AWS Solutions Architect : Associate Level

Source: https://docs.aws.amazon.com/

Secure and Highly Available Architecture

Learning Objectives

By the end of the lesson, you will be able to:

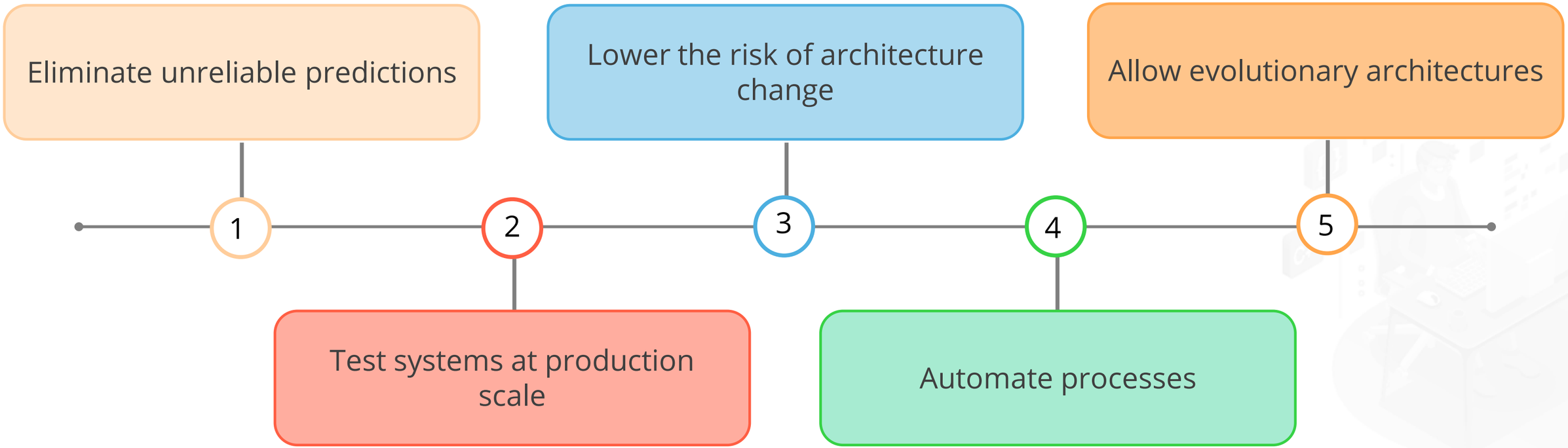
- Define AWS Well-Architected Framework
- Plan and design cloud infrastructure using the five pillars of AWS
- User AWS CLoudFormation to provision AWS resources
- Implement AWS security solutions
- Utilize Amazon recommended best practices for AWS resources

TECHNOLOGY

AWS Well-Architected Framework

AWS Well-Architected Framework

The following are the five design principles of AWS Well-Architected Framework:



Eliminate Unreliable Predictions

AWS helps users eliminate the unreliable prediction of their infrastructure capacity needs.

Users can use as much or as little capacity as they need and automatically scale up and down as required.

Test Systems at Production Scale

In traditional environments, it is difficult to test new products due to high costs or unavailability of resources.

AWS cloud allows users to create duplicate environments just for the purpose of testing.

Users can shut down the testing environments and pay only for the time they were up and running.

Lower the Risk of Architecture Change

AWS automates the creation of exact replicas of your production environments to make architecture changes as efficient as possible.

Users can backup their data while implementing architecture changes.

Automate Processes

Users can automate the creation and replication of their systems at low costs and with less effort.

Users can track the automation and audit the impact.

AWS allows the users to revert to previous parameters, if and when necessary.

Allow Evolutionary Architectures

In traditional IT environments, users are stuck with their design decisions for the lifetime of the on-premise systems.

With AWS, systems and architectures can evolve over time.

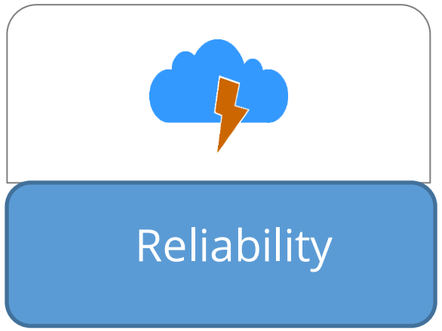
AWS allows innovations to be implemented straight away.

Five Pillars of AWS Well Architected Framework

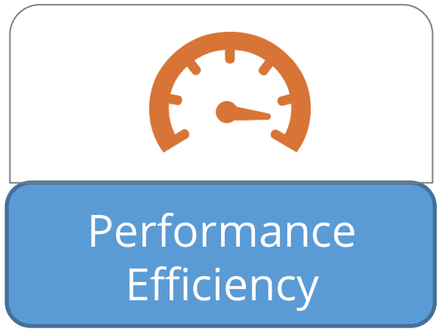
Five Pillars

The AWS Well-Architected Framework is based on the following five pillars:

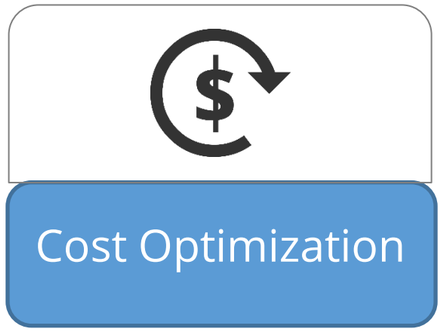
Security



Reliability



Performance Efficiency



Cost Optimization

Operational Excellence

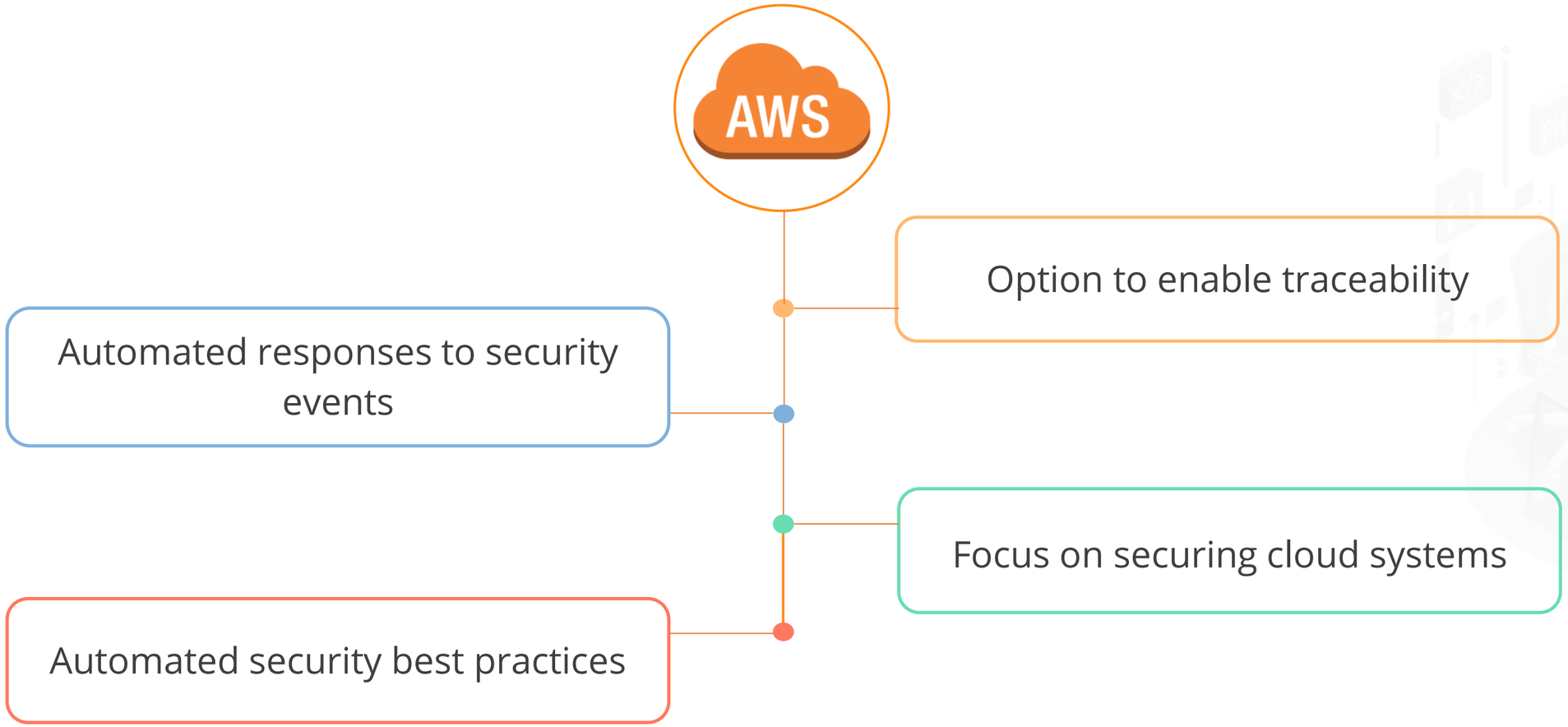
Security

The ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.

Source: aws.amazon.com

Security

AWS provides the following Security options:



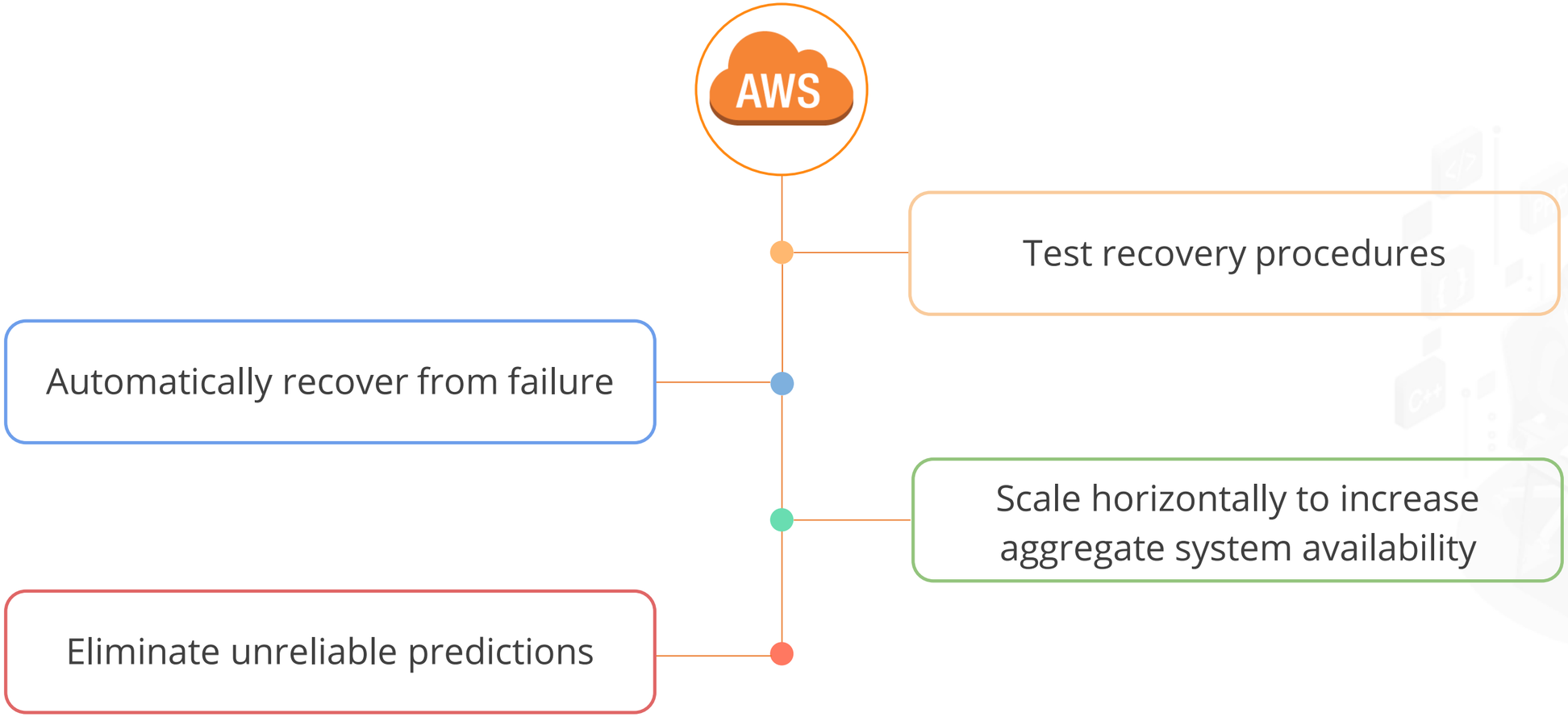
Reliability

The ability of a system to recover from infrastructure or service failures, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues.

Source: aws.amazon.com

Reliability

Reliability in the cloud allows the users to:



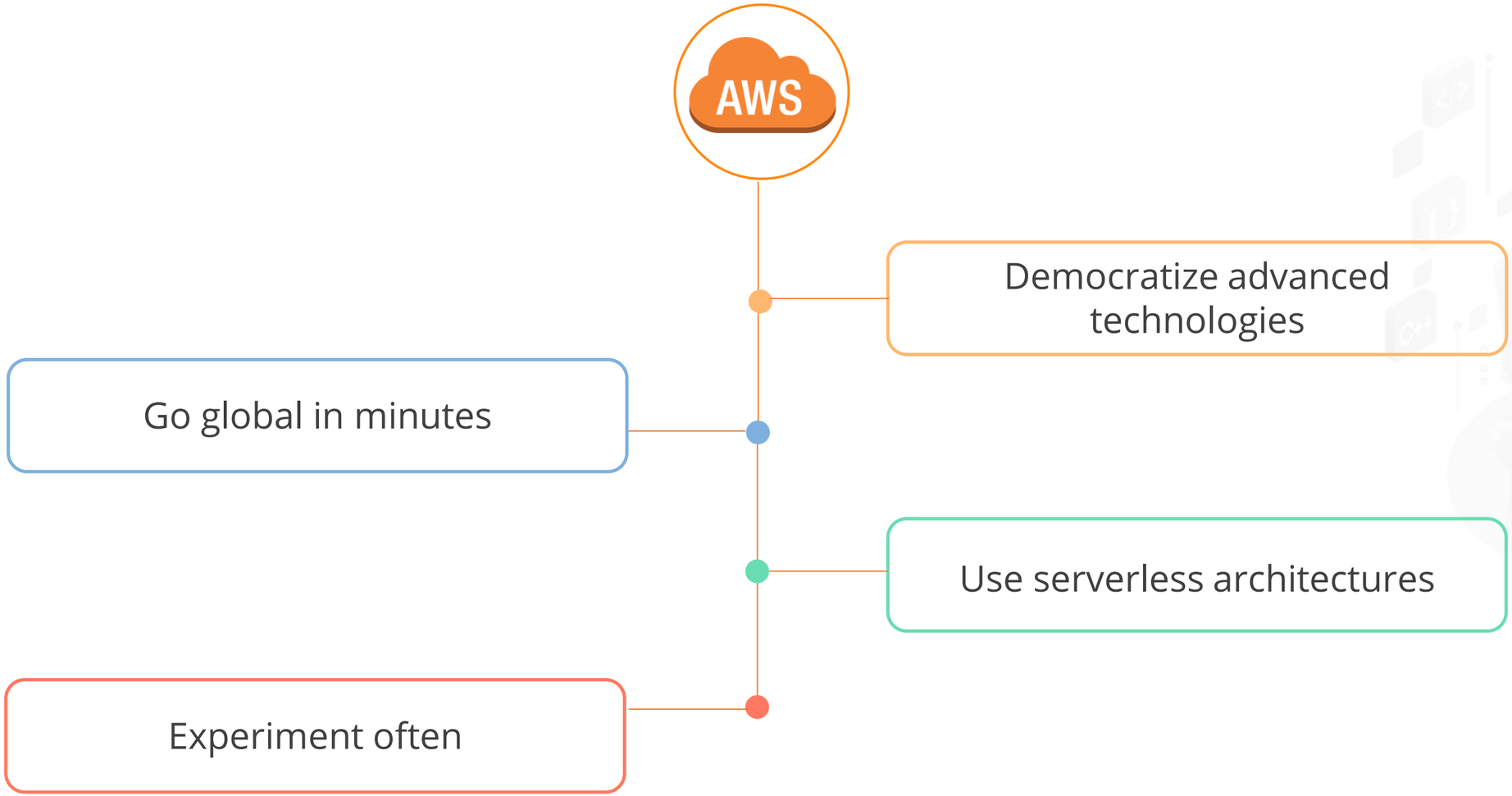
Performance Efficiency

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

Source: aws.amazon.com

Performance Efficiency

AWS provides products such as NoSQL, Media Transcoding, and Machine Learning as services, which increase Performance Efficiency and allow the users to:



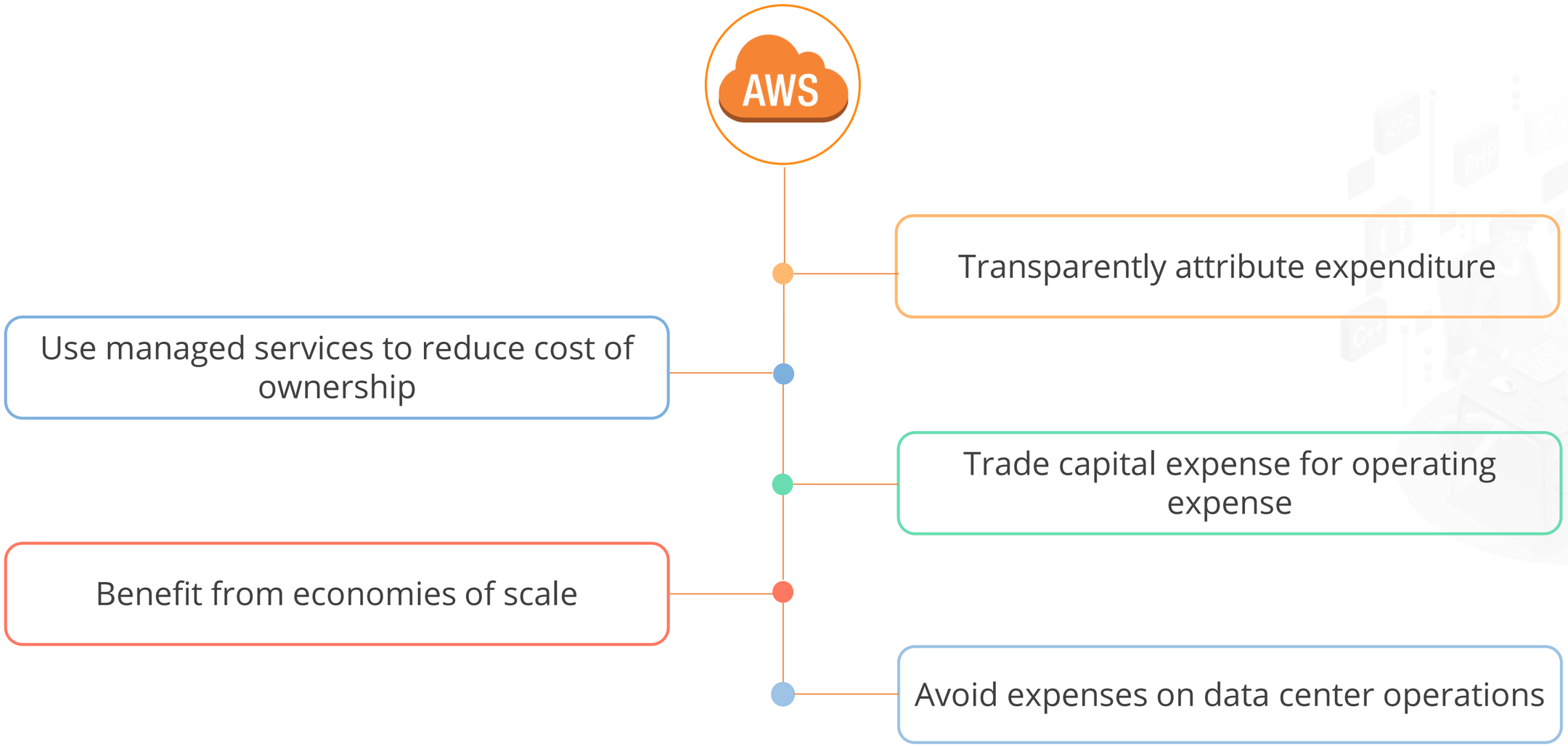
Cost Optimization

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

Source: aws.amazon.com

Cost Optimization

AWS cloud provides Cost Optimization in the following ways:

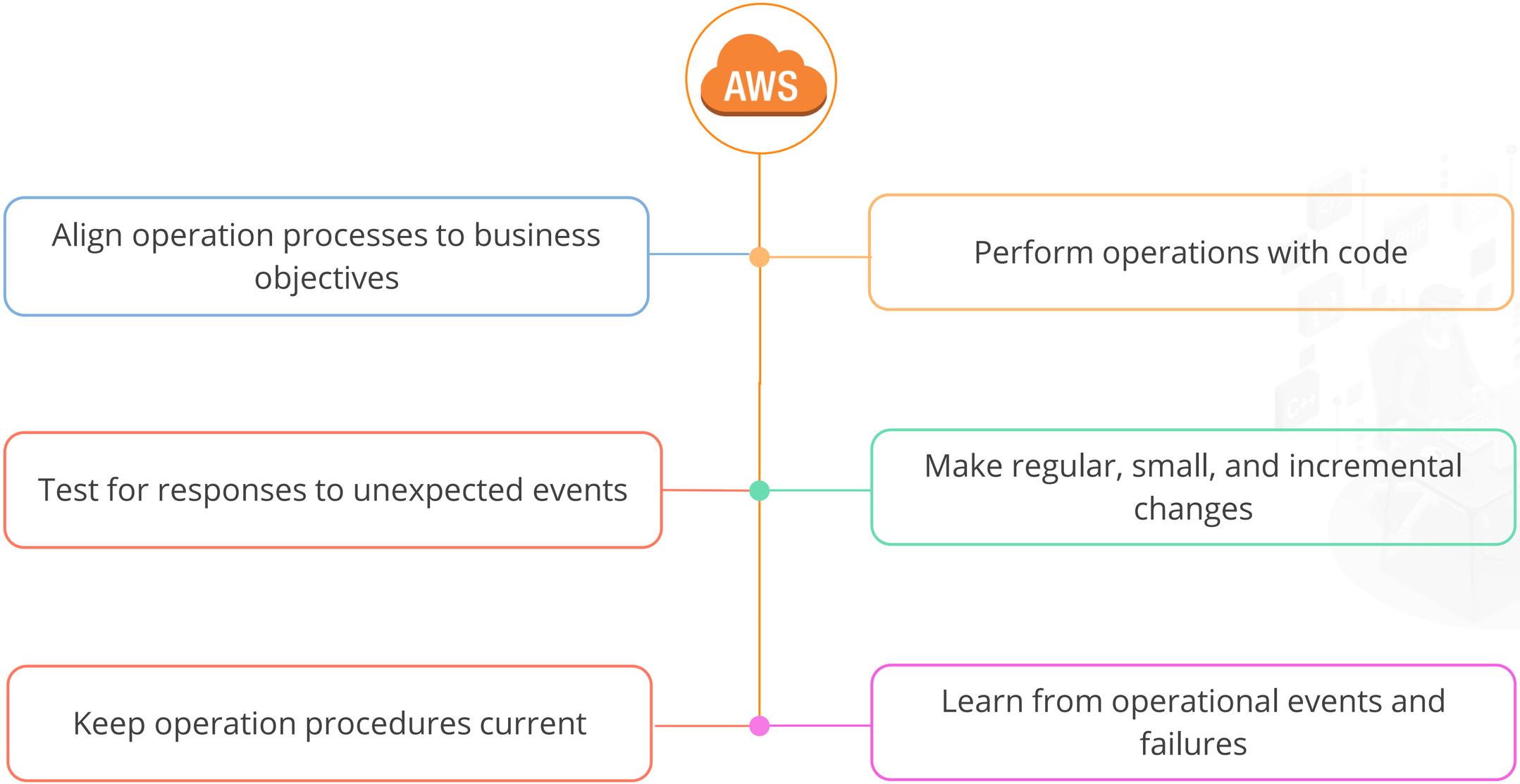


Operational Excellence

Operational practices and procedures used to manage production workloads.

Source: aws.amazon.com

Operational Excellence



TECHNOLOGY

AWS CloudFormation

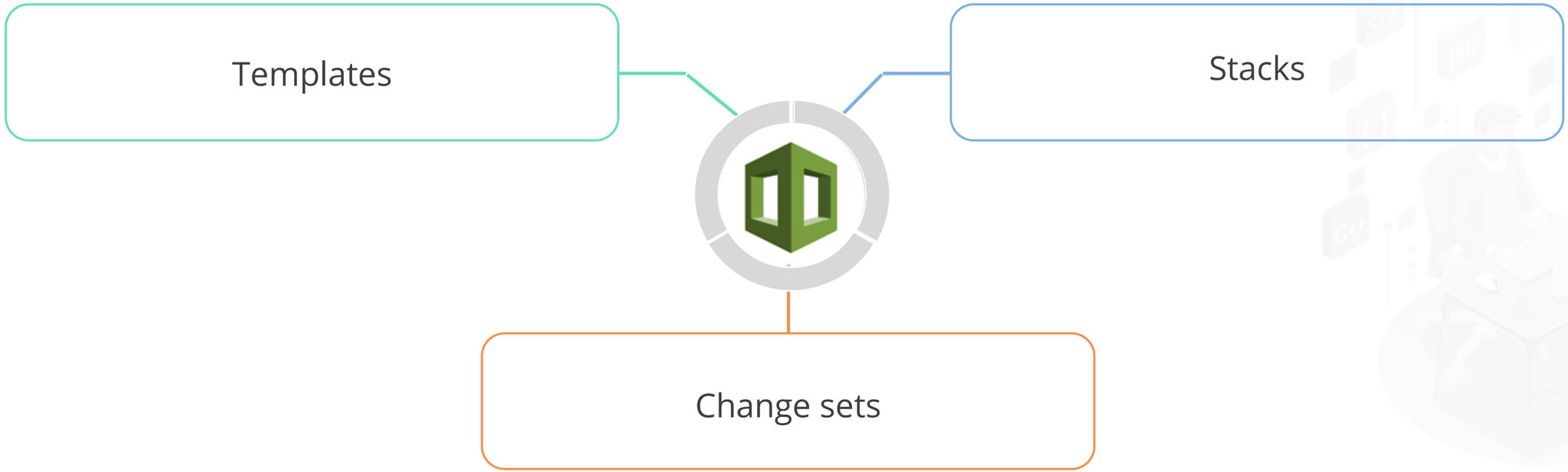
AWS CloudFormation

AWS CloudFormation helps users to set up Amazon Web Services resources so that they can spend less time managing those resources and more time focusing on the applications that run in AWS.

AWS CloudFormation

AWS CloudFormation Concepts

The following concepts are used in AWS CloudFormation:



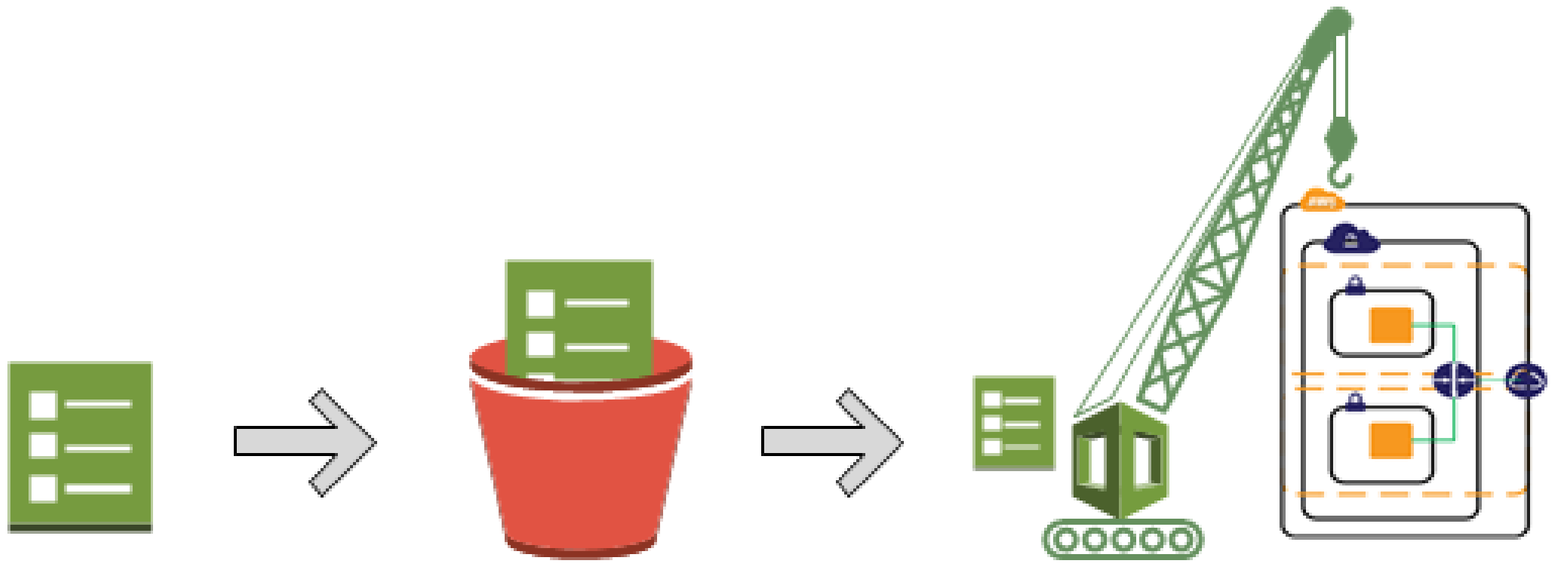
AWS CloudFormation Template

The following template provisions an instance with an **ami-0ff8a91507f77f867** AMI ID, **t2.micro** instance type, **key** key pair name, and an Amazon EBS volume.

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Description" : "A sample template",
  "Resources" : {
    "MyEC2Instance" : {
      "Type" : "AWS::EC2::Instance",
      "Properties" : {
        "ImageId" : "ami-0ff8a91507f77f867",
        "InstanceType" : "t2.micro",
        "KeyName" : "key",
        "BlockDeviceMappings" : [
          {
            "DeviceName" : "/dev/sdm",
            "Ebs" : {
              "VolumeType" : "io1",
              "Iops" : "200",
              "DeleteOnTermination" : "false",
              "VolumeSize" : "20"
            } } ] } }
              }
      }
```

Working of CloudFormation

When users create a stack, AWS CloudFormation makes underlying service calls to AWS to provision and configure the resources.



CloudFormation Template

Template saved in S3 bucket

AWS CloudFormation

Source: aws.amazon.com

Create an Amazon EC2 Instance Using AWS CLoudFormation

Duration: 10 min.

Problem Statement:

You are given a project to create an Amazon EC2 instance using AWS CloudFormation.

ASSISTED PRACTICE

Assisted Practice: Guidelines to Create an Amazon EC2 Instance Using AWS CLoudFormation

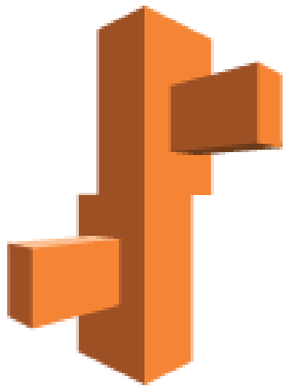
Steps to perform:

1. Go to your Amazon Console
2. Open the CloudFormation console
3. Create a new stack
4. Fill in the required information about the stack
5. Skip to the review page and click on the Create stack button

AWS Elastic Beanstalk

AWS Elastic Beanstalk

AWS Elastic Beanstalk is used to deploy and manage applications in the AWS cloud without having to learn about the infrastructure that runs those applications.



AWS Elastic Beanstalk

AWS Elastic Beanstalk Concepts

The following concepts are used in AWS Elastic Beanstalk:

01	02	03	04
Application	**Application version**	**Environment**	**Environment tier**

It is a logical collection of Elastic Beanstalk components. In Elastic Beanstalk, an application is conceptually similar to a folder.

AWS Elastic Beanstalk Concepts

The following concepts are used in AWS Elastic Beanstalk:

01	02	03	04
Application	Application version	Environment	Environment tier

It refers to a specific, labeled iteration of deployable code for a web application. An application version points to an Amazon S3 object that contains the deployable code.

AWS Elastic Beanstalk Concepts

The following concepts are used in AWS Elastic Beanstalk:

01	02	03	04
Application	Application version	Environment	Environment tier

It is a collection of AWS resources running an application version. Each environment runs only one application version at a time.

AWS Elastic Beanstalk Concepts

The following concepts are used in AWS Elastic Beanstalk:

01	02	03	04
Application	**Application version**	**Environment**	**Environment tier**

It designates the type of application that the environment runs and determines what resources Elastic Beanstalk provisions to support it.

AWS Elastic Beanstalk Concepts

The following concepts are used in AWS Elastic Beanstalk:

05	06	07
Environment configuration	**Saved configuration**	**Platform**

It identifies a collection of parameters and settings that define how an environment and its associated resources behave.

AWS Elastic Beanstalk Concepts

The following concepts are used in AWS Elastic Beanstalk:

05	06	07
Environment configuration	**Saved configuration**	**Platform**

It is a template that can be used as a starting point for creating unique environment configurations.

AWS Elastic Beanstalk Concepts

The following concepts are used in AWS Elastic Beanstalk:

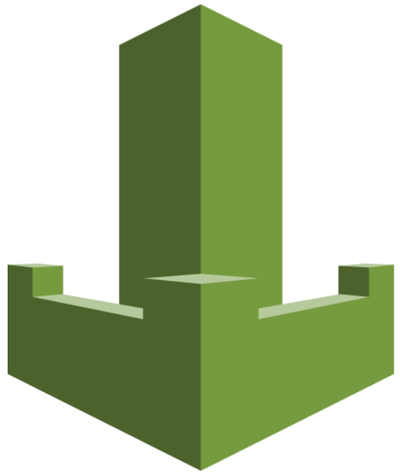
05	06	07
Environment configuration	**Saved configuration**	**Platform**

It is a combination of an operating system, programming language runtime, web server, application server, and Elastic Beanstalk components.

AWS WAF and AWS Shield

What Is AWS WAF?

AWS WAF is a web application firewall that lets users monitor the HTTP and HTTPS requests that are forwarded to an Amazon CloudFront distribution, an Amazon API Gateway REST API, or an Application Load Balancer.



AWS WAF

AWS WAF

AWS WAF enables users to:

01	Allow all the requests except the ones that they specify
02	Block all the requests except the ones that they specify
03	Count the requests that match the properties that they specify

Benefits of AWS WAF

The following are the benefits of AWS WAF:

01	Additional protection against web attacks using conditions
02	Real-time metrics and sampled web requests
03	Automated administration using the AWS WAF API

What Is AWS Shield?

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency.

AWS Shield

Benefits of AWS Shield

The following are some of the benefits of AWS Shield:

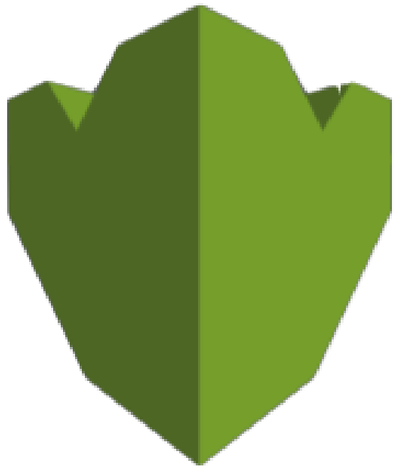
01	Seamless integration and deployment
02	Customizable protection
03	Managed protection and attack visibility
04	Cost efficiency

TECHNOLOGY

AWS Key Management Service

AWS Key Management Service

AWS Key Management Service (AWS KMS) is a managed service that enables users to create and control customer master keys (CMKs), the encryption keys used to encrypt the data.



AWS Key Management Service

AWS KMS Concepts

The following are the concepts used in AWS KMS:

01 **Data keys**

02 **Aliases**

03 **Cryptographic operations**

04 **Key identifiers (KeyId)**

05 **Key material origin**

06 **Key spec**

07 **Key usage**

AWS KMS Concepts

The following are the concepts used in AWS KMS:

08 **Envelope encryption**

09 **Encryption context**

10 **Key policies**

11 **Grants**

12 **Grant tokens**

AWS Best Practices

AWS Best Practices

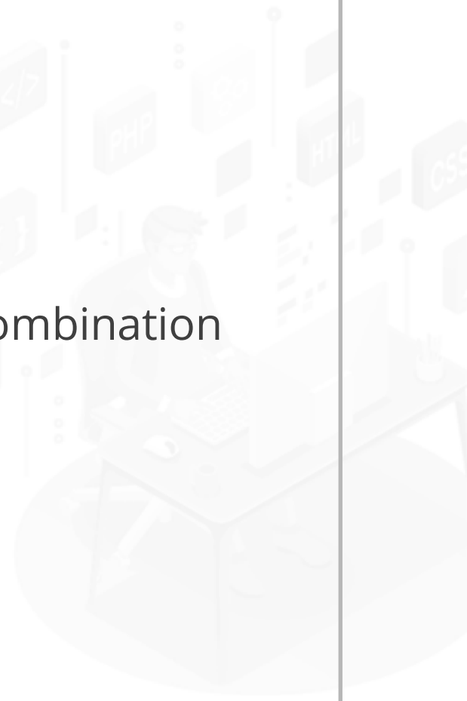
Amazon recommends certain best practices for their services to ensure that users leverage the most out of the Amazon Web Services.

AWS Best Practices

The following are the best practices to help secure the Amazon Web Services:

- Strong password
- Group email alias
- Multi-factor authentication
- Users and roles for access
- Access Keys

AWS recommends creating a strong password with a combination of letters, numbers, and special characters.



AWS Best Practices

The following are the best practices to help secure the Amazon Web Services:

- Strong password
- Group email alias
- Multi-factor authentication
- Users and roles for access
- Access Keys

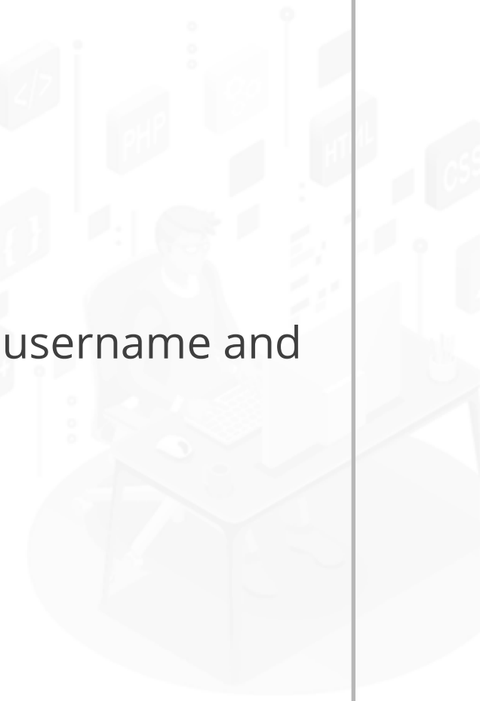
It enables users to add multiple trusted members to manage the AWS account in the absence of the root user.

AWS Best Practices

The following are the best practices to help secure the Amazon Web Services:

- Strong password
- Group email alias
- Multi-factor authentication
- Users and roles for access
- Access Keys

It provides an extra layer of authentication on top of the username and password.



AWS Best Practices

The following are the best practices to help secure the Amazon Web Services:

- Strong password
- Group email alias
- Multi-factor authentication
- Users and roles for access
- Access Keys

IAM users and roles allow users to keep track of their AWS resources. It determines who has access to the AWS resources and up to what extent.

AWS Best Practices

The following are the best practices to help secure the Amazon Web Services:

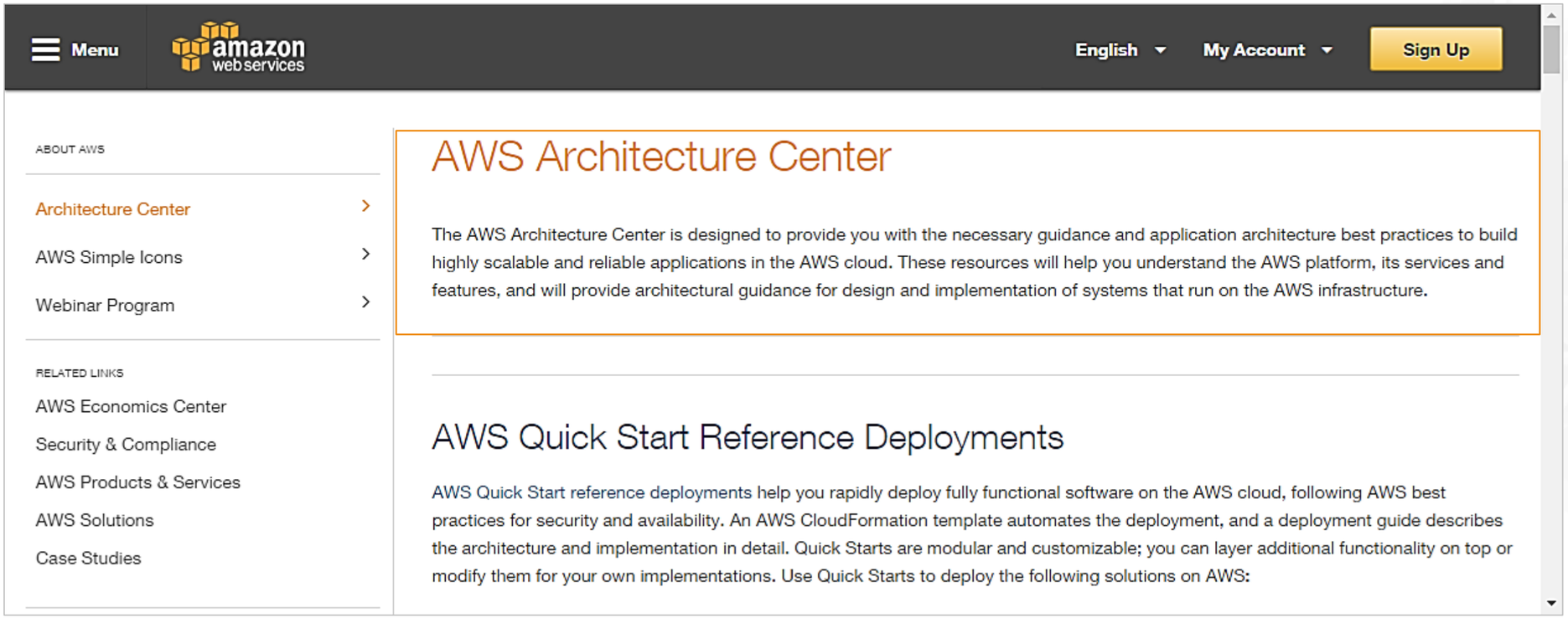
- Strong password
- Group email alias
- Multi-factor authentication
- Users and roles for access
- Access Keys

AWS recommends not to create or use the access keys associated with the root account for programmatic access to the account.

Accessing AWS References

AWS Architecture Center

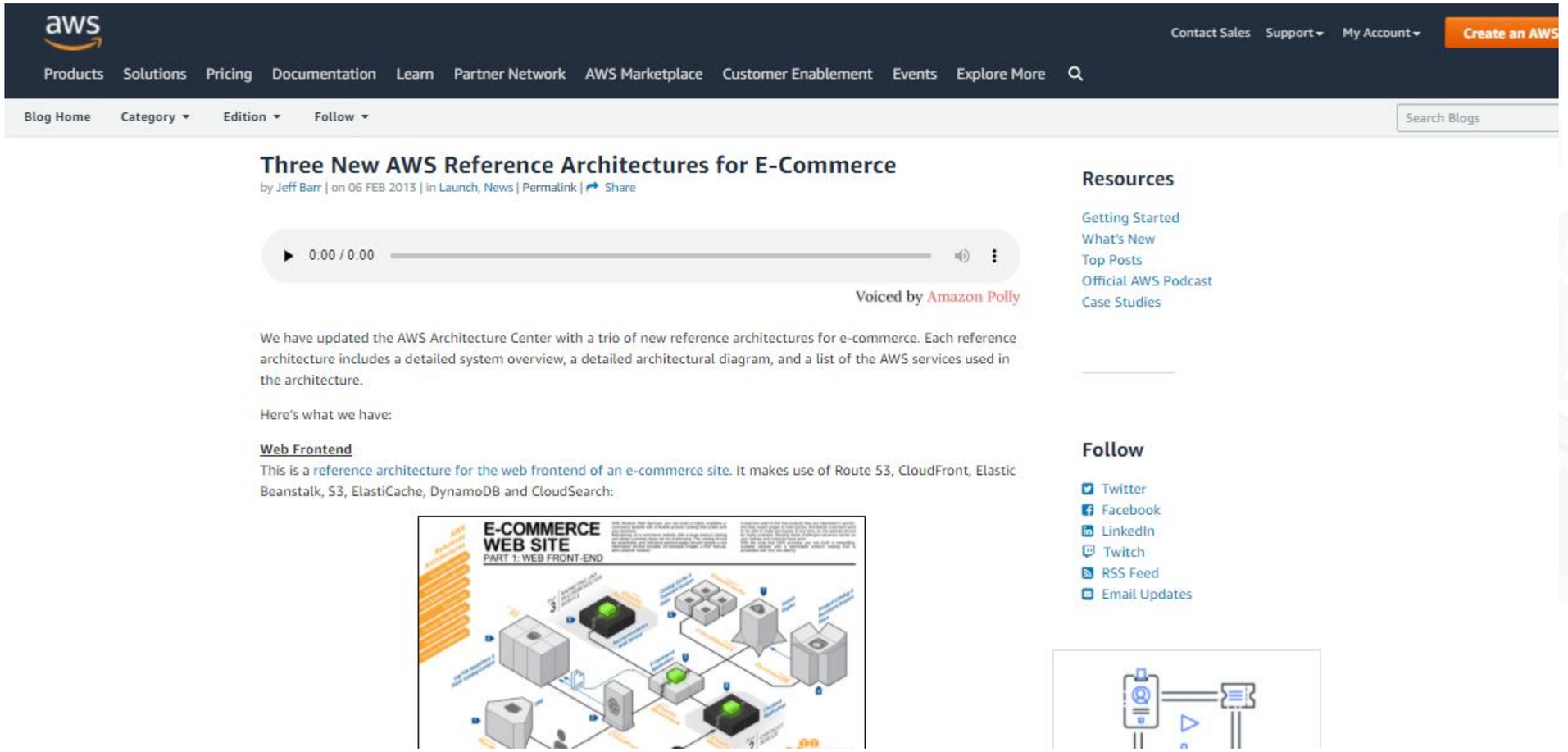
AWS Architecture Center provides application architecture best practices to build highly scalable and reliable applications in the AWS cloud.



Source: aws.amazon.com

AWS Reference Architectures

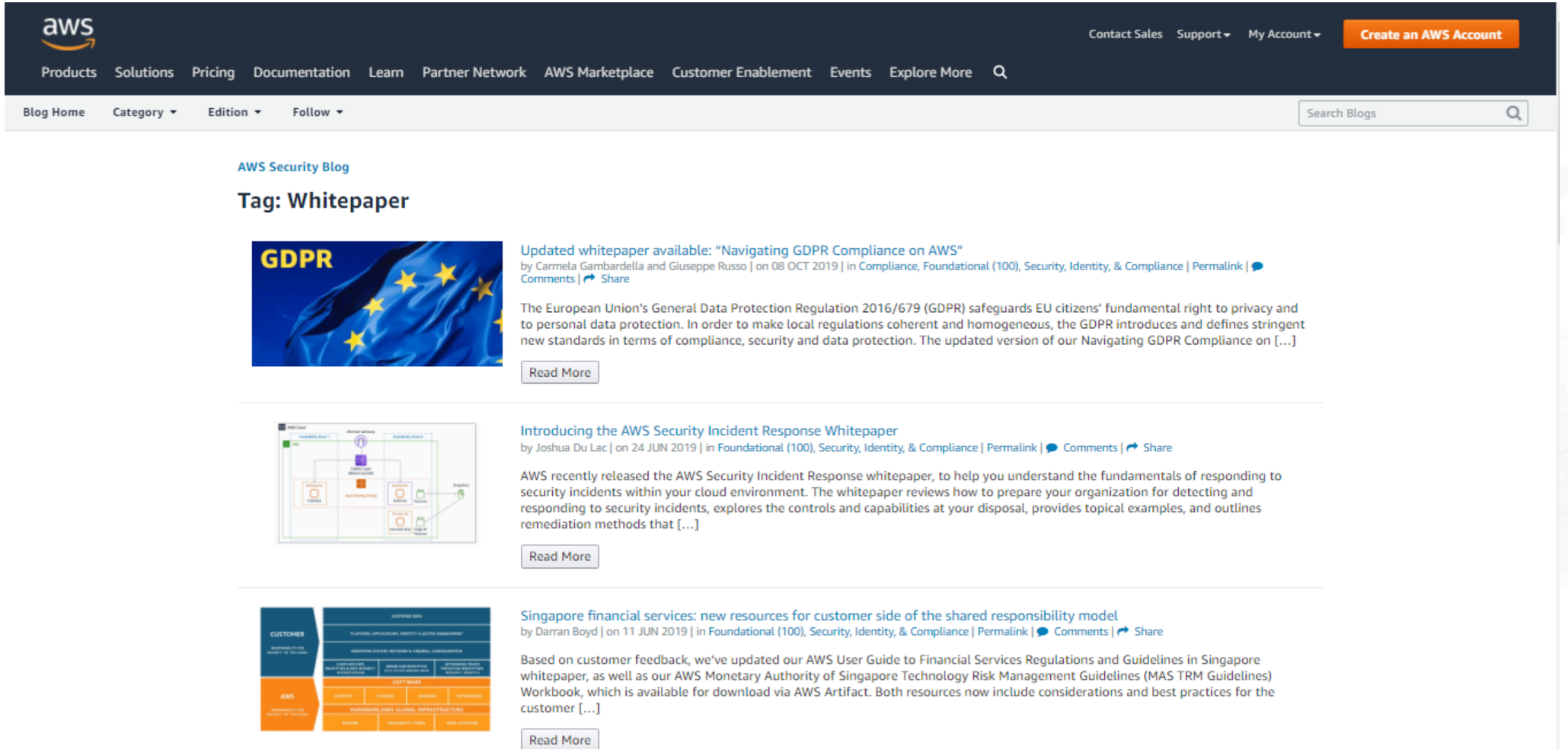
AWS Reference Architecture Datasheets provide architectural guidance to build an application on the AWS cloud infrastructure.



Source: aws.amazon.com

AWS Whitepapers

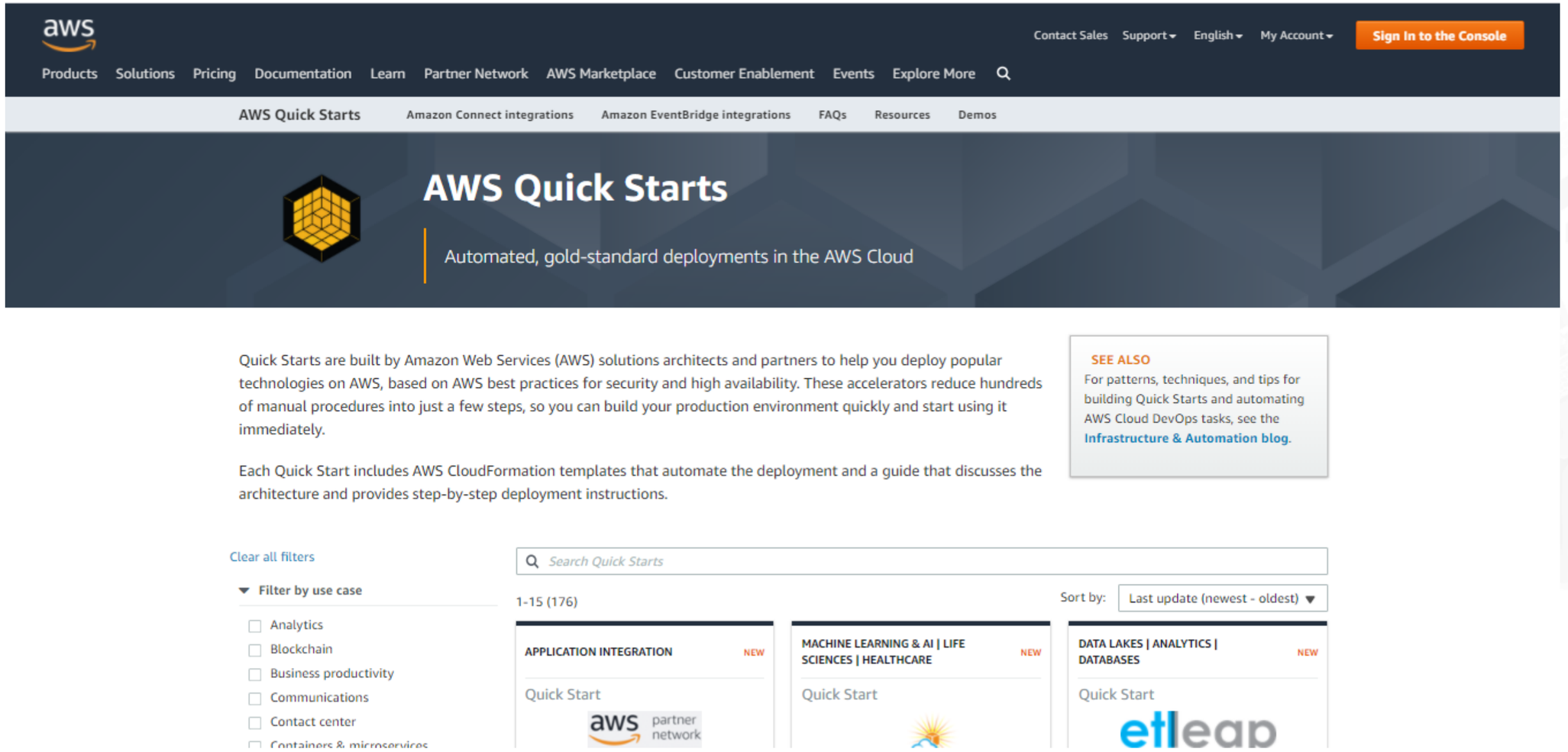
Technical AWS whitepapers cover all the AWS related topics and concepts such as architecture, security, and economics.



Source: aws.amazon.com

AWS Quick Start Reference Deployments

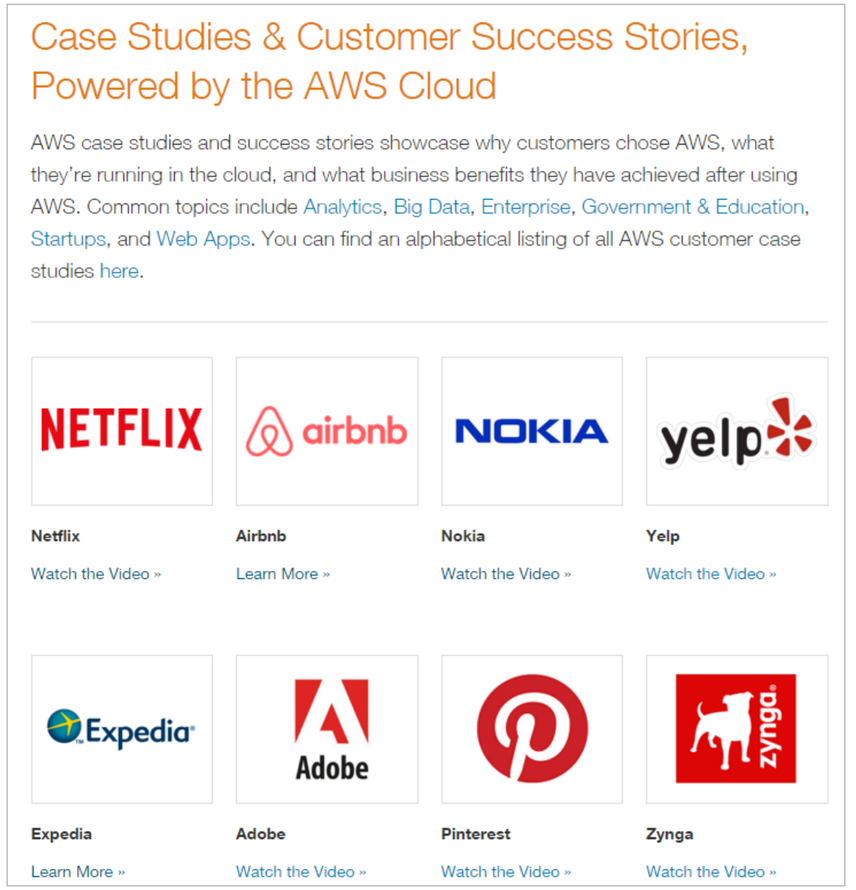
Users can rapidly deploy a fully functional environment for many enterprise software applications using the AWS CloudFormation templates.



Source: aws.amazon.com

Case Studies

AWS maintains a large list of case studies and success stories from their clients. These case studies highlight why some of the largest and most successful companies use AWS.



Source: aws.amazon.com

Key Takeaways

- AWS Framework helps users to understand the pros and cons of the decisions they make while building systems on AWS.
- Security, Reliability, Performance Efficiency, Cost Optimization, and Operational Excellence are the five pillars of the AWS Framework.
- Cloud computing helps achieve an optimal server configuration by providing various features.
- Users can use Amazon recommended best practices for their services to ensure that they leverage the most out of the Amazon Web Services.
- AWS Architecture Center provides application architecture best practices to build highly scalable and reliable applications in the AWS cloud.