

# Sounding the Alarm with IAM and CloudWatch

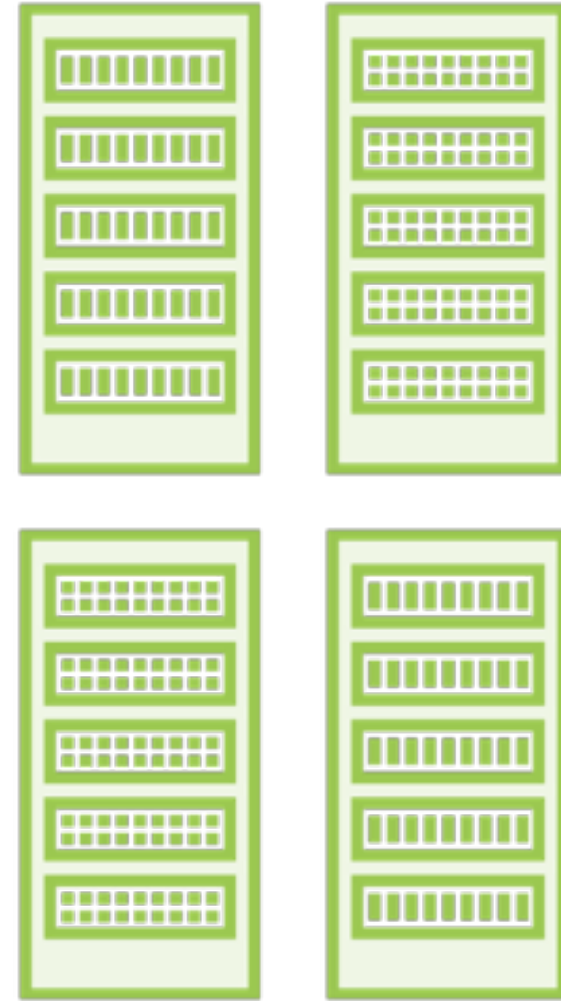
---



**Ryan Lewis**

WEB ENGINEER

@ryanmurakami   [www.ryanhlewis.com](http://www.ryanhlewis.com)



CloudWatch

**Set Alarms &  
Notifications in  
response to Events**

IAM

**Simple User and  
Access Management**

# Summary

**Watching the Clouds**

**The Simplest Notification Service**

**The First CloudWatch Alarm**

**Users? Policies? Groups?**

**Security is the Best Policy**

# CloudWatch Overview

---

CEO



Director



Boss



You at  
2AM



# CloudWatch

Service to set alarms based on Service metric thresholds

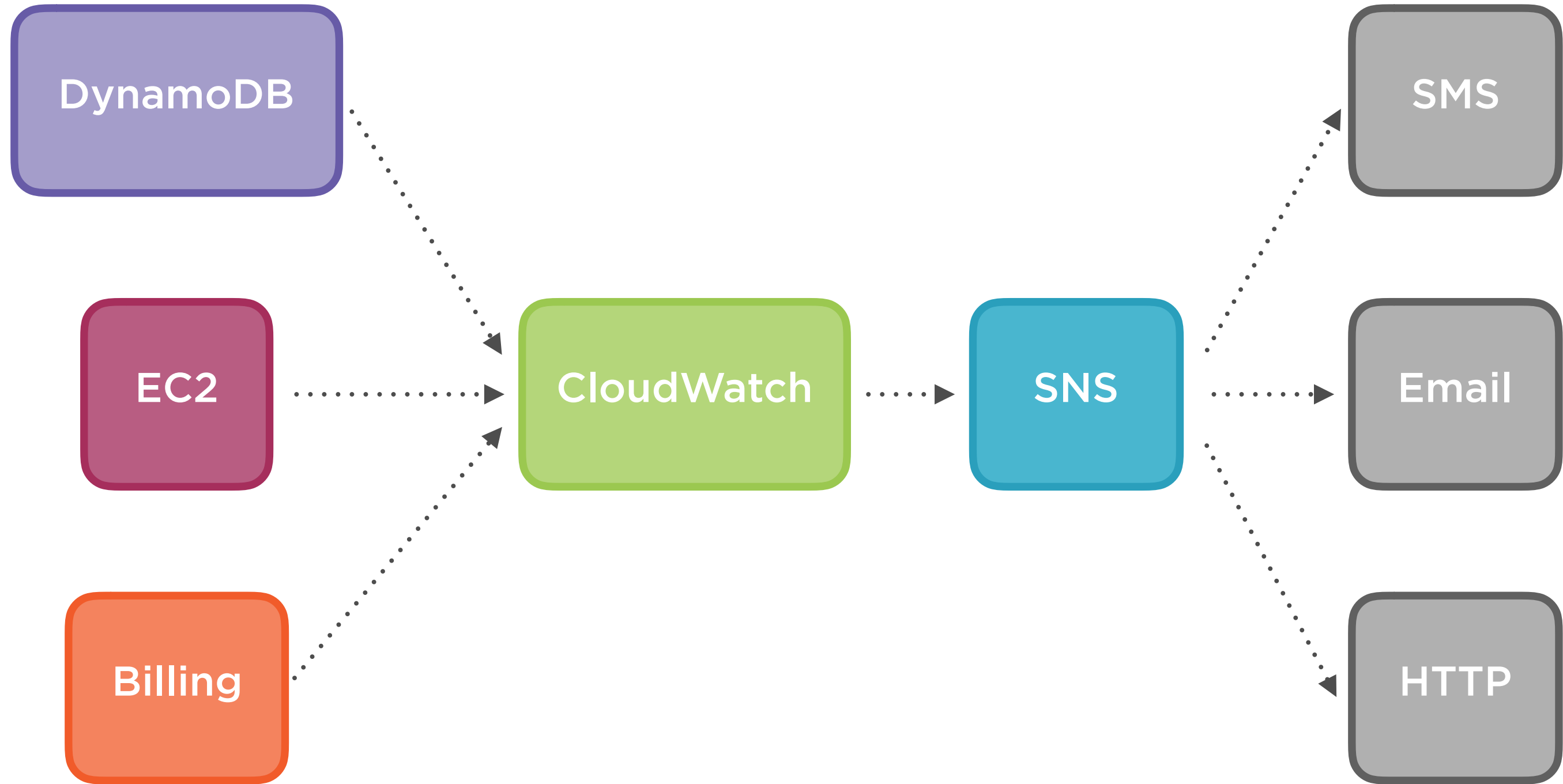
# CloudWatch Metric Examples

**DynamoDB  
Read/Write  
Throughput**

**EC2  
CPU  
Usage**

**Estimated  
Billing  
Charges**



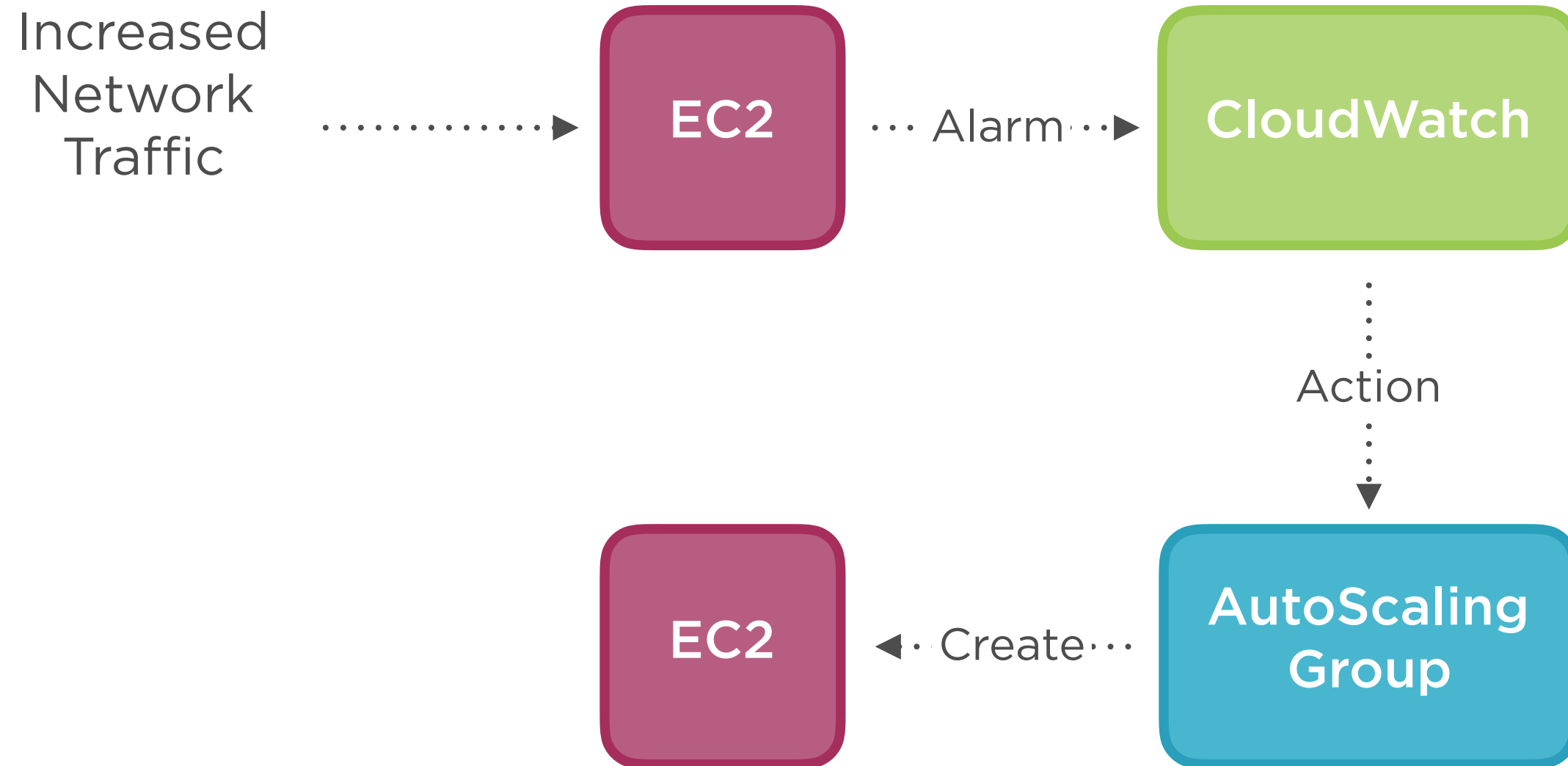


# CloudWatch Alarm Actions

**Send Notification via SNS**

**Trigger AutoScaling Action**

**Trigger EC2 Action**

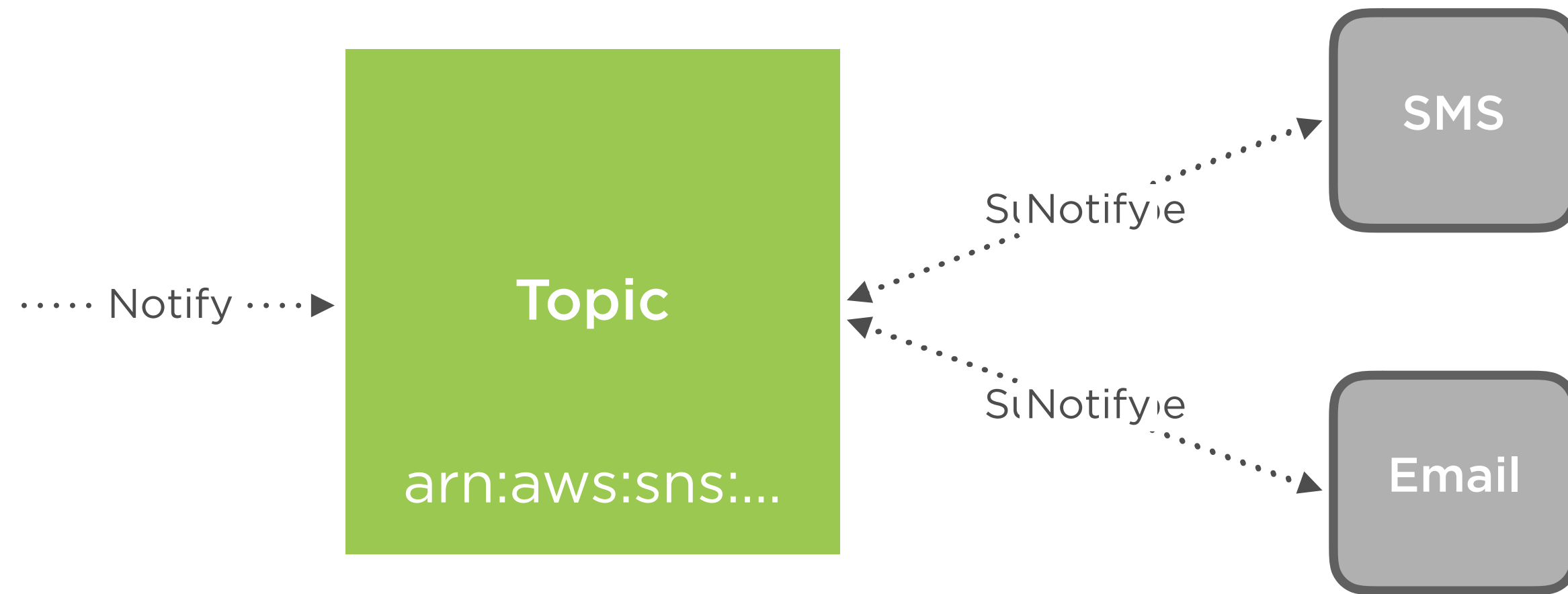


“CloudWatch lets me sleep at night.”

- **AWS Developer not awake at 2am**

# Simple Notification Service

---



## Objective

Create an SNS Topic with Email Subscription



Imagine an email with a  
“Confirm Subscription” link  
here



# Creating a CloudWatch Alarm

---

## Objective

Create a CloudWatch Billing Alarm

Billing Alerts are only  
enabled in the North Virginia  
Region

CloudWatch is used by  
many services throughout  
AWS

# Identity & Access Management Overview

---

# Identity & Access Management (IAM)

Service to configure authentication and access for user accounts

# IAM User Management Aspects

**Passwords**

**Multi-Factor Authentication**

**Access Keys**

**SSH Keys**

# IAM Policy

**Policy**

**Permission**

**Resource Permission**

**Service Permission**



# IAM Policy Examples

## Developer Group Policy

EC2 Full Access

## Tester Group Policy

DynamoDB  
Read-Only

S3 Full Access  
Test Bucket

“I use IAM for all my AWS security needs.”

- **A Very Cooperative Developer Co-Worker**

# Securing Your AWS Account

---

Protect your AWS Account

# Root Account Permissions

**Administer all services**

**Modify billing information**

**Manage users**

# Multi-Factor Authentication

Authentication that requires more than one factor to authenticate

# MFA with AWS

**“Know” a Password**

**“Have” a Device**

# MFA Process

1. Enter Username and Password

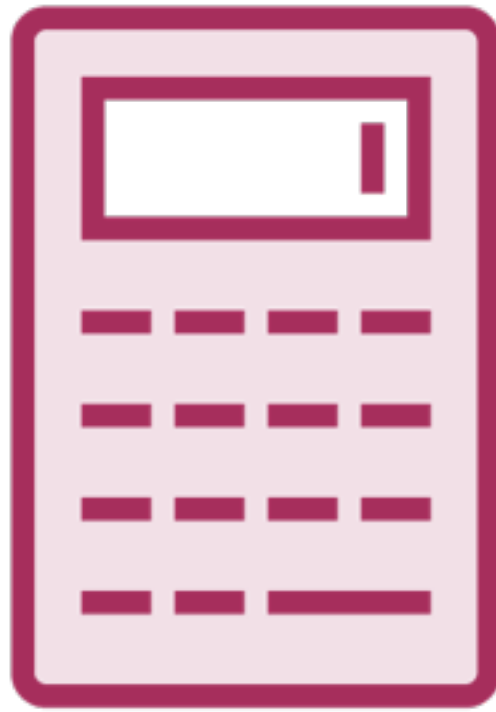


2. Enter MFA Authentication Code





# MFA Devices



Hardware



Virtual  
(Smartphone)

Download an MFA App

## Objective

Setup MFA on Your Root AWS Account

MFA increases the security  
of your AWS account

# Understanding Policies

---

Users have no permissions  
by default

# Policy Statement Properties

## Action

Operation  
user can  
perform on  
services

## Effect

“Allow”  
or  
“Deny”

## Resource

Specific  
Resources  
user can  
perform  
action on

# IAM Policy Types

## AWS Managed Policy



## Customer Managed Policy





Use Policies to give  
Permissions

# Configuring Users and Groups

---

# IAM Users

Permissions  
via Policies



Authentication  
(Password, MFA)

# IAM Groups



Permissions  
via Policies

## Objective

Create a New User

## Objective

Create a New Group

## Objective

Create a Password Policy

## Objective

Assign a Password to Our User



# Conclusion

---

# Summary

**CloudWatch & SNS - BFFs 4ever**

**You'll thank me later**

**IAM Security Lockdown**

**Don't mess with root access**

Up Next:

Getting Inside the Virtual Machine with EC2 and  
VPC

# VPC & EC2

**Partition  
Resources  
in the  
Cloud**

**Deploy  
Virtual  
Machines**