Track 4| Session 5

架構即代碼 – AWS CDK 與 CDK8S 聯手打造下一代的 K8S 應用

Pahud Hsieh

Developer Advocate
Amazon Web Services

aws SUMMIT ONLINE

想像一下

We Need to Build A Huge Building Like This

https://www.flickr.com/photos/rghedin/9050773796/

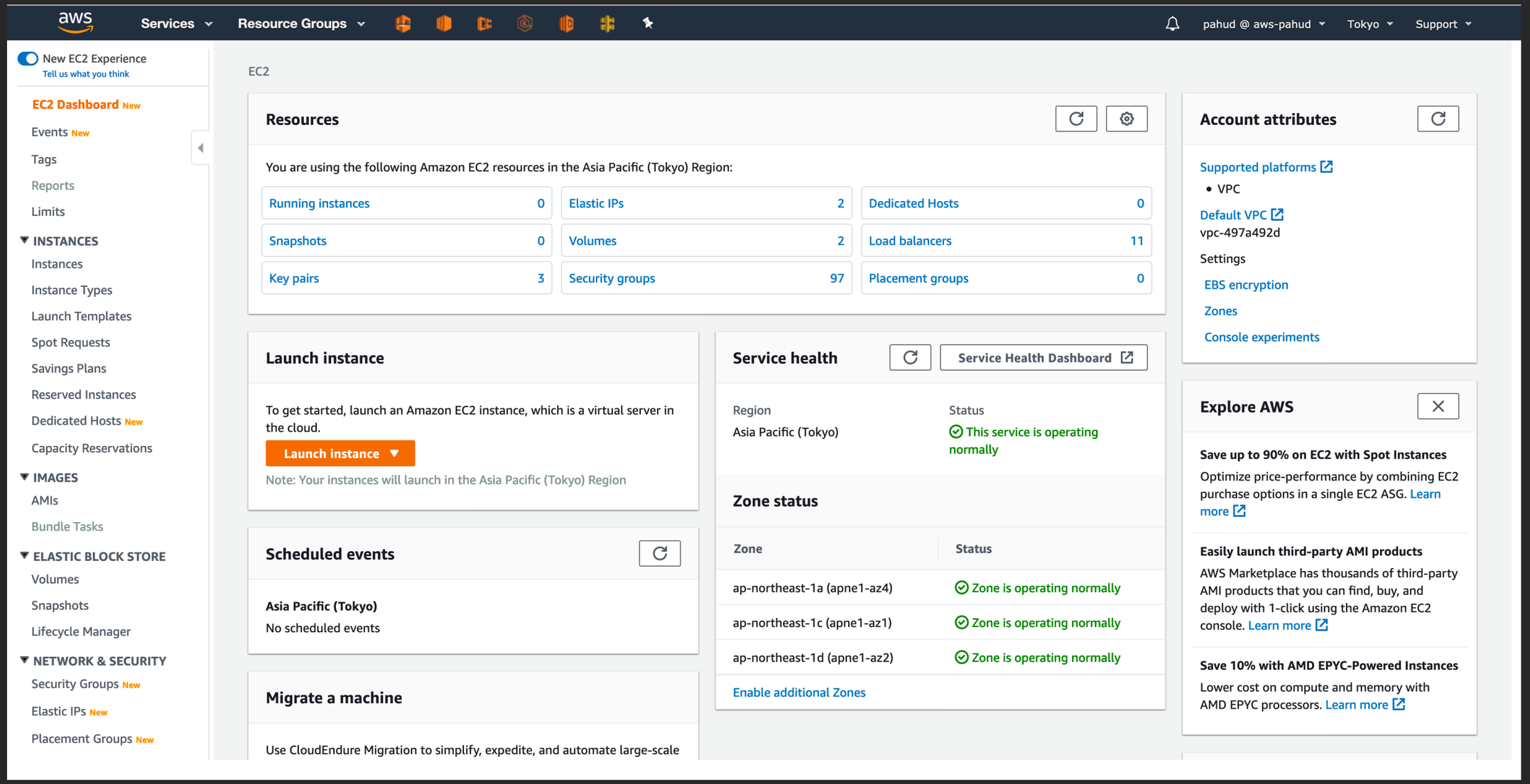
Our Teams

- Owner (You)
  - You can control everything
- Designer/Architect (設計師/建築師)
  - Structural, internal and external design
  - Compliance
  - Security
- Construction(施工團隊)
  - working with the building blocks by design

How the construction team works?

Construction Team

Working with Mouse Clicks in the AWS Console



Construction Workers

AWS CLI or Shell Scripts

```
#!/bin/bash

# create vpc
aws ec2 create-vpc \
--ipv6-cidr-block-network-border-group us-west-2-lax-1 \
--cidr-block 10.0.0.0/16
# create subnets
# create internet gateway and nat gateways
# create routing table and routes
# create ec2 instances
aws ec2 run-instances --image-id ami-xxxxxxxx --count 1 \
--instance-type t2.micro \
--key-name MyKeyPair --security-group-ids sg-903004f8 \
--subnet-id subnet-6e7f829e
```

Designer and Architect?

Designer and Architect

Using Templates

```
"Resources" : {
  "EC2Instance" : {
    "Type" : "AWS::EC2::Instance",
    "Properties" : {
      "InstanceType" : { "Ref" : "InstanceType" },
      "SecurityGroups" : [ { "Ref" : "InstanceSecurityGroup" } ],
      "KeyName" : { "Ref" : "KeyName" },
      "ImageId" : { "Fn::FindInMap" : [ "AWSRegionArch2AMI", { "Ref" : "AWS::Region" },
                        { "Fn::FindInMap" : [ "AWSInstanceType2Arch", { "Ref" : "InstanceType" }, "Arch" ] } ] }
    }
  },

  "InstanceSecurityGroup" : {
    "Type" : "AWS::EC2::SecurityGroup",
    "Properties" : {
      "GroupDescription" : "Enable SSH access via port 22",
      "SecurityGroupIngress" : [ {
        "IpProtocol" : "tcp",
        "FromPort" : "22",
        "ToPort" : "22",
        "CidrIp" : { "Ref" : "SSHLocation"}
      } ]
    }
  }
},
```

Designer and Architect

Using Templates

It could be…

Thousands of lines in JSON or YAML

What Do You Want?

Give me a VPC out-of-the-box

```
new ec2.Vpc();
```

Give me a EC2 in this VPC

```
new ec2.Instance(stack, 'instance', {
   vpc,
});
```

Give me a S3 bucket out-of-the-box

```
new s3.Bucket();
```

Grant the EC2 instance role to read/write the bucket

```
const vpc = new ec2.Vpc();

const instance = new ec2.Instance(this, ‘Instance’, { vpc, …});

const bucket = new s3.Bucket();

bucket.grantReadWrite(instance.role);
```

And it compiles into this

```yaml
Resources:
  Bucket83908E77:
    Type: AWS::S3::Bucket
    UpdateReplacePolicy: Retain
    DeletionPolicy: Retain
    Metadata:
      aws:cdk:path: XxxStack/Bucket/Resource
  Vpc8378EB38:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.0.0.0/16
      EnableDnsHostnames: true
      EnableDnsSupport: true
      InstanceTenancy: default
      Tags:
        - Key: Name
          Value: XxxStack/Vpc
    Metadata:
      aws:cdk:path: XxxStack/Vpc/Resource
  VpcPublicSubnet1Subnet5C2D37C4:
    Type: AWS::EC2::Subnet
    Properties:
      CidrBlock: 10.0.0.0/18
      VpcId:
        Ref: Vpc8378EB38
      AvailabilityZone:
        Fn::Select:
          - 0
          - Fn::GetAZs: ""
      MapPublicIpOnLaunch: true
      Tags:
        - Key: aws-cdk:subnet-name
          Value: Public
        - Key: aws-cdk:subnet-type
          Value: Public
        - Key: Name
          Value: XxxStack/Vpc/PublicSubnet1
    Metadata:
      aws:cdk:path: XxxStack/Vpc/PublicSubnet1/Subnet
  VpcPublicSubnet1RouteTable6C95E38E:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId:
        Ref: Vpc8378EB38
      Tags:
        - Key: Name
          Value: XxxStack/Vpc/PublicSubnet1
    Metadata:
      aws:cdk:path: XxxStack/Vpc/PublicSubnet1/RouteTable
  VpcPublicSubnet1RouteTableAssociation97140677:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
```

And takes care of this

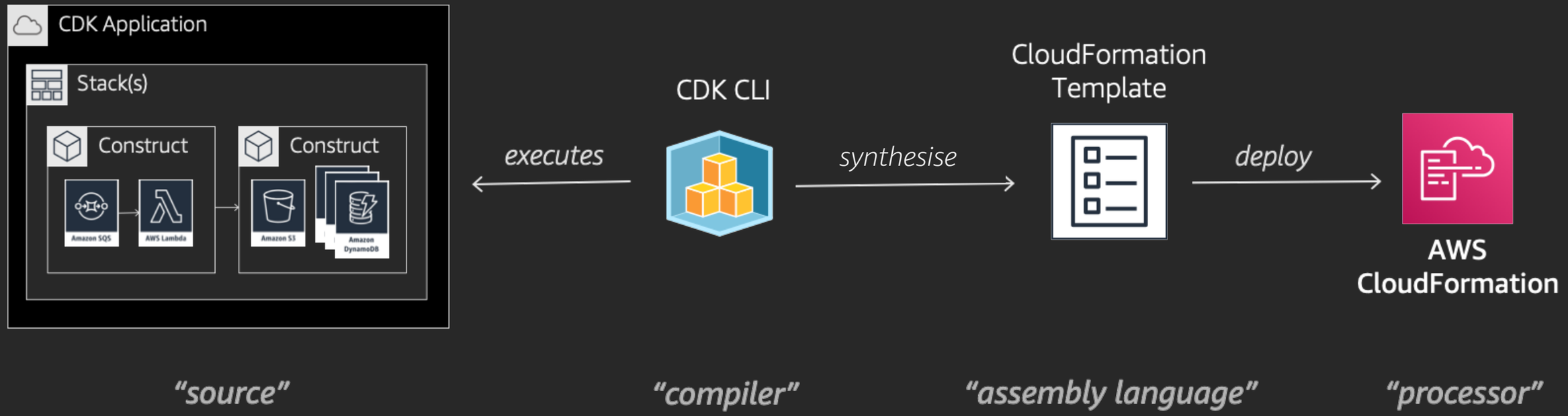
```
InstanceInstanceRoleDefaultPolicy4ACE9290:
  Type: AWS::IAM::Policy
  Properties:
    PolicyDocument:
      Statement:
        - Action:
            - s3:GetObject*
            - s3:GetBucket*
            - s3:List*
            - s3:DeleteObject*
            - s3:PutObject*
            - s3:Abort*
          Effect: Allow
          Resource:
            - Fn::GetAtt:
                - Bucket83908E77
                - Arn
            - Fn::Join:
                - ""
                - - Fn::GetAtt:
                      - Bucket83908E77
                      - Arn
                  - /*
      Version: "2012-10-17"
    PolicyName: InstanceInstanceRoleDefaultPolicy4ACE9290
    Roles:
      - Ref: InstanceInstanceRoleE9785DE5
  Metadata:
    aws:cdk:path: XxxStack/Instance/InstanceRole/DefaultPolicy/Resource
InstanceInstanceProfileAB5AEF02:
  Type: AWS::IAM::InstanceProfile
  Properties:
    Roles:
      - Ref: InstanceInstanceRoleE9785DE5
  Metadata:
    aws:cdk:path: XxxStack/Instance/InstanceProfile
InstanceC1063A87:
  Type: AWS::EC2::Instance
  Properties:
    AvailabilityZone:
      Fn::Select:
        - 0
        - Fn::GetAZs: ""
    IamInstanceProfile:
      Ref: InstanceInstanceProfileAB5AEF02
    ImageId:
      Ref: SsmParameterValueawsserviceamiamazonlinuxlatestamznamihvmx8664gp2C96584B6F00A464EAD1953AFF4B05118Parameter
    InstanceType: t3.large
    SecurityGroupIds:
      - Fn::GetAtt:
          - InstanceInstanceSecurityGroupF0E2D5BE
```

Minimal required IAM Policy

IAM Instance Profile

What is the AWS Cloud Development Kit (AWS CDK)

The big picture - from AWS CDK app to CloudFormation to provisioned infrastructure



CDK for Kubernetes (CDK8S)

Define Kubernetes apps and components using familiar languages

AWS CDK + CDK8S – What is the Experience

Everything Under the Kubernetes – AWS CDK

All cloud infrastructure

- VPC Networking, Amaozn EKS Cluster, Managed Nodegroup, Fargate Profile,etc.

Everything Above the Kubernetes – CDK8S

Kubernetes Resources

- deployment, service, daemonset, ingress, namespaces, pod, roles, rolebindings, jobs, etc.

Everything You Need

- Your Favorite IDE with Your Favorite Language

Demo

aws SUMMIT ONLINE

Thank you!

Pahud Hsieh
Developer Advocate
@pahudnet

aws SUMMIT ONLINE