On Architecture

Technology architecture teams are often composed of a set of roles such as Technical Architect (infrastructure), Solutions Architect (software),Data Architect, Networking Architect, and Security Architect.

At AWS, we prefer to **distribute capabilities into teams** rather than having acentralized team with that capability.

General Design Principles

**Stop guessing your capacity needs**

**Test systems at production scale**

**Automate to make architectural experimentation easier**

**Allow for evolutionary architectures**

**Drive architectures using data**

**Improve through game days**

The Five Pillars of the Framework

1.Operational Excellence

2. Security

3. Reliability

4. Performance Efficiency

5. Cost Optimization

Operational Excellence

Design Principles

•**Perform operations as cod**e: By performing operations ascode, you limit human error and enable consistent responses to events.

•**Annotate documentation:** Automate, Use annotations as an input to your operations code.

**• Make frequent, small, reversible changes:**

• **Refine operations procedures frequently:** look for opportunities to improve them.

•**Anticipate failure**: pre-mortem exercises, gamedays

•**Learn from all operational failures**: Drive improvement through lessons learned from all operational events and failures.

**Operational Excellence: Definition**

Three best practice areas for operational excellence in the cloud:

•**Prepare**

**OPS 1: How do you determine what your priorities are?**

**OPS 2: How do you design your workload so that you can understand its state?**

**OPS 3: How do you reduce defects, ease remediation, and improve flow into production?**

**OPS 4: How do you mitigate deployment risks?**

**OPS 5: How do you know that you are ready to support a workload?**

•**Operate**

**OPS 6: How do you understand the health of your workload?**Define, capture, and analyze workload

**OPS 7: How do you understand the health of your operations?**Define, capture, and analyze operations metrics

**OPS 8: How do you manage workload and operations events?**

**•Evolve**

**OPS 9: How do you evolve operations?** continuous incremental improvement

Key AWS Services

**The AWS service that is essential to Operational Excellence is AWS *CloudFormation***,**which you can use to create templates based on best practices.** This enables you to provision resources in an orderly and consistent fashion from your development through production environments. The following services and features support the three areas in operational excellence:

•**Prepare**: **AWS Config** and AWS Config rules can be used to create standards for workloads and to determine if environments are compliant with those standardsbefore being put into production.

•**Operate**: **Amazon CloudWatch** allows you to monitor the operational health of a workload.

• **Evolve**: **Amazon Elasticsearch Service (Amazon ES)** allows you to analyze your log data to gain actionable insights quickly and securely.

Security

Design Principles

There are seven design principles for security in the cloud:

**• Implement a strong identity foundation:**  principle of least privilege and enforce separation of duties, Centralize privilege management and reduce reliance on long-term credentials.

• **Enable traceability:** Monitor, alert, and audit actions and changes to your environment real time. Integrate logs and metrics with systems to automatically respond and take action.

**• Apply security at all layers:** apply a defense-in-depth approach to all layers (e.g., edge network, VPC, subnet, load balancer, every instance, operating system, and application).

**• Automate security best practices:** Create secure architectures, the implementation of controls that are defined and managed as code in version-controlled templates.

**• Protect data in transit and at rest:** Classify your data into sensitivity levels and use mechanisms, such as encryption, tokenization, and access control where appropriate.

**• Keep people away from data:** This reduces the risk of loss or modification and human error when handling sensitive data.

**• Prepare for security events:** have incident management process, Run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery.

Security Definition

There are five best practice areas for security in the cloud:

• Identity and Access Management

**SEC 1: How do you manage credentials and authentication? SEC 2: How do you control human access?**

**SEC 3: How do you control programmatic access?**

• Detective Controls

**SEC 4: How do you detect and investigate security events?**

**SEC 5: How do you defend against emerging security threats?**

• Infrastructure Protection

**SEC 4: How do you detect and investigate security events?**

**SEC 5: How do you defend against emerging security threats?**

• Data Protection

**SEC 6: How do you protect your networks?**

**SEC 7: How do you protect your compute resources?**

Compute resources include EC2 instances, containers, AWS Lambda functions, database services, IoT devices, and more.

• Incident Response

**SEC 8: How do you classify your data?**

**SEC 9: How do you protect your data at rest?**

**SEC 10: How do you protect your data in transit?**Protecting your data: encryption, unauthorized access or exposure.

**SEC 11: How do you respond to an incident?**

Key AWS Services – Security

**•Identity and Access Management – IAM**

•**Detective Controls**: **AWS Config** provides **CloudTrail** a detailed inventory of your AWS resources and configuration.

Amazon **GuardDuty** is a managed threat detection service monitors for malicious or unauthorized behavior.

Amazon **CloudWatch** is a monitoring service for AWS resources which can trigger CloudWatch Events to automate security responses.

• **Infrastructure Protection**: **AWS Shield** for DDoS mitigation. **AWS WAF** is a web application firewall that is deployed on either Amazon CloudFront or Application Load Balancer to help protect your webapplications from common web exploits.

• **Data Protection**: Services such as ELB, Amazon Elastic Block Store (Amazon EBS),Amazon S3, and Amazon Relational Database Service (Amazon RDS) include **encryption** capabilities to protect your data in transit and at rest. **Amazon Macie** automatically discovers, classifies and protects sensitive data, while **AWS Key Management Service (AWS KMS)** makes it easy for you to create and control keysused for encryption.18

• **Incident Response**:. AWS CloudFormation can be used to create a trusted environment or clean room for conducting investigations.

Resources – Security

Documentation

• AWS Cloud Security

• AWS Compliance

• AWS Security Blog

Whitepaper

• Security Pillar

• AWS Security Overview

• AWS Security

Best Practices

• AWS Risk and Compliance

Video

• AWS Security State of the Union

• Shared Responsibility Overview

Reliability

Design Principles

There are five design principles for reliability in the cloud:

**• Test recovery procedures:**

**• Automatically recover from failure:**

• **Scale horizontally to increase aggregate system availability:**

**• Stop guessing capacity:**

**•Manage change in automation:**

Definition

There are three best practice areas for reliability in the cloud:

• Foundations

**REL 1: How do you manage service limits?**

**REL 2: How do you manage your network topology?**

• Change Management

**REL 3: How does your system adapt to changes in demand?**

**REL 4: How do you monitor your resources?**

**REL 5: How do you implement change?**

• Failure Management

**REL 6: How do you back up data?**

**REL 7: How does your system withstand component failures?**

**REL 9: How do you plan for disaster recovery?**

Key AWS Services

Foundations: AWS IAM, AWS Shield for DDOS

Change Management: AWS Config and AWS Cloudtrail, Amazon Auto Scaling

Failure Management: AWS CloudFormation

Resources

Refer to the following resources to learn more about our best practices for Reliability.

Documentation

• Service Limits

• Service Limits Reports Blog

• Amazon Virtual Private Cloud

• AWS Shield

• Amazon CloudWatch

• Amazon S3

• AWS KMS Whitepaper

• Reliability Pillar

• Backup Archive and Restore Approach Using AWS

• Managing your AWS Infrastructure at Scale

• AWS Disaster Recovery

• AWS Amazon VPC Connectivity Options

Video

• How do I manage my AWS service limits?

• Embracing Failure: Fault-Injection and Service ReliabilityProduct

• AWS Premium Support

• Trusted Advisor

**Performance Efficiency**

Design Principles

There are five design principles for performance efficiency in the cloud:

• Democratize advanced technologies:

• Go global in minutes:

• Use serverless architectures:

• Experiment more often:

• Mechanical sympathy: use tech to align with what you need

Definition

In AWS, compute is available in three forms: instances, containers, and functions

There are four best practice areas for performance efficiency in the cloud:

• Selection

**PERF 1: How do you select the best performing architecture?**

**COMPUTE-** available in three forms:

1.**Instances -** are virtualized servers

2.**Containers** - method of operating system

3.**Functions –** abstract execution

environment from code (Lambda)

**PERF 2: How do you select your compute solution?**

**STORAGE** - lock, file, or object

**PERF 3: How do you select your storage solution?**

**DATABASE –** availability, consistency, partition tolerance, latency, durability, scalability,and query capability

**PERF 4: How do you select your database solution?**

**NETWORK –**

**PERF 5: How do you configure your networking solution?**

• Review

**PERF 6: How do you evolve your workload to take advantage of new releases?**

• Monitoring

**PERF 7: How do you monitor your resources to ensure they are performing as expected?**

• Tradeoffs

**PERF 8: How do you use tradeoffs to improve performance?**

Key AWS Services

AWS service that is essential to Performance Efficiency is Amazon CloudWatch

The following services and features support the four areas in performance efficiency:

• Selection

•Compute: Auto Scaling

•Storage: Amazon EBS

S3 for serverless content delivery, and S3 transfer acceleration

•Database: Amazon RDS

AmazonDynamoDB

• Network: Amazon Route 53

Amazon VPC endpoints

and AWS Direct Connect

• Review: **The AWS Blog and the What's New section**

• Monitoring: Amazon CloudWatch

• Tradeoffs: **Amazon ElastiCache, Amazon CloudFront, and AWS Snowball** to improve performance.

Resources

Refer to the following resources to learn more about our best practices for

Performance Efficiency.

Documentation

• Amazon S3 Performance Optimization

• Amazon EBS Volume

Performance

Whitepaper

• Performance Efficiency Pillar

Video

• AWS re:Invent 2016: Scaling Up to Your First 10 Million Users (ARC201)

• AWS re:Invent 2017: Deep Dive on Amazon EC2 Instances

Cost Optimization

Design Principles

There are five design principles for cost optimization in the cloud:

**• Adopt a consumption model:** Pay for what you need

**• Measure overall efficiency:** Measure the business output of the workload and the costs associated with delivering it.

**• Stop spending money on data center operations:**

**• Analyze and attribute expenditure:** (ROI)

**• Use managed and application level services to reduce cost of ownership:**

Definition

There are four best practice areas for cost optimization in the cloud:

• Expenditure Awareness

**COST 1: How do you govern usage?**

**COST 2: How do you monitor usage and cost?**

**COST 3: How do you decommission resources?**

• Cost-Effective Resources

**COST 4: How do you evaluate cost when you select services?**

**COST 5: How do you meet cost targets when you select resource type and size?**

**COST 6: How do you use pricing models to reduce cost? COST 7: How do you plan for data transfer charges?**

• Matching supply and demand

**COST 8: How do you match supply of resources with demand?**

• Optimizing Over Time

**COST 9: How do you evaluate new services?**

**Key AWS Services**

**• Expenditure Awareness:** **AWS Cost Explorer** allows you to view and track your usage in detail.

**AWS Budgets notify you if your usage or spend exceeds** actual orforecast budgeted amounts.

**• Cost-Effective Resources:** You can use **Cost Explorer for Reserved Instance recommendations**, and see patterns in how much you spend on AWS resources over time. Use **Amazon CloudWatch** and **Trusted Advisor** to help right size your resources. You can use **Amazon Aurora on RDS to remove database licensing costs.**

**AWS Direct Connect and Amazon CloudFront can be used to optimize data transfer.**

**•Matching supply and demand:** **Auto Scaling**

**•Optimizing Over Time:** **The AWS News Blog and the What's New section on the AWS website** are resources for learning about newly launched features and services.**AWS Trusted Advisor** inspects your AWS environment and finds opportunities to save you money by eliminating unused or idle resources or committing to Reserved Instance capacity.

**Resources**

Refer to the following resources to learn more about our best practices for Cost Optimization.

Documentation

• Analyzing Your Costs with Cost Explorer

• AWS Cloud Economics Center

• AWS Detailed Billing Reports

Whitepaper

• Cost Optimization Pillar

Video

• Cost Optimization on AWSTool

• AWS Total Cost of Ownership (TCO) Calculators

• AWS Simple Monthly Calculator