Module 2
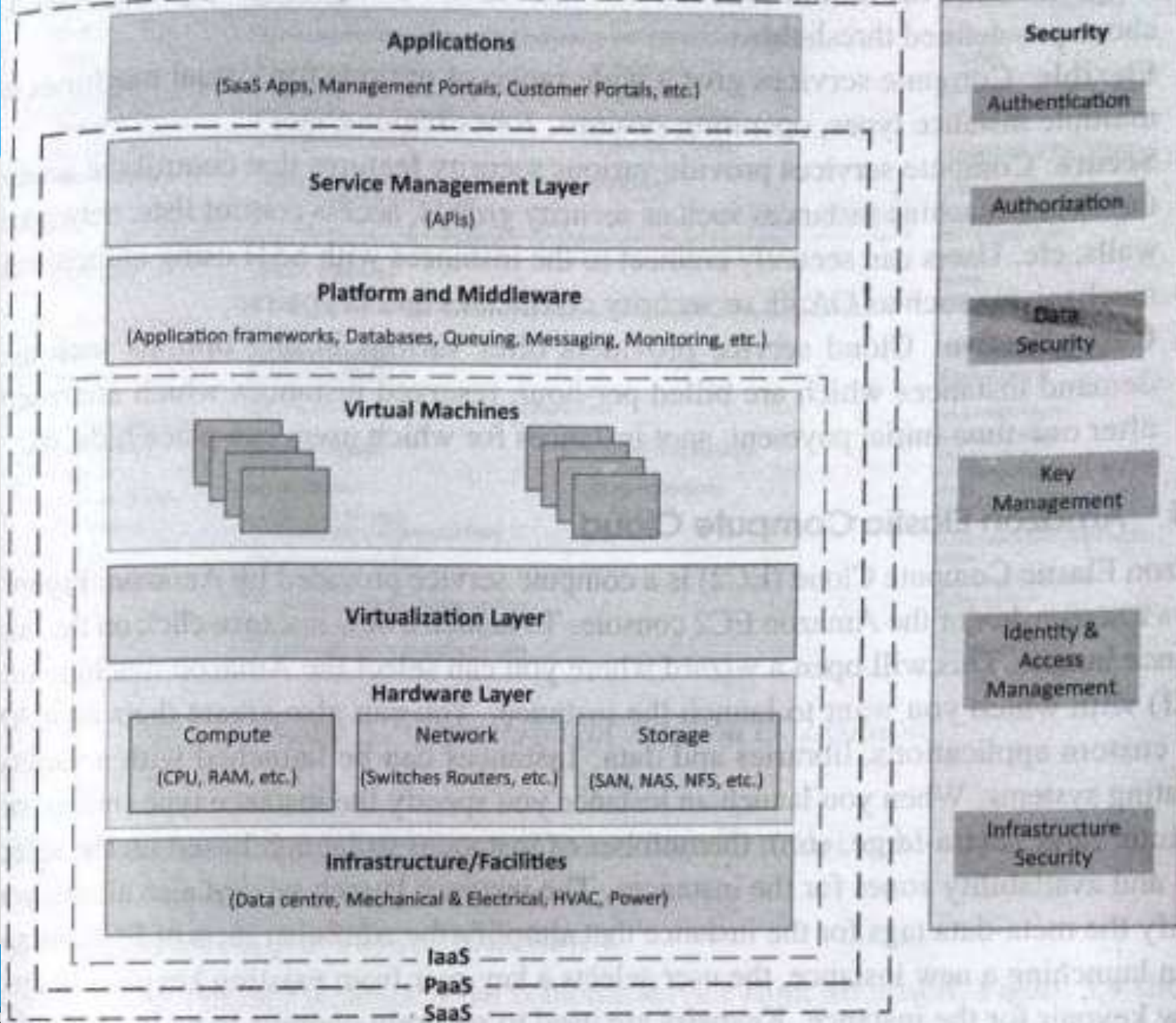# Cloud computing services
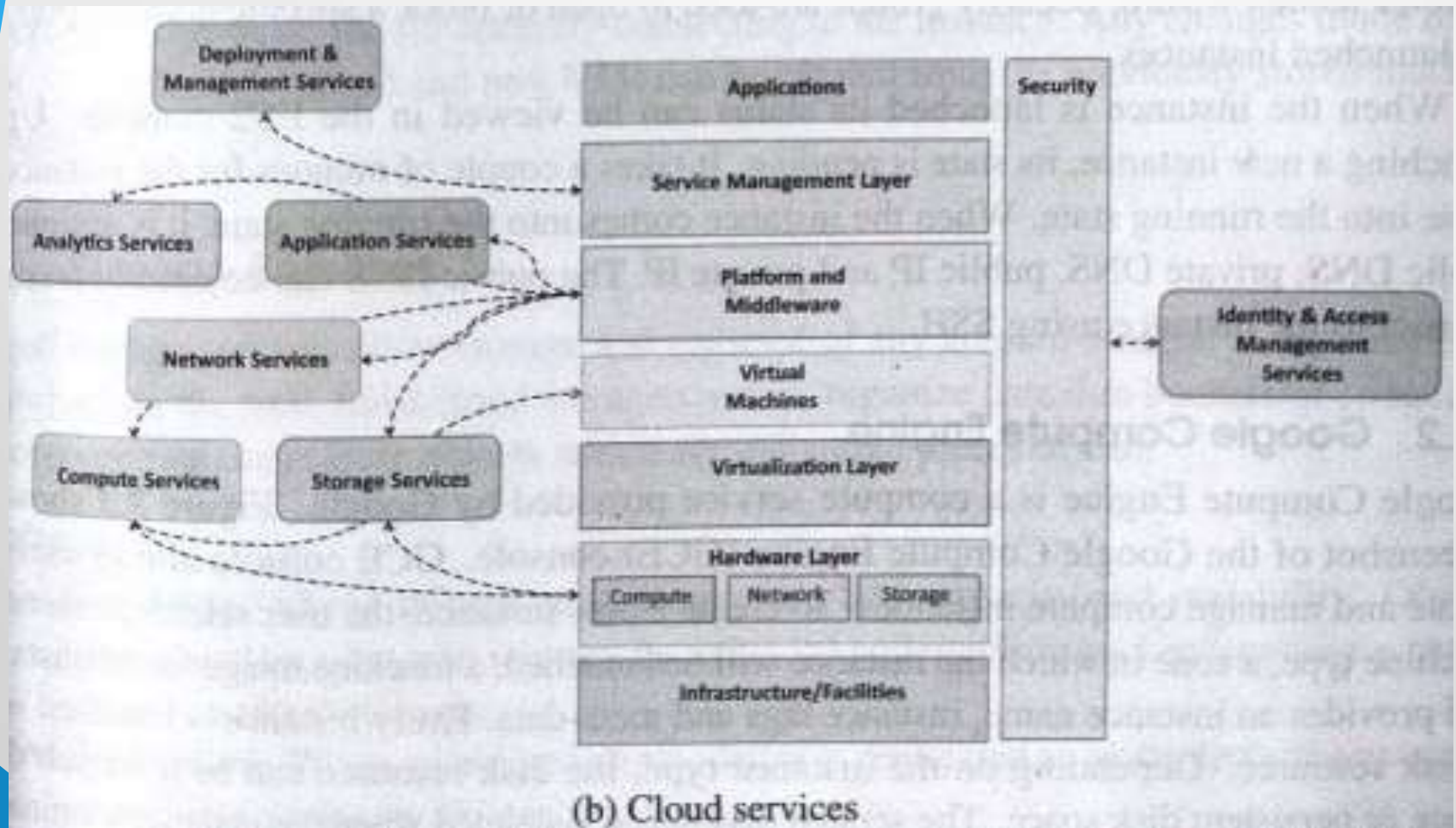
- Compute Services
- Storage Services
- Database Services
- Application Services

Applications	Security
(SaaS Apps, Management Portals, Customer Portals, etc.)	Authentication

Service Management Layer	Authorization
(APIs)	

Platform and Middleware	Data Security
(Application frameworks, Databases, Queuing, Messaging, Monitoring, etc.)	

Virtual Machines

Key Management

Virtualization Layer

Identity & Access Management

Hardware Layer

Compute	Network	Storage
(CPU, RAM, etc.)	(Switches Routers, etc.)	(SAN, NAS, NFS, etc.)

Infrastructure Security

Infrastructure/Facilities

(Data centre, Mechanical & Electrical, HVAC, Power)

IaaS

PaaS

SaaS

(a) Cloud reference model

Cloud Reference Model

- Infrastructure an facilities layer that includes physical infrastructure such as data centers, electrical & mechanical equipment etc.

- Hardware layer includes physical compute, network and storage hardware

- Virtualization layer partitions the physical hardware resources into multiple virtual resources that enabling pooling of resources

- Computing services provided in the form of Virtual Machines (VMs) along with the storage and network resources

- Platform and middleware layer provides standardized stack of services such as database service, queuing service, application framework and run-time environments etc.

- Service Management layer provides APIs for requesting, managing & monitoring cloud resources

- Application layer provides SaaS applications such as email, cloud storage application, management portals etc.

(b) Cloud services

Compute Services

- Provides dynamically scalable compute capacity in the cloud

- Can be provisioned on demand in the form of virtual machines

- Compute services can be accessed from web console that provides graphical user interface for provisioning, managing and monitoring these services

- Cloud provider also provides APIs for various programming languages (e.g java, python etc.)

Features:

i.   Scalable

ii.   Flexible

iii. Secure

iv. Cost effective

1. Amazon Elastic Compute cloud

- EC2 is a compute service provides by Amazon

- It provides secure and resizable compute capacity in cloud

- Provides Scaling (scaling up or down) as per demand

- It creates instances and launch them. Also mention type of instance e.g. micro, small, medium , large , so on…

- Integrated with other services

- Pay as per use

- It supports for different OSs

- Provides secure network by;

- By selecting key-pair, which is used to securely connect to instance after it launches.

- Security groups are associated with the instance

Figure 3.2: Screenshot of Amazon EC2 console

2. Google Compute Engine

- Compute service provided by google

- To create a new instance, the user selects an instance machine type, a zone in which the instance will be launched, a machine image for the instance and provides –instance name, tags and meta-data

- Every instance is launched with disk resource

- Types of disks:

i. Scratch disk space: This space is deleted when instance terminates

ii. Persistent disk space: it live beyond the life of an instant

- In and out traffic to instance is controlled by network option

- Traffic between instances in same network, over any port and any protocol ,it provides SSH connections

  For other connections, firewall rules are implemented

Figure 3.3: Screenshot of Google Compute Engine console

3. Windows Azure Virtual Machines

- Compute service from Microsoft

- To create a new instance

    - Select instance type

    - Select machine image

- For security: username and password can be defined or upload a certificate file for securely connecting to the instance.

- Any changes made to the VM are persistently stores

- New VMs can be created from previously stored machine images
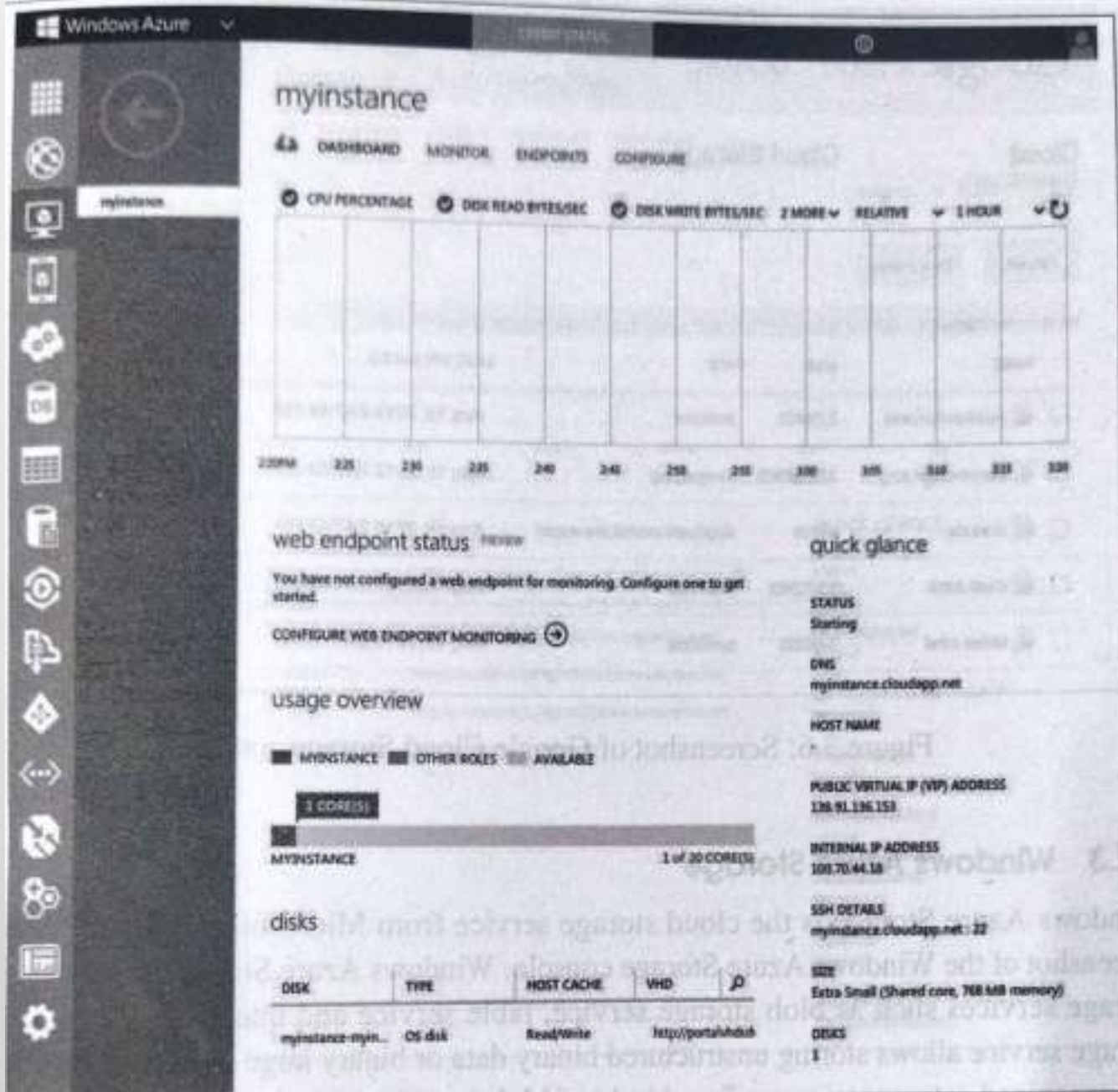
Figure 3.4: Screenshot of Windows Azure Virtual Machines console

Storage Services

- It allows storage and retrieval of any amount of data, at any time and from any location

- Cloud storage services organizes data into buckets or containers

Features:

i. Scalability & Capacity

ii. Replication

iii. Access policies: ACL (Access Control Lists), bucket/container level policies etc.

iv. Encryption: Encrypts all data stored in cloud storage

v. Consistency

1. Amazon Simple Storage Service (S3)

- Cloud based data storage infrastructure

- Highly reliable, scalable, fast, fully redundant, affordable storage infrastructure

- Data organized on S3 is in the form of buckets

- S3 console provides simple wizard for creating a new bucket and uploading files

- It support any kind of file storage

- While uploading following points can be mentioned:

- Redundancy

- Encryption options

- Access permissions

Amazon S3 ✕

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

▼ Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight 3

Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. Learn more ⤢

General configuration

Bucket name

| myawsbucket |

Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming ⤢

AWS Region

| Asia Pacific (Mumbai) ap-south-1   ▼ |

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

| **Choose bucket** |

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership
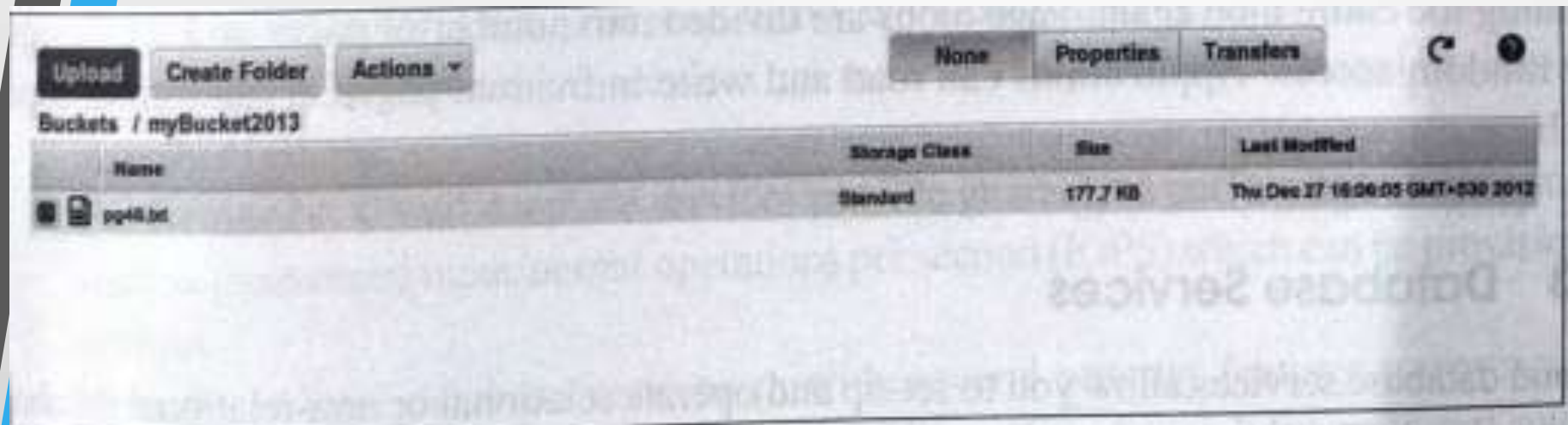
Activate Wi

Figure 3.5: Screenshot of Amazon S3 console

2. Google cloud storage

- Objects in GCS are organized using buckets

- ACLs are used to control access to objects and buckets

- ACLs can be configured to share objects and buckets with the entire world, Google group, Google hosted domain or specific Google account holders
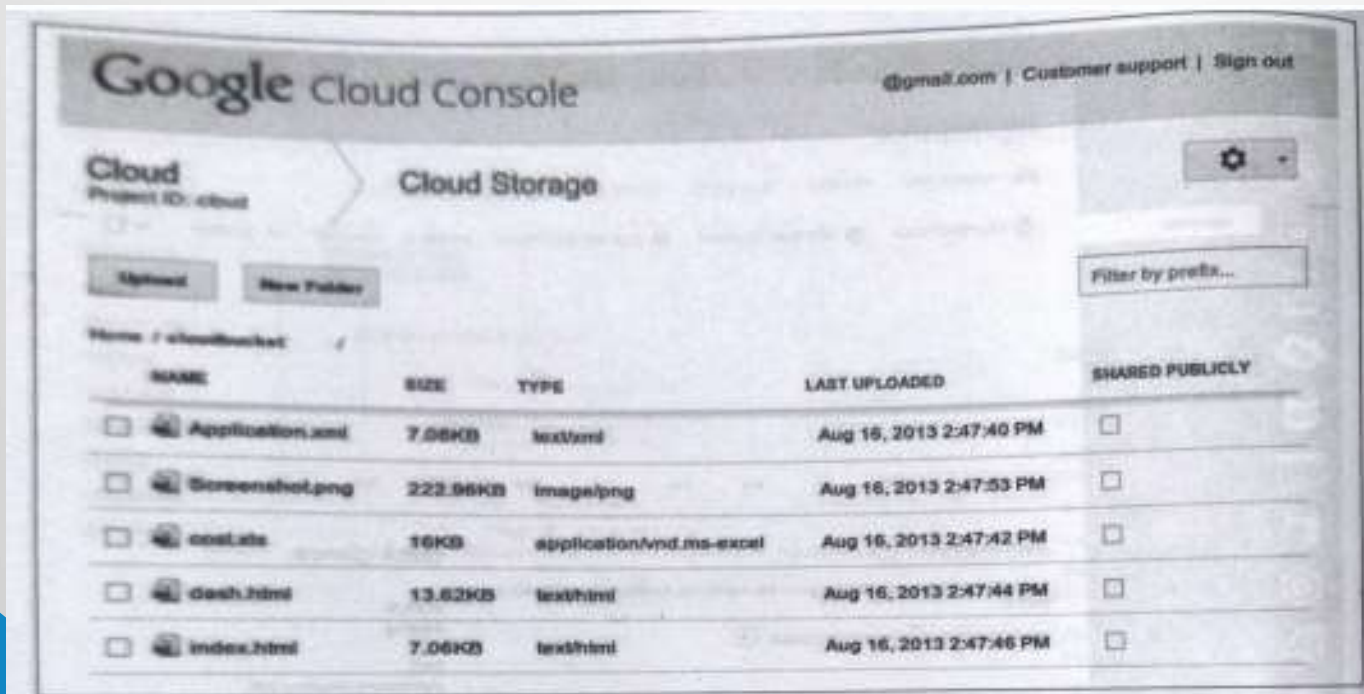
Figure 3.6: Screenshot of Google Cloud Storage console

3. Windows Azure storage

- Cloud storage service from Microsoft

- It provides following storage services:

i. Blob storage service: Large amount of unstructured data

ii. Table service: Non relational structure data

iii. Queue service: Stores large number of messages that can be accessed from anywhere via authenticated call using http/https
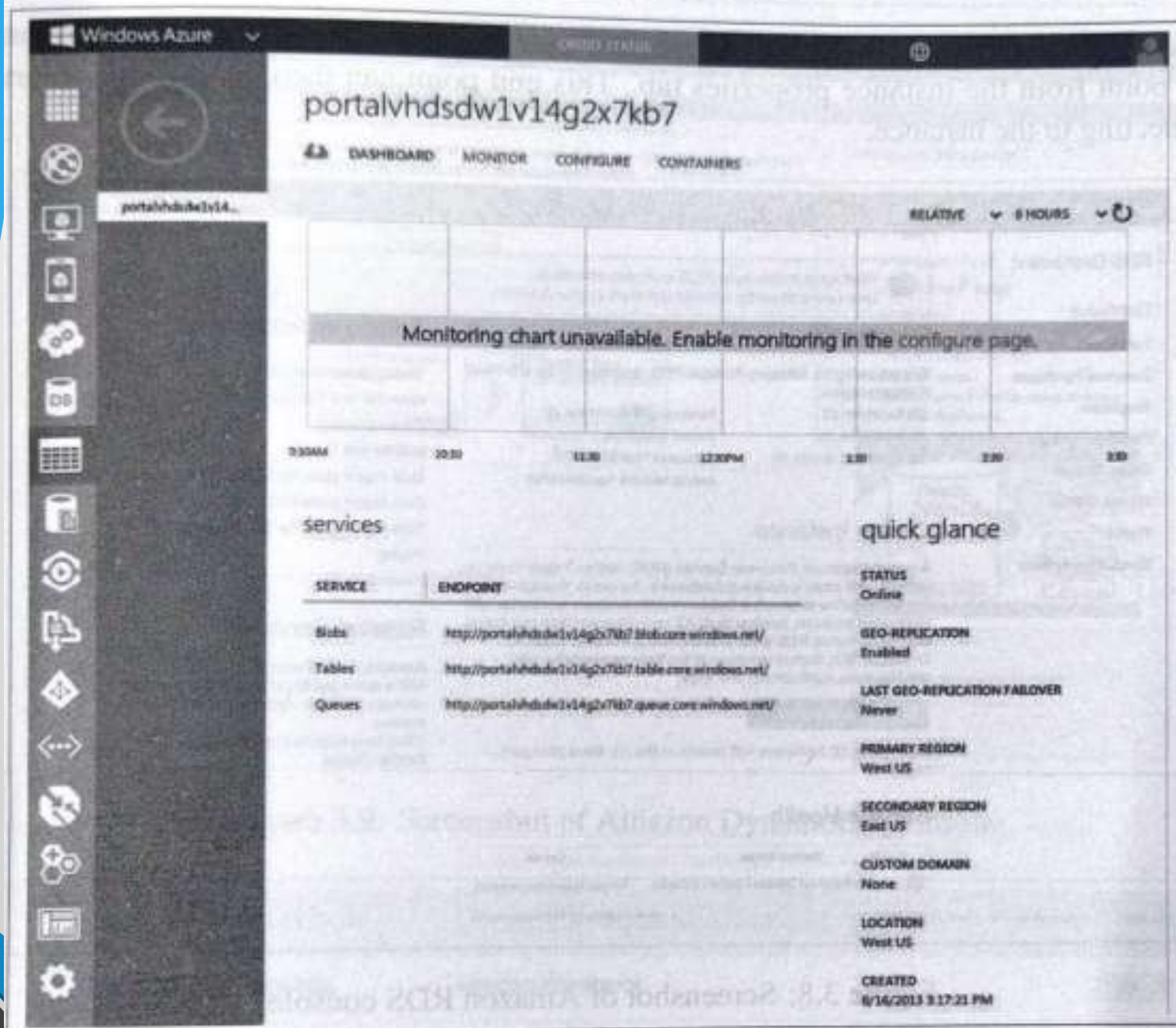
Figure 3.7: Screenshot of Windows Azure Storage console

Features of Amazon S3

1. Storage classes

- **Amazon S3 offers a range of storage classes designed for different use cases**

- For example, you can **store mission-critical production data** in S3 Standard for frequent access, save costs by storing infrequently accessed data in S3 Standard-IA

- **Archive data** at the lowest costs in S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval, and S3 Glacier Deep Archive

- You can store data with changing or unknown access patterns in S3 Intelligent-Tiering

2. **Storage management**

Amazon S3 has storage management features that you can use to manage costs, meet regulatory requirements, reduce latency, and save multiple distinct copies of your data for compliance requirements

- **S3 Lifecycle –** Configure a lifecycle policy to manage your objects and store them cost effectively throughout their lifecycle.

- **S3 Object Lock –** Prevent Amazon S3 objects from being deleted or overwritten for a fixed amount of time or indefinite

- **S3 Replication –** Replicate objects and their respective metadata and object tags to one or more destination buckets in the same or different AWS Regions

- **S3 Batch Operations –** Manage billions of objects at scale with a single S3 API request or a few clicks in the Amazon S3 console

3. Access management

Amazon S3 provides features for auditing and managing access to your buckets and objects. Default access –Private

- **S3 Block Public Access** –By default, Block Public Access settings are turned on at the account and bucket level.

- **AWS Identity and Access Management (IAM)** – Create IAM users for your AWS account to manage access to your Amazon S3 resources

- **Bucket policies** – Use IAM-based policy language to configure resource-based permissions for your S3 buckets and the objects in them

- **Amazon S3 access points** – Configure named network endpoints with dedicated access policies to manage data access at scale for shared datasets

- **Access control lists (ACLs)** – Grant read and write permissions for individual buckets and objects to authorized users

- **S3 Object Ownership** – Disable ACLs and take ownership of every object in your bucket, simplifying access management for data stored in Amazon S3

- **Access Analyzer for S3 –** Evaluate and monitor your S3 bucket access policies

4. Data processing

To transform data and trigger workflows to automate a variety of other processing activities at scale, following features can be used:

- S3 Object Lambda – Add your own code to S3 GET requests to modify and process data as it is returned to an application. Filter rows, dynamically resize images, redact confidential data, and much more.

- Event notifications – Trigger workflows that use Amazon Simple Notification Service (Amazon SNS), Amazon Simple Queue Service (Amazon SQS), and AWS Lambda when a change is made to your S3 resources.

5. **Storage logging and monitoring**

Amazon S3 provides logging and monitoring tools that you can use to monitor and control how your Amazon S3 resources are being used

i) Automated monitoring tools:

- **Amazon CloudWatch metrics for Amazon S3 –** Track the operational health of your S3 resources and configure billing alerts

- **AWS CloudTrail –** Record actions taken by a user, a role, or an AWS service in Amazon S3. CloudTrail logs provide you with detailed API tracking for S3 bucket-level and object-level operations

ii) Manual monitoring tools:

- **Server access logging –** Get detailed records for the requests that are made to a bucket. You can use server access logs for many use cases, such as conducting security and access audits

- **AWS Trusted Advisor –** Evaluate your account by using AWS best practice checks to identify ways to optimize your AWS infrastructure, improve security and performance, reduce costs, and monitor service quotas.

6. **Analytics and insights**

- **Amazon S3 Storage Lens –** Understand, analyze, and optimize your storage. S3 Storage Lens provides 29+ usage and activity metrics and interactive dashboards to aggregate data for your entire organization, specific accounts, AWS Regions, buckets

- **Storage Class Analysis –** Analyze storage access patterns to decide when it's time to move data to a more cost-effective storage class

- **3 Inventory with Inventory reports –** Audit and report on objects and their corresponding metadata and configure other Amazon S3 features to take action in Inventory reports.

7. **Strong consistency**

- Amazon S3 provides strong read-after-write consistency for PUT and DELETE requests of objects in your Amazon S3 bucket in all AWS Regions

S3 – How it works?

- Amazon Simple Storage Service (Amazon S3) is an object storage service offering industry-leading scalability, data availability, security, and performance

- Customers of all sizes and industries can store and protect any amount of data for virtually

- With cost-effective storage classes and easy-to-use management features, you can optimize costs, organize data, and configure fine-tuned access controls to meet specific business, organizational, and compliance requirements

- To store your data in Amazon S3, you first create a bucket and specify a bucket name and AWS Region. Then, you upload your data to that bucket as objects in Amazon S3. Each object has a *key* (or *key name*), which is the unique identifier for the object within the bucket.

Analytics data

Log files

Application data

Videos and pictures

Backup and archival
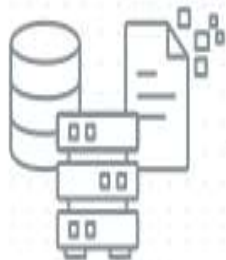
Move data

Move your data to Amazon S3 from wherever it lives – in the cloud, in applications, or on-premises

Amazon S3

Object storage built to store and retrieve any amount of data from anywhere

Store data

Create bucket, specify the Region, access controls, and management options. Upload any amount of data

Control access to data

Optimize cost with storage classes

Replicate data to any Region

Access from on-premises or VPC

Protect and secure your data

Gain visibility into your storage

Artificial Intelligence (AI)

Advanced analytics

Machine Learning (ML)

Analyze data

Use AWS and 3rd party services to analyze your data to gain insights

- **Buckets:** A bucket is a container for objects stored in Amazon S3. You can store any number of objects in a bucket and can have up to 100 buckets in your account.

- **Objects:** Objects consist of object data and metadata. The metadata is a set of name-value pairs that describe the object. These pairs include some default metadata, such as the date last modified, and standard HTTP metadata

- **Keys:** An *object key* (or *key name*) is the unique identifier for an object within a bucket. Every object in a bucket has exactly one key. The combination of a bucket, object key, and optionally, version ID (if S3 Versioning is enabled for the bucket) uniquely identify each object

- **S3 Versioning:** You can use S3 Versioning to keep multiple variants of an object in the same bucket

- **Version ID:** When you enable S3 Versioning in a bucket, Amazon S3 generates a unique version ID for each object added to the bucket. Objects that already existed in the bucket at the time that you enable versioning have a version ID of null.

Database Services -DBaaS

- **Allows to set up and operate relational or non-relational database in cloud**

- It relieves the application developers from time consuming database administration tasks

- Popular **relational databases** provided by various cloud service providers include **MySQL, Oracle, SQL Server etc.**

- **Non-relational (No-SQL) databases** provided by cloud service providers are mostly proprietary solutions

- Cloud provider takes care of everything from periodic upgrades to **backups for 24/7**

What is Database?

- **Data is an information about an object along with metadata**(the data providing information about one or more aspects of the data)

- **Object can be anything that is real and can be defined using different attributes**

- **A Database is a collection of organized data, information and records**

- **DBMS: Database Management that creates and manages databases**

- **Platform: SQL (MySQL – free & open source)**

Types of Database

Relational Database

- Stored in table/s (rows & columns)
- Schema is fixed
- Does not perform well for variable schema
- Vertical scaling possible

Non-Relational Database

- Schema not fixed
- Key-value stores (fast & provides quick access)
- Supports heavy read/write

DBaaS Features

- **Scalability:** allows provisioning as much compute and storage resources as required to meet the application workload levels

- **Reliability:** provides automated backup and snapshot options

- **Performance:** provides guaranteed performance with options such as input/output operations per second (IOPS)

- **Security:** provides several security features to restrict the access to the database instances and stored data such as network firewalls and authentication mechanisms.

Benefits

- Cost savings

- Up/down scaling

- Simple management

- Rapid development and faster time to market

- Encrypted data and application security

- Reduced risk

- Software quality

Amazon Relational Data store

- RDS is amazon relational database service

- Easy to set up, operate and scale a relational database in cloud

- Console provides an instance launch wizard that allows you to select type of database to create (MySQL, Oracle or SQL server) database instance size, allocated storage, DB instance identifier, DB username and password
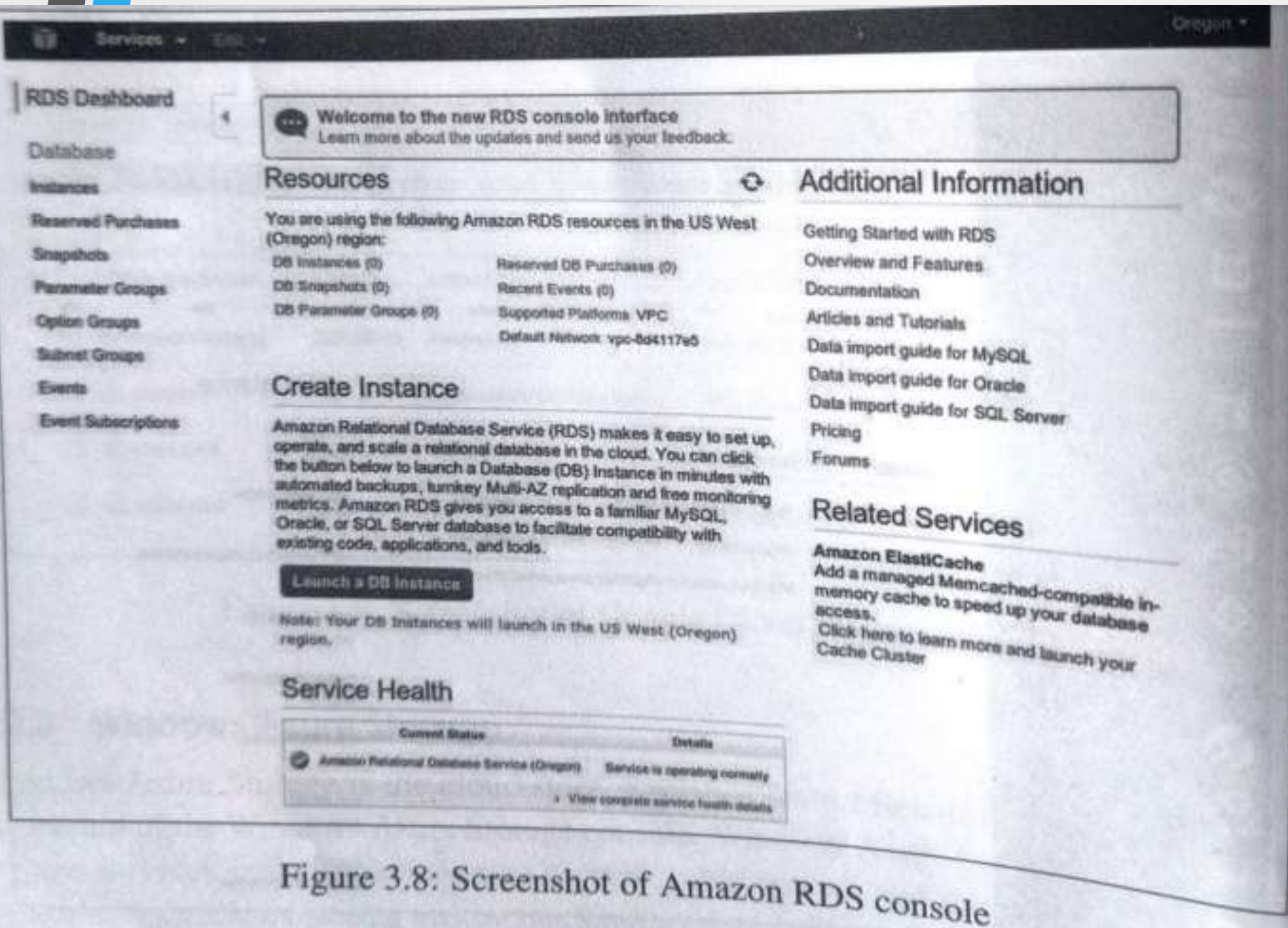
Figure 3.8: Screenshot of Amazon RDS console

Amazon DynamoDB

- **Amazon non-relational database service**

- **DyanamoDB data model includes include table, items and attributes**

- **To store data in DynamoDB , you have to create one or more tables and specify how much throughput capacity you want to provision and reserve for reads/writes**

- Fully managed service that automatically spreads the data and traffic for the stored tables over number of servers to meet the throughput requirements specified by users
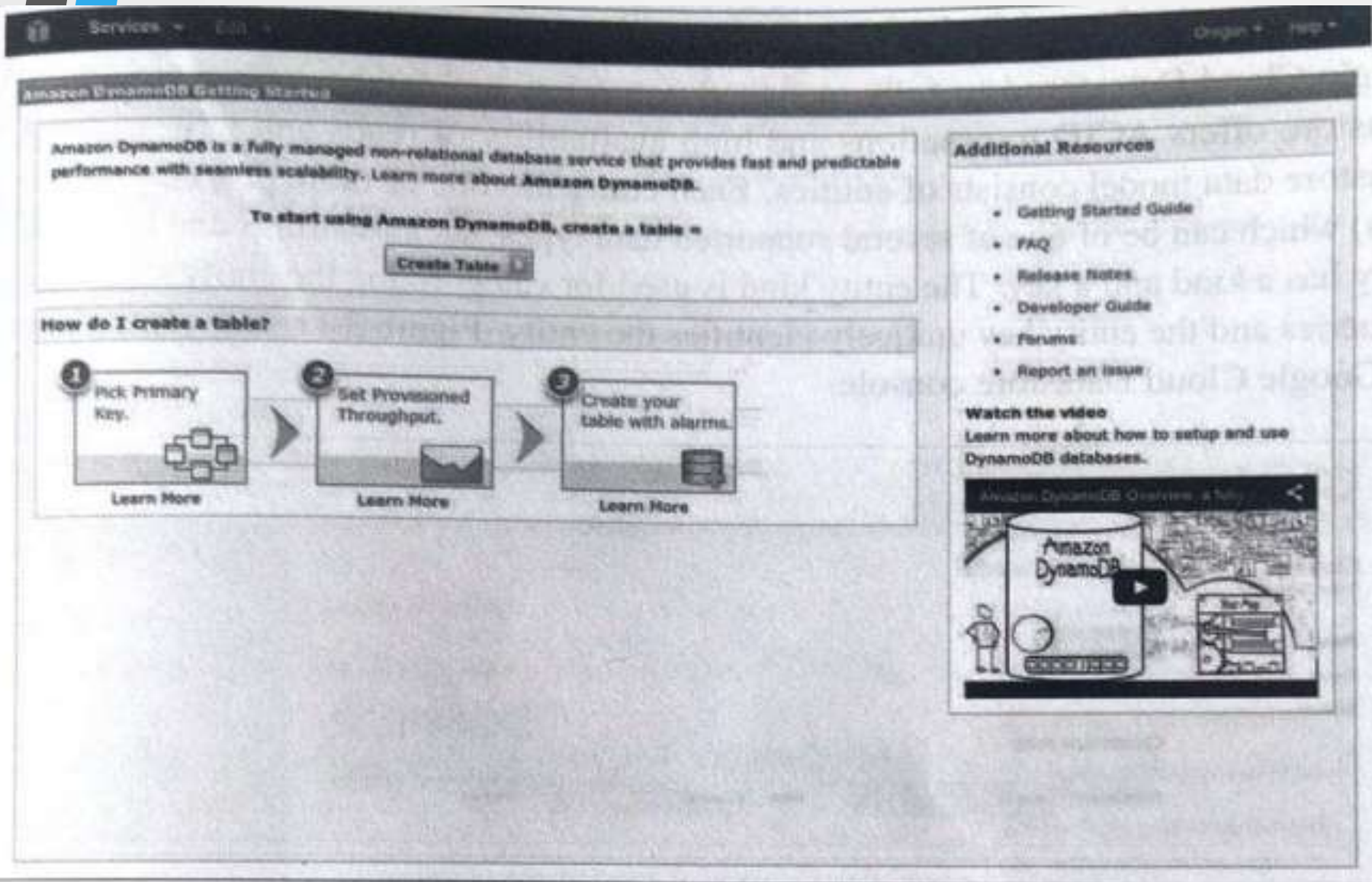
Figure 3.9: Screenshot of Amazon DynamoDB console

Google cloud SQL

- Relational database service from Google

- Allows you to host MySQL databases in Google's cloud

- Google cloud SQL also provides synchronous & asynchronous replication services

- Supports ability to import/ export databases

- To create instance- Select region – Select database tier – billing plan – replication mode

- Daily backups can be scheduled in Google cloud

Figure 3.10: Screenshot of Google Cloud SQL console

Google cloud datastore

- Fully managed non-relational database by Google

- It offers ACID (Atomicity, Consistency, Isolation, Durability) transactions and high availability of read/write

- Datastore model consist of entities

- Each entity has one or more properties (Key-value pair)

Figure 3.11: Screenshot of Google Cloud Datastore console

Windows Azure SQL database

- Relational database service from Microsoft

- It does not provide each customer a separate instance of SQL server

- Instead SQL database is multi-tenant service with logical SQL database server for each customer

Windows Azure Table Service

- Non-relational (No-SQL) database service by Microsoft

- This mode consist of tables having multiple entities

- Tables are divided into some number of partitions, each of which can be store in separate machine

- Each partition in table holds a specified number of entities, each containing several properties

- Each property can be one of the several supported data types

- Tables do not have fixed schema and different entities in a table can have different properties

Application Services

- Application runtime and frameworks
- Queuing services
- Email services
- Notification services
- Media services

1. Application Runtime & Frameworks

- Allows developer to develop and host applications in the cloud

- Provide support for programming languages like java, python, ruby etc.

- Application runtime automatically allocate resources for applications and handle application scaling

Google App Engine

Provides PaaS and includes both application runtime & web framework.

Features:

- **Runtime:** It supports applications developed in Java, Python, PHP and Go programming languages

- **Sandbox:** Application run in secure sandbox environment isolated from other applications. Sandbox provides limited access to underlying OS. Distributes web requests for application across multiple servers.

- **Web frameworks:** It provides simple python web application framework called Webapp2. It also supports any framework written in pure python that speaks WSGI, including django, cherryPy, Pylons, web.py etc.

- **Datastore:** No SQL data storage service

- **Authentication:** App Engine applications can be integrated with Google accounts for user authentication

- **URL Fetch service:** It allows applications to access resources on the internet

- **Email services:** Allows applications to send email messages

- **Image manipulation service:** Allows applications to resize, crop, rotate, flip and enhance images

- **Memcache:** High performance in-memory key-value cache service that applications can use for caching data items that do not need a persistent storage

- **Task Queues:** Allows applications to do work in the background by breaking up work into small, discrete units, called taks which are enqueued in task queues

- **Scheduled Tasks service:** App Engine provides a Cron service for scheduled tasks that trigger events at **specified times and regular intervals.**
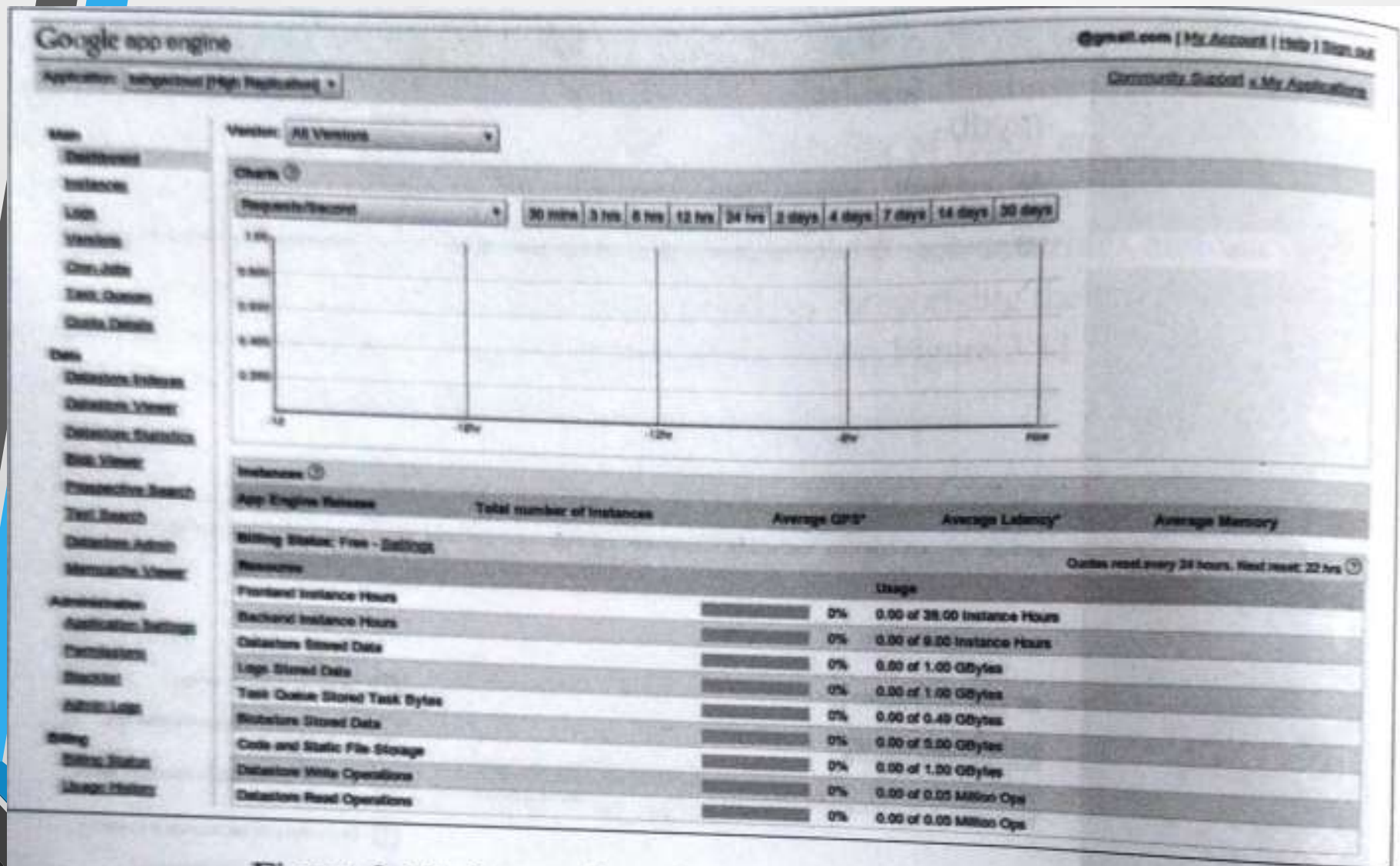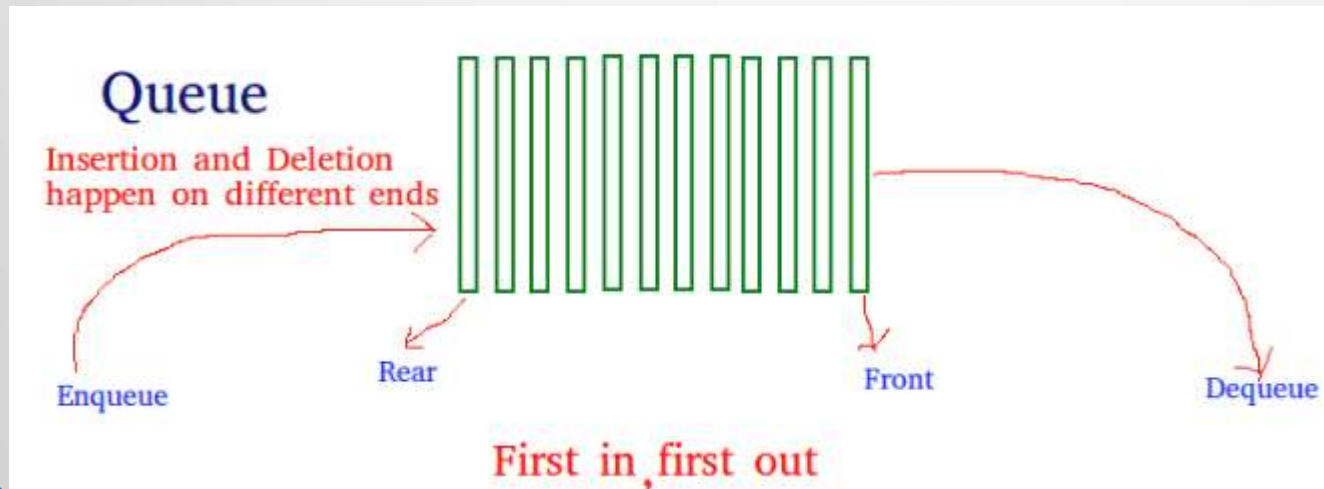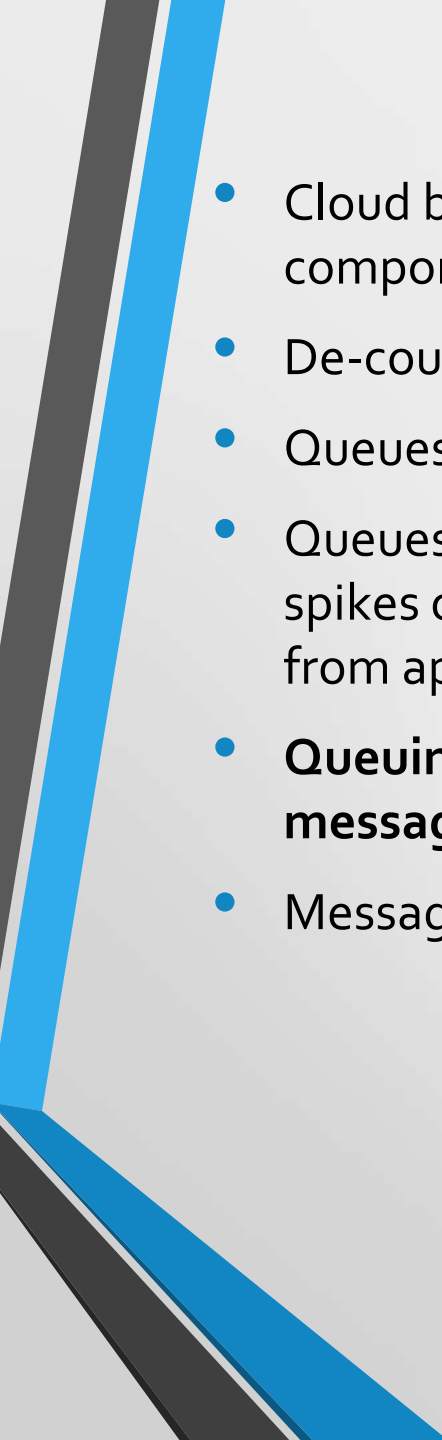
Figure 3.13: Screenshot of Google App Engine console
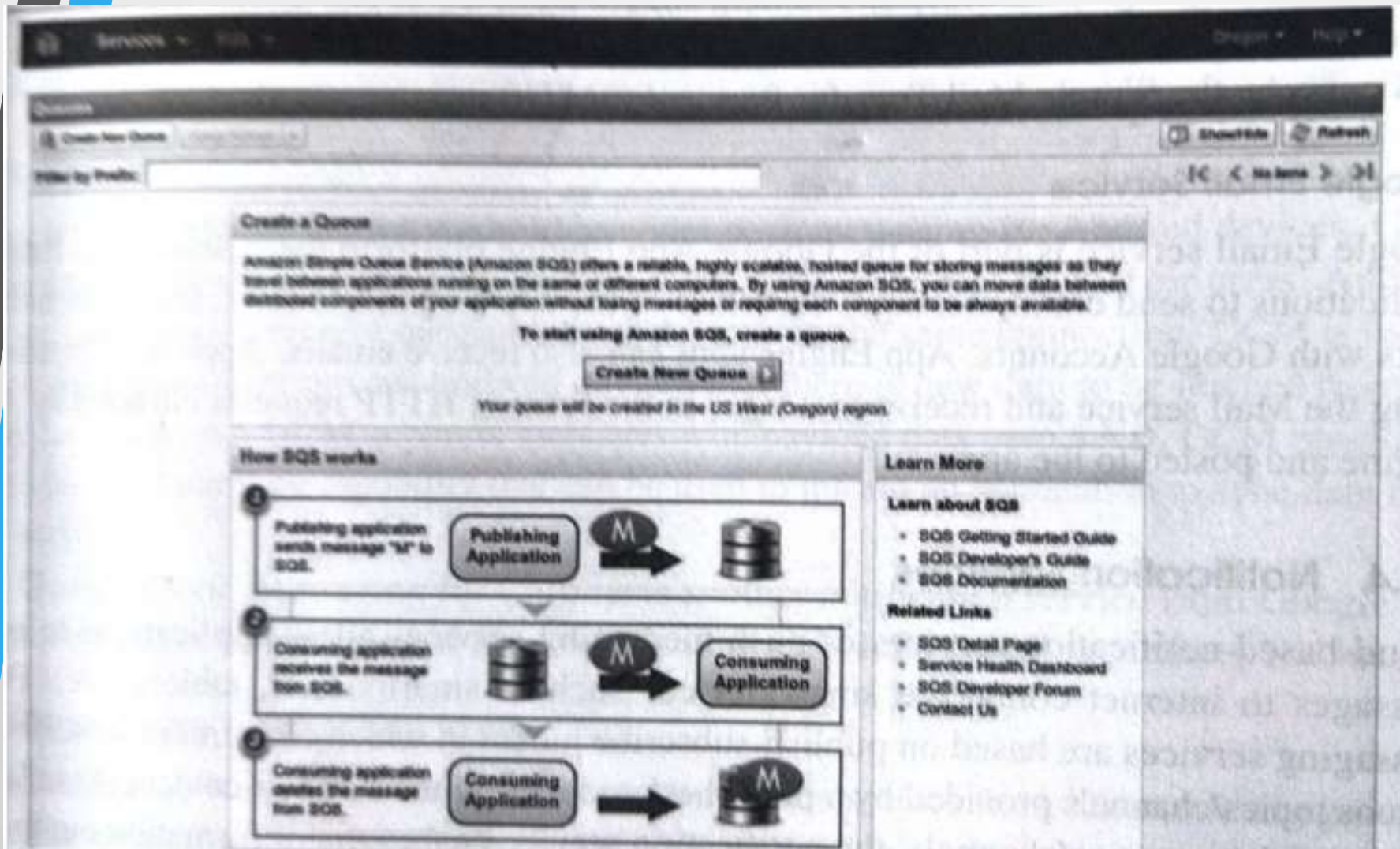
2. Queueing Services

What is Queue?

- A Queue is a linear structure which follows a particular order in which the operations are performed

- The order is First In First Out (FIFO)

- Cloud based queuing services allow de-coupling application components

- De-coupled components communicate via messaging queues

- Queues are used for asynchronous processing

- Queues also act as overflow buffers to handle temporary volume spikes or mismatches in message generation and consumption rates from application components

- **Queuing services from various cloud service provider allow short messages of a few kilo-bytes in size**

- Message can be enqueued and read from the queues simultaneously

Amazon Simple Queue Service

- **SQS is queuing service by Amazon**

- **It is distributed queue that supports messages of up to 256 KB in size**

- **SQS supports multiple writers & readers and locks messages while they are being processed**

- **SQS service trade-offs on FIFO capability and does not guarantee that message will be delivered in FIFO order**

- Application that requires FIFO ordering of messages can place additional sequencing information in each message so that they can re-ordered after retrieving from queue

Screenshot of Amazon SQS console

Google Task Queue service

- Queuing service from Google

- It is part of Google App Engine platform

- Task Queues allow applications to execute tasks in background

- There are two different configurations for Task Queues-

  - Push Queue

    - Pull Queue

- Push queue is default queue that processes tasks based on processing rate

- Pull queues allow task consumers to lease a specific number of tasks for a specific duration. The tasks are processed and deleted before the lease ends

Windows Azure Queue Service

- Queuing service by Microsoft

- It allows storing large number of messages that can be accessed from anywhere in the world via authenticated calls using http or https

- Size of single message can be 64 KB

3. Email Services

Amazon Simple Email service

- It is bulk and transactional email-sending service from Amazon

- It is outbound-only

- To ensure high email deliverability, SES uses content filtering technologies to scan the outgoing email messages

- SES can be accessed and used from SES console, Simple Mail Transfer Protocol (SMTP) interface or SES API

Google Email Service (Gmail)

- Part of Google App Engine platform that allows App Engine applications to send email messages

- App engine can also receives emails

4. Notification Services

- **Cloud based notification services or push messaging services allow applications to push messages to internet connected smart devices**

- Push messaging services are bases on publish-subscribe model

- Topic /Channel provided by publisher/producer

- Consumers subscribe for the Topic/Channel

- For new contents or intimations, messages are pushed on Topic/Channel

- Consumer applications on smart devices can increase their consumer engagement with the help of push notifictions

Amazon Simple Notification Service (SNS)

- Fast and fully managed Push messaging service from Amazon

- SNS has two types of clients – Publisher & Subscriber

- Publishers communicate asynchronously with subscribers by producing and sending messages to topics

- Topic is a logical access point and communication channel (Each topic has unique name within an account, Each topic assigned with ARN)

- Subscribers are the consumers who subscribe to topics to receive notifications

- SNS can deliver notifications as SMS, email or to SQS queues or http endpoint

- SNS console has wizards for creating a new topic, publishing to a topic and subscribing to a topic

Continue..

- Can send message to single user or to multiple users

- There is no upfront cost for the service, pay per use

- Reliable

- Messages can be transmitted using multiple protocol schemes
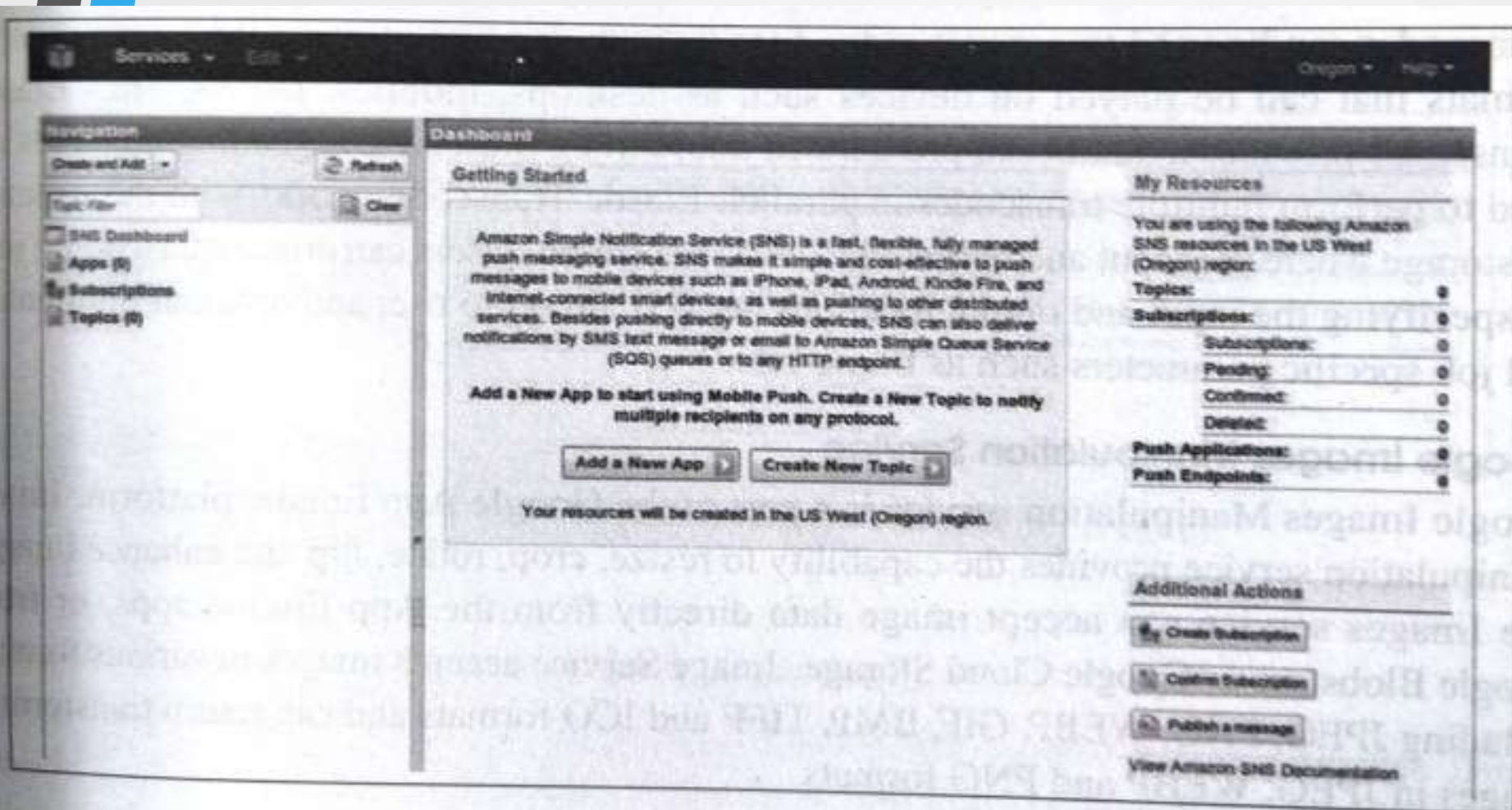
- Access policies can be defined

Figure 3.15: Screenshot of Amazon SNS console

Google Cloud Messaging

- Google cloud messaging for Android provides push messaging for Android devices

- It allows applications to send data from application servers to their users and android devices

- GCM is useful for applications on Android devices that there is new data to be fetched from the application servers

- GCM provides 'send-to-sync' message capability that can be used to inform an application to sync data from server

- GCM supports messages with payload data upto 4KB

Windows Azure Notification Hubs

- Push notification service from Microsoft that provides a common interface to send notifications to all major mobile platforms

- Platform specific infrastructure called Platform Notification Systems (PNS) are used to deliver notification messages

- Devices register their PNS handles with Notification Hub

- Each notification hub contains credentials for each supported PNS

- These credentials are used to connect to PNS and send push notifications to the applications.