Cloud, The Hard Way

HELLO!

I am Will Bengtson

I love the cloud

You can find me at `@__muscles`

0.
PREFACE

The Hard Way is Easier

THE HARD WAY IS EASIER

- Cover the basics
- Build on them
- Run free

1.
INTRODUCTION

Getting started in the cloud

GETTING STARTED IN THE CLOUD

- Challenges
- Understand Datacenter vs. AWS

CHALLENGES

- Dynamic environment
- Huge scale
- Diverse applications

DATACENTER VS AWS

Datacenter	AWS
Firewall	Security Group
RBAC	IAM
Cluster	Auto Scaling Group
Syslog	CloudWatch
VLAN	VPC
Datacenter	Region / AZ

MAPS

MAPS

@__muscles

2.
EXERCISE 0

Let’s get to the root of things

ROOT ACCOUNT

- First AWS account
- Highest level of access
- Sensitive

USE CASES OF ROOT

- Break glass superuser
- S3 Bucket ACL

THROW AWAY THE KEY

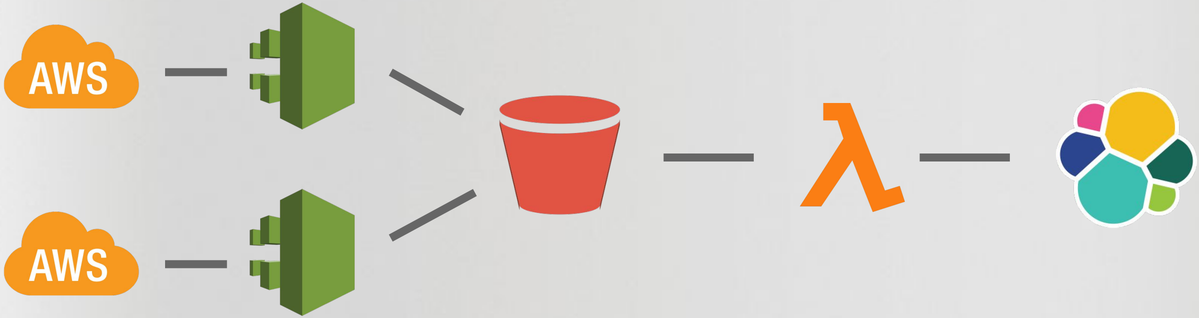
3.
EXERCISE 1

Auditing - CloudTrail

CLOUDTRAIL

- Logs AWS API activity
  - Like a credit card statement
- AWS API transactions
  - Who / When / What (Call) / Which (Resource)

EXAMPLE: HOW TO CLOUDTRAIL



4.
EXERCISE 2

Identity and Access Management (IAM)

IDENTITY AND ACCESS MANAGEMENT (IAM)

- Users
- Groups
- Roles
- Policies

IAM USERS

- Can log into the console
- Credentials are static
- Avoid if you can

IAM GROUPS

- Used to provide similar permissions to users
- Think of them like AD groups

IAM ROLES

- Preferred method for operating in AWS
- Similar to users, but credentials are temporary
- Used throughout all services within AWS
- Single Sign-On (SSO)

POLICIES

- Permissions that can be applied to anything
- Managed Policies
- Inline policies

Works EVERYWHERE!

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::sans-sj"
    }
  ]
}
```

5.
EXERCISE 3

Simple Storage Service (S3)

S3

- It is like a folder on the internet
- Can be used to store your data on AWS
- Cheap

S3

- Buckets
  - Globally unique
  - Can make files (objects) public
- Objects
  - Contain data and metadata
  - Can be public even though bucket is not!

6.
EXERCISE 4

Base AMI

BASE AMI

- Immutability
  - No SSH
  - Config change == new build
- Every application has the same base layer
  - Logging
  - Security
  - Secrets Management

7.
EXERCISE 5

Lambda

Lambda A.K.A Serverless

- Someone else’s container
- Highly scalable
- Pay for what you use
- Multiple languages
    - Bring your own runtime

Lambda A.K.A Serverless

- Deploy in VPC
- Configurable memory and runtime
  - More memory ~= more power
- Easy to get started
- Be careful with versions

8.
TOOLS

Some awesome open source

STREAMALERT

REPOKID

CLOUD INQUISITOR

CLOUD CUSTODIAN

THANKS!

Any questions?

@__muscles