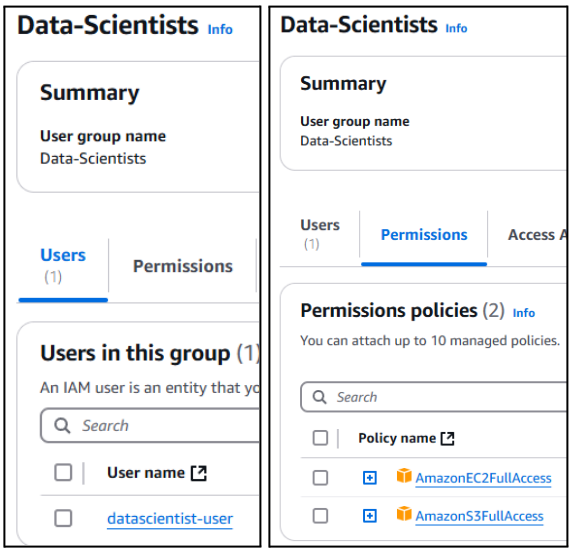
Policy name
AmazonS3ReadOnlyAccess
IAMUserChangePassword

Additional Task: The permissions were set by adding users to groups. This enables any new users added to the same group to inherit the same permissions. See the visual below.

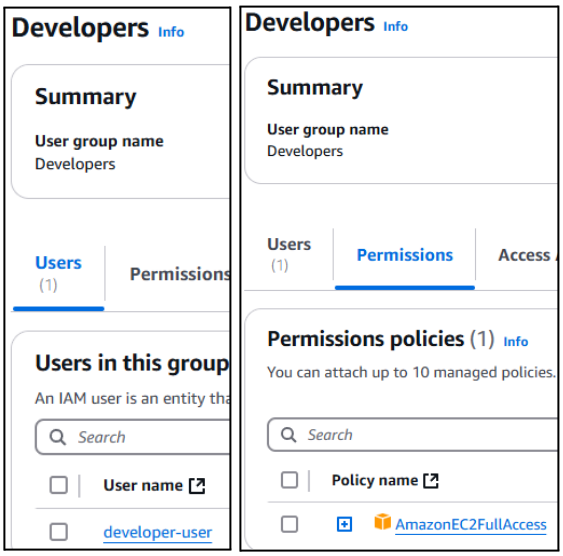
Groups



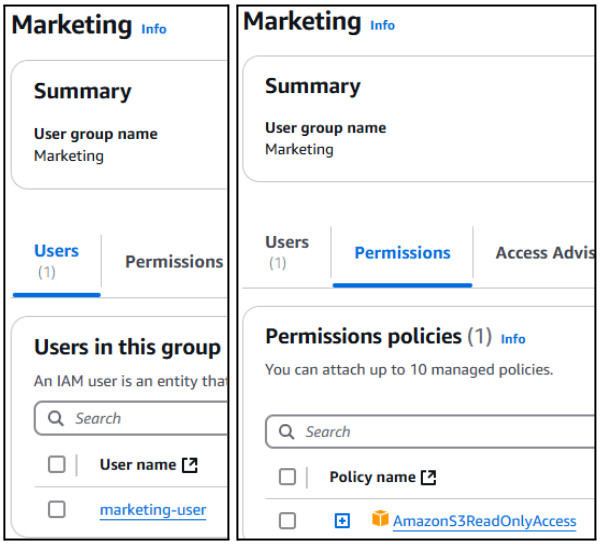
Data Scientist Group: Users/Permissions



Developer Group: Users/Permissions



Marketing Groups: Users/Permissions



Task 3: Create EC2 Instance

EC2 > Instances

EC2
- Dashboard
- EC2 Global View
- Events
- Instances

Instances (1) Info

Last updated 1 minute ago | Connect | Instance state | Actions | Launch instances

Find Instance by attribute or tag (case-sensitive) | All states

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
techstart-web...	i-0205742d8e6f8335b	Running	t2.micro	2/2 checks passed	View alarms +	us-east-2a	ec2-18-225-92-103.us-...	18.225.92.103	–

Instance summary for i-0205742d8e6f8335b (techstart-web-app) Info

Connect | Instance state | Actions

Updated 2 minutes ago

Instance ID
i-0205742d8e6f8335b

IPv6 address
–

Hostname type
IP name: ip-172-31-12-20.us-east-2.compute.internal

Answer private resource DNS name
IPv4 (A)

Auto-assigned IP address
18.225.92.103 [Public IP]

IAM Role
–

IMDSv2
Required

Operator
–

Public IPv4 address
18.225.92.103 | open address

Instance state
Running

Private IP DNS name (IPv4 only)
ip-172-31-12-20.us-east-2.compute.internal

Instance type
t2.micro

VPC ID
vpc-09ae54d0536031729

Subnet ID
subnet-0e65ac6fe3ff4cd5a

Instance ARN
arn:aws:ec2:us-east-2:727646475213:instance/i-0205742d8e6f8335b

Private IPv4 addresses
172.31.12.20

Public IPv4 DNS
ec2-18-225-92-103.us-east-2.compute.amazonaws.com | open address

Elastic IP addresses
–

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Auto Scaling Group name
–

Managed
false

Details | Status and alarms | Monitoring | Security | Networking | Storage | Tags

Instance details Info

AMI ID
ami-060a84cbcb5c14844

AMI name
al2023-ami-2023.7.20250414.0-kernel-6.1-x86_64

Stop protection
Disabled

Instance auto-recovery
Default

AMI Launch index
0

Credit specification
standard

Usage operation
RunInstances

Enclaves Support
–

Allow tags in instance metadata
Disabled

Monitoring
disabled

Allowed image
-

Launch time
Thu Apr 24 2025 00:44:11 GMT-0500 (Central Daylight Time) (about 23 hours)

Lifecycle
normal

Key pair assigned at launch
tech-start

Kernel ID
–

RAM disk ID
–

Boot mode
uefi-preferred

Use RBN as guest OS hostname
Disabled

Platform details
Linux/UNIX

Termination protection
Disabled

AMI location
amazon/al2023-ami-2023.7.20250414.0-kernel-6.1-x86_64

Stop-hibernate behavior
Disabled

State transition reason
–

State transition message
–

Owner
727646475213

Current instance boot mode
legacy-bios

Answer RBN DNS hostname IPv4
Enabled

Host and placement group Info

Host ID
–

Host resource group name
–

Virtualization type
hvm

Number of vCPUs
1

Affinity
–

Tenancy
default

Reservation
r-0281bc6abfdd351a2

Placement group
–

Placement group ID
–

Partition number
–

Capacity reservation Info

Capacity Reservation ID
–

Capacity Reservation setting
open

Task 4: Types of storage options and build / create S3 Storage.

Part 1: AWS Storage Types

1. Amazon S3 (Simple Storage Service)

- **Object storage** for files, backups, media, logs, etc.
- Durable, scalable, and great for static website hosting or storing data shared across teams.
- **Best for**:
  - Hosting static content (e.g., `index.html`)
  - Marketing team data (read-only access)
  - Data scientists uploading/downloading files

2. Amazon EBS (Elastic Block Store)

- **Block storage** attached to EC2 instances (like a hard drive).
- Persistent — survives even if the instance is stopped/rebooted.
- **Best for**:
  - Storing your EC2 web server's OS, installed software, or logs
  - Hosting databases on EC2

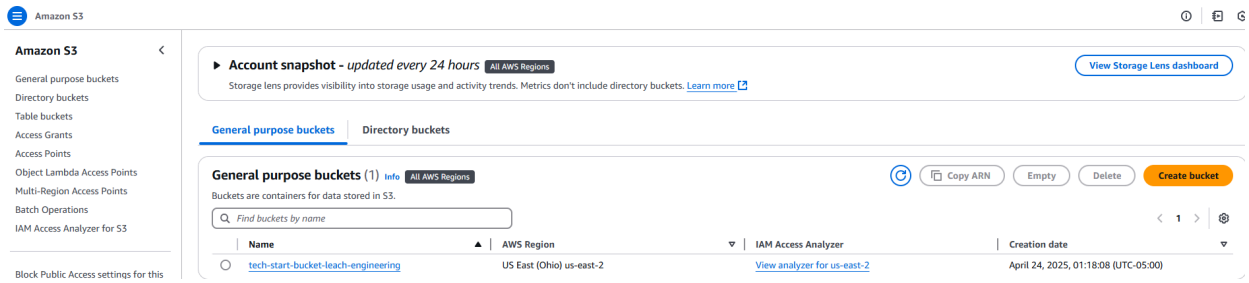
3. Amazon EFS (Elastic File System)

- **File-level storage** shared across multiple EC2 instances.
- Automatically scales, accessible via NFS.
- **Best for**:
  - Applications needing shared file systems (e.g., microservices, machine learning jobs)

Summary:

Team or Feature	Recommended Storage	Why
Web app (on EC2)	EBS	Used by the EC2 instance to store OS and web files
File storage (images, backups, reports)	S3	Scalable, easy to manage, and accessible across users
Shared storage across EC2 (optional)	EFS	Not needed for this project unless you're sharing files between multiple EC2s

Part 2: Build / Create S3 Storage



Knowledge Check:

1. Explain the importance of Availability Zones

- **Definition:**
  An **Availability Zone (AZ)** is a distinct, isolated data center within an AWS Region. Each region contains multiple AZs, which are designed to be physically separate but interconnected through low-latency, high-throughput networking.

- **Contribution to Reliability and Scalability:**
  Availability Zones allow AWS to provide fault tolerance and high availability by enabling workloads to be distributed across multiple physical locations. If one AZ experiences an outage, services in other AZs can continue operating. This setup also enables scalable architectures, where applications can elastically grow across zones to handle more demand.

- **Real-World Example:**
  A web application hosted in AWS can run EC2 instances in two or more Availability Zones with a load balancer distributing traffic. If one zone fails, the application remains accessible via the other zone(s), ensuring business continuity.

---

2. Differences and use cases of AWS CloudWatch vs. AWS CloudTrail

- **AWS CloudWatch**
  - Monitors performance metrics, logs, and alerts in near real-time.
  - **Use case:** You use CloudWatch to monitor CPU usage on an EC2 instance and trigger an alarm when it exceeds 80%, automatically launching a new instance to handle increased load.

- **AWS CloudTrail**
  - Logs API activity and user actions across your AWS account for governance, compliance, and auditing.
  - **Use case:** You use CloudTrail to track who deleted an S3 bucket or modified IAM permissions, allowing for audit and rollback investigation.

- **Using Both Together:**
  In a real-world application, you might use CloudWatch to monitor system health and auto-scale infrastructure, while using CloudTrail to audit all user activity and investigate incidents — giving both operational insight and security visibility.

---

3. Importance of a Well-Architected Framework

The AWS Well-Architected Framework is essential during a cloud migration because it ensures that critical elements like cost management, security, performance efficiency, and operational excellence are embedded into the design from the beginning, not added as afterthoughts.

- **Cost Optimization:**
  Migrating systems without proper cost planning can lead to overspending. The framework encourages evaluating resource usage early, ensuring that only necessary services are provisioned and that cost-saving features like reserved instances, storage lifecycle rules, and scaling policies are used effectively.

  Example: Migrating to AWS with S3 Intelligent-Tiering storage for infrequently accessed marketing files helps TECH-Start minimize storage costs automatically.

- **Security:**
  A rushed migration can leave vulnerabilities open. The framework emphasizes setting up secure access control, encryption, monitoring, and auditing from the start.

  Example: Implementing IAM roles instead of root access ensures that each TECH-Start team member has only the permissions they need post-migration.

- **Performance Efficiency:**
  Migration isn't just about copying servers over—it's about improving performance. The framework guides teams to choose modern architectures (like serverless or scalable services) rather than simply replicating old designs.

  Example: Instead of lifting and shifting a legacy app, TECH-Start could move to EC2 with Auto Scaling for dynamic traffic handling.

- **Operational Excellence:**
  The framework stresses building operational visibility early by automating deployments, monitoring system health, and preparing for failure recovery.

  Example: Setting up CloudWatch alarms during migration allows TECH-Start to immediately detect and respond to issues without manual checking.

- **Reliability:**
  Migrations must be planned for resilience. The framework ensures that workloads are spread across Availability Zones and that backup and disaster recovery are addressed early.

  Example: Hosting the TECH-Start website across two AZs with an Elastic Load Balancer ensures users won't experience downtime during an AZ outage.

Summary

Following the AWS Well-Architected Framework during migration reduces risk, controls costs, improves security, and sets a foundation for future scalability. It transforms a simple cloud lift into a strategic, resilient modernization for long-term success.