AWS Summary

AWS Service Summary

Global Service

- Identity and Access Management(IAM)
- Route 53(DNS service)
- CloudFront(Content Delivert Network)
- WAF(Web Application Firewall)

Region-scoped service

- Infrastructure as Service(EC2)
- Elastic Beanstalk(Platform as Service)
- Lambda
- Rekognition

Identity and Access Management(IAM)

IAM: Users & Groups

- Root account created by default, shouldn't be used or shared
- Users are people with your organization, and can be grouped
- Groups only contain users, not other groups
- Users don't have to belong to a group, and user can belong to multiple groups

IAM: Permissions

- Users or Groups can be assigned JSON documents called policies
- These policies define the permission of the users
- In AWS you apply the least privilege principle: don't give more permissions than a user needs

IAM: Policies Structure

- Consists of
  - Version: policy language version, always include "2012-10-17"
  - Id: an identifier for the policy(optional)
  - Statement: one or more individual statements(required)
- Statements consists of
  - Sid: an identifier for the statement(optional)

    - Effect: whether the statement allows or denies access
    - Principal: account/user/role to which this policy applied to
    - Action: list of actions this policy allows or denies
    - Resource: list of resources to which the actions applied to
    - Condition: conditions for when this policy is in effect(optional)

Multi Factor Authentication - MFA

- Users have access to your account and can possibly change configurations or delete resource in your AWS account
- You want to protect your Root Accounts and IAM users
- MFA = password you know + security device you own
- MFA devices options in AWS
    - Virtual MFA device
    - Universal 2nd Factor(U2F) Security Key

IAM Roles for Services

IAM Security Tools

IAM Credentials Report(account-level)

- a report that lists all your account's users and the status of their various credentials IAM Access Advisor(user-level)
- Access advisor shows the service permissions granted to a user and when those services were last accessed
- You can use this information to revise your policies

Simple Storage Service（S3）

S3概念

数据对象是由内容和元数据组成

- 元数据
    - 最后修改日期
    - 内容类型
    - 用户自定义
- 每个对象由键来确定
- 存储桶可提供访问控制
- 存储桶位于同一个区域内
  当数据存储在存储桶中之后，返回的是一个URL，对应的URL的format是：
  **https://bucket-name.s3.amazonaws.com/sample+key/name.jpg

Elastic Cloud Compute（EC2）

EC2 = Elastic Compute Cloud = Infrastructure as a Service
It mainly consists in the capablity of:

- Renting virtual machines(EC2)
- Storing data on virtual drives(EBS)
- Distributing load across machines(ELB)
- Scaling the services using an auto-scaling group(ASG)

EC2 User Data

- It is possible to bootstrap our instances using an EC2 User data script
- bootstrapping means launching commands when a machine starts
- That script is only run once at the instance first start
- EC2 user data is used to automate boot tasks such as:
  - Installing updates
  - Installing software
  - Downloading common files from the internet
  - Anything you can think of
- The EC2 User Data Script runs with the root user

Elastic Load Balancing （ELB）

- 向EC2的实例HTTP，HTTPS和TCP流量分发请求，实现负载均衡
- 支持运行状态检查，帮助清除替换不健康的实力
- 提供流量，延迟信息，帮助动态扩展和缩减所需要的资源

Auto Scaling

- 自动的扩展您的EC2的数量
- 非常适合使用率波动的应用程序
- 无需额外的费用

Cloud Watch

收集EC2上的CPU等相关系统的数据，根据设置的阈值，发出警告，并通知Auto Scaling Group，然后利用ELB扩展或者缩减EC2的数量

Elastic Block Store（EBS）

- EBS类似于一块虚拟硬盘，可以用与EC2实例，利用EBS将数据同计算分离。
- EBS服务独立持续存在，可以在需要的时候将EBS同EC2相连，并且连接之后，可以像任何其他物理硬盘那样使用该卷，并在改卷中放置任何类型的文件系统。

- 在使用EBS存储数据的时候，如果计算实例EC2发生故障，不必担心数据丢失。
- 一个卷每次只能与一个实例相连接，而单个实例却可以与许多卷相连接，所以可以添加多个卷并将整个卷的数据分类，以提供I/O和吞吐量性能。

AWS Deploy Summary

Elastic Beanstalk

Code Deploy

EC2 Container Service