Getting Started Resource Center ⌄

Overview

Fundamentals ▾

Learning Paths ▾

Category Deep Dive ▾

Hands-On Tutorials

Resources

AWS FUNDAMENTALS

Core Concepts

Introduction

This **AWS Fundamentals Course** is designed to teach you the core concepts you need to work effectively within AWS.

When first starting, AWS can seem overwhelming. A cloud-native paradigm of building infrastructure can be a radical departure from the traditional on-premises way of doing things. And regardless if this is your first time working with infrastructure or you've been tuning Linux kernels for the last decade, it can be hard to know where to start with AWS's selection of over 175 services.

The AWS Fundamentals Course is designed to help you get started with AWS regardless of your experience. In this course, we will teach you about the five pillars of AWS, mental models to use

when thinking about the cloud, and key concepts that will be applicable across any service you end up using.

Structure

The AWS Fundamentals Course will be divided into five modules. Each module will follow the following format:

- **Intro**: A short description of the pillar we will be focusing on

- **Mental Model**: A guiding mental model to help you understand the concepts introduced in each pillar

- **Concepts**: Key concepts covering broad foundational topics for each pillar

- **Conclusion**: Summary of what we discussed

- **Further Reading**: Additional links and resources

The Five Pillars

The Five Pillars covered in the AWS Fundamentals Course come from the AWS Well-Architected Framework. The Well-Architected Framework is the distillation of over a decade of experience building scalable applications on the cloud.

The Five Pillars consist of the following areas: Operational Excellence, Security, Reliability, Performance Efficiency, and Cost Optimization.
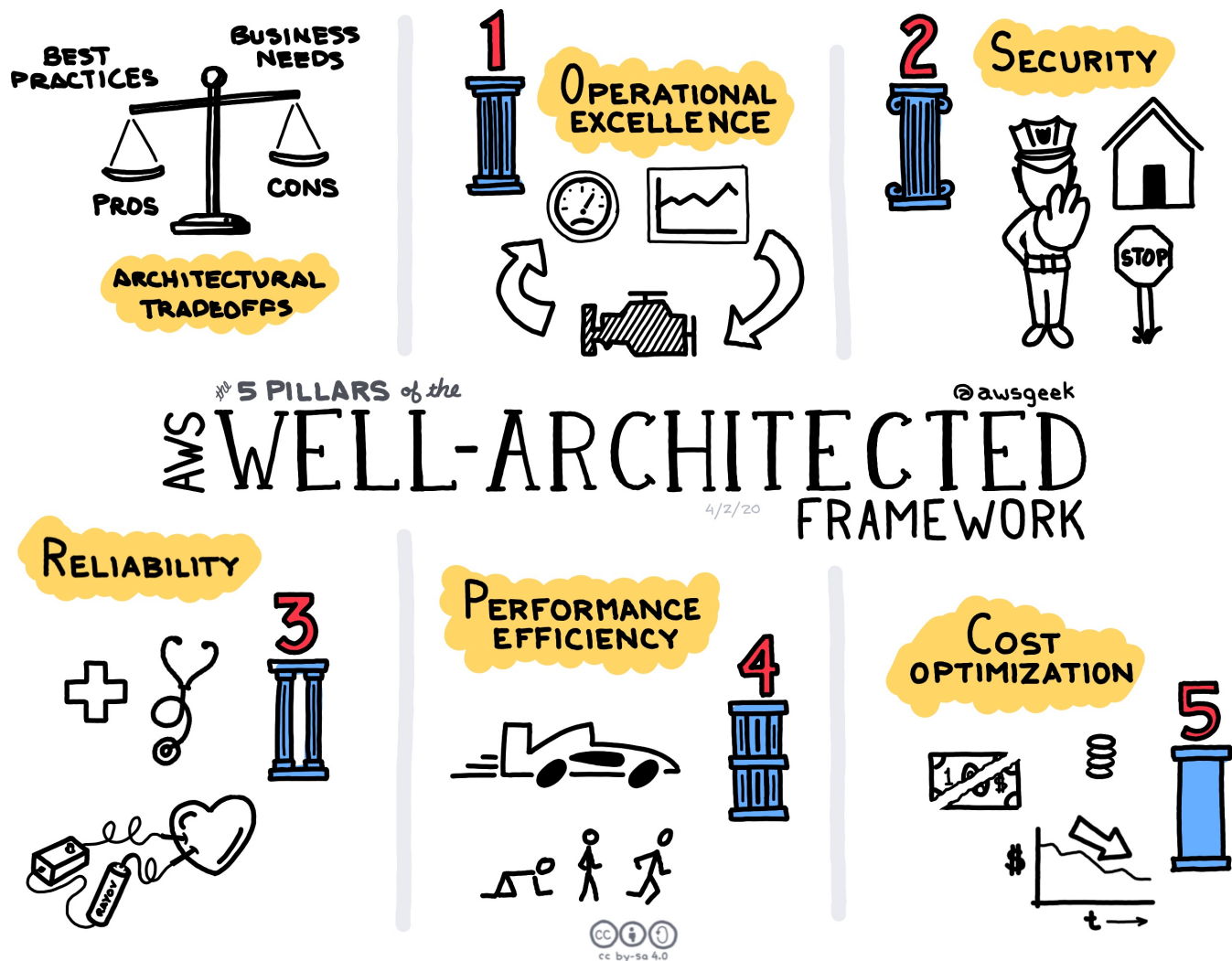
Operational Excellence

The operational excellence pillar focuses on how you can continuously improve your ability to run systems, create better procedures, and gain insights.

Mental Model

When thinking about operational excellence in the cloud, it is useful to think of it in terms of **automation**.

Human error is the primary cause of defects and operational incidents. The more operations that can be automated, the less chance there is for human error.

In addition to preventing error, automation helps you continuously improve your internal processes. They promote a set of repeatable bests practices that can be applied across your entire organization.

Concepts

When you think of operations as automation, you want to focus your efforts in the areas that currently require the most manual work and might have the biggest consequence for error. You'll also want to have a process in place to track, analyze, and improve your operational efforts.

We will focus on the following two concepts for operational excellence:

1. Infrastructure as Code

2. Observability

Infrastructure as Code   ⊕

Observability   ⊕

Conclusion

In this module, you have learned about the pillar of operational excellence. You have learned about the mental model of thinking about operations as automation. You have learned about IaC and how it can be used to provision your services automatically using the same tools and processes that you currently use for code. You have learned about observability and how to collect, analyze, and act on metrics to continuously improve your operational efforts.

Further Reading

- Operational Excellence Pillar Whitepaper

Security

The security pillar focuses on how to secure your infrastructure on the cloud. Security and compliance is a shared responsibility between AWS and the customer. In this shared responsibility model, AWS is responsible for the security of the cloud. This includes the physical infrastructure, software, and networking capabilities of AWS cloud services. The customer is responsible for

security in the cloud. This includes the configuration of specific cloud services, the application software, and the management of sensitive data.

If your workloads must meet FedRAMP, DoD SRG, ITAR, CJIS or other strict compliance requirements, or they contain data classified as Controlled Unclassified Information (CUI), please see the AWS GovCloud (US) section of the course.

Mental Model

When thinking about security in the cloud, it is useful to adopt the model of **zero trust**.

In this model, all application components and services are considered discrete and potentially malicious entities. This involves the underlying network fabric, all agents that have access to your resources, as well as the software that runs inside your service.

Concepts

When we think of security in terms of zero trust, it means we need to apply security measures at all levels of our system. The following are three important concepts involved in securing systems with zero trust in the cloud:

1. Identity and Access Management (IAM)
2. Network Security
3. Data Encryption

Identity and Access Management (IAM)   +

Network Security   +

Data Encryption   +

Conclusion

In this module, you have learned about the security pillar of AWS. You have learned about the mental model of zero trust. You have learned about IAM and the principle of least privilege. You have learned about AWS network security and the principle of defence in depth. You have learned about data encryption and applying it both in transit and at rest.

Further Reading

- [Security Pillar Whitepaper](#)

Reliability

The reliability pillar focuses on how you can build services that are resilient to both service and infrastructure disruptions. Much like with performance efficiency, while the cloud gives you the means to build resilient services that can withstand disruption, it requires that you architect your services with reliability in mind.

Mental Model

When thinking about reliability in the cloud, it is useful to think in terms of **blast radius**. You can think of blast radius as the maximum impact that might be sustained in the event of a system failure. To build reliable systems, you want to minimize the blast radius of any individual component.

Concepts

When you think in terms of the blast radius, the question of failure is no longer **a question of if** but **a matter of when**. To deal with failure when it happens, the following techniques can be used to limit the blast radius:

1. Fault Isolation
2. Limits

Fault Isolation   ⊕

Limits   ⊕

Conclusion

In this module, you have learned about the reliability pillar of AWS. You have learned about the mental model of thinking in terms of blast radius. You have learned about using fault isolation zones to limit blast radius. You have learned about service limits and how to increase yours to avoid service disruption.

Further Reading

- Reliability Pillar Whitepaper

Performance Efficiency

The performance efficiency pillar focuses on how you can run services efficiently and scalably in the cloud. While the cloud gives you the means to handle any amount of traffic, it requires that you choose and configure your services with scale in mind.

Mental Model

When thinking about performance efficiency in the cloud, it is useful to think of your services as **cattle, not pets**.

In the on-premises model of doing things, servers were expensive and often manually deployed and configured. It could take weeks before a server was actually delivered and physically plugged into your data center. Because of this, servers were treated like pets - each one was unique and required a lot of maintenance. Some of them even had names.

The cloud way of thinking about servers is as cattle. Servers are commodity resources that can be automatically provisioned in seconds. No single server should be essential to the operation of the service.

Concepts

Thinking of servers as cattle gives us many performance-related benefits. In the "pet model" of managing servers, it is quite common to use the same type of server (or even the same server) for multiple workloads - it was too much of a hassle to order and provision different machines. In the "cattle model," provisioning is cheap and quick which gives us the freedom to select the server type that most closely matches our workload.

The "cattle model" also makes it easy for us to scale our service. Because every server is interchangeable and quick to deploy, we can quickly scale our capacity by adding more servers.

We will focus on the following two concepts for performance efficiency:

1. Selection

2. Scaling

Selection ⊕

Scaling ⊕

Conclusion

In this module, you have learned about the performance efficiency pillar of AWS. You have learned about the mental model of treating your servers as cattle instead of pets. You have learned how to choose the right service as well as its configuration based on your performance goals. You have learned about scaling services and the tradeoffs between vertical and horizontal scaling.

Further Reading

- [Performance Efficiency Pillar Whitepaper](#)

Cost Optimization

The cost optimization pillar helps you achieve business outcomes while minimizing costs.

Mental Model

When thinking about cost optimization in the cloud, it is useful to think of cloud spend in terms of **OpEx instead of CapEx**. OpEx is an ongoing pay-as-you-go model whereas CapEx is a one-time purchase model.

Traditional IT costs on on-premises data centers have been mostly CapEx. You pay for all your capacity upfront regardless if you end up using it. Purchasing new servers could be a lengthy

process that involved getting sign-off from multiple parties. This is because CapEx costs were often significant and mistakes costly. After you have made a purchase, the actual servers could still take weeks to come in.

In AWS, your costs are OpEx. You pay on an ongoing basis for the capacity that you use. Provisioning new servers can be done in real-time by engineering without the need for a lengthy approval process. This is because OpEx costs are much smaller and can be reversed if requirements change. Because you only pay for what you use, any excess capacity can simply be stopped and terminated. When you do decide to use a service, provisioning can be done in the order of seconds and minutes.

Concepts

Going from a CapEx model to an OpEx model fundamentally changes your approach to costing your infrastructure. Instead of large upfront fixed costs, you think in small ongoing variable expenses.

This pay-as-you-go model introduces the following changes to your cost optimization process:

1. Pay For Use

2. Cost Optimization Lifecycle

Pay For Use (+)

Cost Optimization Lifecycle (+)

Conclusion

In this module, you have learned about the pillar of cost optimization. You have learned about applying an OpEx-focused model for your cloud spend. You have learned about cost optimization techniques like right sizing, serverless, reservations, and spot instances. You have learned about reviewing, tracking, and optimizing your budget using services like the Cost Explorer, tags, and budgets.

Further Reading

- Cost Optimization Pillar Whitepaper

AWS GovCloud (US)

This section is for those whose workloads must meet FedRAMP, DoD SRG, ITAR, CJIS or other strict compliance requirements, or they contain data classified as Controlled Unclassified Information (CUI).

AWS GovCloud (US) helps address the specific compliance and regulatory needs of U.S. government agencies at the federal, state, and local levels, as well as U.S. commercial organizations in aerospace, defense manufacturing, law enforcement, healthcare, financial services, energy, and other heavily regulated industries. Designed to host sensitive data and regulated workloads in the cloud, AWS GovCloud (US) Regions are isolated AWS regions operated by employees who are U.S. citizens on U.S. soil.

AWS GovCloud (US) gives government customers and their partners the flexibility to architect secure cloud solutions that comply with the FedRAMP High baseline; the DOJ's Criminal Justice Information Systems (CJIS) Security Policy; U.S. International Traffic in Arms Regulations (ITAR); Export Administration Regulations (EAR); Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) for Impact Levels 2, 4 and 5; FIPS 140-2; IRS-1075; and other compliance regimes.

From Controlled Unclassified Information (CUI), Personally Identifiable Information (PII), sensitive patient medical records, and financial data to law enforcement data, export controlled data and other forms of CUI, AWS GovCloud (US) Regions can help customers address compliance at every stage of their cloud journey.

Further Reading

- Overview of AWS GovCloud (US)

- AWS Services Available in AWS GovCloud (US)

- AWS Services in Scope by Compliance Program

Congratulations!

You have now completed the AWS Fundamentals Course. In this course, you have learned the following:

- The Five Pillars of the AWS Well-Architected Framework

- Important mental models that represent a cloud-native way of thinking about the five pillars

- Key concepts within each of the five pillars

At this point, you have learned the fundamentals of building secure, performance efficient, reliable, operationally excellent, and cost-optimized services in the cloud. While we have only scratched the surface of what there is to know, you now have a solid starting point for the rest of your AWS journey. Now that you have completed the AWS Fundamentals Course, go ahead and apply what you've learned to build your next great service on AWS.

Launch Your First Application!

Sign In to the Console

Learn About AWS

What Is AWS?

What Is Cloud Computing?

AWS Inclusion, Diversity & Equity

What Is DevOps?

What Is a Container?

What Is a Data Lake?

AWS Cloud Security

What's New

Blogs

Press Releases

Resources for AWS

Getting Started

Training and Certification

AWS Solutions Portfolio

Architecture Center

Product and Technical FAQs

Analyst Reports

AWS Partner Network

Developers on AWS

Developer Center

SDKs & Tools

.NET on AWS

Python on AWS

Java on AWS

PHP on AWS

Javascript on AWS

Help

Contact Us

AWS Careers

File a Support Ticket

Knowledge Center

AWS Support Overview

Legal

Sign In to the Console

Amazon is an Equal Opportunity Employer: *Minority / Women / Disability / Veteran / Gender Identity / Sexual Orientation / Age.*

Language

عربي |

Bahasa Indonesia |

Deutsch |

English |

Español |

Français |

Italiano |

Português |

Tiếng Việt |

Türkçe |

Русский |

ไทย |

日本語 |

한국어 |

中文 (简体) |

中文 (繁體)

Privacy

|

Site Terms

|

Cookie Preferences

|