

Introduction to Security and Architecture on AWS

AWS ARCHITECTURE CORE CONCEPTS



David Tucker

TECHNICAL ARCHITECT & CTO CONSULTANT

@_davidtucker_ davidtucker.net

Security and Architecture Overview

Overview

Reviewing core concepts around security and architecture

Exploring the AWS Shared Responsibility Model

Introducing the AWS Well Architected Framework

Examining fault tolerance and high availability on AWS

Understanding provided tools for compliance

Acceptable Use Policy

AWS's policy for acceptable and unacceptable uses of their cloud platform. All users must agree with this policy to have an account on the platform.

Acceptable Use Policy

Sending unsolicited mass emails is prohibited

Hosting or distributing harmful content is prohibited

Penetration tests are allowed for a list of specific services

Least Privilege Access

When granting permission for a user to access AWS resources, you should grant them the minimum permissions needed to complete their tasks and no more.

Shared Responsibility Model

“Security and Compliance is a shared responsibility between AWS and the customer.”

Amazon Web Services, Shared Responsibility Model

Shared Responsibility Summary

AWS Responsibility

AWS is responsible for the security
of the cloud

Customer Responsibility

Customer is responsible for security
in the cloud

Shared Responsibility Model

AWS Responsibility

Access & Training for Amazon Employees

Global Data Centers & Underlying Network

Hardware for Global Infrastructure

Configuration Management for Infrastructure

Patching Cloud Infrastructure & Services

Customer Responsibility

Individual Access to Cloud Resources & Training

Data Security & Encryption (both in transit and at rest)

Operating System, Network, and Firewall Configuration

All Code Deployed onto Cloud Infrastructure

Patching guest OS and custom applications

AWS Well-architected Framework

AWS Well-architected Framework

The Well-architected Framework is a collection of best practices across five key pillars for how to best create systems that create business value on AWS.

Pillars of the Well-architected Framework

Operational Excellence

Running and monitoring systems for business value

Security

Protecting information and business assets

Reliability

Enabling infrastructure to recover from disruptions

Performance Efficiency

Using resources efficiently to achieve business value

Cost Optimization

Achieving minimal costs for the desired value



Contact Sales Support English My Account

Sign In to the Console

Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Customer Enablement Events Explore More

AWS Well-Architected

Learn, measure, and build using architectural best practices

AWS Architecture Center

This is My Architecture

AWS Solutions

AWS Well-Architected

The **Well-Architected Framework** has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on five pillars — operational excellence, security, reliability, performance efficiency, and cost optimization — the Framework provides a consistent approach for customers and partners to evaluate architectures, and implement designs that will scale over time.

The **AWS Well-Architected Tool** is now available. The user guide can be located [here](#).

APN Partners are available to help you along the way as you build and manage your workloads. [Engage an AWS Well-Architected Partner](#). If you are an APN Partner interested in joining the Well-Architected Partner Program, [click here](#).

High-availability and Fault Tolerance

“Everything fails all the time.”

Werner Vogels - CTO, Amazon

Reliability on AWS

Fault Tolerance

Being able to support the failure of components within your architecture

High Availability

Keeping your entire solution running in the expected manner despite issues that may occur

Building Solutions on AWS

Most managed AWS services provide high-availability out of the box

When building solutions directly on EC2 fault tolerance must be architected

Multiple availability zones should be leveraged

Some services can enable fault tolerance in your custom applications

- Simple Queue Service (SQS)
- Route 53

Compliance

Common Compliance Standards

PCI-DSS

Compliance standard for
processing credit cards

HIPAA

Compliance standard for
healthcare data

SOC 1, SOC 2, SOC 3

Third-party reviews of
operational processes

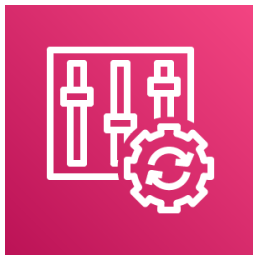
FedRAMP

Standards for US
government data handling

ISO 27018

Standard for handling
Personally Identifiable Info

Compliance Services



AWS Config

Provides conformance packs for standards



AWS Artifact

Provides self-service access to reports



Amazon GuardDuty

Provides intelligent threat detection

Demo

**Examining compliance reports in AWS
Artifact**

**Exploring conformance packs in AWS
Config**

Scenario Based Review

Scenario 1



Jane's company is building an application to process credit cards

They will be processing cards directly and not through a service

Their bank needs a PCI DSS compliance report for AWS

Where would Jane go to get the information?

Scenario 2



Tim's company is considering a transition to the cloud

They store personal information securely in their system

Tim's CTO has asked what the company's responsibility is for security

What would you tell Tim's CTO?

Scenario 3



Ellen is a solutions architect at a startup

They are building a new tool for digital asset management

Ellen is curious how to best leverage the capabilities of AWS in this application

What resources would you recommend for Ellen and her team?

Summary

Summary

Reviewed core concepts around security and architecture

Explored the AWS Shared Responsibility Model

Introduced the AWS Well-architected Framework

Examined fault tolerance and high availability on AWS

Understood provided tools for compliance

Scenario 1



Jane's company is building an application to process credit cards

They will be processing cards directly and not through a service

Their bank needs a PCI DSS compliance report for AWS

Where would Jane go to get the information?

Solution: AWS Artifact

Scenario 2



Tim's company is considering a transition to the cloud

They store personal information securely in their system

Tim's CTO has asked what the company's responsibility is for security

What would you tell Tim's CTO?

Solution: Review the Shared Responsibility Model

Scenario 3



**Ellen is a solutions architect at a startup
They are building a new tool for digital
asset management**

**Ellen is curious how to best leverage the
capabilities of AWS in this application**

**What resources would you recommend
for Ellen and her team?**

**Solution: AWS Well Architected
Framework**