Week 1 Notes and Resources

Key Topics

AWS Cloud

The AWS Cloud lets you build applications quickly and cost effectively - you pay for the resources you need and can quickly add more resources when you need them.

Free Tier

You can explore AWS and complete the exercises for this course within the AWS Free Tier. AWS automatically provides alerts using AWS Budgets to help you track your free tier usage. See AWS Free Tier Usage Alerts using AWS Budgets for more.

EC2

Amazon Elastic Compute Cloud allows you to run virtual servers in AWS.
Your virtual server is known as an EC2 Instance. It runs on a physical host that is inside an AWS Availability Zone (AZ). There will be 2 or more AZ within an AWS Region. This design allows you to build applications that are resilient to large scale events that could impact an AZ.

If you'd like to learn more about AWS facilities, take a 'digital tour' of an AWS data center!

VPC

Your network in AWS is provided by Amazon Virtual Private Cloud (VPC). You can create a VPC within an AWS region and within that VPC you define subnets to manage related sets of servers or other AWS resources. VPC lets you define rules for how network traffic from your subnets is routed. You can also decide whether your network should be connected to the Internet, to corporate networks, or to keep the network completely private.

The IP Address ranges for VPC and Subnets are specified using CIDR notation. If you'd like to know more about IP addressing within VPC, see the VPCs and Subnets in the User Guide for Amazon VPC. You can also learn more about CIDR notation in section 3.1 of RFC4632 or in Classless Interdomain Routing on Wikipedia.

Security in AWS

You are given a lot of flexibility in AWS to configure and build your applications the way you want. Given that you control your resources, security in AWS is a shared responsibility between AWS and you. AWS will provide secure facilities and building blocks for your application. AWS also provides guidance, and tools that can help you operate securely.

For example, if you are using EC2, it is your responsibility to take advantage of features such as Security Groups (firewall), Private Subnets (to provide network isolation) and encryption options to build secure applications. You are also responsible for keeping the operating system and application stack patched on your server.

If you use AWS managed services like RDS, you still have to make security decisions, but operational tasks like patching the Operating System and SQL engine can be done automatically on your behalf. When using APIs like Amazon S3 API, the underlying infrastructure and maintenance is fully abstracted from you and you are only responsible for calling the API and configuring your access and encryption policies.

For more on the Shared Security Model, see Shared Responsibility Model on the AWS Compliance site.

Additional Services Used

CloudFormation

An AWS service that can take in a declarative document called a 'template' and use it to provision AWS resources on your behalf so you don't have to. We used this to create a VPC to the specifications needed for the course.

EC2 Metadata service

This is a service that intercepts calls to 169.254.169.254 from your EC2 instance to communicate metadata to the instance. This IP address is in the range for IPv4 Link-Local IP addresses as defined by RFC 3927 and the details about the properties the instance that can be retrieved are documented here in the EC2 User Guide.

What you accomplished this week

- You signed up for an AWS Account
- You launched your first web server into AWS
- You built the virtual network we'll use in upcoming exercises and connected to your EC2 instance

Learn About Verified Certificates