Index

1. s3
2. lambda
3. ec2 instance
4. rds
5. api gateway
6. cloudwatch
7. vpc
8. sqs
9. elastic cache (redis)
10. sso
11. guardduty
12. config
13. kms
14. security hub
15. cloud trail
16. simple email service (ses)
17. simple notification service

Redis

in-memory data store

high-performance and versatile caching, messaging, and data structure storage system

category of NoSQL databases

key-value store

designed for speed and efficiency,

fast data retrieval and low-latency operations

beyond simple key-value pairs, including strings, hashes, lists, sets, sorted sets, bitmaps, hyperloglogs, and geospatial indexes

caching

reduce the load on backend databases and improve response times.

publish/subscribe (pub/sub) capabilities

different parts of an application to communicate asynchronously

real-time messaging systems and event-driven architectures.

persistence options, - snapshots (snapshots of the dataset saved to disk) and append-only files (log-like files of write operations), to provide durability and data recovery capabilities.

high availability and data redundancy

Atomic Operations, Lua Scripting, Cluster Support,

**Amazon simple email service**

bulk email sending - transactional emails, marketing emails, or newsletter emails,

**AWS Security Hub**

Check security

**AWS Config**

detailed view of the configuration of AWS resources

how the resources are related to one another

how they were configured in the past

you can see how the configurations and relationships change over time.

**AWS Key Management Service**

create and control the cryptographic keys

**AWS CloudTrail**

records all API calls

It creates log files containing information about who performed the action, what action was performed, which resource was affected, and when the action occurred.

tracking and auditing changes to your resources, helping with security, compliance, and investigative needs.

**AWS GuardDuty**

threat detection service

protect your AWS resources and workloads by identifying potentially malicious or unauthorized activities

continuously monitors your AWS environment for suspicious behavior and generates findings that provide insights into potential security threats

It uses machine learning, anomaly detection, and threat intelligence to identify patterns of behavior that could indicate an attack.

**AWS Single Sign-On (SSO)**

Hardware Skills - AVR, 8051,PIC, ARM, ST

Peripheral Interface - I2C displays, ZigBee, ESP, LTE, GPS, Generic devices

Software Tools - Atmel Studio, Arduino, MPLAB IDE, Proteus, IDLE, JUPYTER, Keil.

Development experience with ESP32 board based applications.