AWS Architecting & Ecosystem Section

Well Architected Framework
General Guiding Principles

- Stop guessing your capacity needs
- Test systems at production scale
- Automate to make architectural experimentation easier
- Allow for evolutionary architectures
  - Design based on changing requirements
- Drive architectures using data
- Improve through game days
  - Simulate applications for flash sale days

AWS Cloud Best Practices – Design Principles

- **Scalability:** vertical & horizontal
- **Disposable Resources:** servers should be disposable & easily configured
- **Automation:** Serverless, Infrastructure as a Service, Auto Scaling…
- **Loose Coupling:**
  - *Monolith* are applications that do more and more over time, become bigger
  - Break it down into smaller, loosely coupled components
  - A change or a failure in one component should not cascade to other components
- **Services, not Servers:**
  - Don't use just EC2
  - Use managed services, databases, serverless, etc !

Well Architected Framework
6 Pillars

- 1) Operational Excellence
- 2) Security
- 3) Reliability
- 4) Performance Efficiency
- 5) Cost Optimization
- 6) Sustainability

- They are not something to balance, or trade-offs, they're a synergy

1) Operational Excellence

- Includes the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures
- Design Principles
  - **Perform operations as code** - Infrastructure as code
  - **Annotate documentation** - Automate the creation of annotated documentation after every build
  - **Make frequent, small, reversible changes** - So that in case of any failure, you can reverse it
  - **Refine operations procedures frequently** - And ensure that team members are familiar with it
  - **Anticipate failure**
  - **Learn from all operational failures**

Operational Excellence AWS Services

- Prepare


AWS CloudFormation


AWS Config

- Operate


AWS CloudFormation


AWS Config


AWS CloudTrail


Amazon CloudWatch


AWS X-Ray

- Evolve


AWS CloudFormation


AWS CodeBuild


AWS CodeCommit


AWS CodeDeploy


AWS CodePipeline

2) Security

- Includes the ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies
- Design Principles
  - **Implement a strong identity foundation** - Centralize privilege management and reduce (or even eliminate) reliance on long-term credentials - Principle of least privilege - IAM
  - **Enable traceability** - Integrate logs and metrics with systems to automatically respond and take action
  - **Apply security at all layers** - Like edge network, VPC, subnet, load balancer, every instance, operating system, and application
  - **Automate security best practices**
  - **Protect data in transit and at rest** - Encryption, tokenization, and access control
  - **Keep people away from data** - Reduce or eliminate the need for direct access or manual processing of data
  - **Prepare for security events** - Run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery
  - **Shared Responsibility Model**

Security
AWS Services

- Identity and Access Management


IAM


AWS-STS

MFA token


AWS Organizations

- Detective Controls


AWS Config


AWS CloudTrail


Amazon CloudWatch

- Infrastructure Protection


Amazon CloudFront


Amazon VPC


AWS Shield


AWS WAF


Amazon Inspector

- Data Protection:


KMS


S3


Elastic Load Balancing (ELB)


Amazon EBS


Amazon RDS

- Incident Response


IAM


AWS CloudFormation


Amazon CloudWatch Events

3) Reliability

- Ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues
- Design Principles
  - **Test recovery procedures** - Use automation to simulate different failures or to recreate scenarios that led to failures before
  - **Automatically recover from failure** - Anticipate and remediate failures before they occur
  - **Scale horizontally to increase aggregate system availability** - Distribute requests across multiple, smaller resources to ensure that they don't share a common point of failure
  - **Stop guessing capacity** - Maintain the optimal level to satisfy demand without over or under provisioning - Use Auto Scaling
  - **Manage change in automation** - Use automation to make changes to infrastructure

Reliability
AWS Services

- Foundations


IAM


Amazon VPC


Service Quotas


AWS Trusted Advisor

- Change Management


AWS Auto Scaling


Amazon CloudWatch


AWS CloudTrail


AWS Config

- Failure Management


Backups


AWS CloudFormation


Amazon S3


Amazon S3 Glacier

Amazon Route 53

4) Performance Efficiency

- Includes the ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve
- Design Principles
  - **Democratize advanced technologies** - Advance technologies become services and hence you can focus more on product development
  - **Go global in minutes** - Easy deployment in multiple regions
  - **Use serverless architectures** - Avoid burden of managing servers
  - **Experiment more often** - Easy to carry out comparative testing
  - **Mechanical sympathy** - Be aware of all AWS services

Performance Efficiency AWS Services

- Selection
- Review
- Monitoring
- Tradeoffs


AWS Auto Scaling


AWS Lambda


Amazon Elastic Block Store (EBS)


Amazon Simple Storage Service (S3)


Amazon RDS


AWS CloudFormation

AWS News Blog


Amazon CloudWatch


AWS Lambda


Amazon RDS


Amazon ElastiCache


AWS Snowball


Amazon CloudFront

5) Cost Optimization

- Includes the ability to run systems to deliver business value at the lowest price point
- Design Principles
  - **Adopt a consumption mode** - Pay only for what you use
  - **Measure overall efficiency** - Use CloudWatch
  - **Stop spending money on data center operations** - AWS does the infrastructure part and enables customer to focus on organization projects
  - **Analyze and attribute expenditure** - Accurate identification of system usage and costs, helps measure return on investment (ROI) - Make sure to use tags
  - **Use managed and application level services to reduce cost of ownership** - As managed services operate at cloud scale, they can offer a lower cost per transaction or service

Cost Optimization AWS Services

- Expenditure Awareness
- Cost-Effective Resources
- Matching supply and demand
- Optimizing Over Time


AWS Budgets


AWS Cost and Usage Report


AWS Cost Explorer


Reserved Instance Reporting


Spot instance


Reserved instance


Amazon S3 Glacier


AWS Auto Scaling


AWS Lambda


AWS Trusted Advisor


AWS Cost and Usage Report

AWS News Blog

6) Sustainability

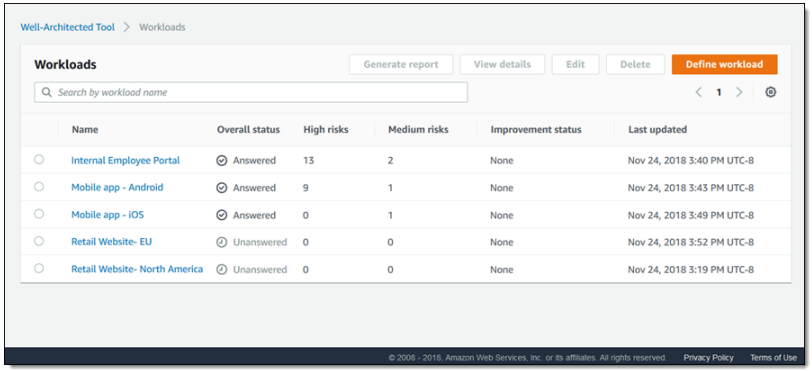
- The sustainability pillar focuses on minimizing the environmental impacts of running cloud workloads.
- Design Principles
  - **Understand your impact** – establish performance indicators, evaluate improvements
  - **Establish sustainability goals** – Set long-term goals for each workload, model return on investment (ROI)
  - **Maximize utilizatio**n – Right size each workload to maximize the energy efficiency of the underlying hardware and minimize idle resources.
  - **Anticipate and adopt new, more efficient hardware and software offerings** – and design for flexibility to adopt new technologies over time.
  - **Use managed services –** Shared services reduce the amount of infrastructure; Managed services help automate sustainability best practices as moving infrequent accessed data to cold storage and adjusting compute capacity.
  - **Reduce the downstream impact of your cloud workloads** – Reduce the amount of energy or resources required to use your services and reduce the need for your customers to upgrade their devices

Sustainability AWS Services

- EC2 Auto Scaling, Serverless Offering (Lambda, Fargate)
- Cost Explorer, AWS Graviton 2, EC2 T instances, @Spot Instances
- EFS-IA, Amazon S3 Glacier, EBS Cold HDD volumes
- S3 Lifecycle Configurations, S3 Intelligent Tiering
- Amazon Data Lifecycle Manager
- Read Local, Write Global: RDS Read Replicas, Aurora Global DB, DynamoDB Global Table, CloudFront

AWS Well-Architected Tool

- Free tool to **review your architectures** against the 6 pillars Well-Architected Framework and **adopt architectural best practices**
- How does it work?
  - Select your workload and answer questions
  - Review your answers against the 6 pillars
  - Obtain advice: get videos and documentations, generate a report, see the results in a dashboard
- Let's have a look: https://console.aws.amazon.com/wellarchitected



https://aws.amazon.com/blogs/aws/new-aws-well-architected-tool-review-workloads-against-best-practices/

AWS Right Sizing

- EC2 has many instance types, but choosing the most powerful instance type isn't the best choice, because the cloud is **elastic**
- Right sizing is the process of matching instance types and sizes to your workload performance and capacity requirements **at the lowest possible cost**
- **Scaling up is easy so always start small**
- It's also the process of looking at deployed instances and identifying opportunities to eliminate or downsize without compromising capacity or other requirements, which results in lower costs
- It's important to Right Size…
  - **before a Cloud Migration**
  - **continuously after the cloud onboarding process (requirements change over time)**
- CloudWatch, Cost Explorer, Trusted Advisor, 3rd party tools can help

AWS Ecosystem – Free resources

- AWS Blogs: https://aws.amazon.com/blogs/aws/
- AWS Forums (community): https://forums.aws.amazon.com/index.jspa
- AWS Whitepapers & Guides: https://aws.amazon.com/whitepapers
- AWS Quick Starts: https://aws.amazon.com/quickstart/
  - Automated, gold-standard deployments in the AWS Cloud
  - Build your production environment quickly with templates
  - Example: WordPress on AWS https://fwd.aws/P3yyv?did=qs_card&trk=qs_card
  - Leverages CloudFormation
- AWS Solutions: https://aws.amazon.com/solutions/
  - Vetted Technology Solutions for the AWS Cloud
  - Example - AWS Landing Zone: secure, multi-account AWS environment
    - https://aws.amazon.com/solutions/implementations/aws-landing-zone/
    - "Replaced" by AWS Control Tower

AWS Ecosystem - AWS Support

DEVELOPER	• Business hours email access to Cloud Support Associates • General guidance: < 24 business hours • System impaired: < 12 business hours
BUSINESS	• 24x7 phone, email, and chat access to Cloud Support Engineers • Production system impaired: < 4 hours • Production system down: < 1 hour
ENTERPRISE	• Access to a Technical Account Manager (TAM) • Concierge Support Team (for billing and account best practices) • Business-critical system down: < 15 minutes

AWS Marketplace

- Digital catalog with thousands of software listings from **independent software vendors** (3rd party)
- Example:
  - Custom AMI (custom OS, firewalls, technical solutions…)
  - CloudFormation templates
  - Software as a Service
  - Containers
- If you buy through the AWS Marketplace, it goes into your AWS bill
- You can **sell your own solutions** on the AWS Marketplace

AWS Training

- AWS Digital (online) and Classroom Training (in-person or virtual)
- AWS Private Training (for your organization)
- Training and Certification for the U.S Government
- Training and Certification for the Enterprise

- AWS Academy: helps universities teach AWS

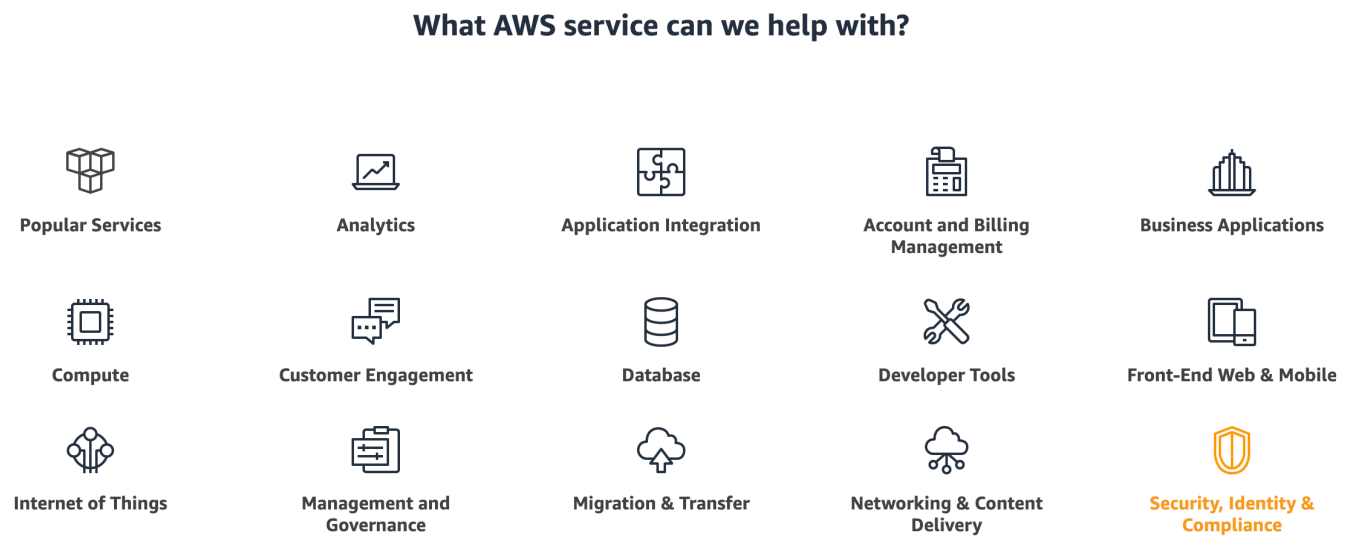
- And your favorite online teacher…
  teaching you all about AWS Certifications and more!

AWS Professional Services & Partner Network

- The AWS Professional Services organization is a global team of experts
- They work alongside your team and a chosen member of the APN
- APN = AWS Partner Network
- **APN Technology Partners:** providing hardware, connectivity, and software
- **APN Consulting Partners:** professional services firm to help build on AWS
- **APN Training Partners:** find who can help you learn AWS
- **AWS Competency Program:** AWS Competencies are granted to APN Partners who have demonstrated technical proficiency and proven customer success in specialized solution areas.
- **AWS Navigate Program:** help Partners become better Partners

AWS Knowledge Center

- Contains the most frequent & common questions and requests



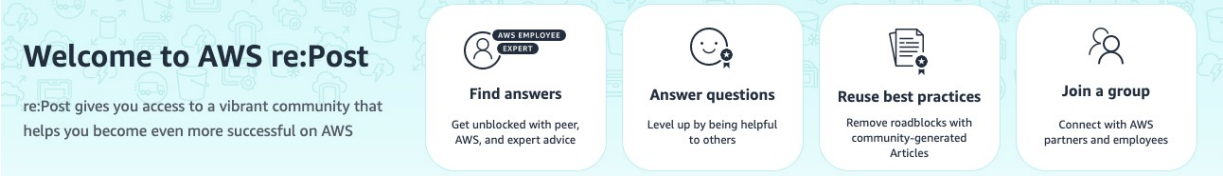
https://aws.amazon.com/premiumsupport/knowledge-center/

AWS IQ

- Quickly find professional help for your AWS projects
- Engage and pay AWS Certified 3rd party experts for on-demand project work
- Video-conferencing, contract management, secure collaboration, integrated billing
- For Customers

- For Experts

AWS re:Post



- **AWS-managed Q&A service** offering crowd-sourced, expert-reviewed answers to your technical questions about AWS that replaces the original AWS Forums
- Part of the AWS Free Tier
- Community members can earn reputation points to build up their community expert status by providing accepted answers and reviewing answers from other users
- **Questions from AWS Premium Support customers that do not receive a response from the community are passed on to AWS Support engineers**
- AWS re:Post is not intended to be used for questions that are time-sensitive or involve any proprietary information