AWS – Well Architected Framework

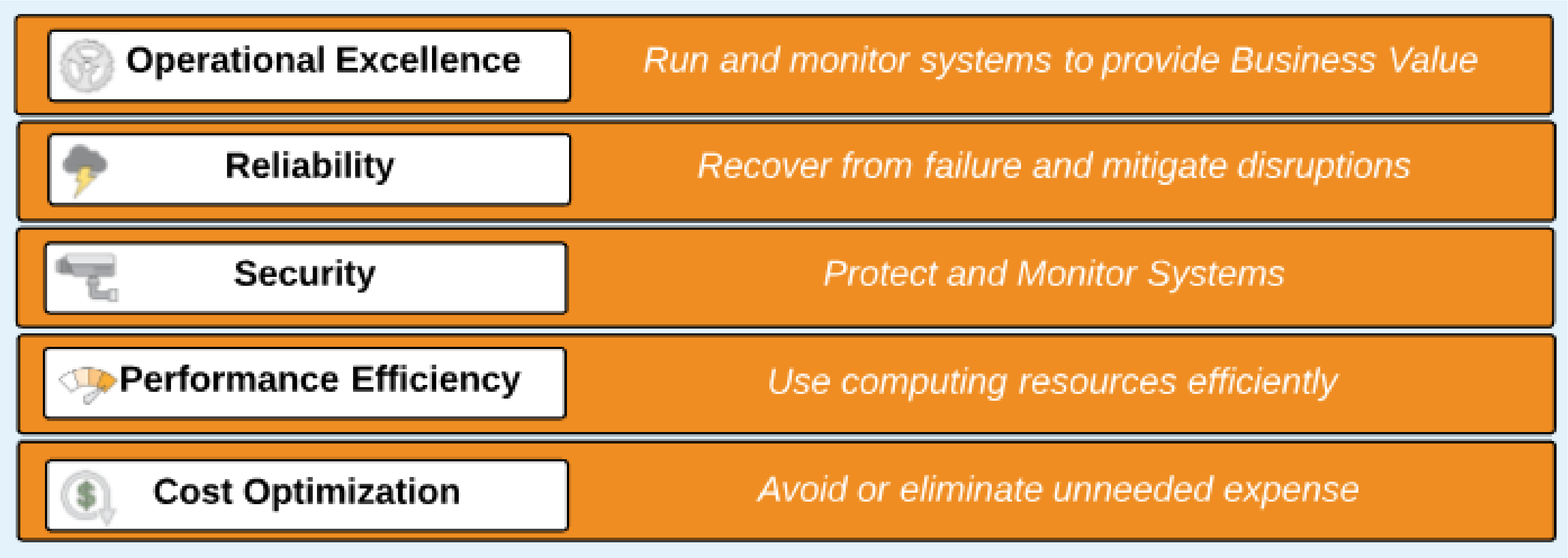
By

Keshav Kummari

What is Well Architected Framework?

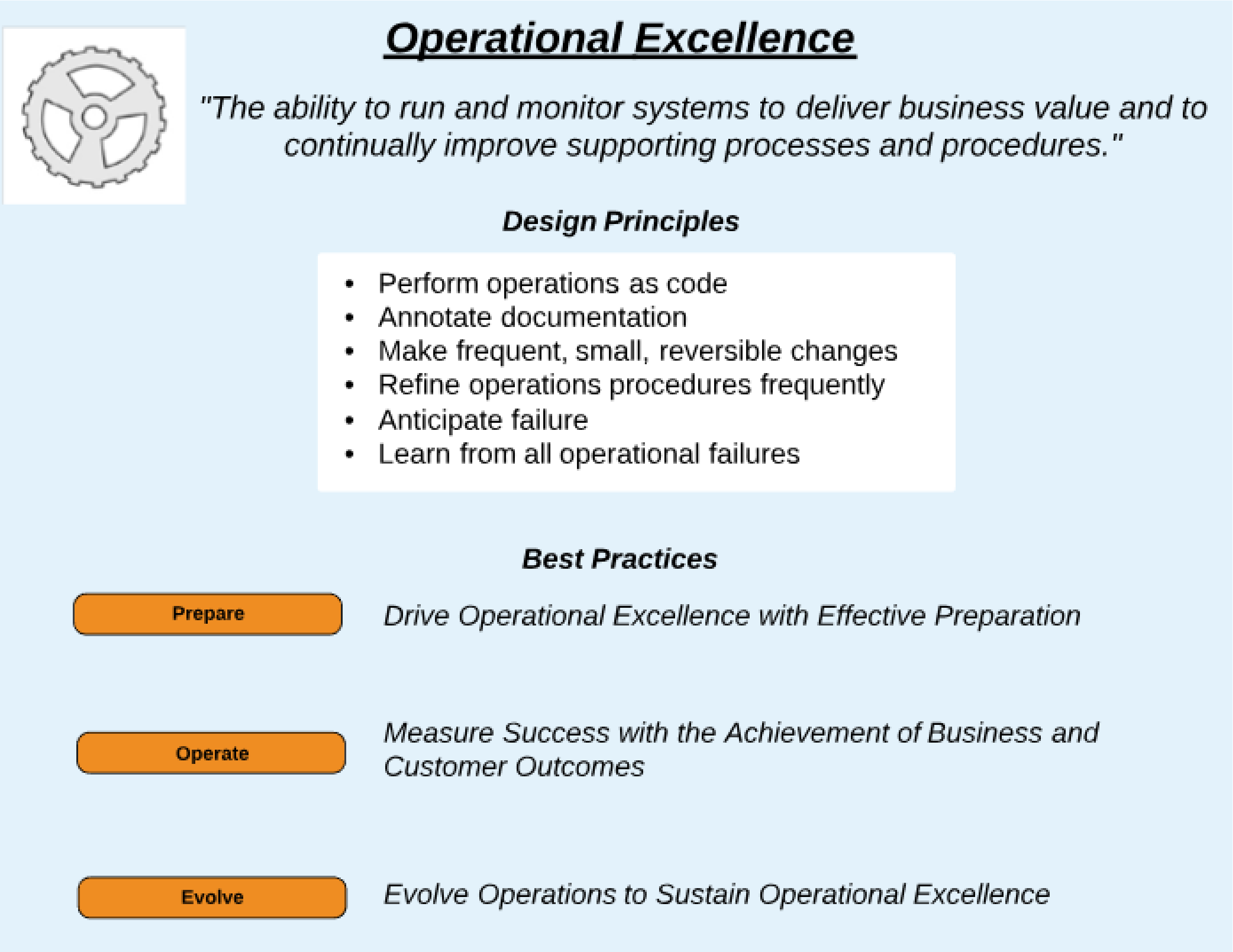
- The Well Architected Framework is a series of best practice recommendations and questions to ask when designing and developing cloud architectures.

- It consists of Five Pillars:



Operational Excellence	*Run and monitor systems to provide Business Value*
Reliability	*Recover from failure and mitigate disruptions*
Security	*Protect and Monitor Systems*
Performance Efficiency	*Use computing resources efficiently*
Cost Optimization	*Avoid or eliminate unneeded expense*

Operational Excellence



Operational Excellence

"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
- Annotate documentation
- Make frequent, small, reversible changes
- Refine operations procedures frequently
- Anticipate failure
- Learn from all operational failures

Best Practices

Prepare *Drive Operational Excellence with Effective Preparation*

Operate *Measure Success with the Achievement of Business and Customer Outcomes*

Evolve *Evolve Operations to Sustain Operational Excellence*

Prepare

Key Services

OPERATIONS AS CODE

AWS CloudFormation

LOG COLLECTION AND MONITORING

AWS Config

Amazon CloudWatch

AWS CloudTrail

flow logs

Operate

Key Services

METRICS DASHBOARDS

Amazon CloudWatch

INSIGHTS

AWS CloudTrail

flow logs

AWS X-Ray

Evolve

Key Services

ANALYZE LOG DATA

Amazon Elasticsearch

STRONG DEVOPS MODEL

AWS CodeBuild

AWS CodeCommit

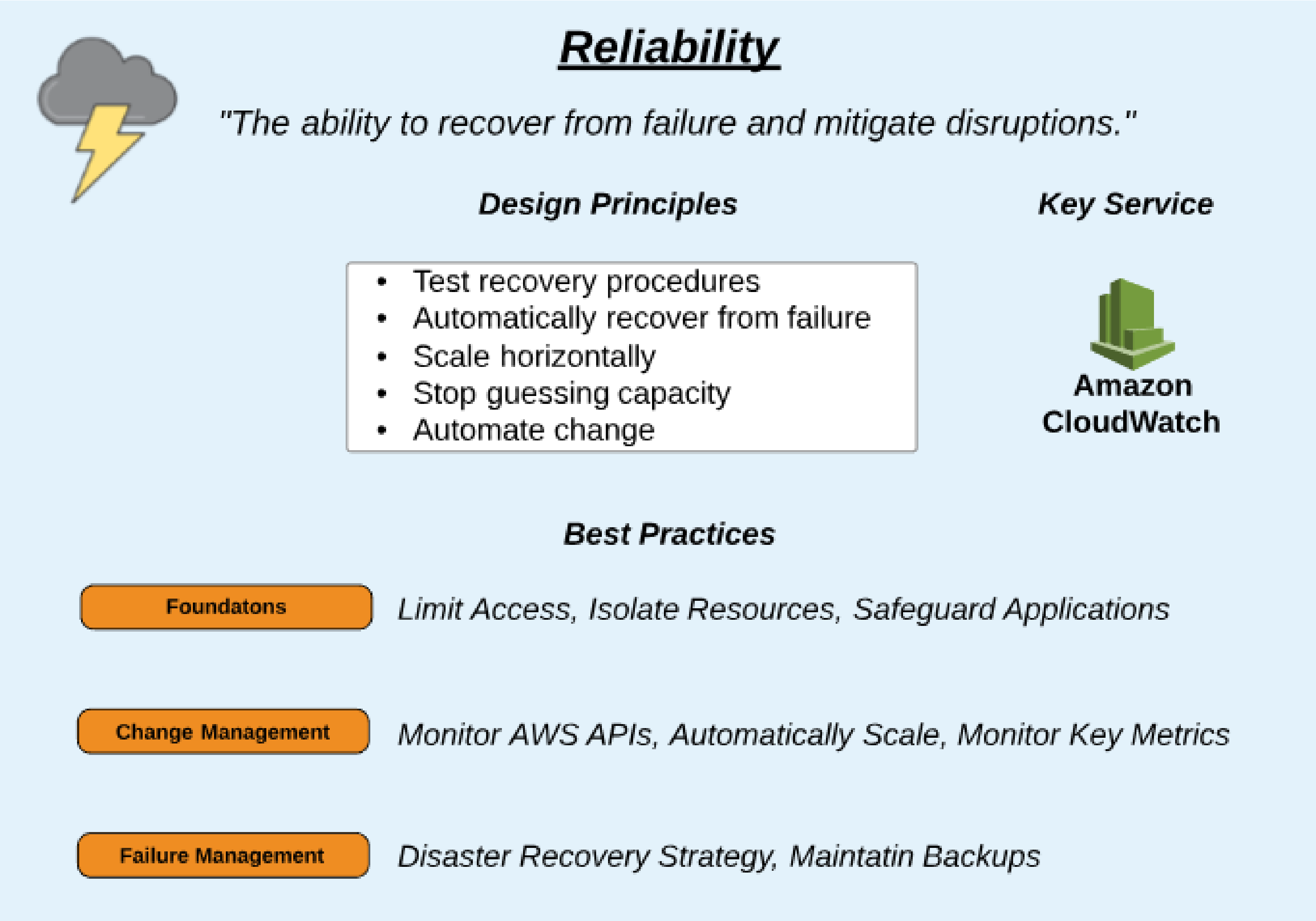
AWS CodeDeploy

AWS CodePipeline

AWS CodeStar

AWS X-Ray

Reliability



Reliability

"The ability to recover from failure and mitigate disruptions."

Design Principles

- Test recovery procedures
- Automatically recover from failure
- Scale horizontally
- Stop guessing capacity
- Automate change

Key Service

Amazon CloudWatch

Best Practices

Foundatons	*Limit Access, Isolate Resources, Safeguard Applications*
Change Management	*Monitor AWS APIs, Automatically Scale, Monitor Key Metrics*
Failure Management	*Disaster Recovery Strategy, Maintatin Backups*

Foundations

Key Services

IAM	Amazon VPC	Trusted Advisor	AWS Shield
ACCESS CONTROL	ISOLATED NETWORKS	SERVICE LIMITS	DDOS PROTECTION

Change Management

Key Services

Amazon CloudWatch	AWS Config	AWS CloudTrail	Auto Scaling
CONTROL ACCESS	CONFIGURATION AWARENESS	AUDIT AWS APIS	DEMAND MANAGEMENT

Failure Management

Key Services

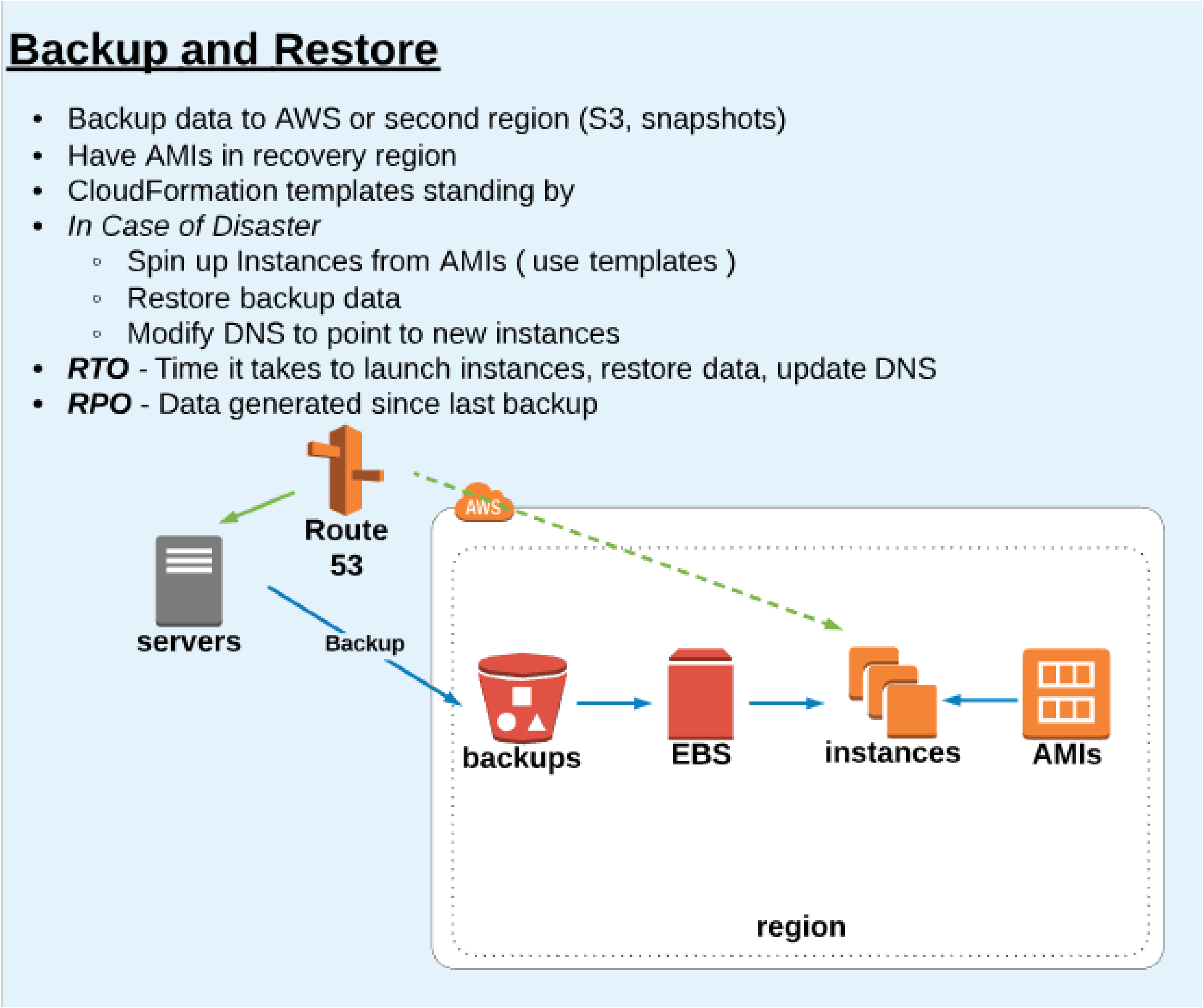
AWS CloudFormation	Amazon S3	Amazon Glacier	AWS KMS
INFRASTRUCTURE AS CODE	DURABLE BACKUPS	DURABLE ARCHIVES	RELIABLE KEY MANAGEMENT

Disaster Recovery Strategy

- RTO (Recovery Time Objective) - How long to recover
- RPO (Recovery Point Objective) - How much data is lost

Backup and Restore | **Pilot Light** | **Low Capacity Standby** | **Multi-Site Active-Active**

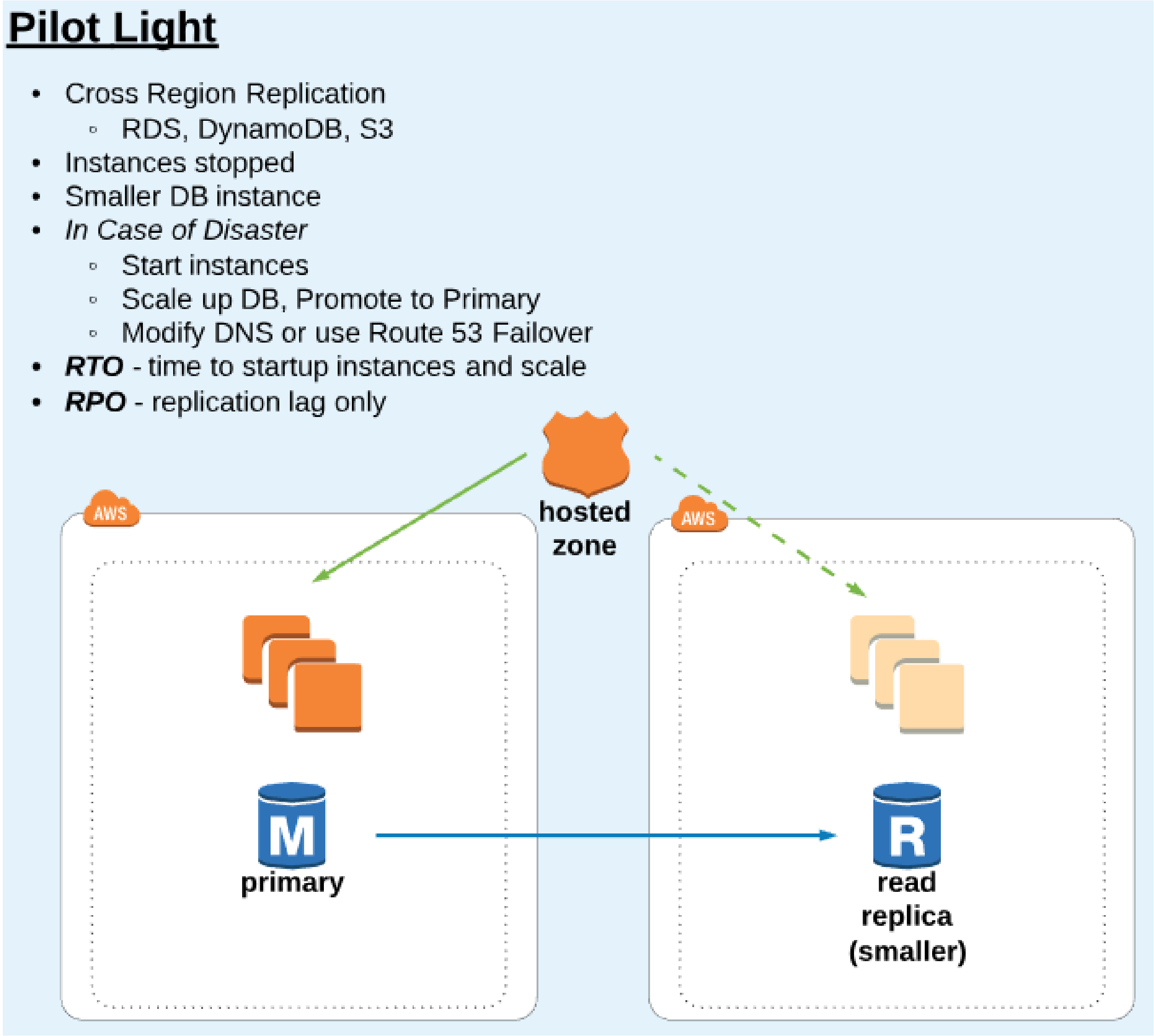
Backup and Restore



Backup and Restore

- Backup data to AWS or second region (S3, snapshots)
- Have AMIs in recovery region
- CloudFormation templates standing by
- *In Case of Disaster*
  - Spin up Instances from AMIs (use templates)
  - Restore backup data
  - Modify DNS to point to new instances
- ***RTO*** - Time it takes to launch instances, restore data, update DNS
- ***RPO*** - Data generated since last backup

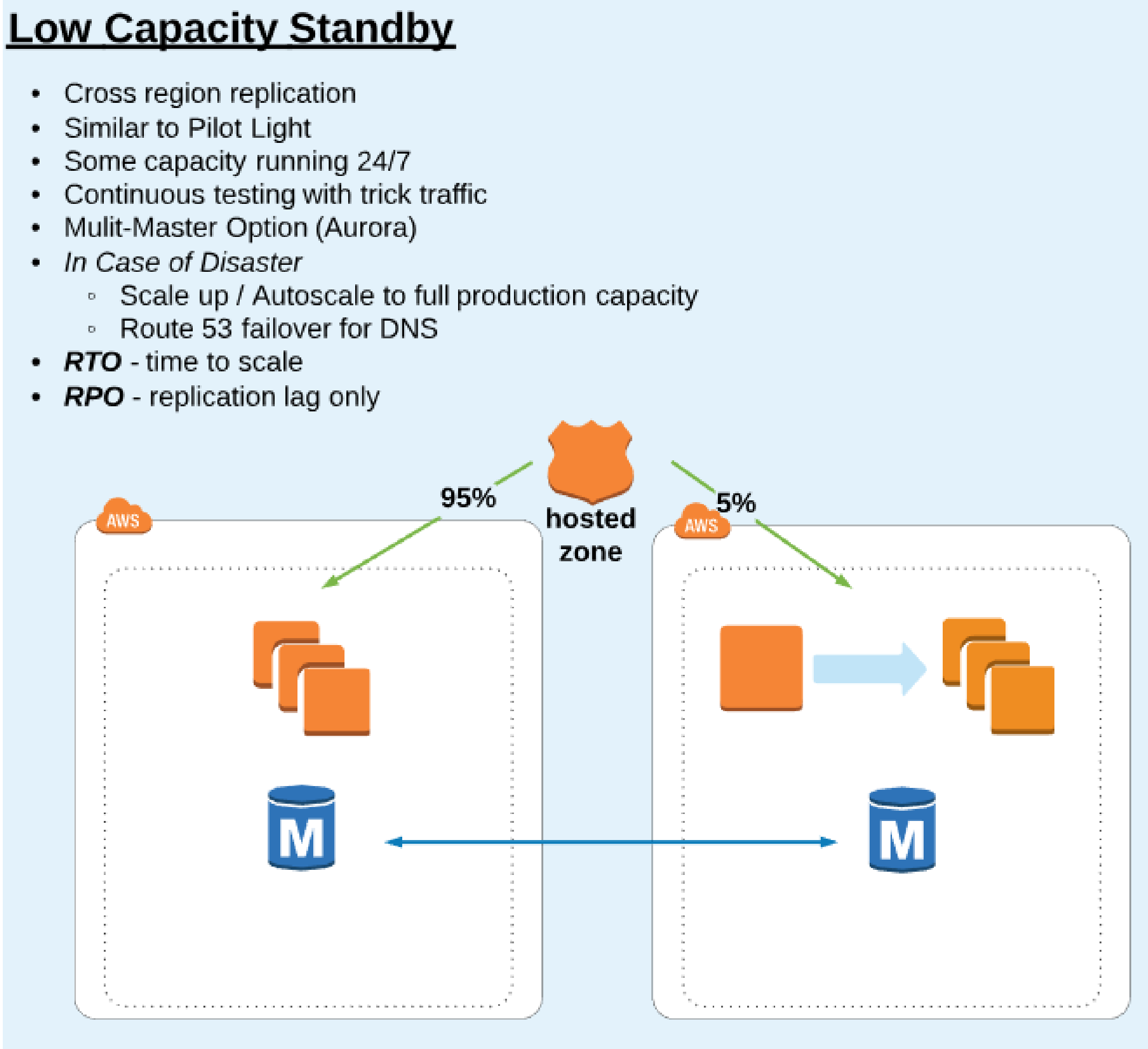
Pilot Light



Pilot Light

- Cross Region Replication
  - RDS, DynamoDB, S3
- Instances stopped
- Smaller DB instance
- *In Case of Disaster*
  - Start instances
  - Scale up DB, Promote to Primary
  - Modify DNS or use Route 53 Failover
- ***RTO*** - time to startup instances and scale
- ***RPO*** - replication lag only

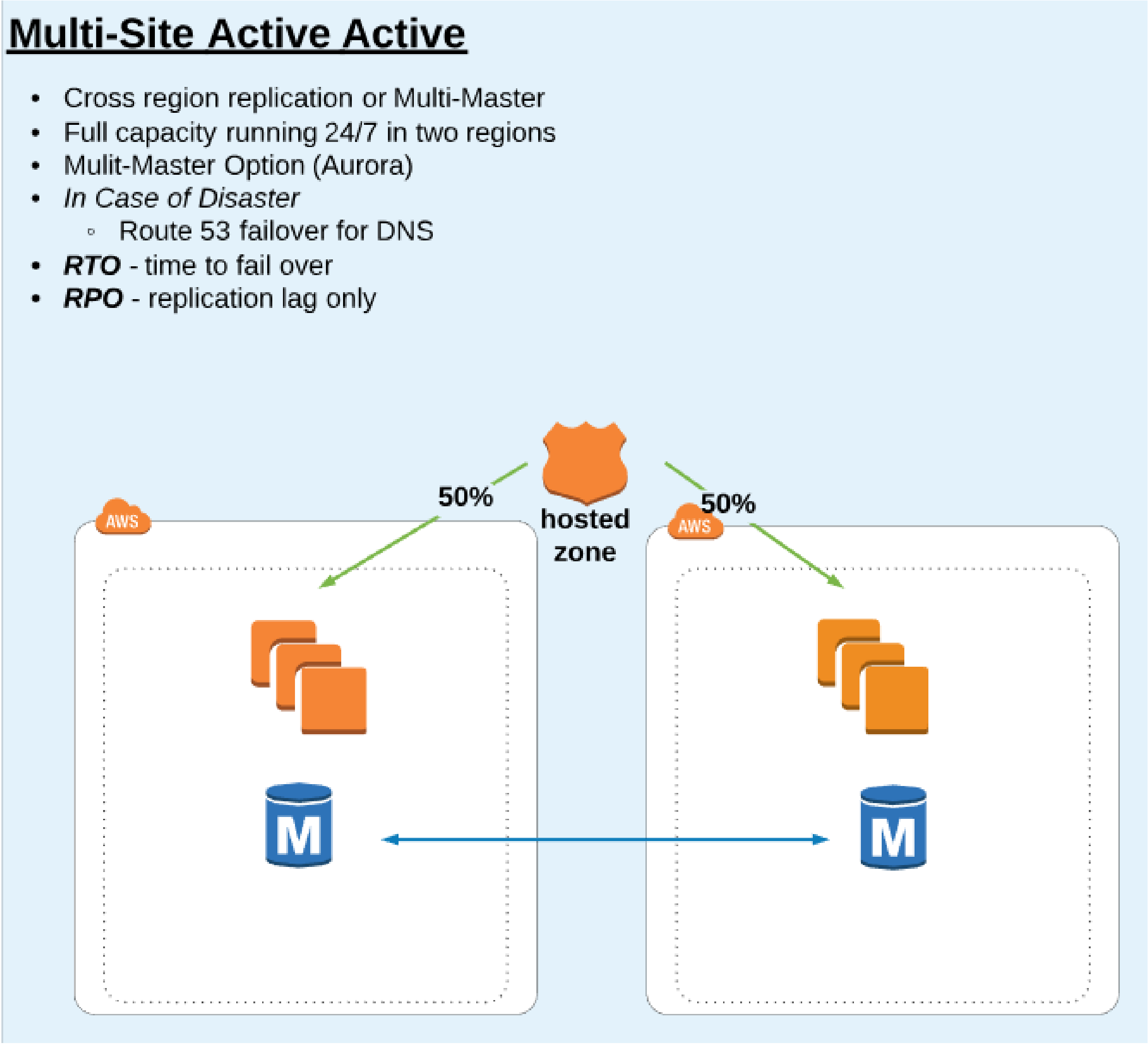
Low Capacity Standby



Low Capacity Standby

- Cross region replication
- Similar to Pilot Light
- Some capacity running 24/7
- Continuous testing with trick traffic
- Mulit-Master Option (Aurora)
- *In Case of Disaster*
  - Scale up / Autoscale to full production capacity
  - Route 53 failover for DNS
- ***RTO*** - time to scale
- ***RPO*** - replication lag only

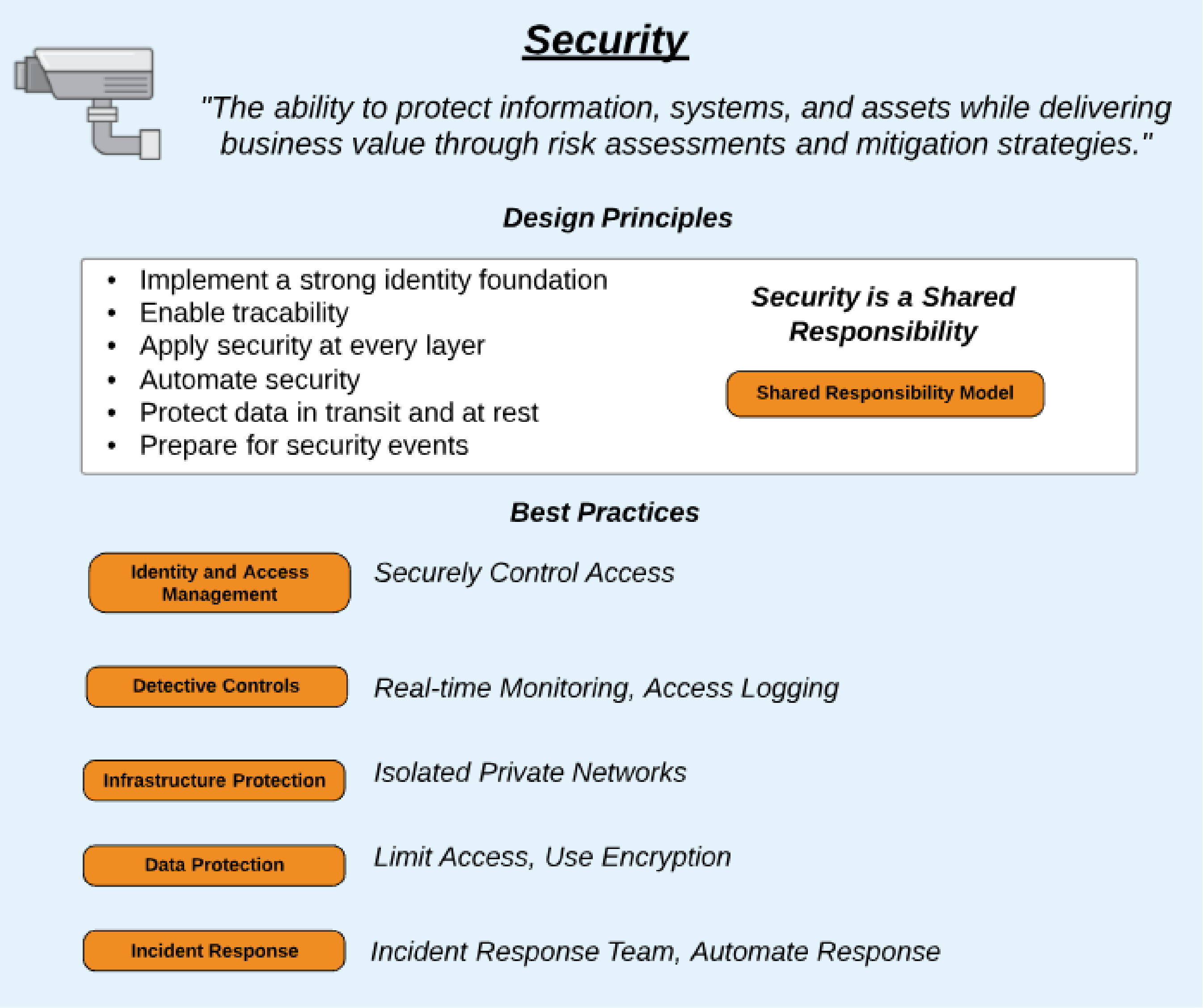
Multi-Site Active Active



Multi-Site Active Active

- Cross region replication or Multi-Master
- Full capacity running 24/7 in two regions
- Mulit-Master Option (Aurora)
- *In Case of Disaster*
  - Route 53 failover for DNS
- ***RTO*** - time to fail over
- ***RPO*** - replication lag only

Security



Security

"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
- Enable tracability
- Apply security at every layer
- Automate security
- Protect data in transit and at rest
- Prepare for security events

Security is a Shared Responsibility

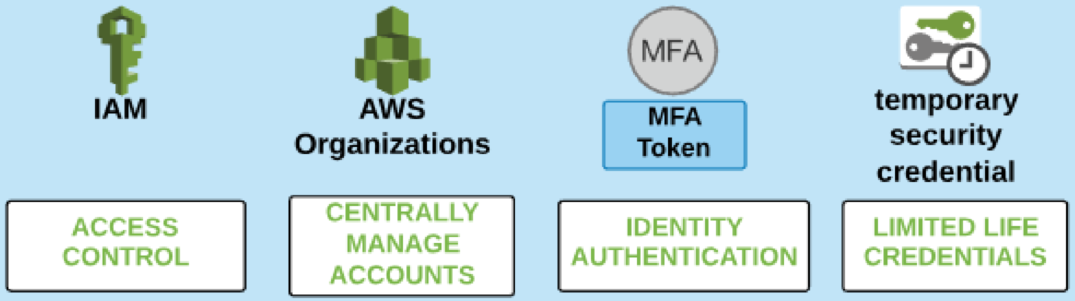
Shared Responsibility Model

Best Practices

Identity and Access Management	*Securely Control Access*
Detective Controls	*Real-time Monitoring, Access Logging*
Infrastructure Protection	*Isolated Private Networks*
Data Protection	*Limit Access, Use Encryption*
Incident Response	*Incident Response Team, Automate Response*

Identity and Access Management

Key Services



IAM

AWS Organizations

MFA Token

temporary security credential

ACCESS CONTROL

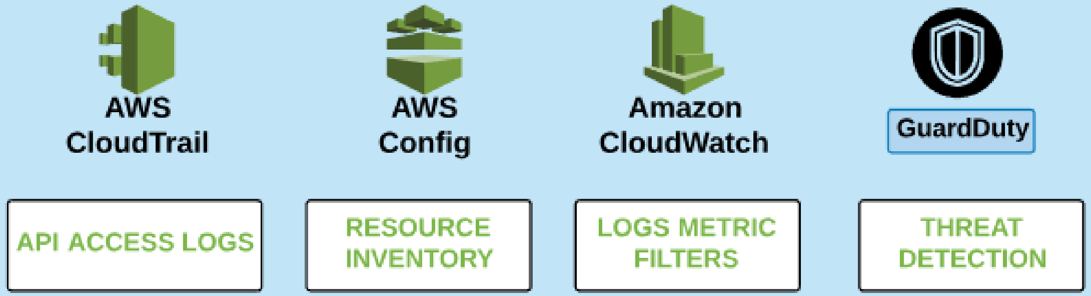
CENTRALLY MANAGE ACCOUNTS

IDENTITY AUTHENTICATION

LIMITED LIFE CREDENTIALS

Detective Controls

Key Services



AWS CloudTrail

AWS Config

Amazon CloudWatch

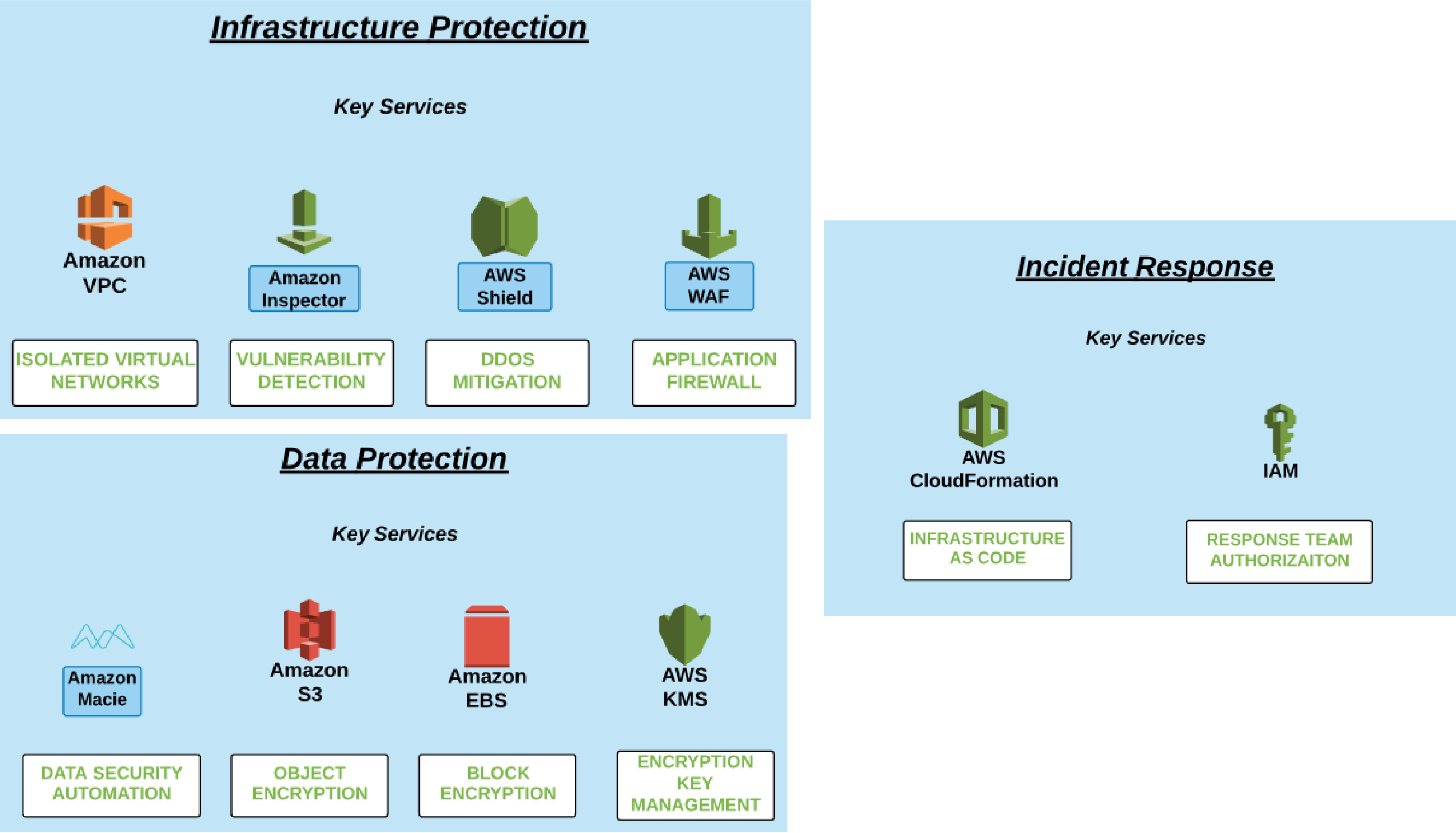
GuardDuty

API ACCESS LOGS

RESOURCE INVENTORY

LOGS METRIC FILTERS

THREAT DETECTION



Infrastructure Protection

Key Services

Amazon VPC

Amazon Inspector

AWS Shield

AWS WAF

ISOLATED VIRTUAL NETWORKS

VULNERABILITY DETECTION

DDOS MITIGATION

APPLICATION FIREWALL

Data Protection

Key Services

Amazon Macie

Amazon S3

Amazon EBS

AWS KMS

DATA SECURITY AUTOMATION

OBJECT ENCRYPTION

BLOCK ENCRYPTION

ENCRYPTION KEY MANAGEMENT

Incident Response

Key Services

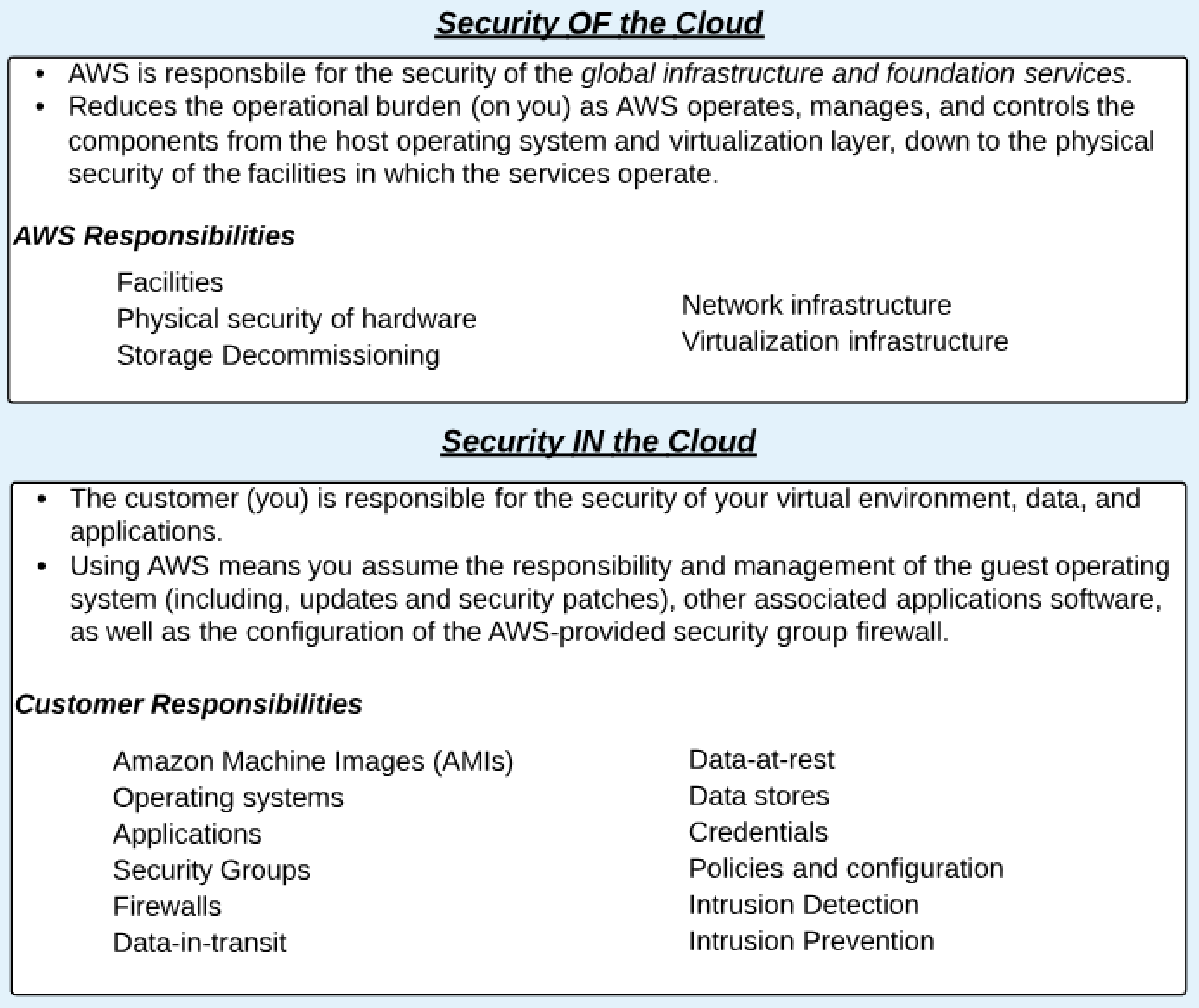
AWS CloudFormation

IAM

INFRASTRUCTURE AS CODE

RESPONSE TEAM AUTHORIZAITON

Shared Security Responsibility Model



Security OF the Cloud

- AWS is responsbile for the security of the *global infrastructure and foundation services*.
- Reduces the operational burden (on you) as AWS operates, manages, and controls the components from the host operating system and virtualization layer, down to the physical security of the facilities in which the services operate.

AWS Responsibilities

Facilities
Physical security of hardware
Storage Decommissioning

Network infrastructure
Virtualization infrastructure

Security IN the Cloud

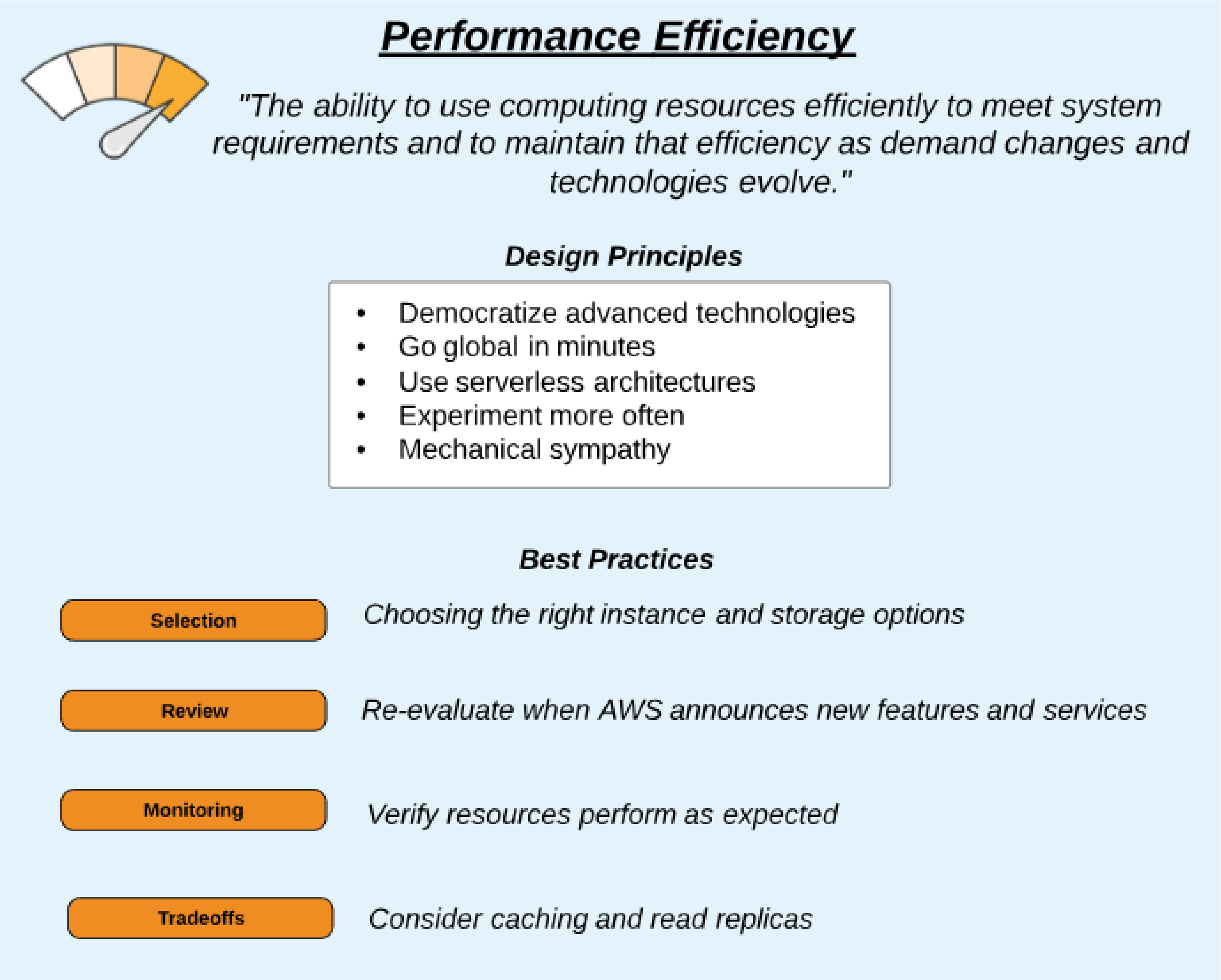
- The customer (you) is responsible for the security of your virtual environment, data, and applications.
- Using AWS means you assume the responsibility and management of the guest operating system (including, updates and security patches), other associated applications software, as well as the configuration of the AWS-provided security group firewall.

Customer Responsibilities

Amazon Machine Images (AMIs)
Operating systems
Applications
Security Groups
Firewalls
Data-in-transit

Data-at-rest
Data stores
Credentials
Policies and configuration
Intrusion Detection
Intrusion Prevention

Performance Efficiency



Performance Efficiency

"The ability to use computing resources efficiently to meet system requirements and to maintain that efficiency as demand changes and technologies evolve."

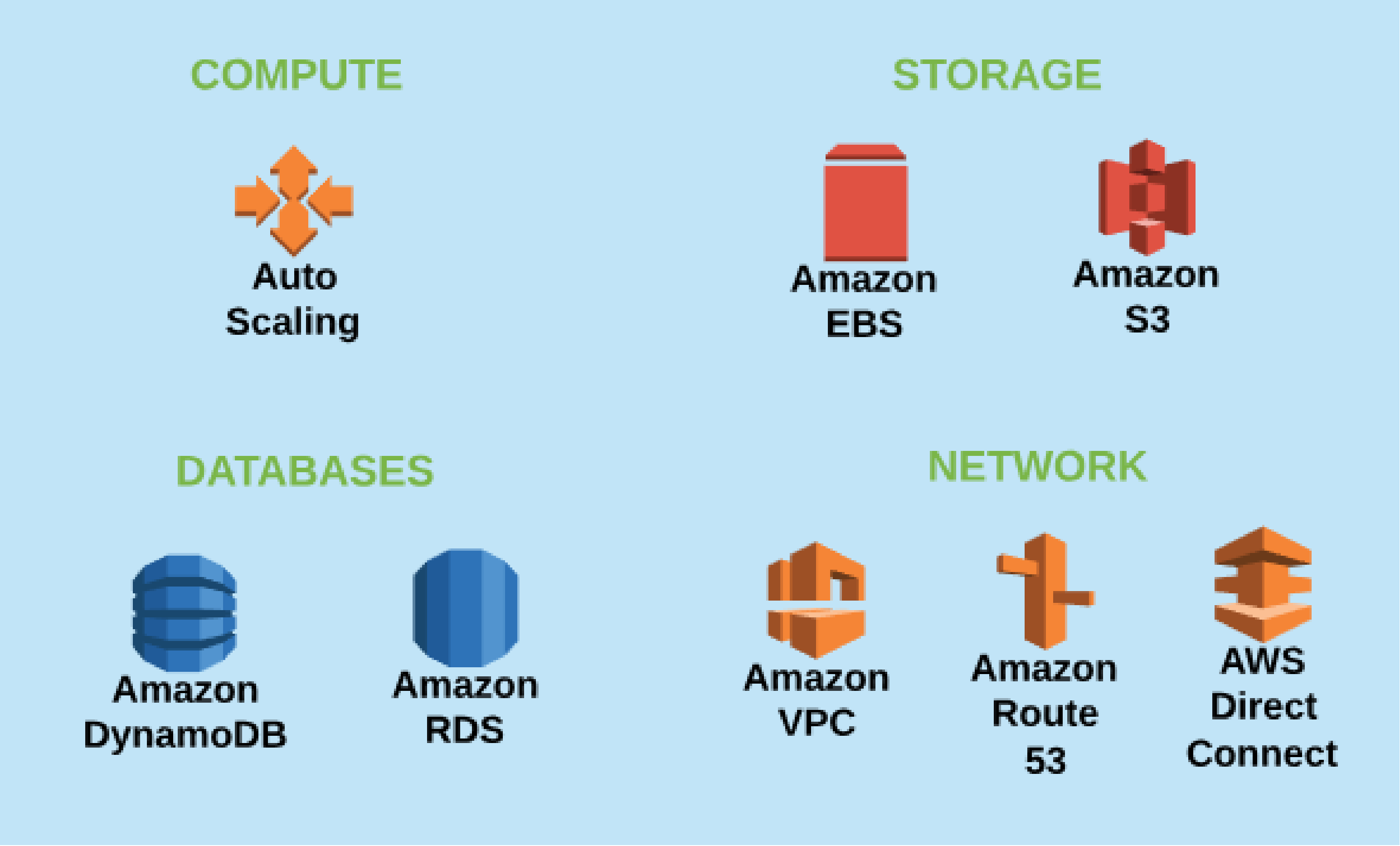
Design Principles

- Democratize advanced technologies
- Go global in minutes
- Use serverless architectures
- Experiment more often
- Mechanical sympathy

Best Practices

Selection	*Choosing the right instance and storage options*
Review	*Re-evaluate when AWS announces new features and services*
Monitoring	*Verify resources perform as expected*
Tradeoffs	*Consider caching and read replicas*

Key Services



COMPUTE

Auto Scaling

STORAGE

Amazon EBS

Amazon S3

DATABASES

Amazon DynamoDB

Amazon RDS

NETWORK

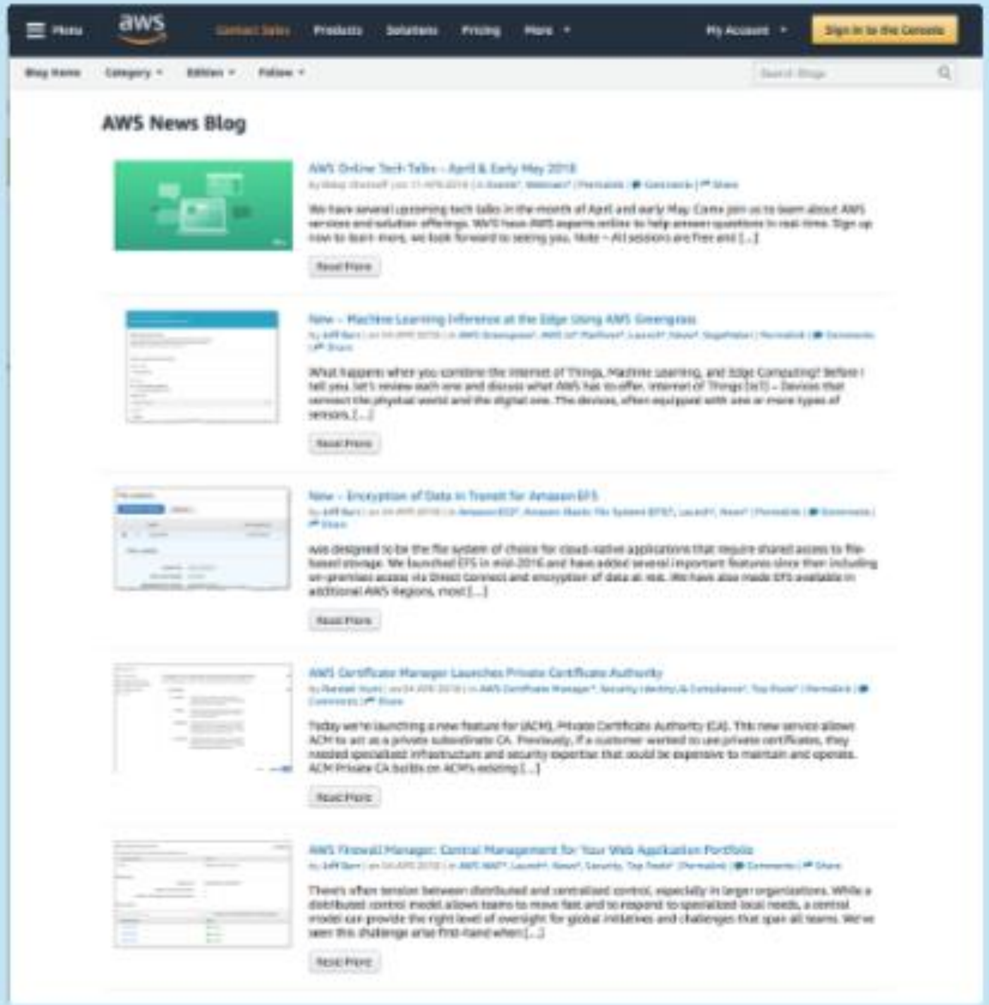
Amazon VPC

Amazon Route 53

AWS Direct Connect

Review

AWS Blog and What's New



AWS News Blog

AWS Online Tech Talks – April & Early May 2018

by [illegible] | on [illegible] | in Events*, Webinars* | Permalink | Comments | Share

We have several upcoming tech talks in the month of April and early May. Come join us to learn about AWS services and solution offerings. We'll have AWS experts online to help answer questions in real-time. Sign up now to learn more, we look forward to seeing you. Note – All sessions are free and […]

Read More

New – Machine Learning Inference at the Edge Using AWS Greengrass

by Jeff Barr | on 04 APR 2018 | in AWS Greengrass*, AWS IoT Platform*, Launch*, News*, SageMaker | Permalink | Comments | Share

What happens when you combine the Internet of Things, Machine Learning, and Edge Computing? Before I tell you, let's review each one and discuss what AWS has to offer. Internet of Things (IoT) – Devices that connect the physical world and the digital one. The devices, often equipped with one or more types of sensors, […]

Read More

New – Encryption of Data in Transit for Amazon EFS

by Jeff Barr | on 04 APR 2018 | in Amazon EC2*, Amazon Elastic File System (EFS)*, Launch*, News* | Permalink | Comments | Share

was designed to be the file system of choice for cloud-native applications that require shared access to file-based storage. We launched EFS in mid-2016 and have added several important features since then including on-premises access via Direct Connect and encryption of data at rest. We have also made EFS available in additional AWS Regions, most […]

Read More

AWS Certificate Manager Launches Private Certificate Authority

by Randall Hunt | on 04 APR 2018 | in AWS Certificate Manager*, Security, Identity, & Compliance*, Top Posts* | Permalink | Comments | Share

Today we're launching a new feature for (ACM), Private Certificate Authority (CA). This new service allows ACM to act as a private subordinate CA. Previously, if a customer wanted to use private certificates, they needed specialized infrastructure and security expertise that could be expensive to maintain and operate. ACM Private CA builds on ACM's existing […]

Read More

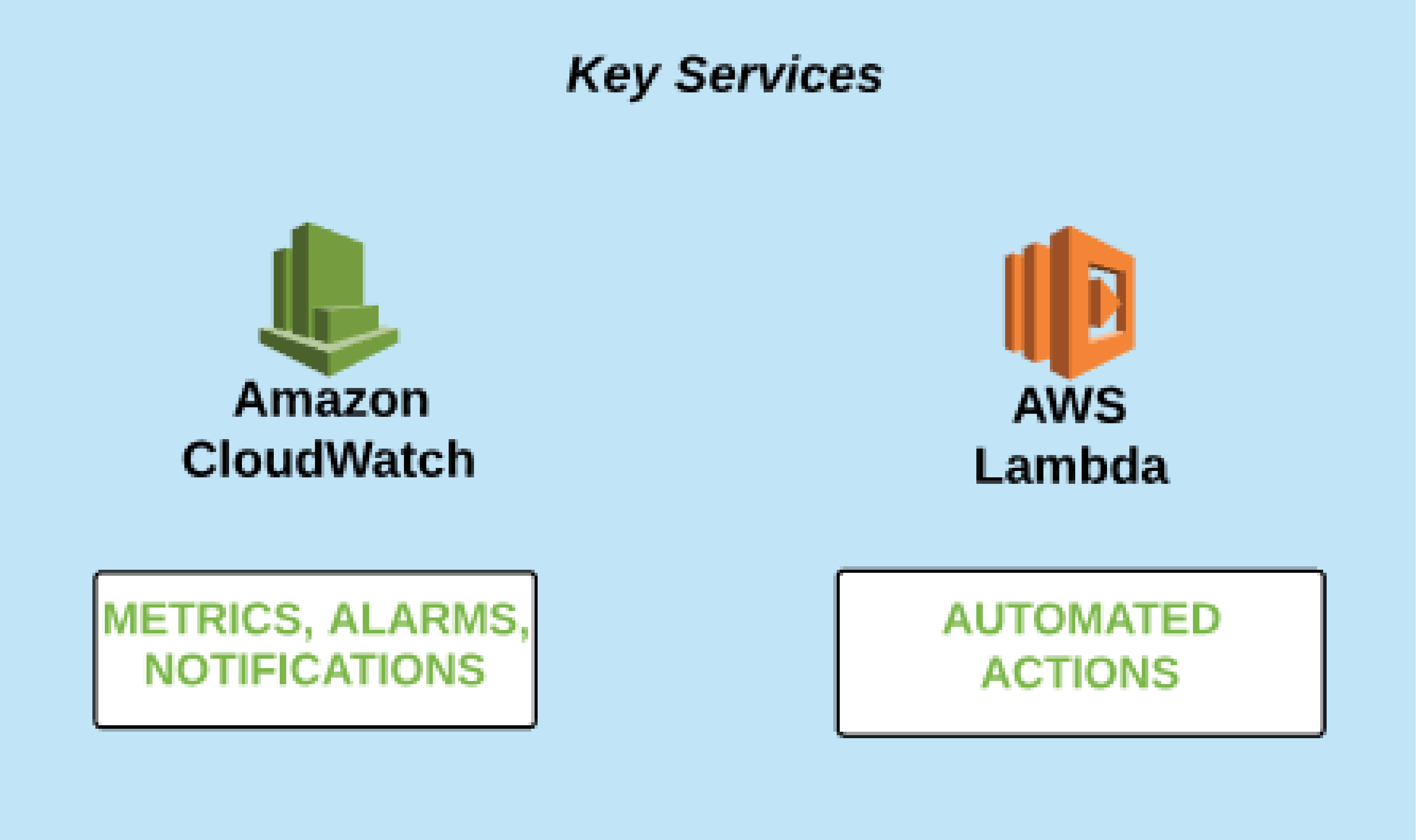
AWS Firewall Manager: Central Management for Your Web Application Portfolio

by Jeff Barr | on 04 APR 2018 | in AWS WAF*, Launch*, News*, Security, Top Posts* | Permalink | Comments | Share

There's often tension between distributed and centralized control, especially in larger organizations. While a distributed control model allows teams to move fast and to respond to specialized local needs, a central model can provide the right level of oversight for global initiatives and challenges that span all teams. We've seen this challenge arise first-hand when […]

Read More

Monitoring



Key Services

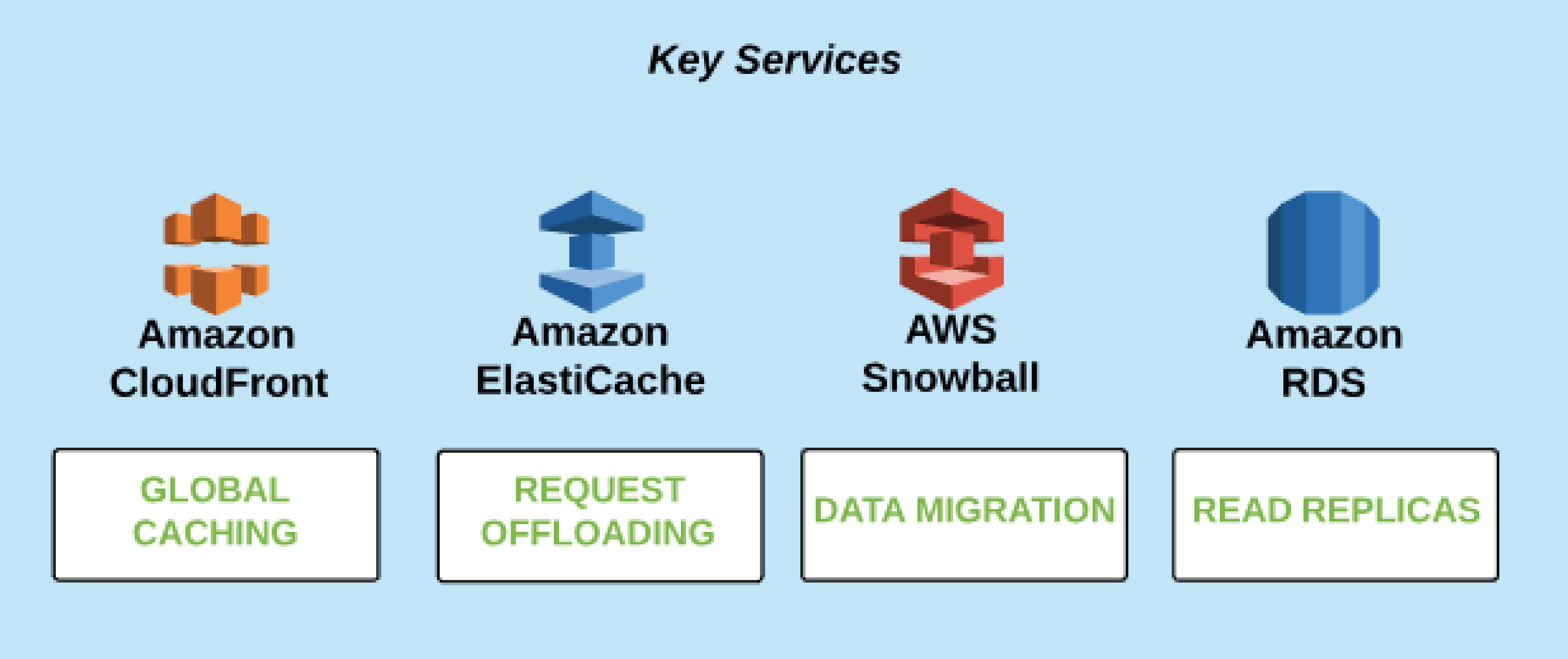
Amazon CloudWatch

METRICS, ALARMS, NOTIFICATIONS

AWS Lambda

AUTOMATED ACTIONS

Tradeoffs



Key Services

Amazon CloudFront

GLOBAL CACHING

Amazon ElastiCache

REQUEST OFFLOADING

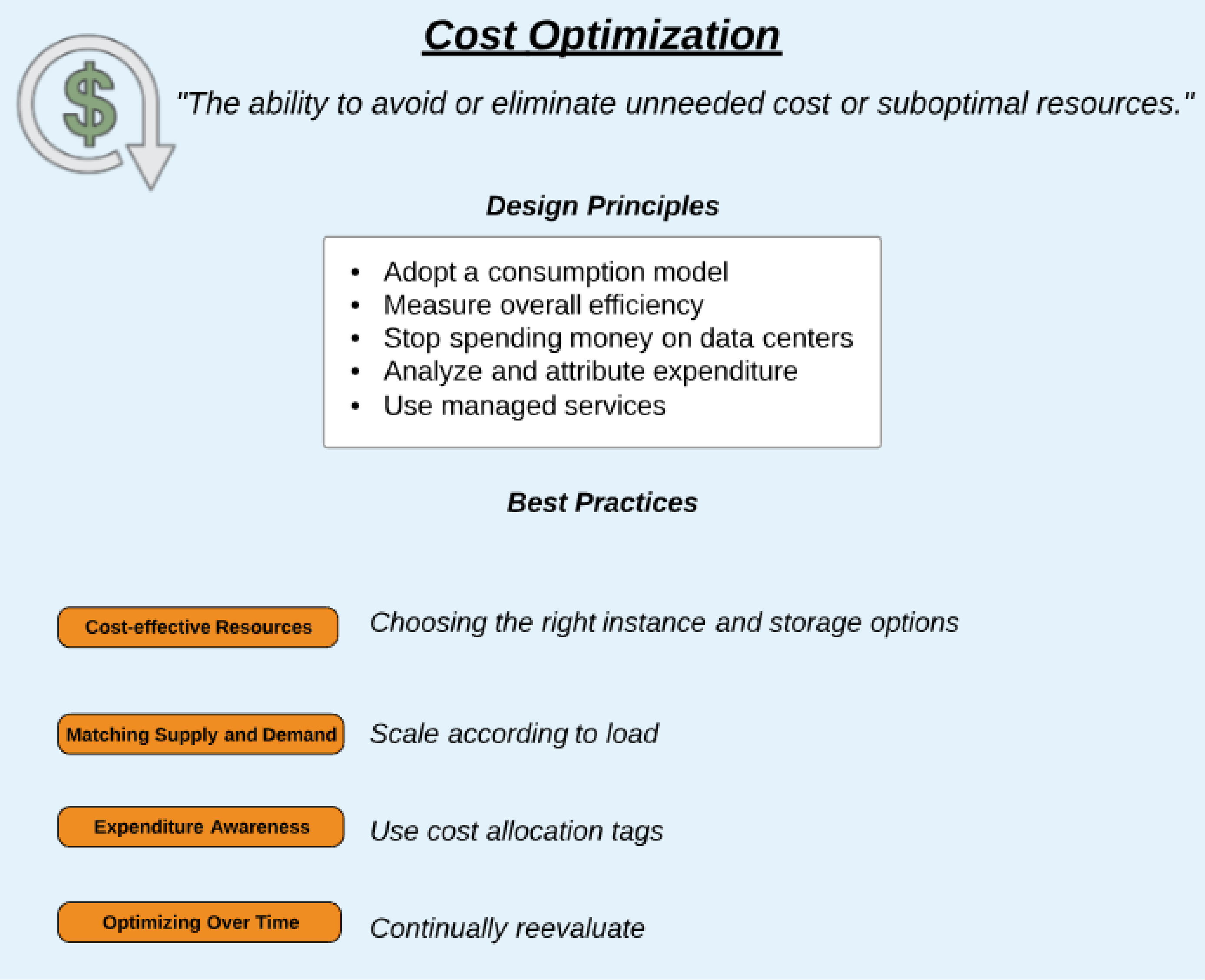
AWS Snowball

DATA MIGRATION

Amazon RDS

READ REPLICAS

Cost Optimization



Cost Optimization

"The ability to avoid or eliminate unneeded cost or suboptimal resources."

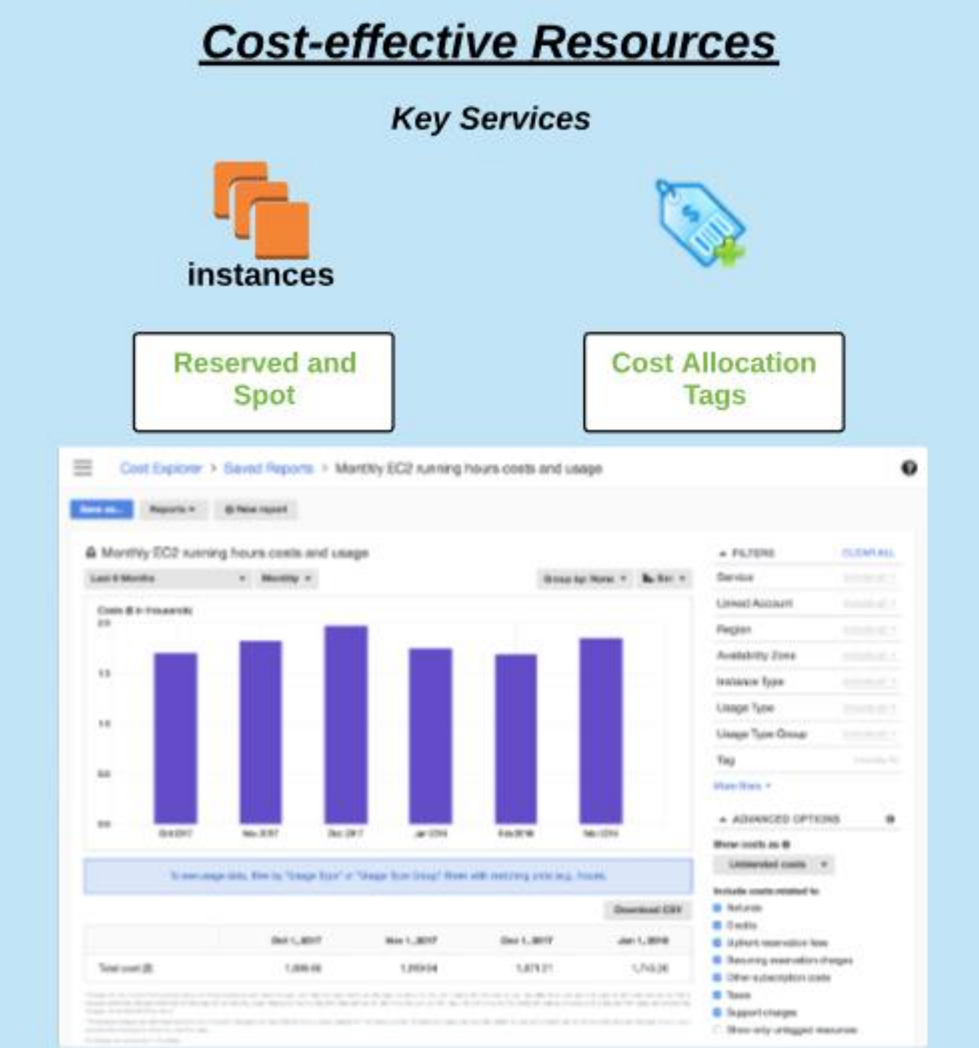
Design Principles

- Adopt a consumption model
- Measure overall efficiency
- Stop spending money on data centers
- Analyze and attribute expenditure
- Use managed services

Best Practices

Cost-effective Resources	*Choosing the right instance and storage options*
Matching Supply and Demand	*Scale according to load*
Expenditure Awareness	*Use cost allocation tags*
Optimizing Over Time	*Continually reevaluate*

Cost-Effective Resources



Cost-effective Resources

Key Services

instances

Reserved and Spot

Cost Allocation Tags

Cost Explorer > Saved Reports > Monthly EC2 running hours costs and usage

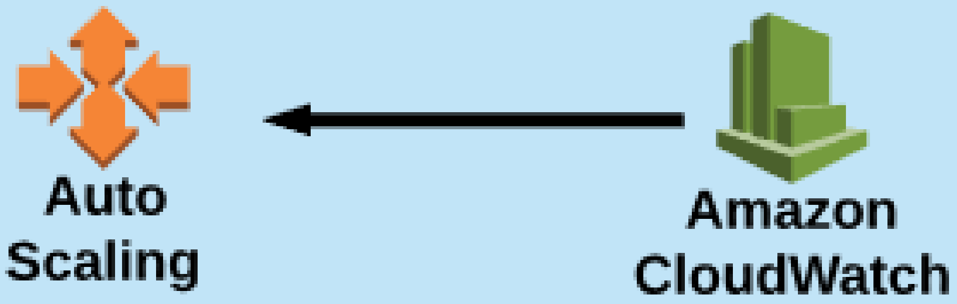
Monthly EC2 running hours costs and usage

Last 6 Months ▾ Monthly ▾

	Oct 1, 2017	Nov 1, 2017	Dec 1, 2017	Jan 1, 2018
Total cost ($)	[illegible]	[illegible]	[illegible]	[illegible]

Matched Supply and Demand

Key Services



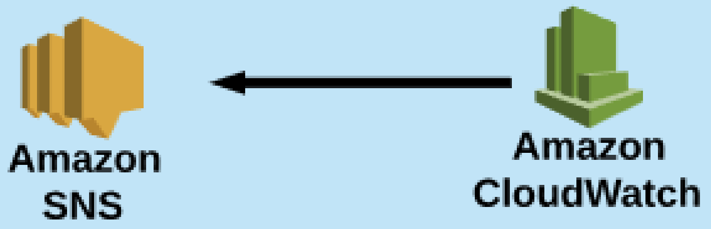
Auto Scaling

Amazon CloudWatch

Scale In when Demand Drops

Expenditure Awareness

Key Services



Amazon SNS

Amazon CloudWatch

Notification when Costs Exceed Budget

Cost Allocation Tags

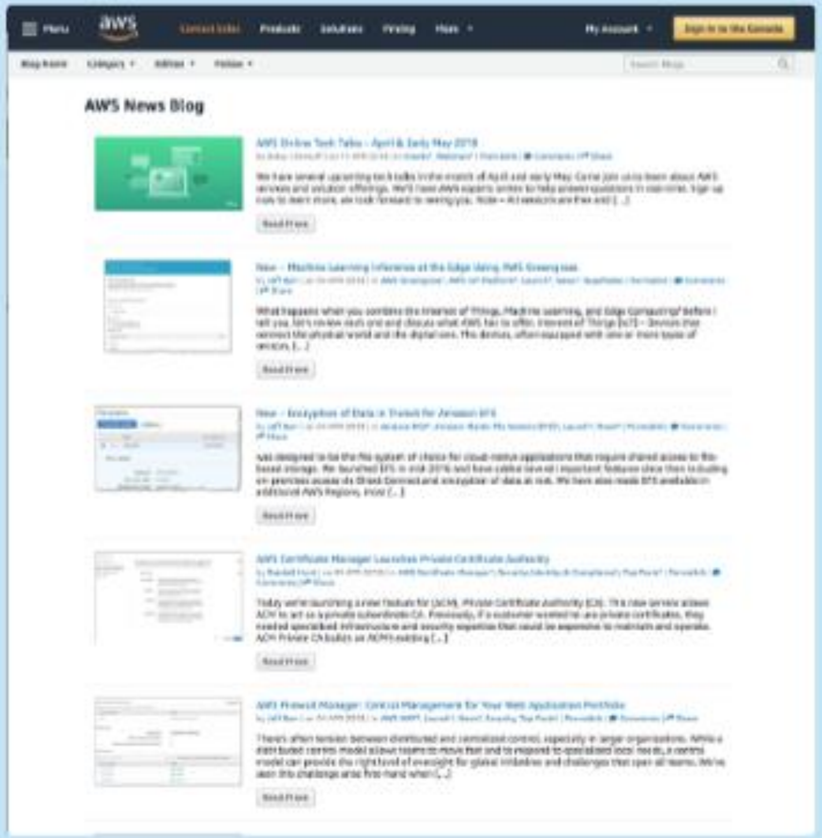
Optimizing Over Time

Optimizing Over Time

Key Services

AWS
Trusted
Advisor

Weekly Update
Email



AWS News Blog

AWS Online Tech Talks – April & Early May 2018

[illegible]

Read More

New – Machine Learning Inference at the Edge Using AWS Greengrass

What happens when you combine the Internet of Things, Machine Learning, and Edge Computing? [illegible]

Read More

New – Encryption of Data in Transit for Amazon EFS

[illegible]

Read More

AWS Certificate Manager Launches Private Certificate Authority

[illegible]

Read More

AWS Firewall Manager: Central Management for Your Web Application Portfolio

[illegible]

Read More