Technical Excellence in the Cloud

Written for AllState, Belfast, October 2017

Contents

Chapter 1 Cloud Fundamentals

Chapter 2 Cloud Infrastructure Overview

Chapter 3 Running Servers

Chapter 4 Security in and of the Cloud

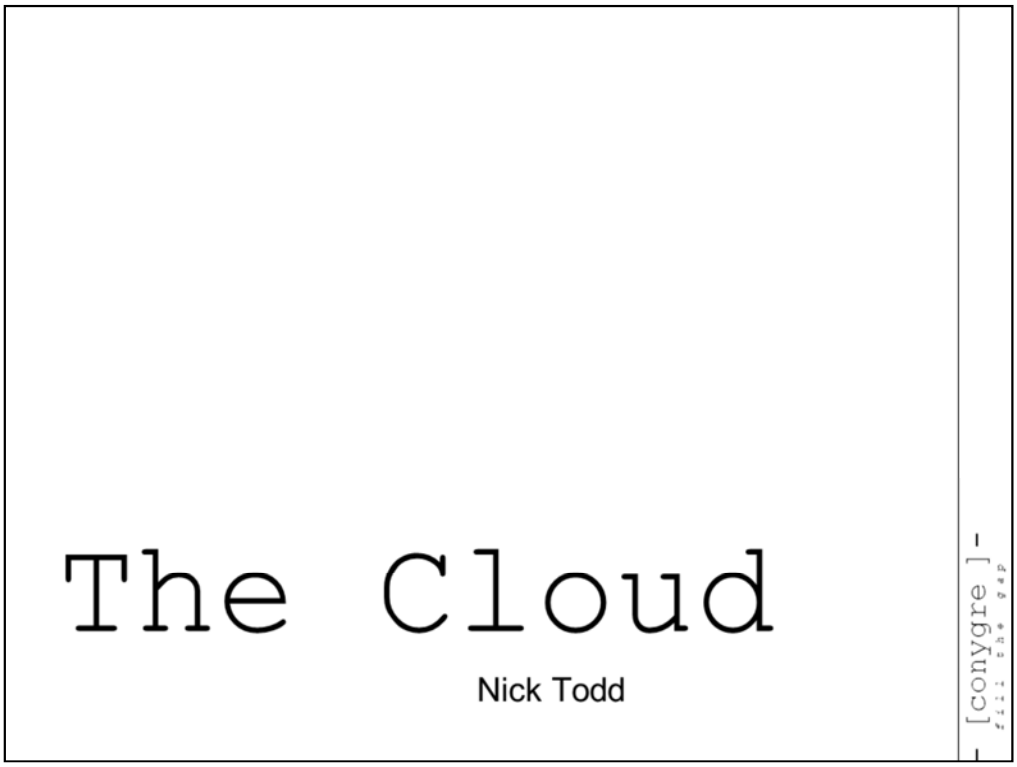
Chapter 5 Storage Options

Chapter 6 Development in the Cloud

Chapter 7 Deployment and Devops

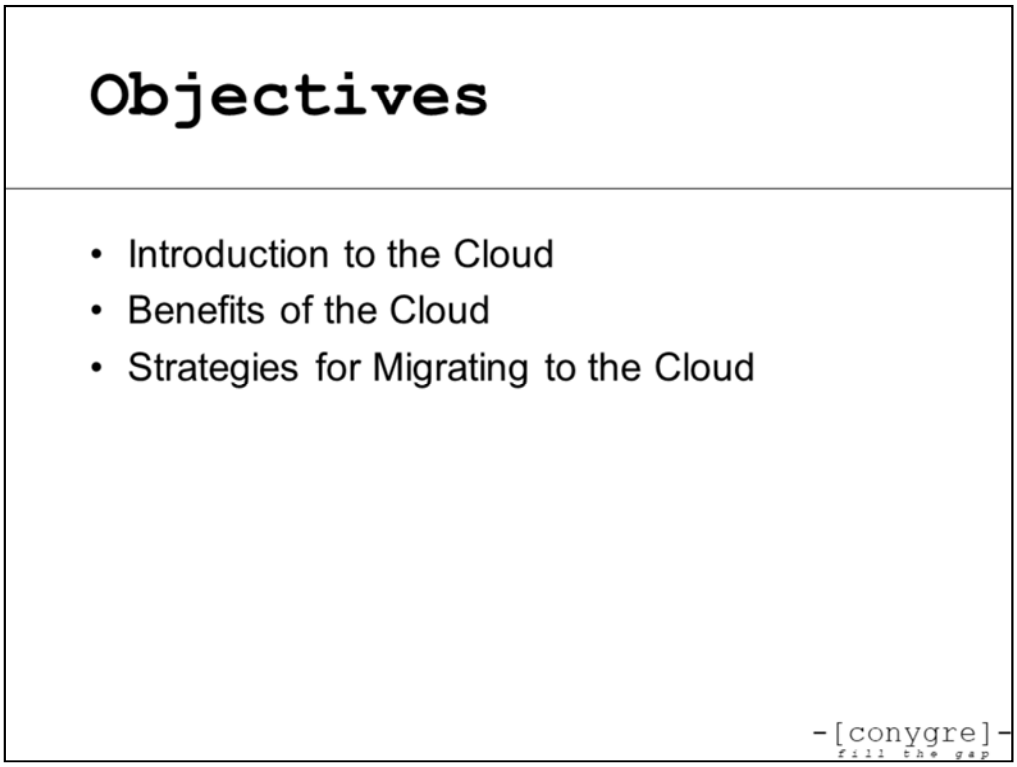
Chapter 8 Container Services with Docker

Web Application Architecture

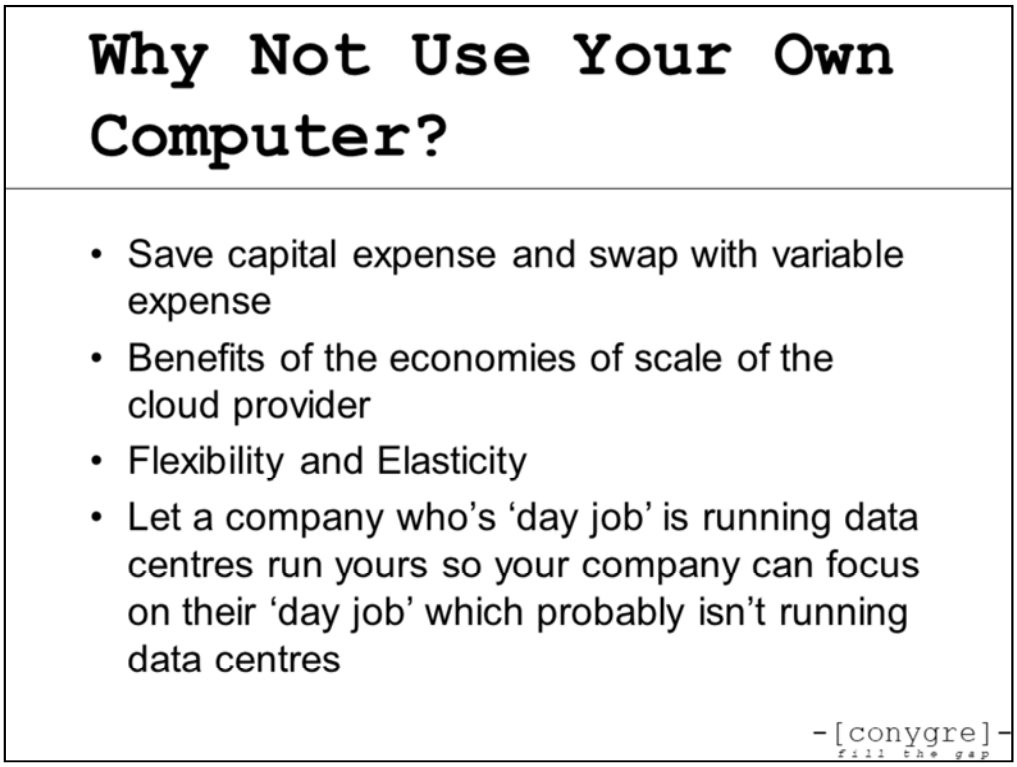


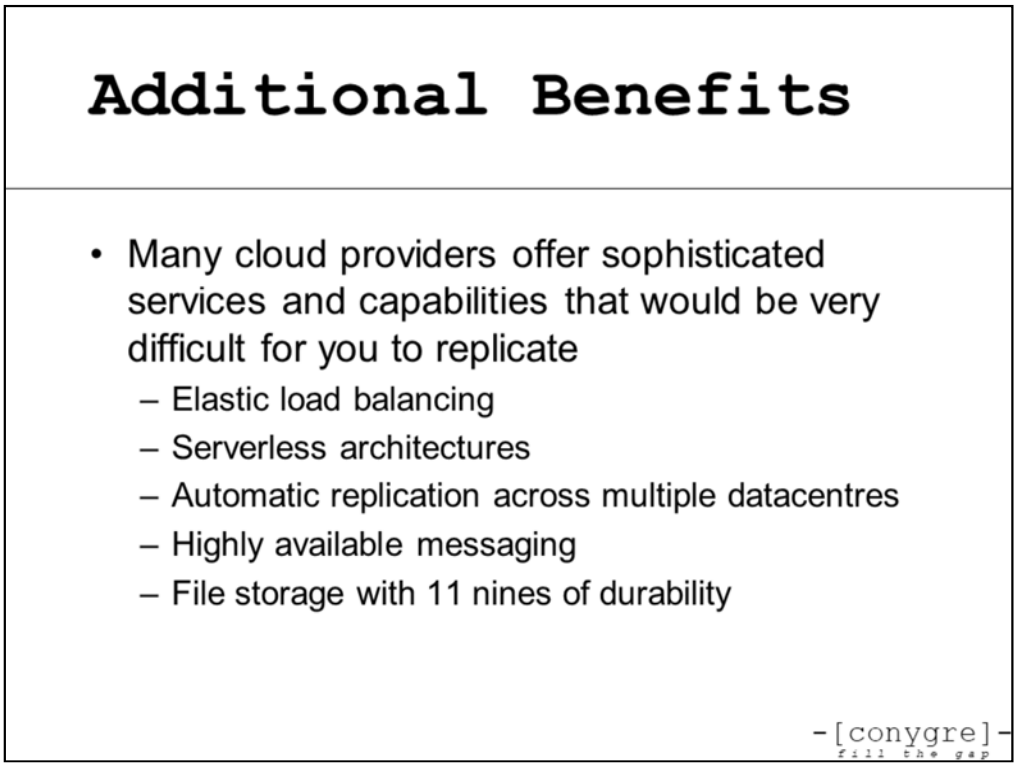
The Prezi presentation near the start of this training can be found here:
http://prezi.com/cxpwi_og7lht/aws-regions-and-availability-zones/

Web Application Architecture

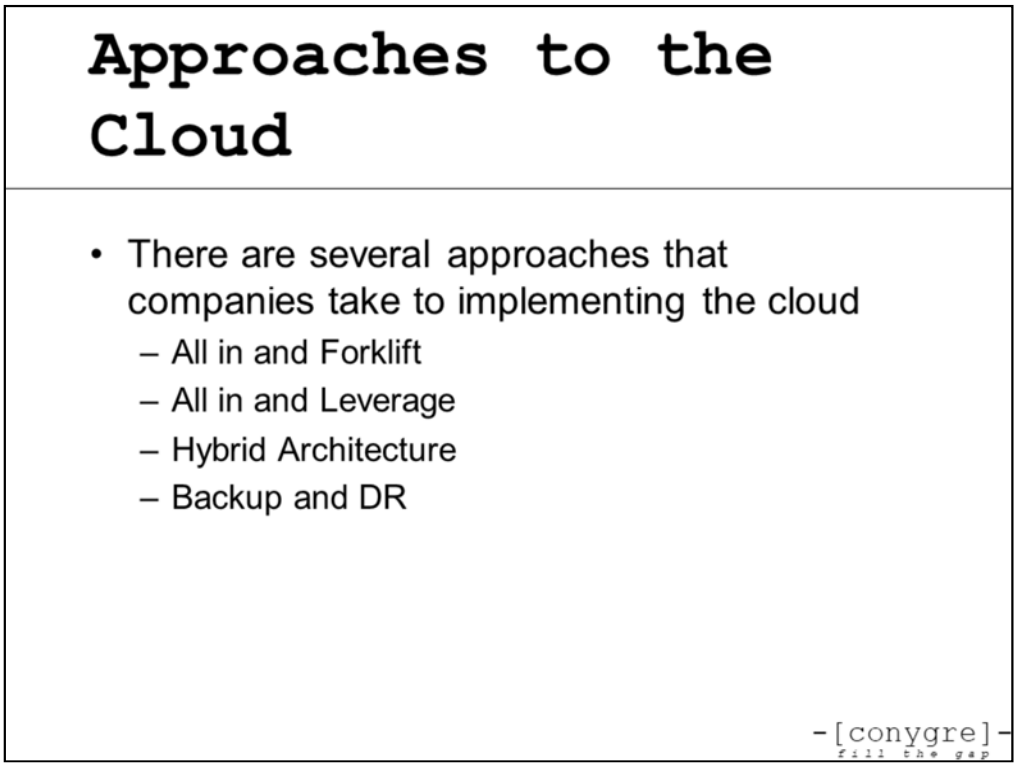


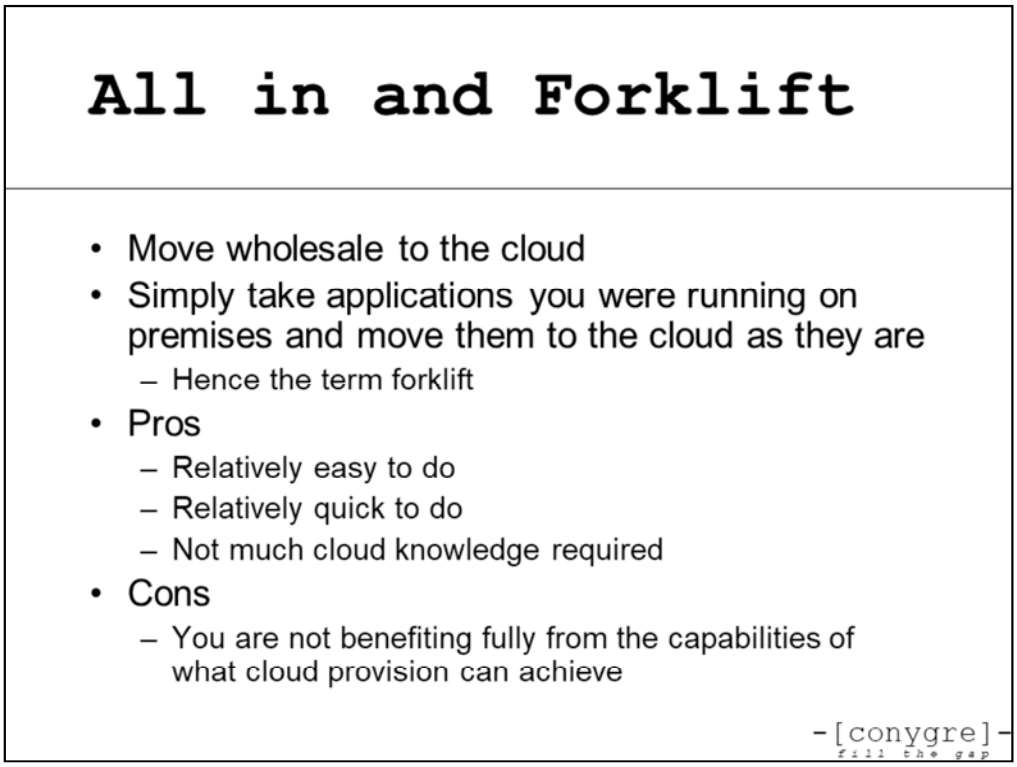
Cloud Fundamentals

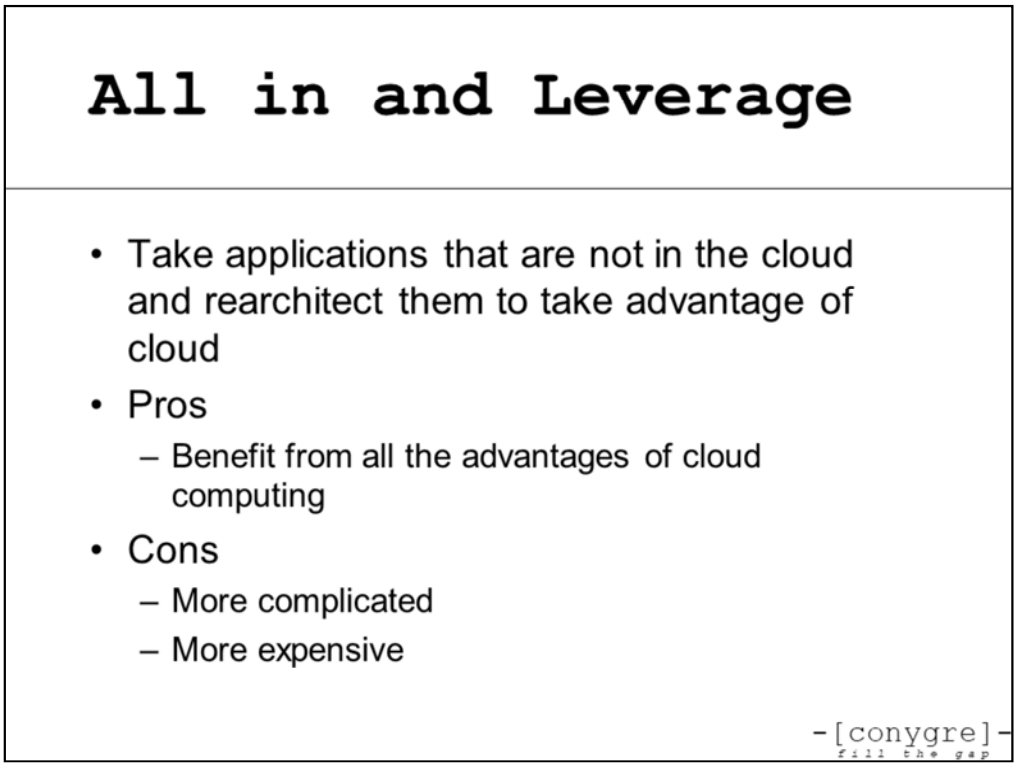


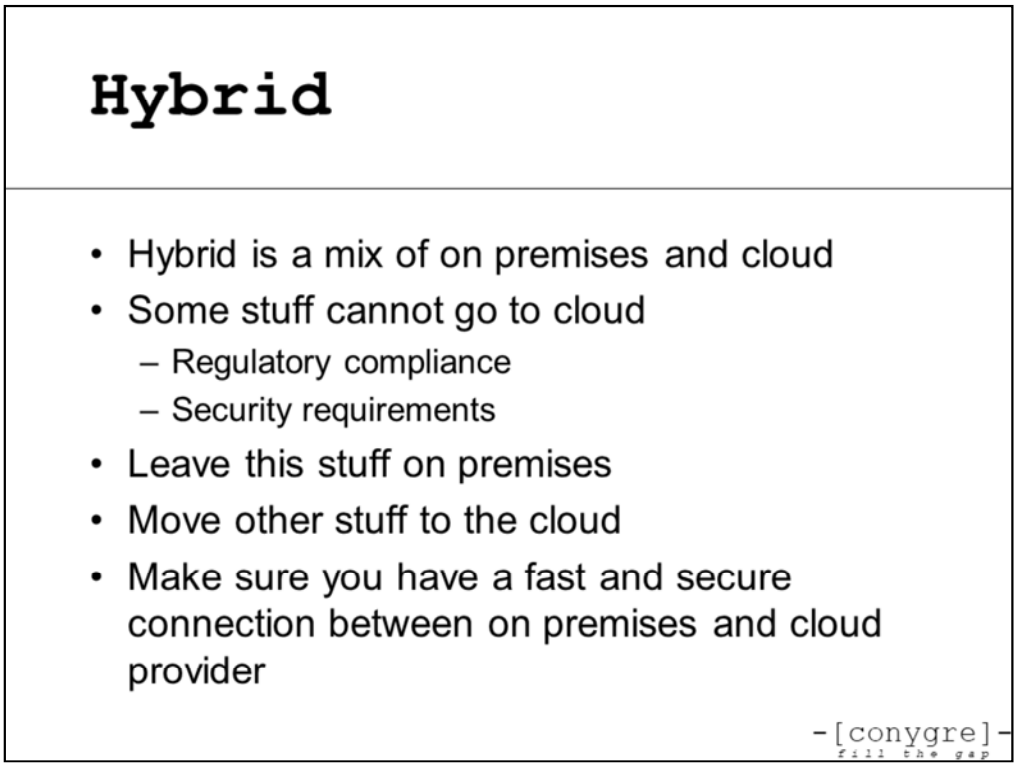


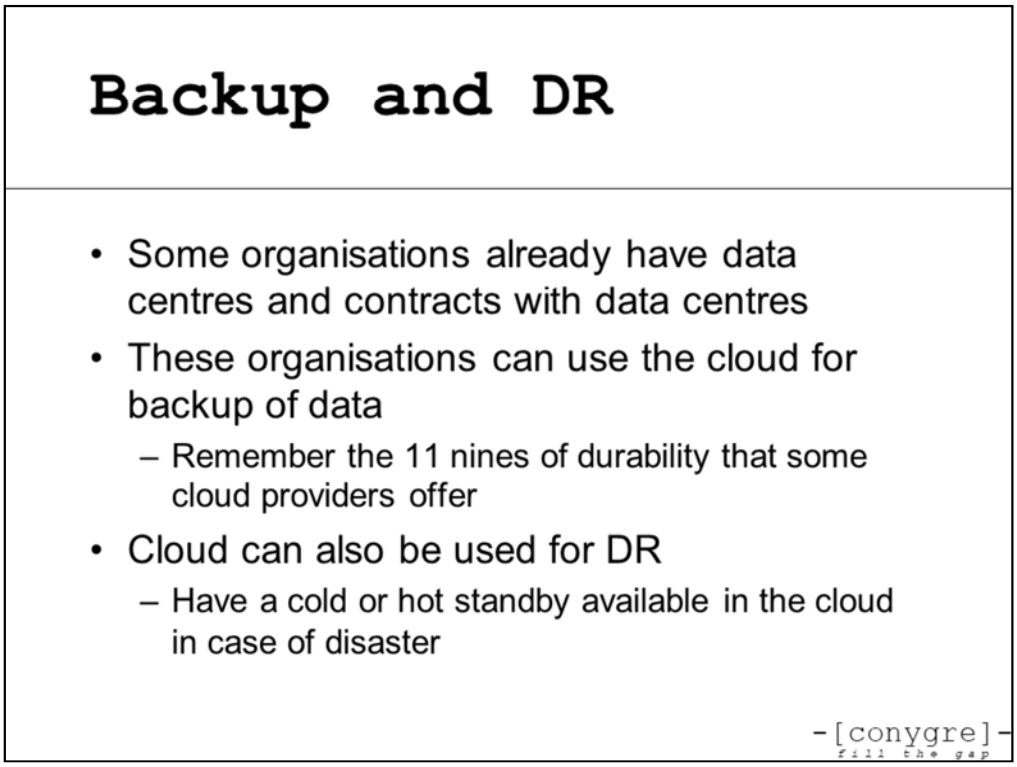
Cloud Fundamentals

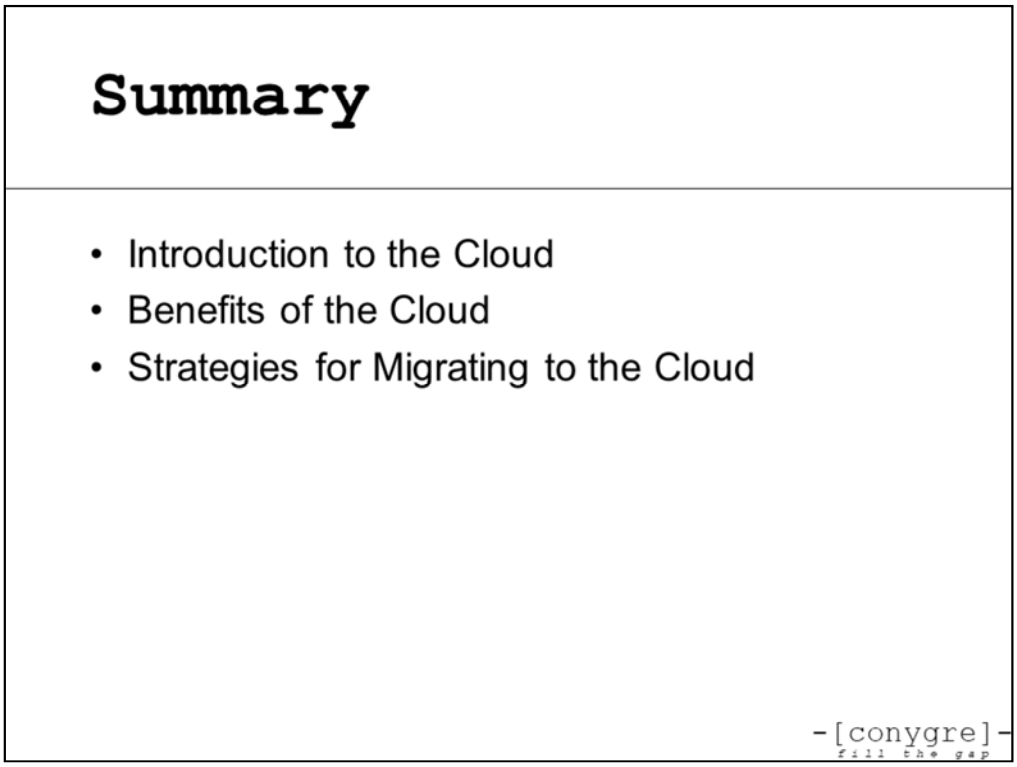




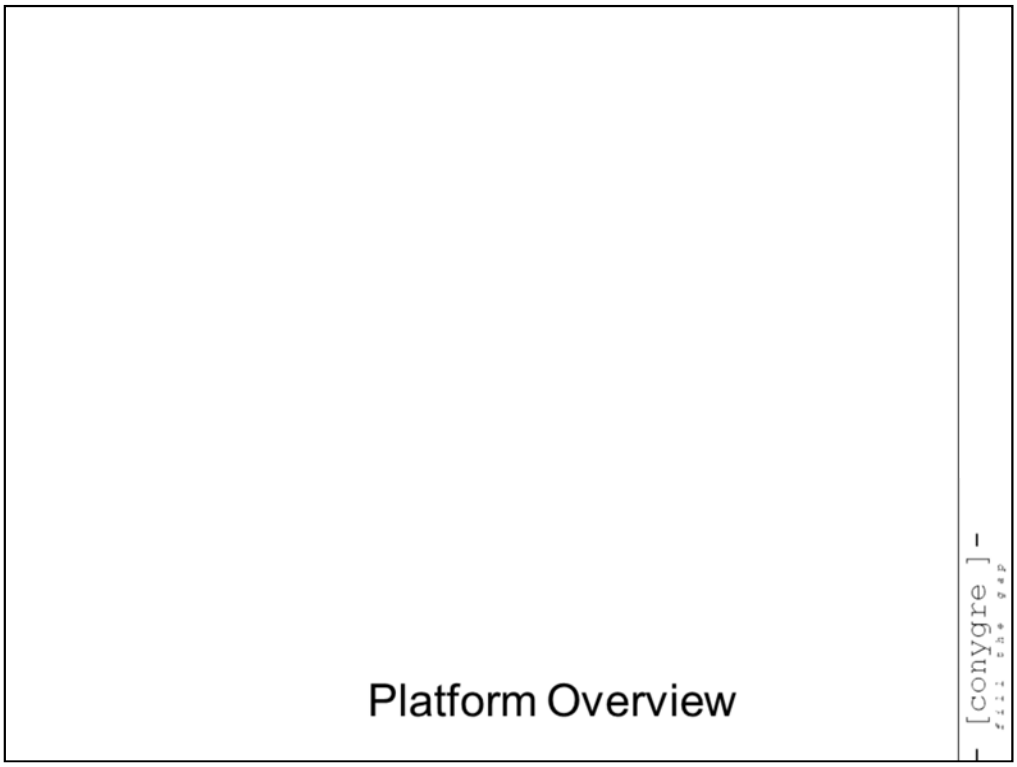




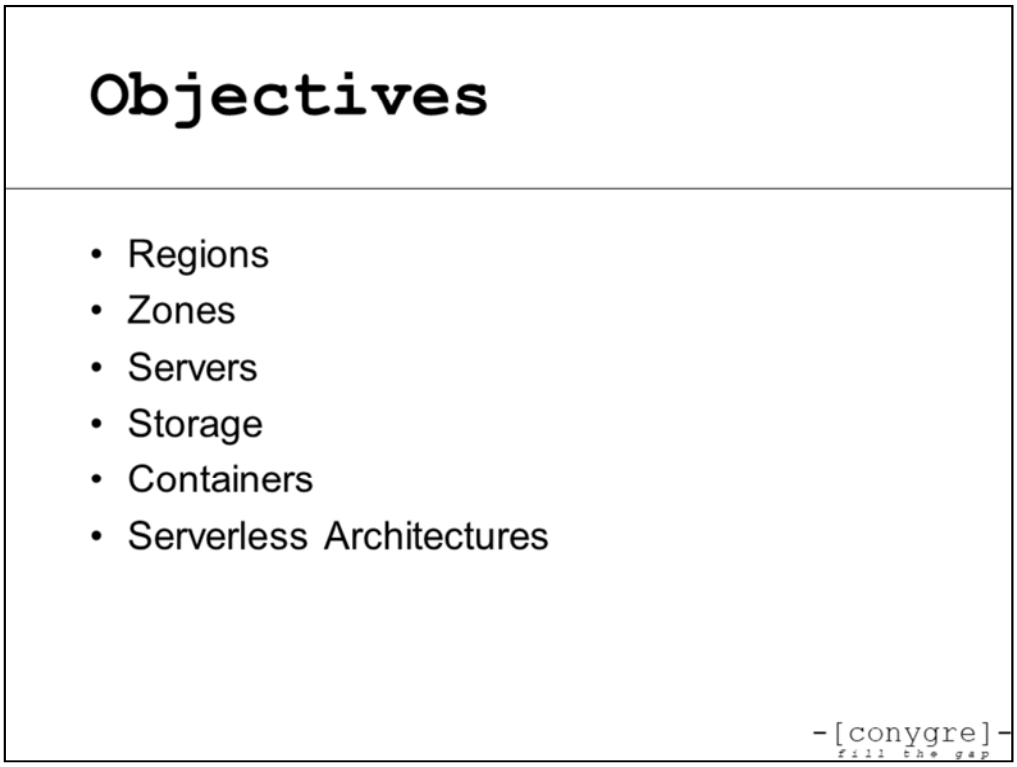




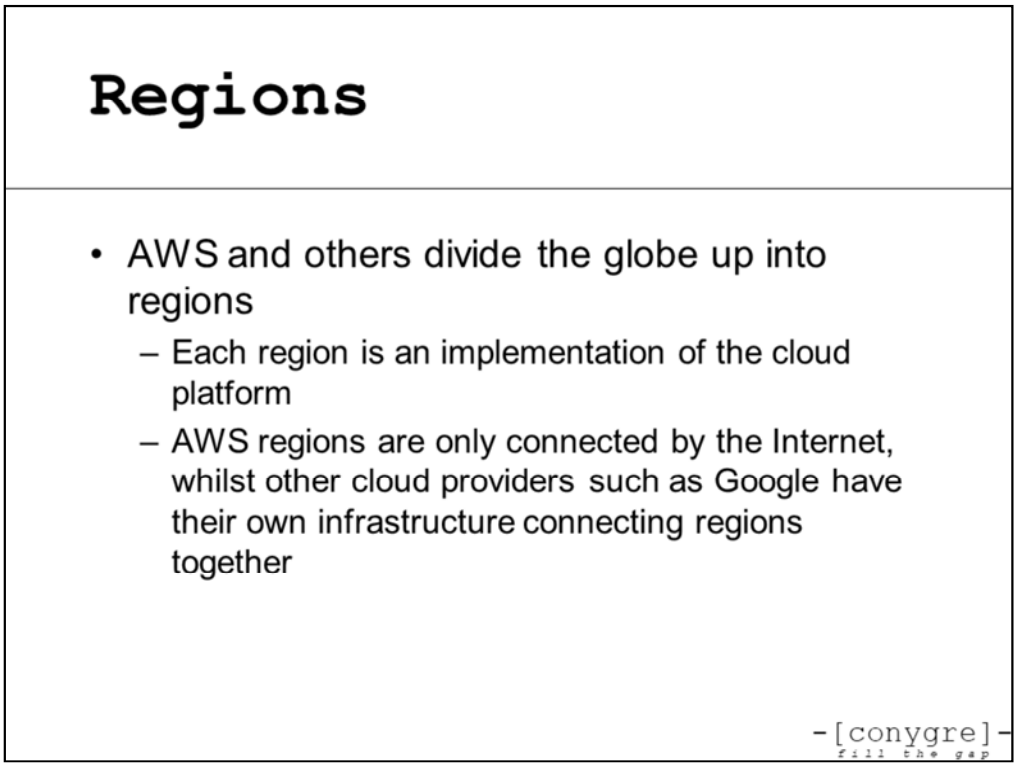
Platform Overview

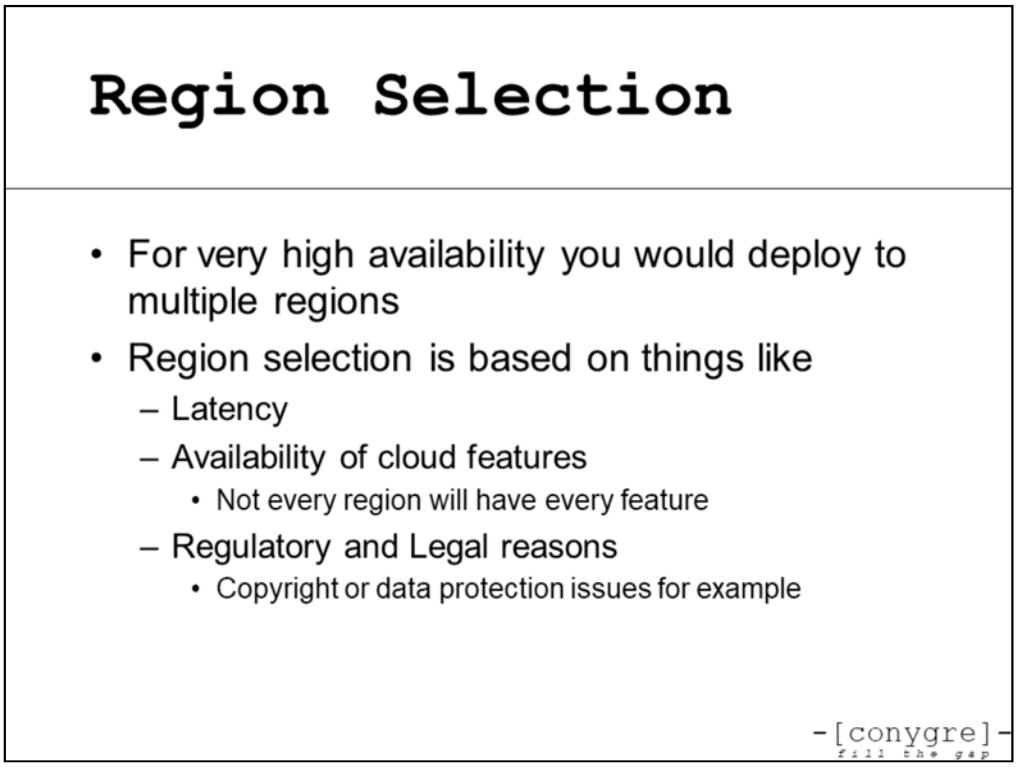


Platform Overview

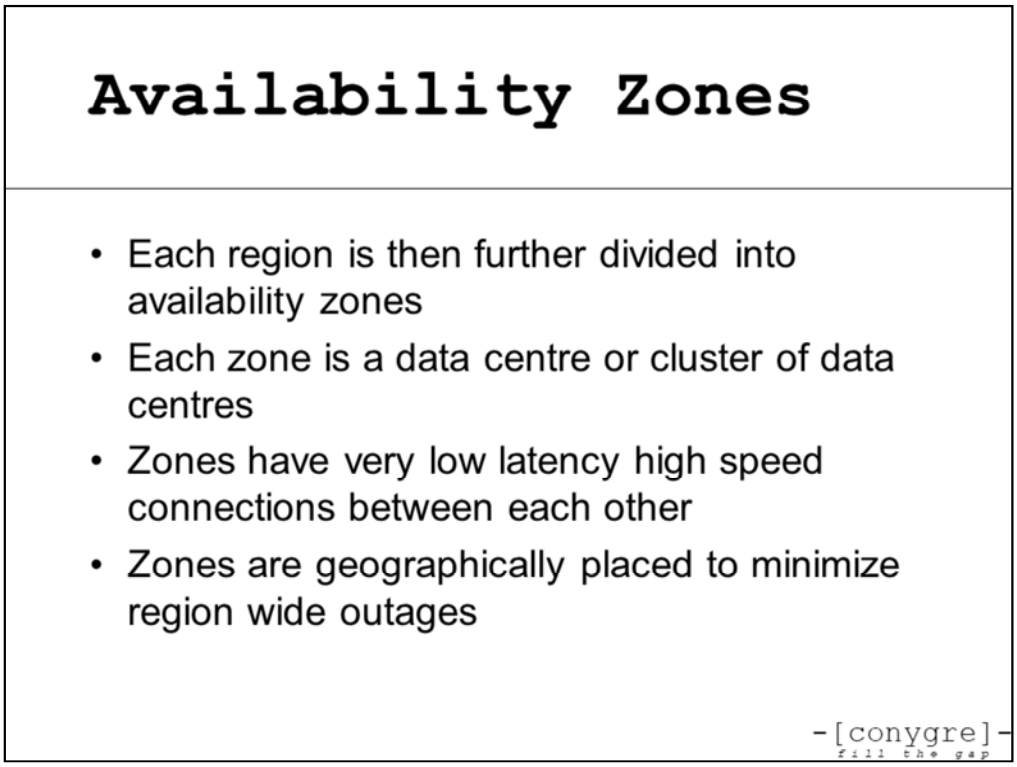


Platform Overview

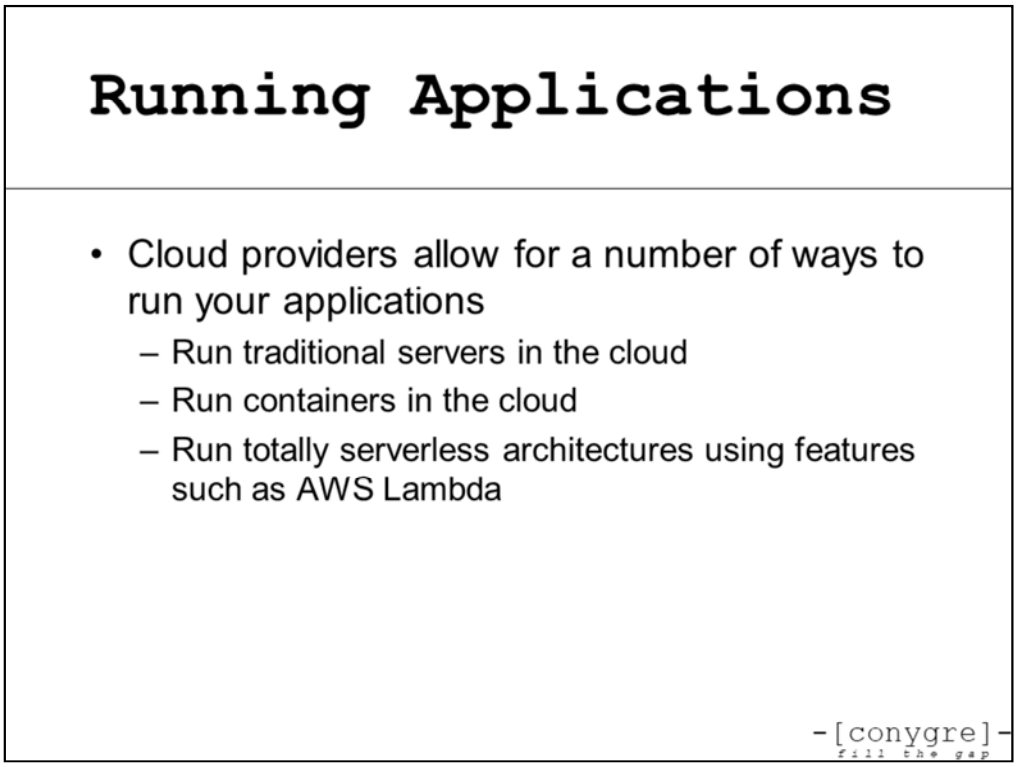




Platform Overview



Platform Overview



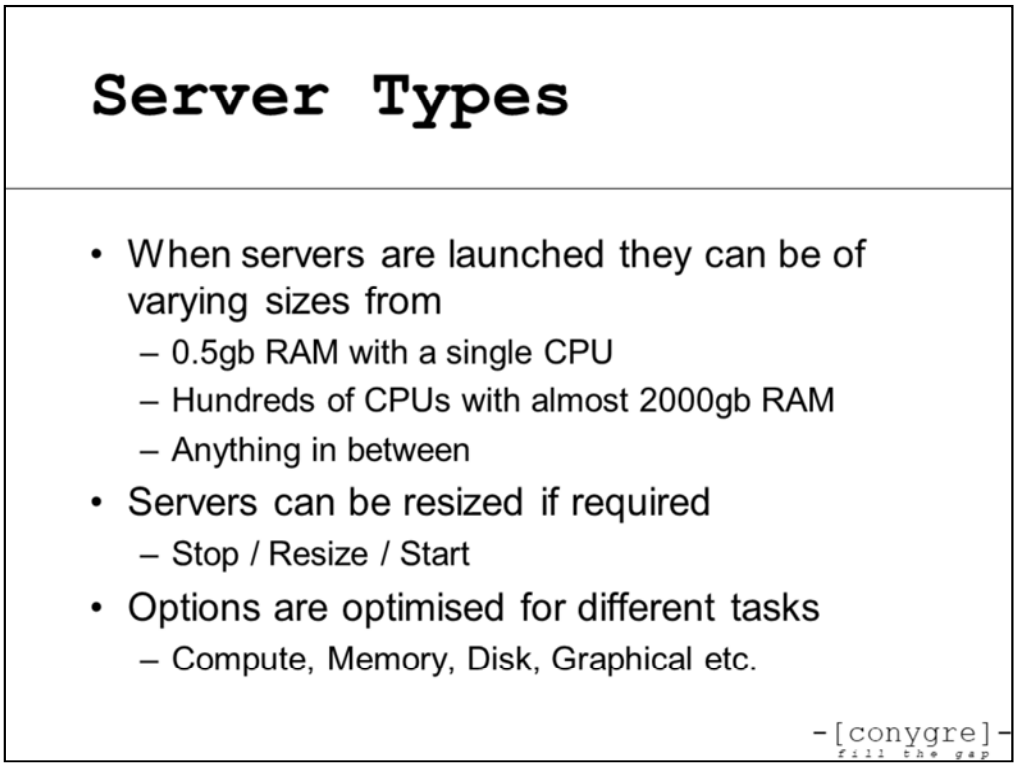
Platform Overview

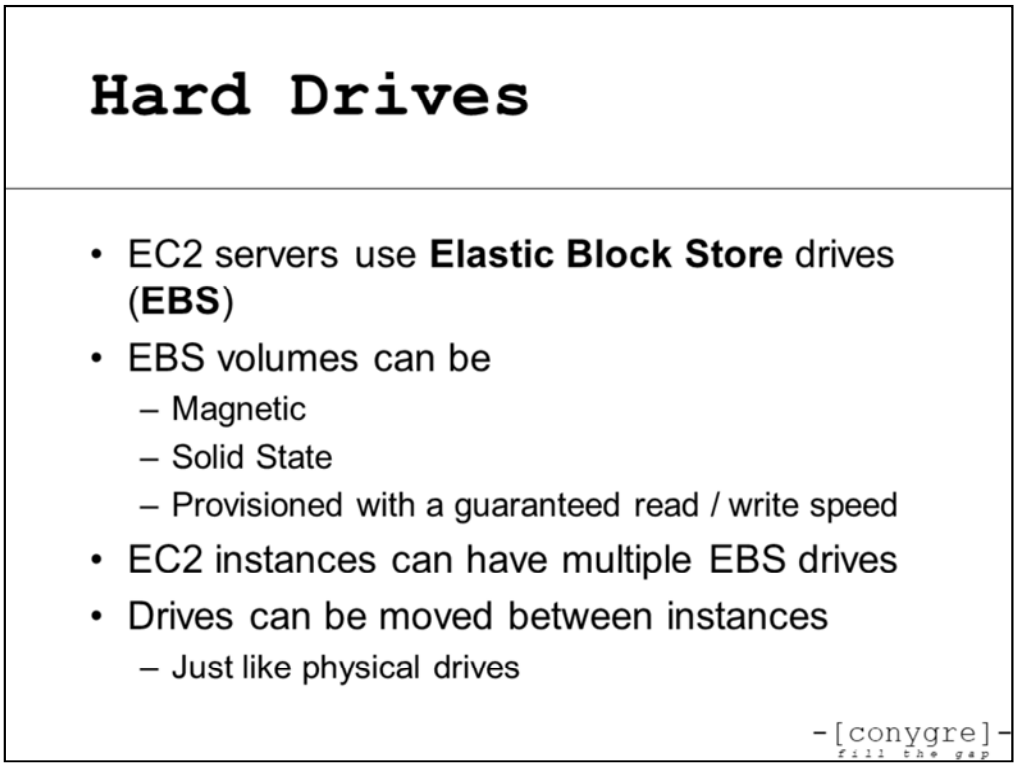
Running Servers – EC2

- **Elastic Compute Cloud** (**EC2**) servers can be launched
- Servers run in availability zones and are launched from **Amazon Machines Images** (**AMI**)
- AMIs can be
  - Standard AWS provided Linux and Windows variations
  - Third Party Provided – lots to choose from!
  - Created by you

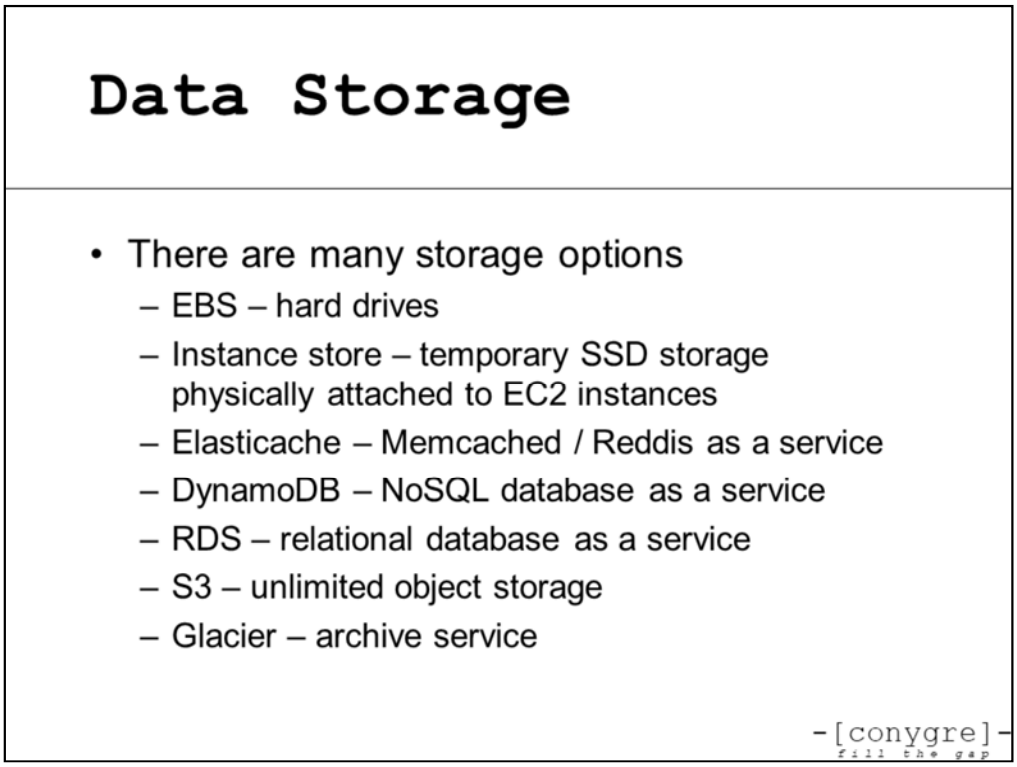
-[conygre]-
fill the gap

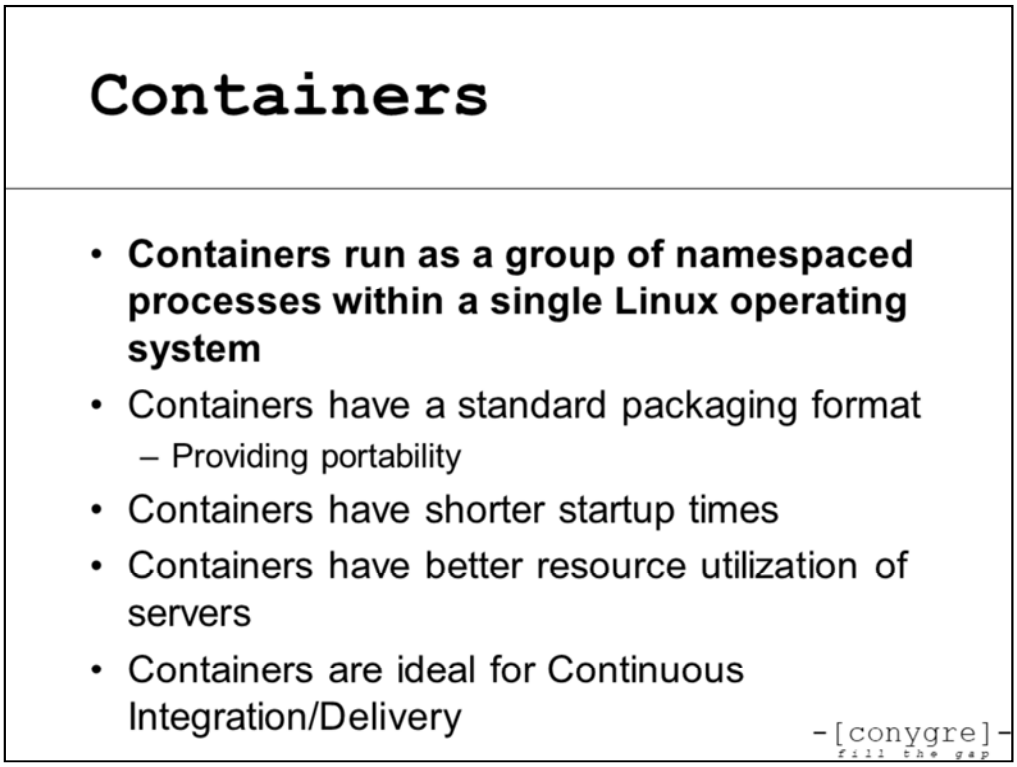
Platform Overview

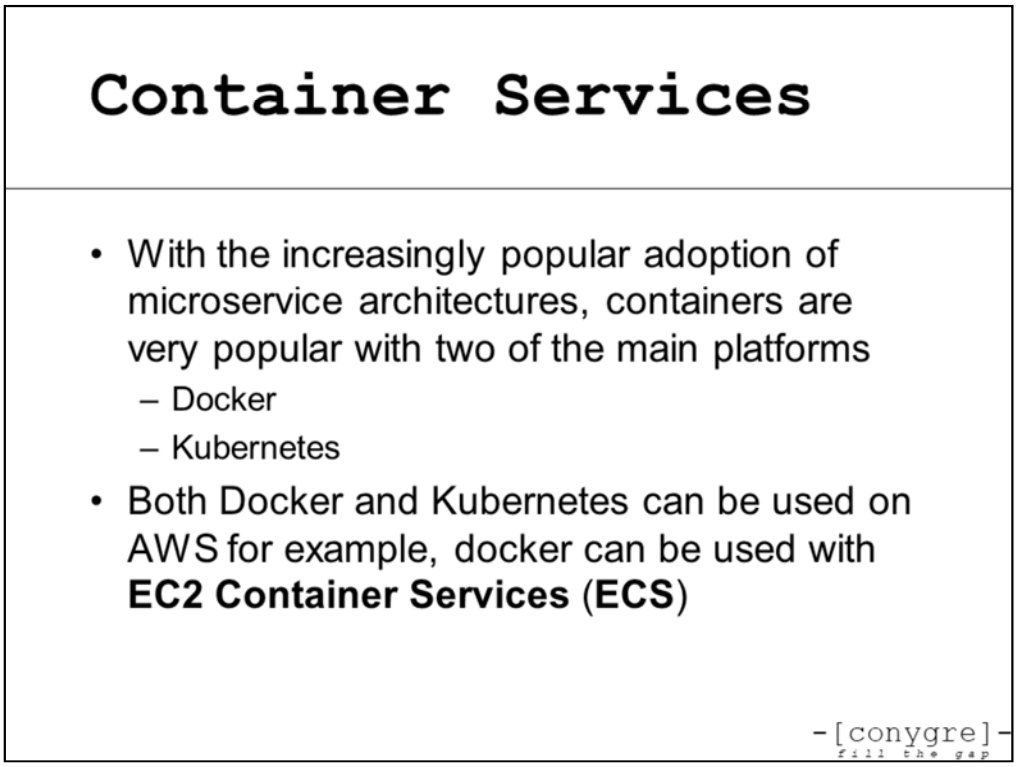




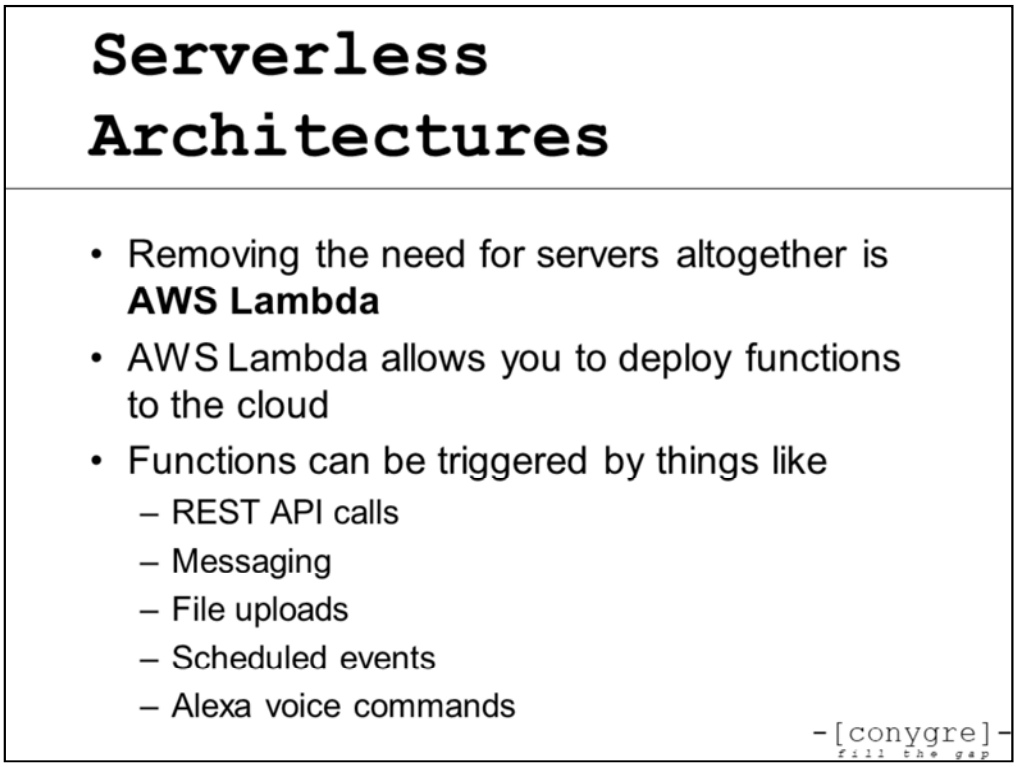
Platform Overview



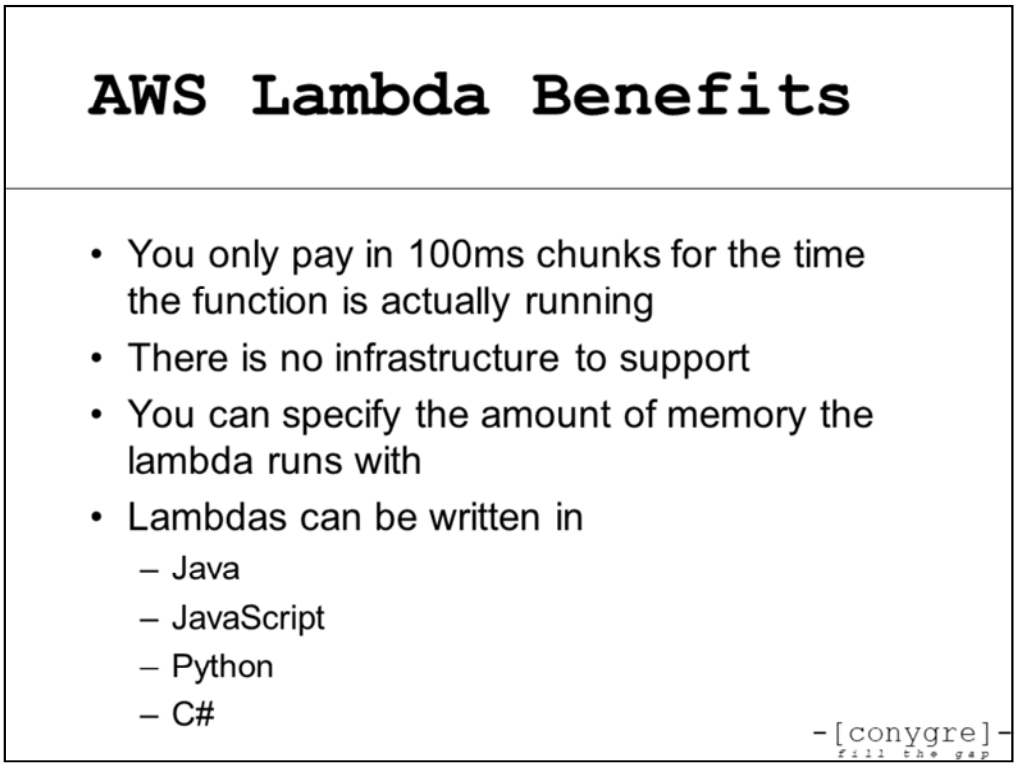




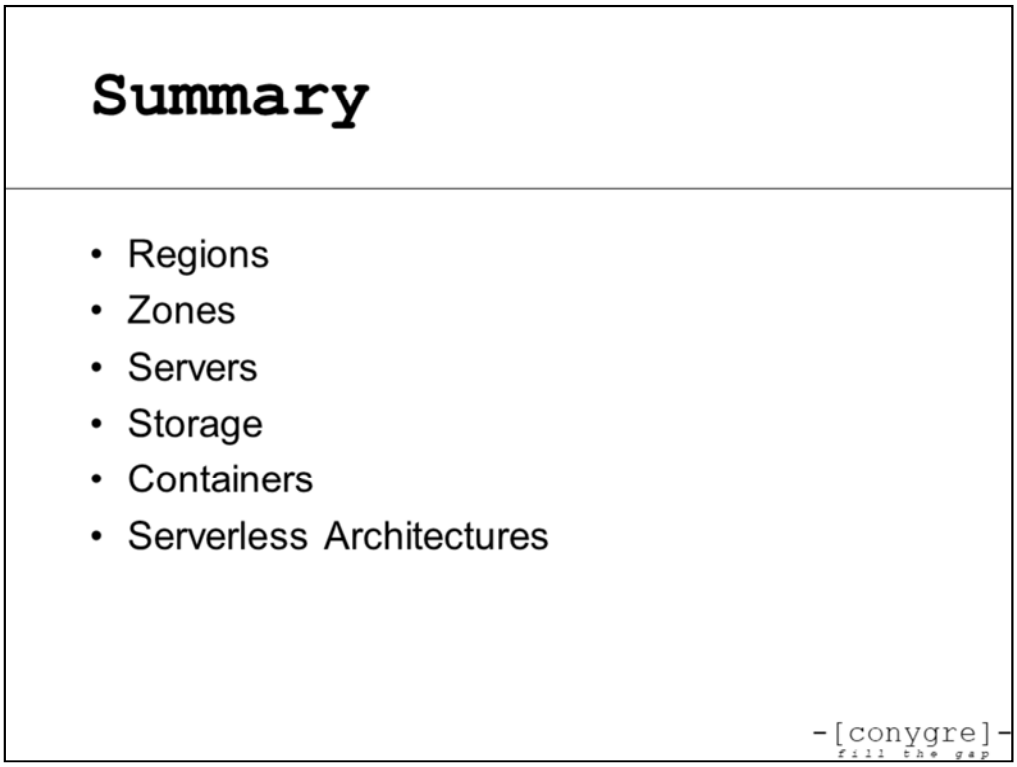
Platform Overview



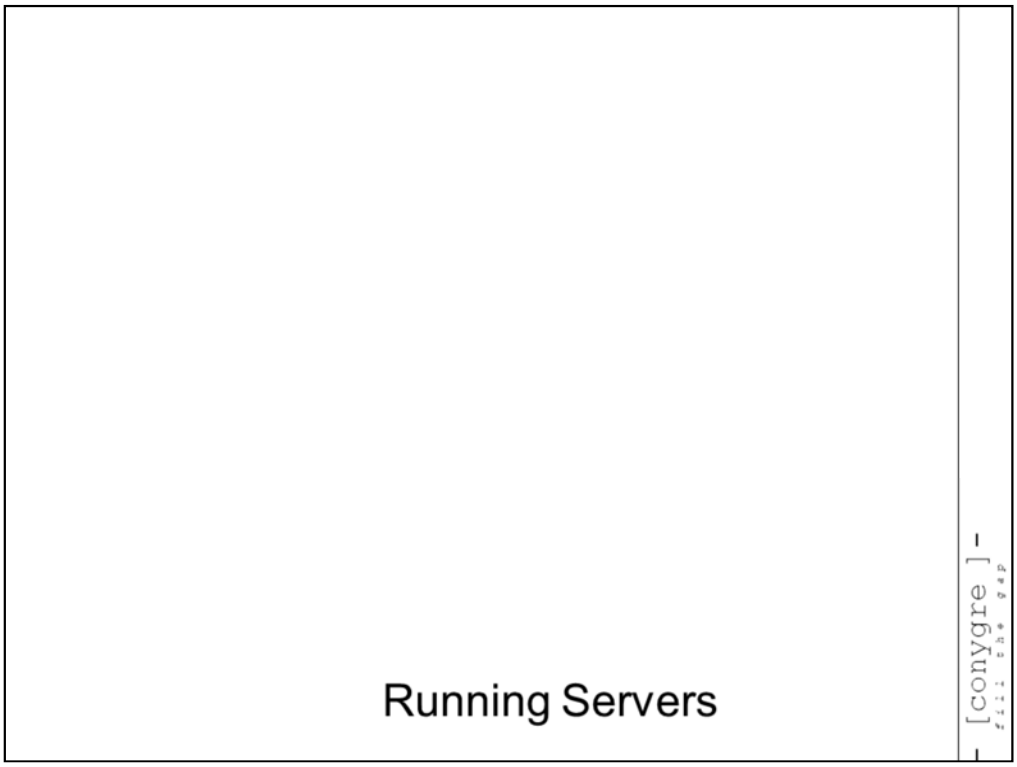
Platform Overview

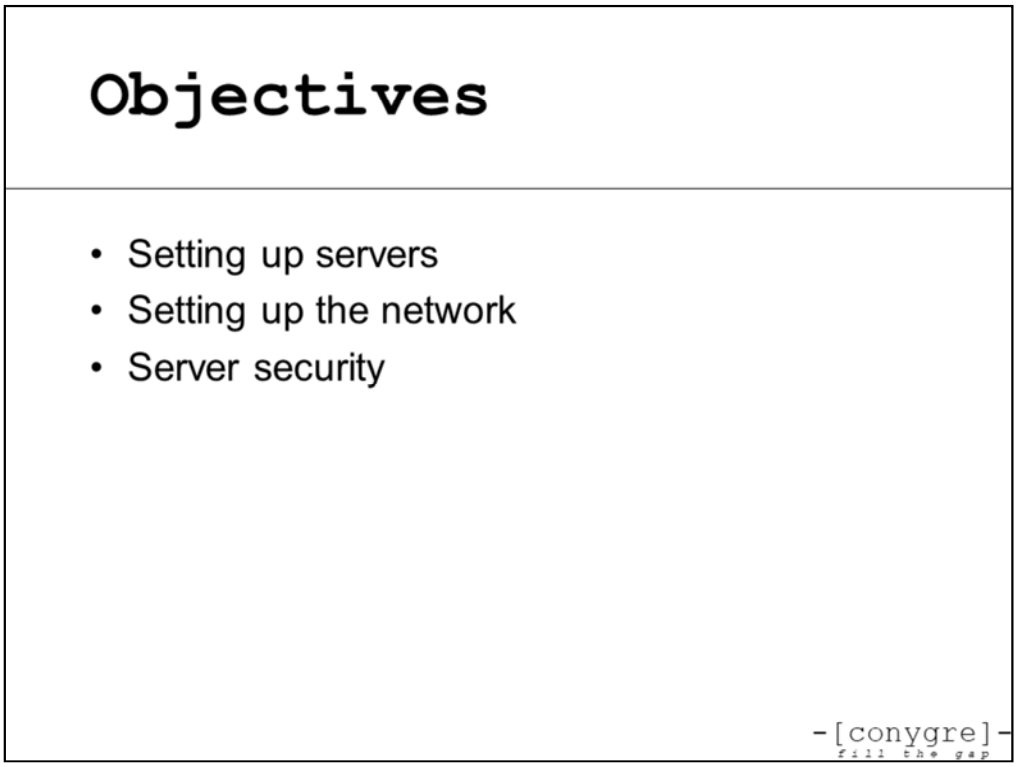


Platform Overview

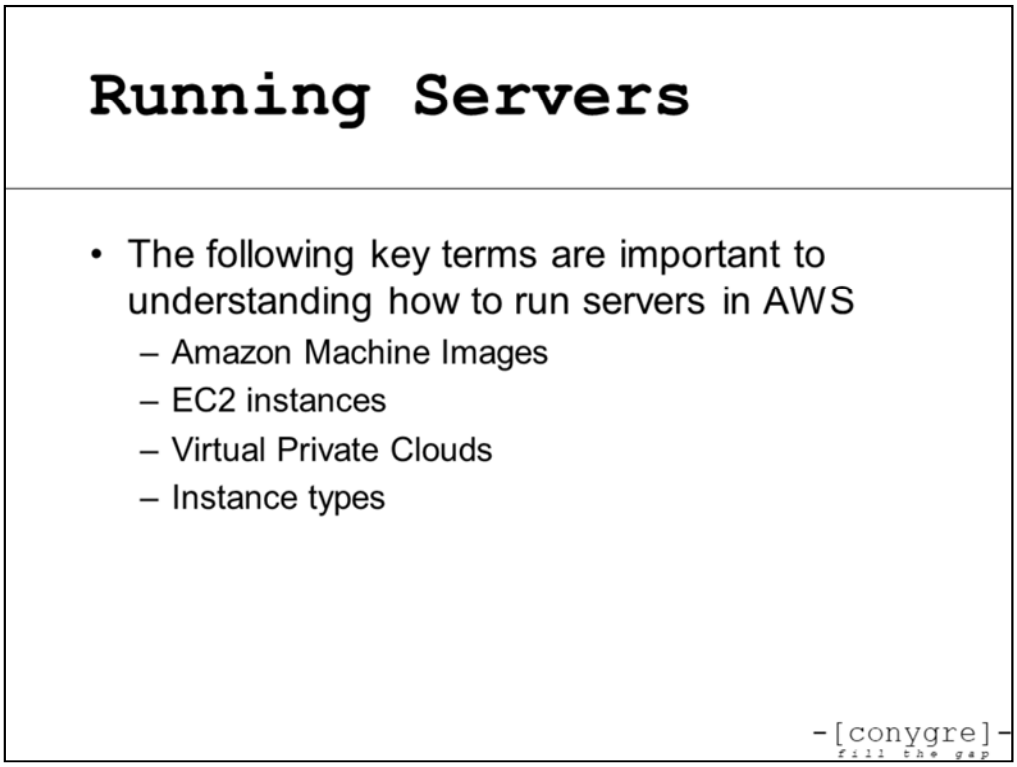


Running Servers





Running Servers



Amazon Machine Images

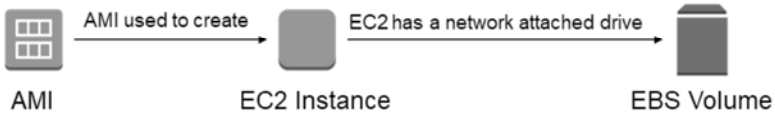
- An Amazon Machine Image (AMI) is the baseline install for your server
- AMIs can be
  - Windows or Linux
  - Provided by Amazon, you, or a third party
  - Can include your entire application, or just be a basic Windows / Linux operating system
- An AMI is the template for your server
  - Like a VMWare Appliance or a Virtual Box image

-[conygre]-
fill the gap

Running Servers

EC2 Instances

- EC2 instances are the servers that you run based on the AMI
- An EC2 instance will have at least one drive, usually an EBS, and will be of a certain type that you decide



-[conygre]-
fill the gap

EC2 Instance Sizing

- EC2 Instances can be of different sizes

Range	Role
T / M	General Purpose servers
C	Compute optimised
I	IO Optimised
G	Graphical processing optimised
R	Memory optimised

- For a full description visit
  - https://aws.amazon.com/ec2/instance-types/
- You can change an instance type by stopping / resizing / restarting a server

-[conygre]-
fill the gap

Block Storage

- The standard block storage option is Elastic Block Store (EBS)
- EBS volumes are network attached and are used by EC2 instances as their hard drives
- EBS volumes can have the following options
  - Magnetic
  - Solid State (the default)
  - Solid State Provisioned (provisioned level of disk IO)
  - Solid State Network Optimized (improved Network IO)
- EBS volumes can also be encrypted

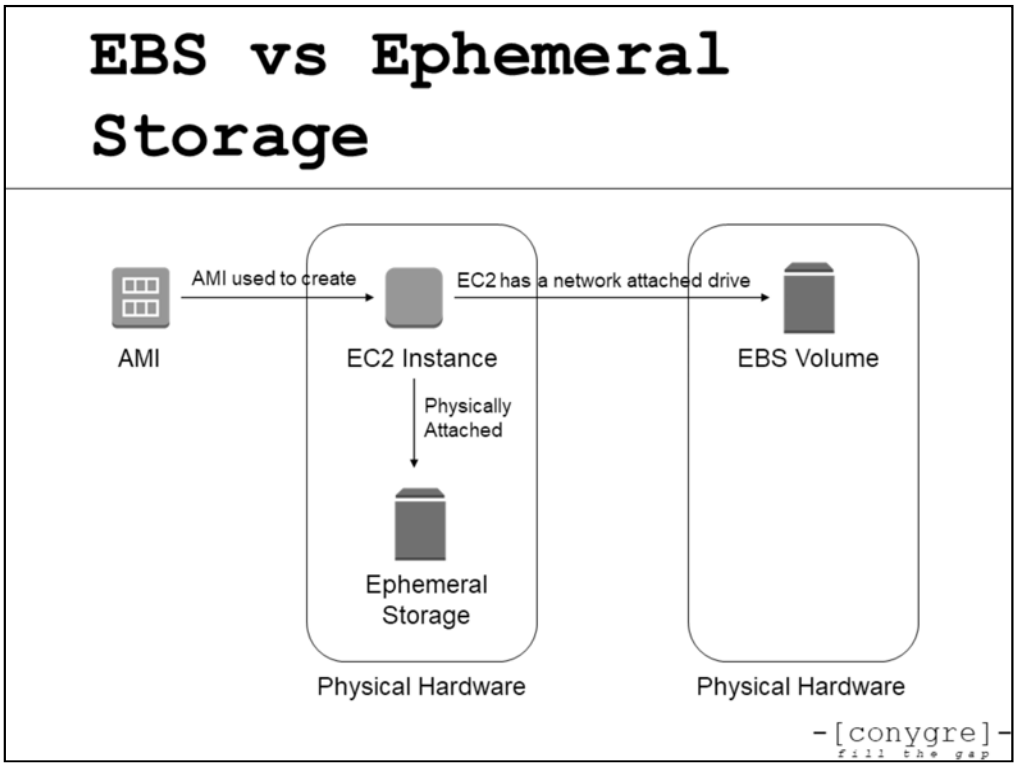
-[conygre]-
fill the gap

Ephemeral Storage

- EC2 instances can also have physically attached drives referred to as ephemeral storage and sometimes referred to as instance storage
- When an EC2 instance is stopped and started they always restart on different hardware
  - Therefore, instance store drives do not survive an EC2 restart
- It is also possible to have EC2 instances that run exclusively on instance store
  - These cannot be stopped and started, only terminated

-[conygre]-
fill the gap

Running Servers



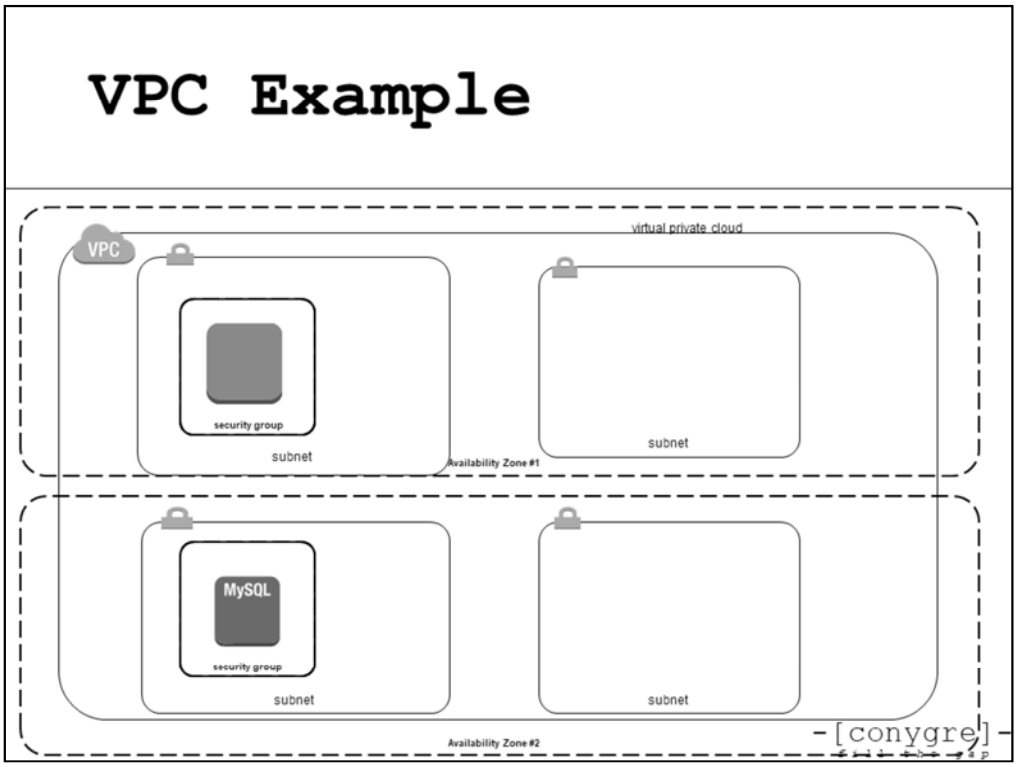
Running Servers

Networking

- EC2 instances run within a Virtual Private Cloud (VPC)
- The VPC is the virtual version of a physical networking environment consisting of
  - IP range
  - Subnets within that range
  - Internet Gateways, and NAT servers
  - VPN Gateways
- A VPC spans availability zones within a region so you can easily run your applications across multiple facilities

-[conygre]-
fill the gap

Running Servers



Running Servers

VPC IP Range

- A VPC has an IP address range
- VPCs can be connected together
  - Only if the IP ranges do not overlap
- VPCs can be connected to on premises via
  - VPN Gateway
  - AWS Direct Connect

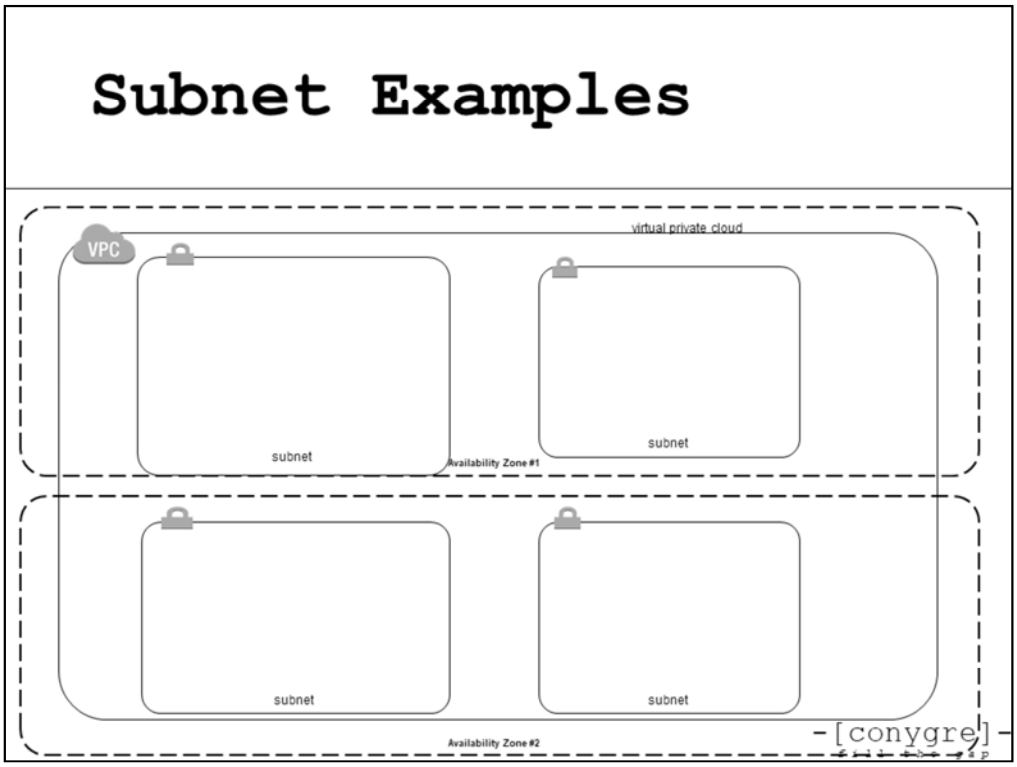
-[conygre]-
fill the gap

Subnets

- A VPC is broken down into **Subnets**
- A Subnet is a subset of the IP addresses in the VPC
- A Subnet
  - Cannot span availability zones
  - Can be on or off the Internet controlled through routing rules
- Subnets to be available to the Internet route through an **Internet Gateway**

-[conygre]-
fill the gap

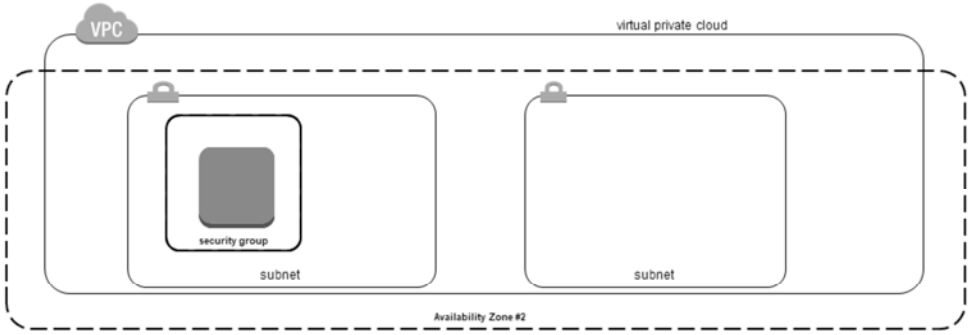
Running Servers



Running Servers

Security Groups

- EC2 instances are launched into subnets, and the access to ports is controlled by **security groups**



-[conygre]-
fill the gap

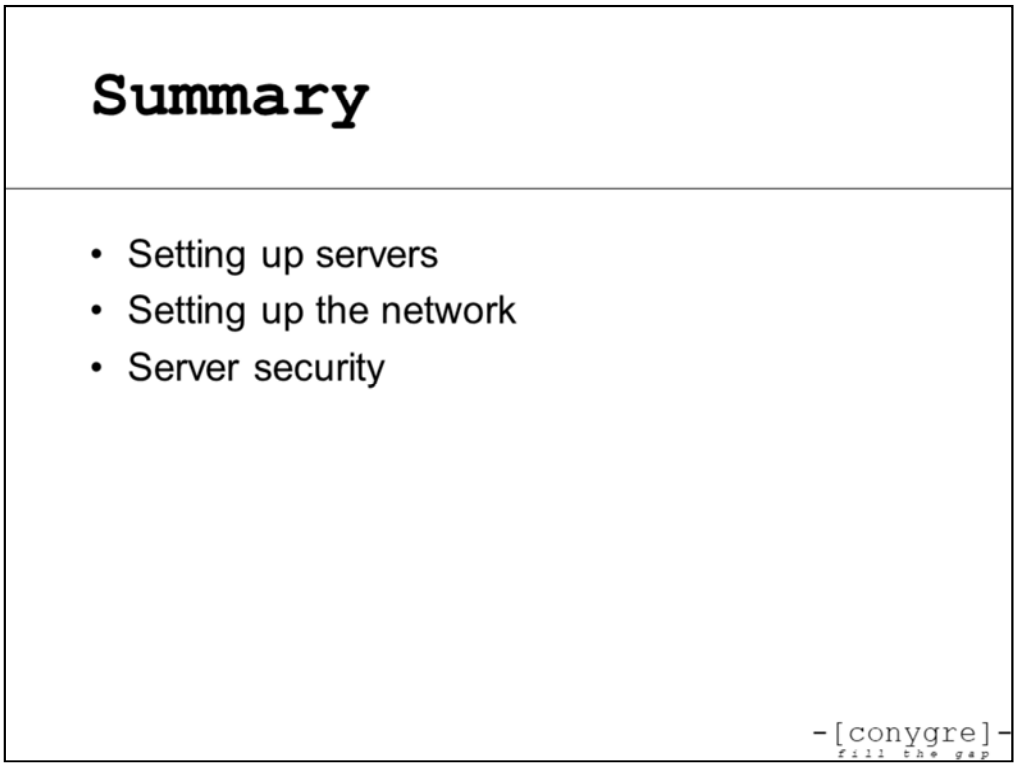
Running Servers

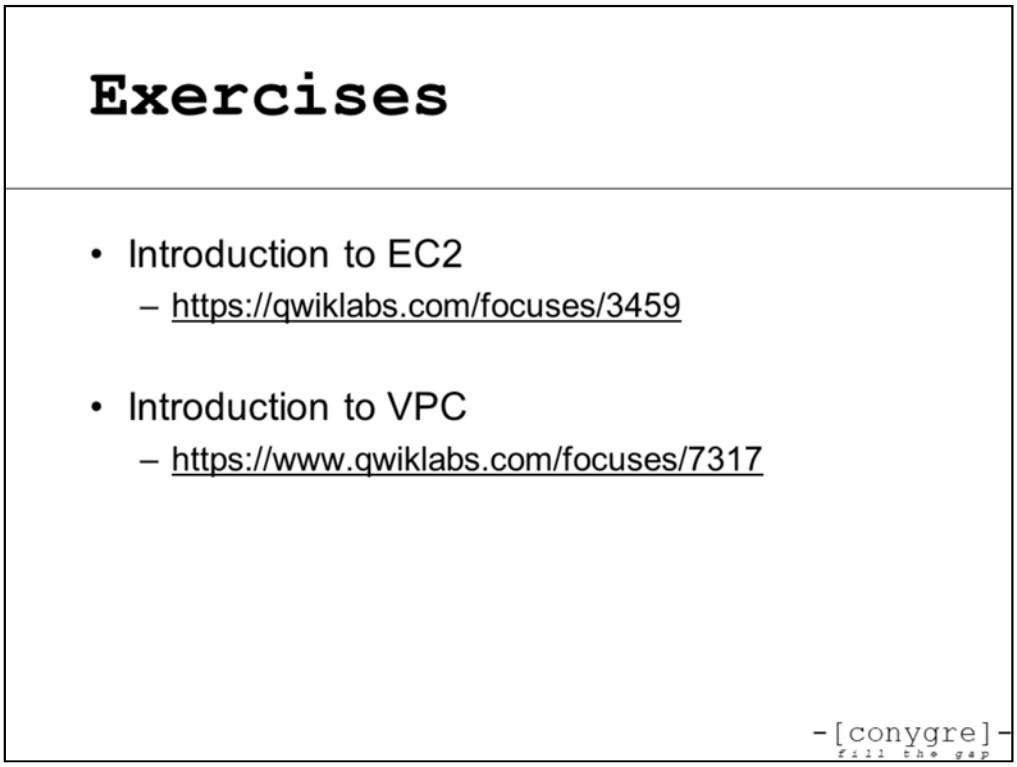
Running Servers

Server LifeCycle

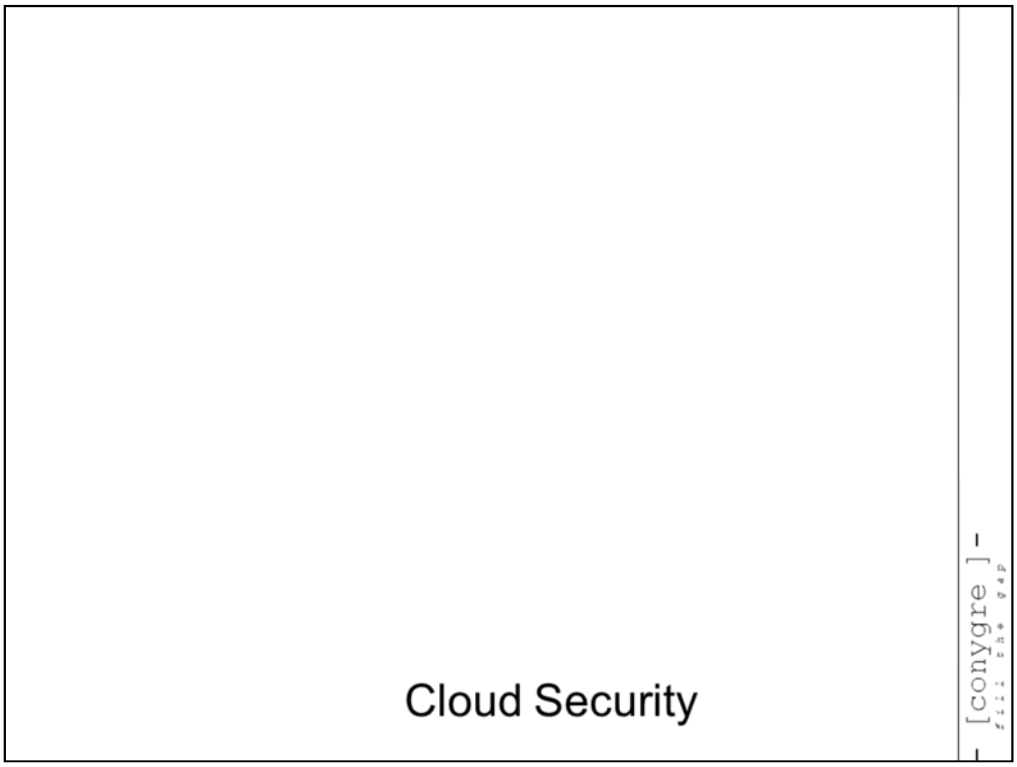
- Servers can be
  - Stopped
  - Restarted
  - Terminated
- Restarting a server causes it to relaunch on new physical hardware in case you are restarting due to a hardware fault
  - Be aware this means you will lose your ephemeral storage!

-[conygre]-
fill the gap

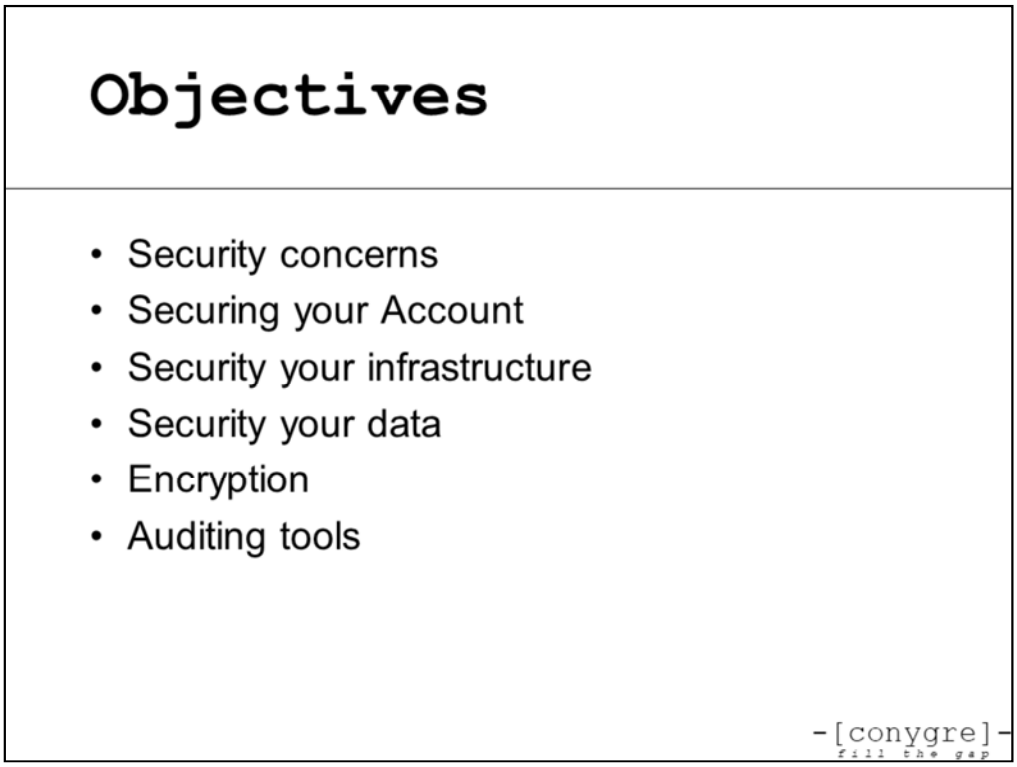




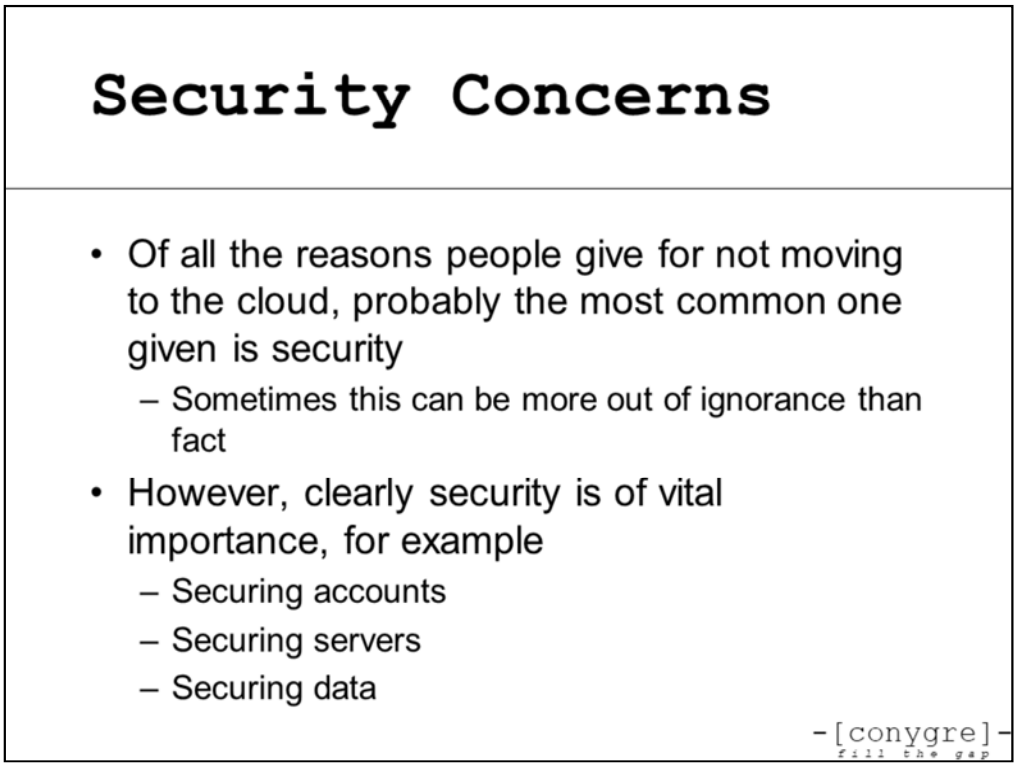
Security



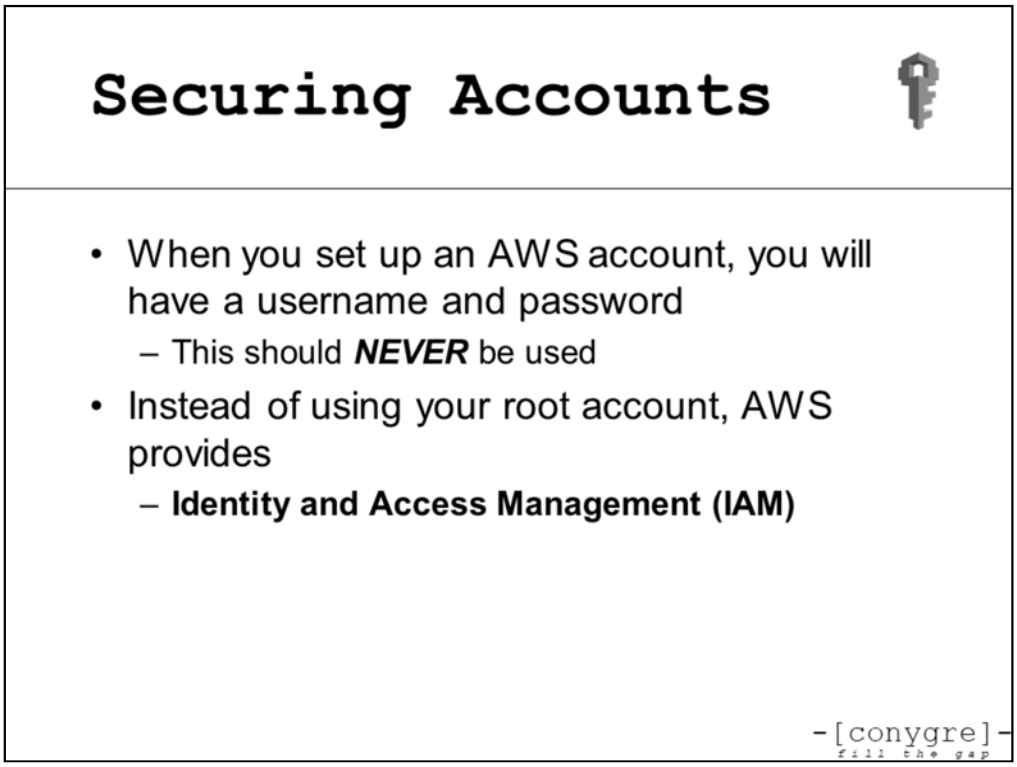
Security



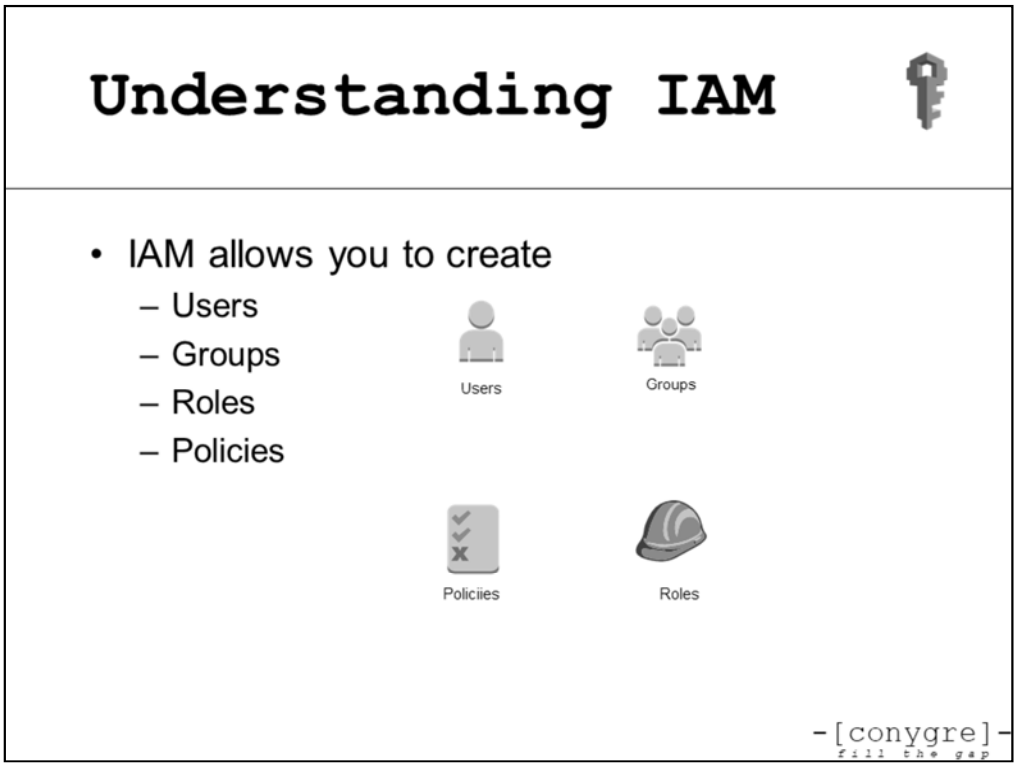
Security



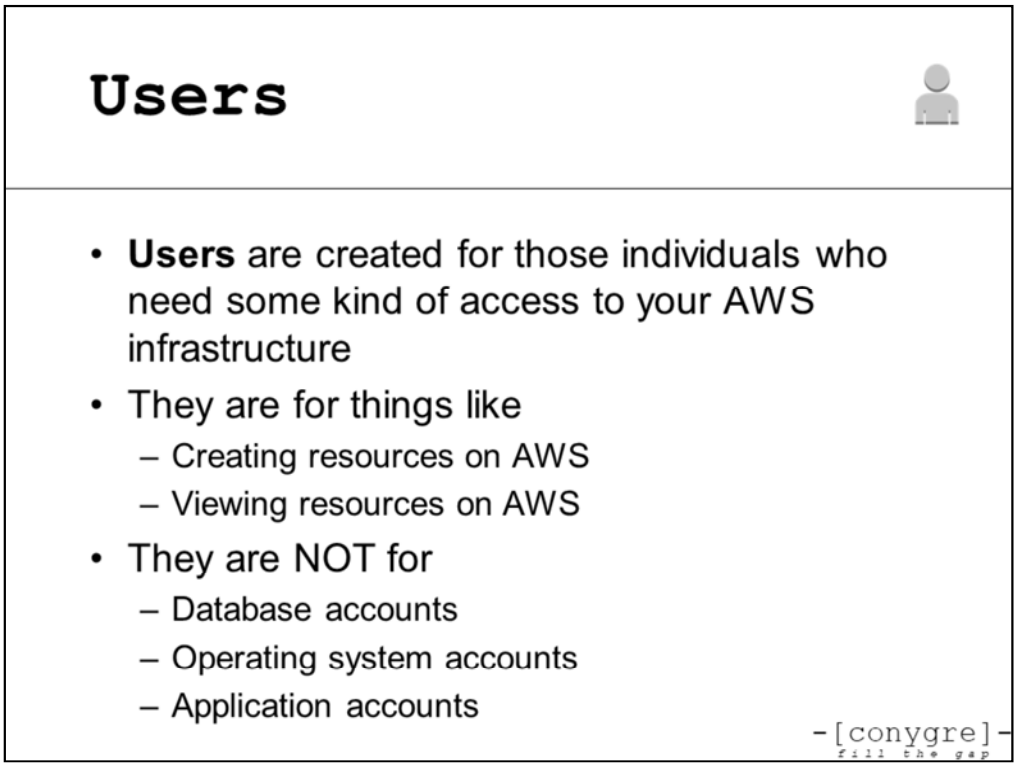
Security



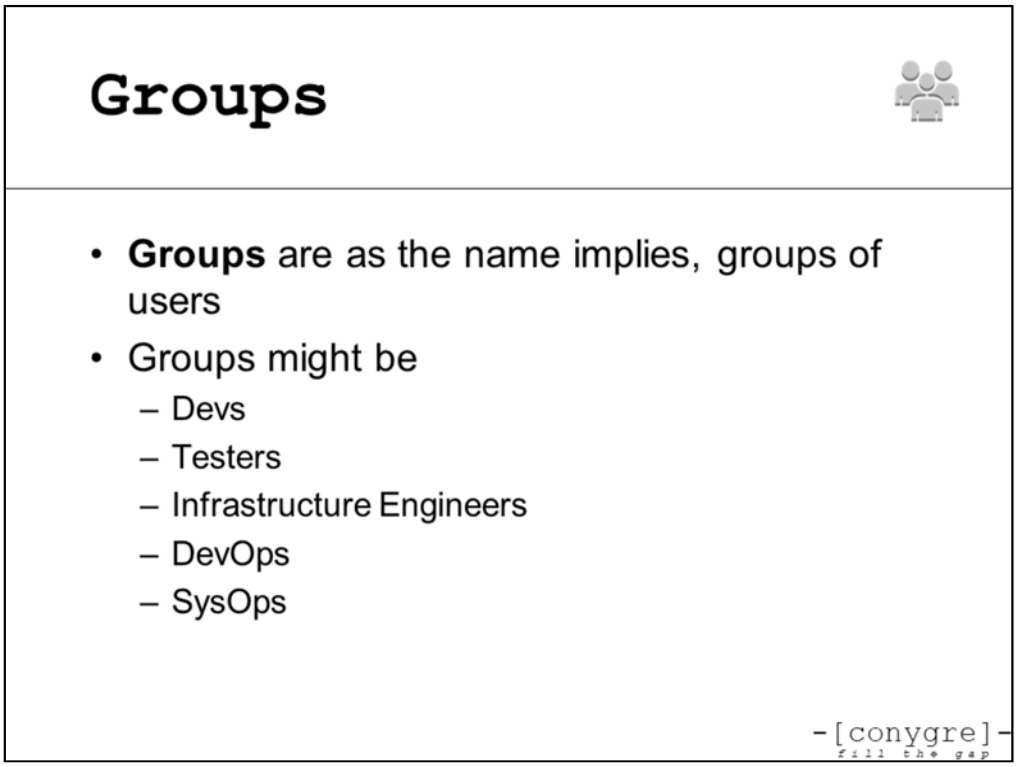
Security



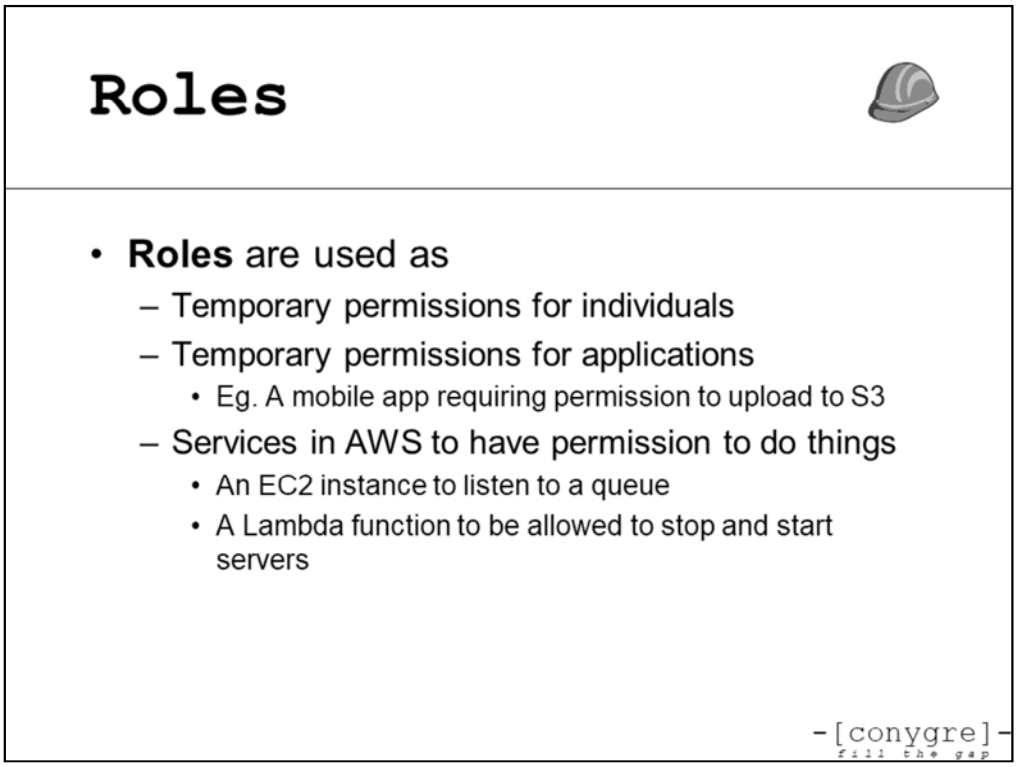
Security



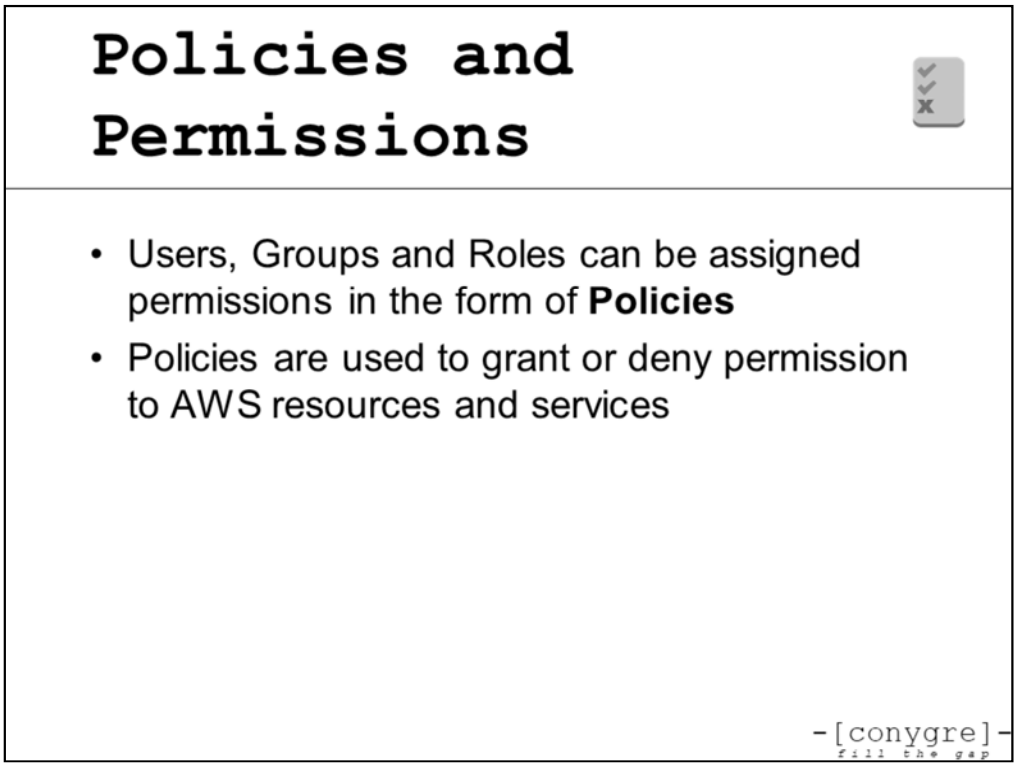
Security



Security



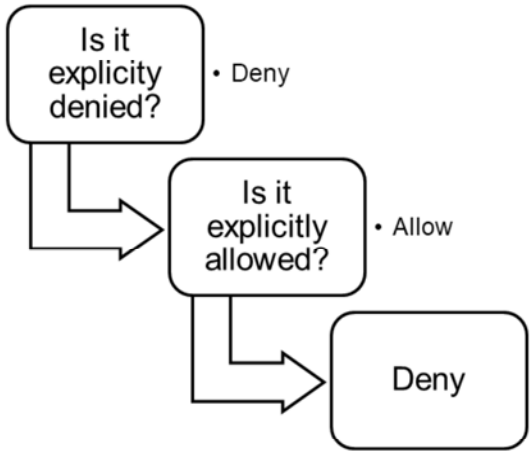
Security



Security

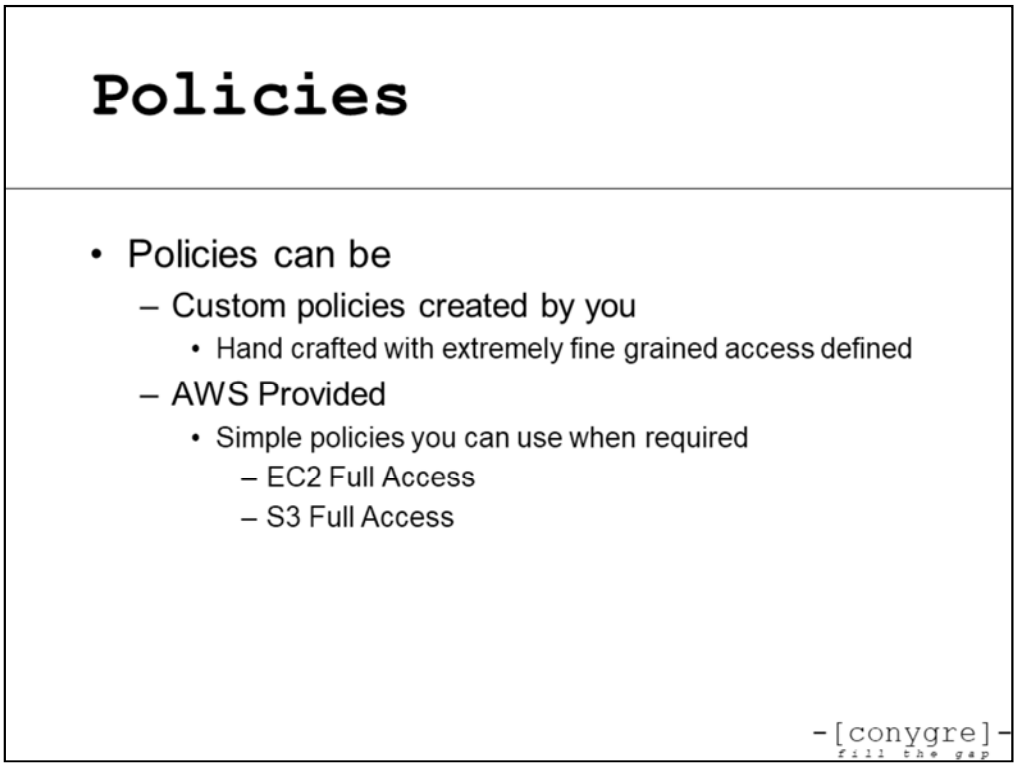
Default Permissions

- Everything is denied by default unless explicitly allowed
- Anything explicitly denied can never be allowed

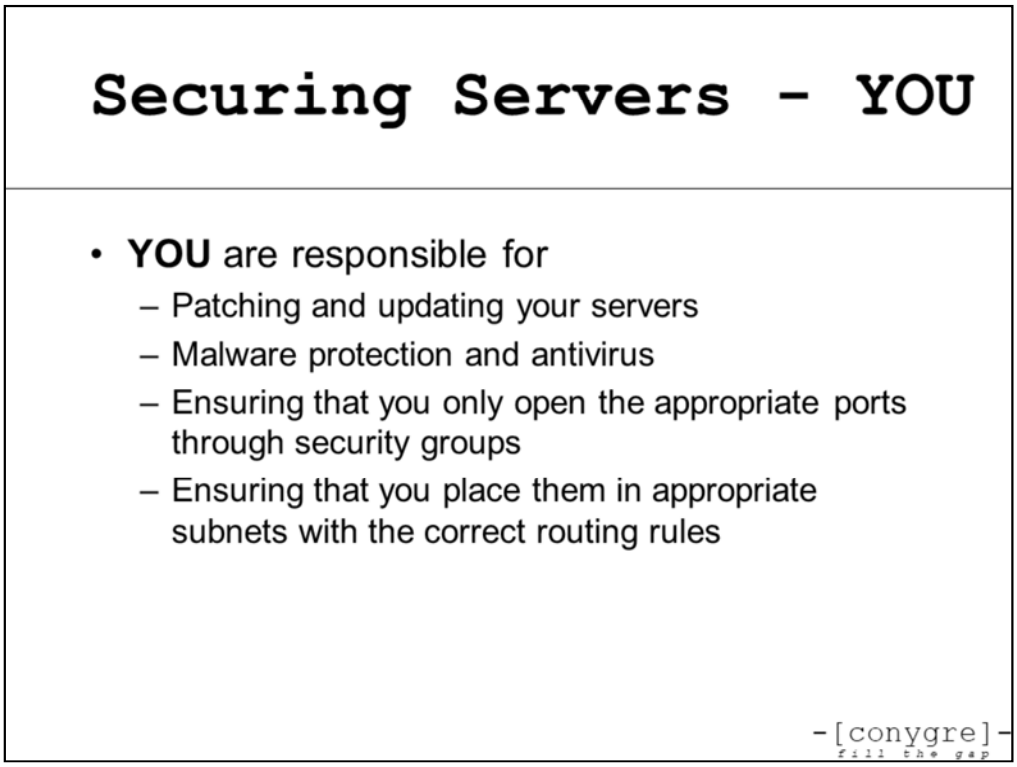


-[conygre]-
fill the gap

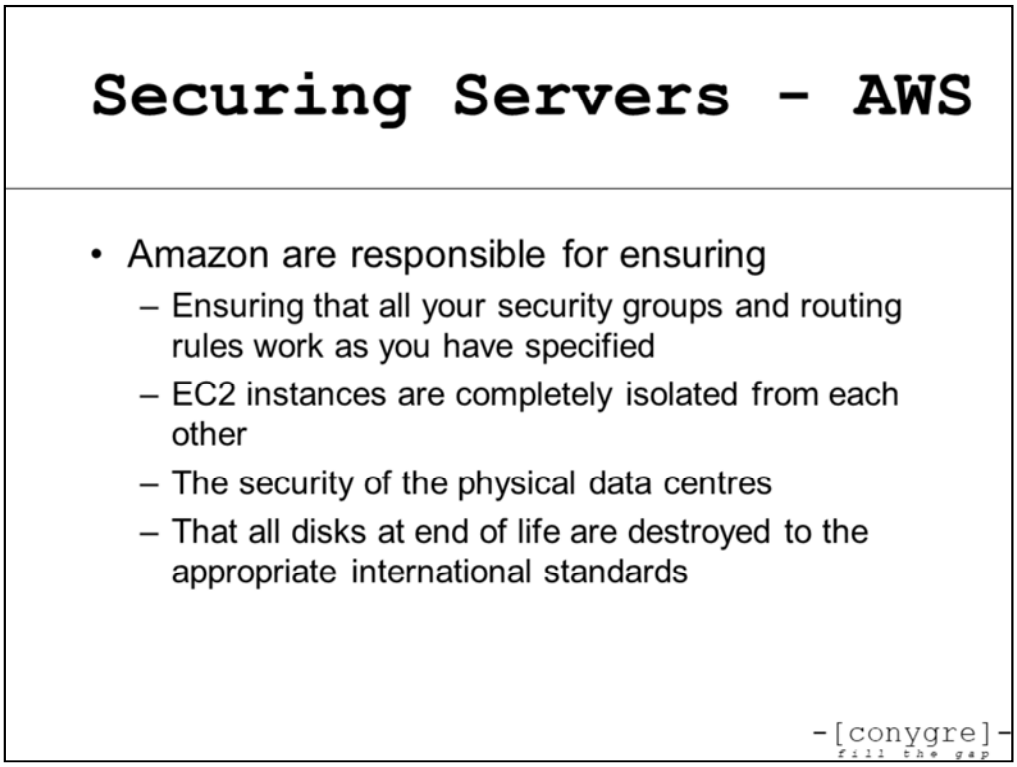
Security

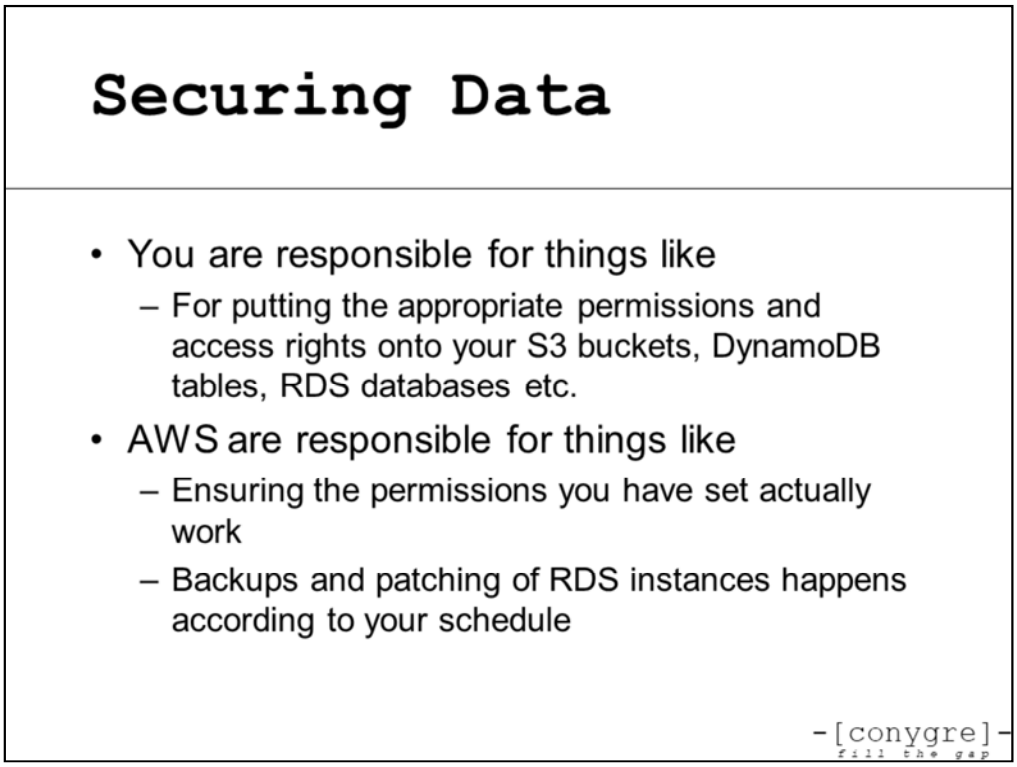


Security

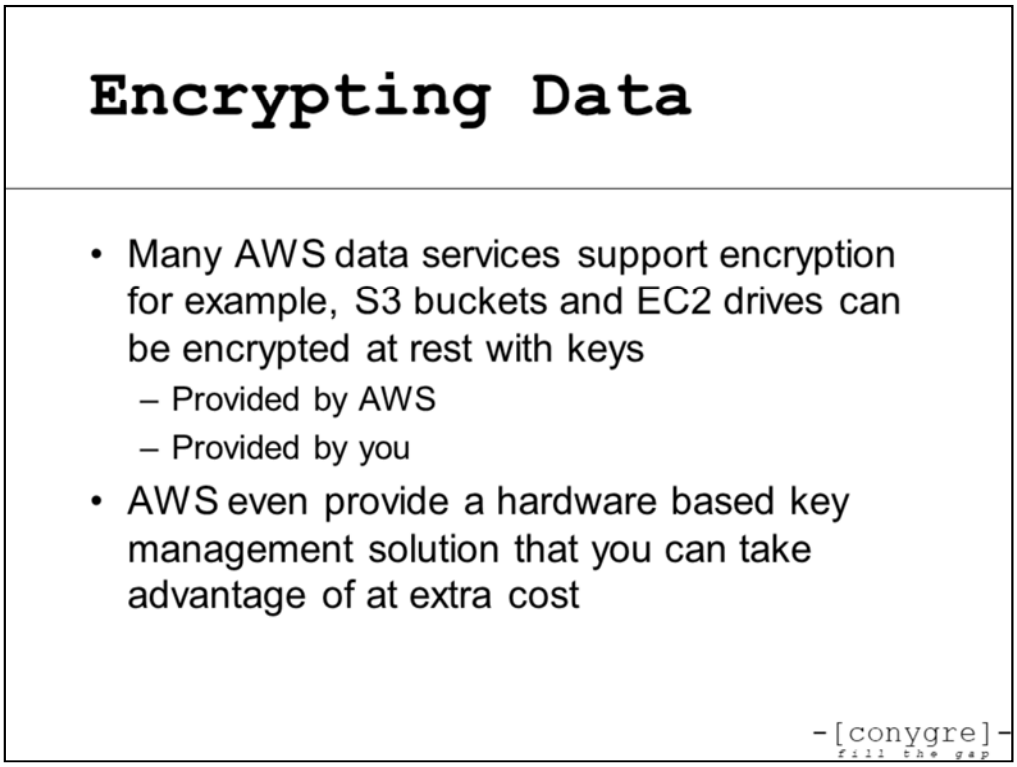


Security

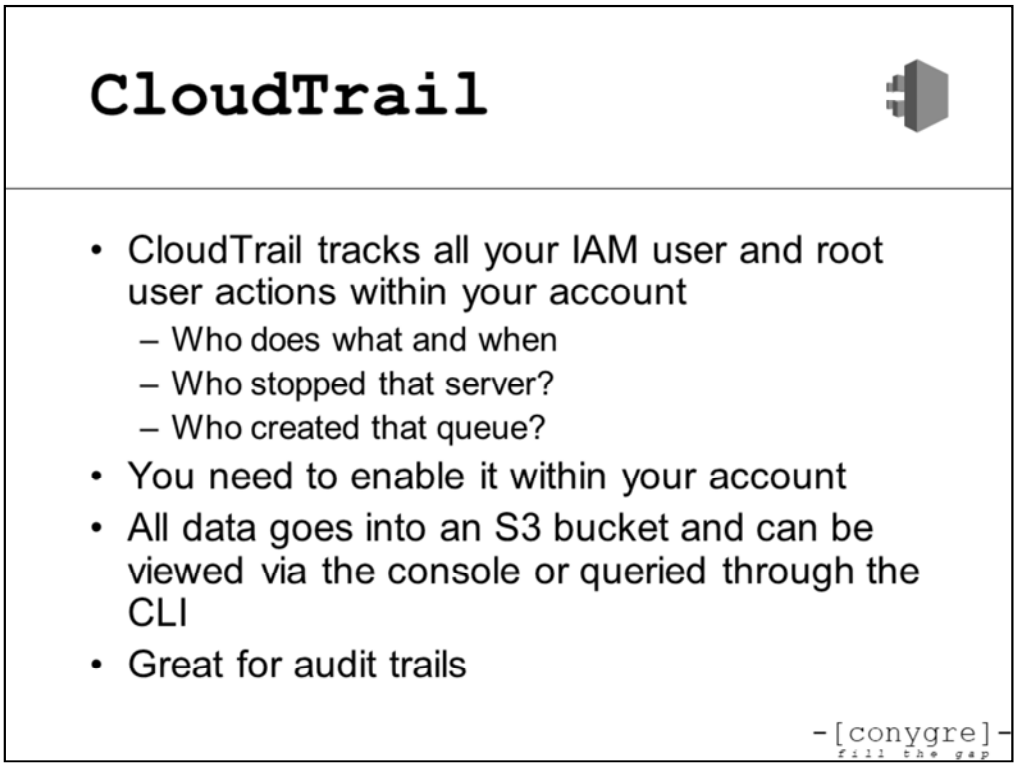




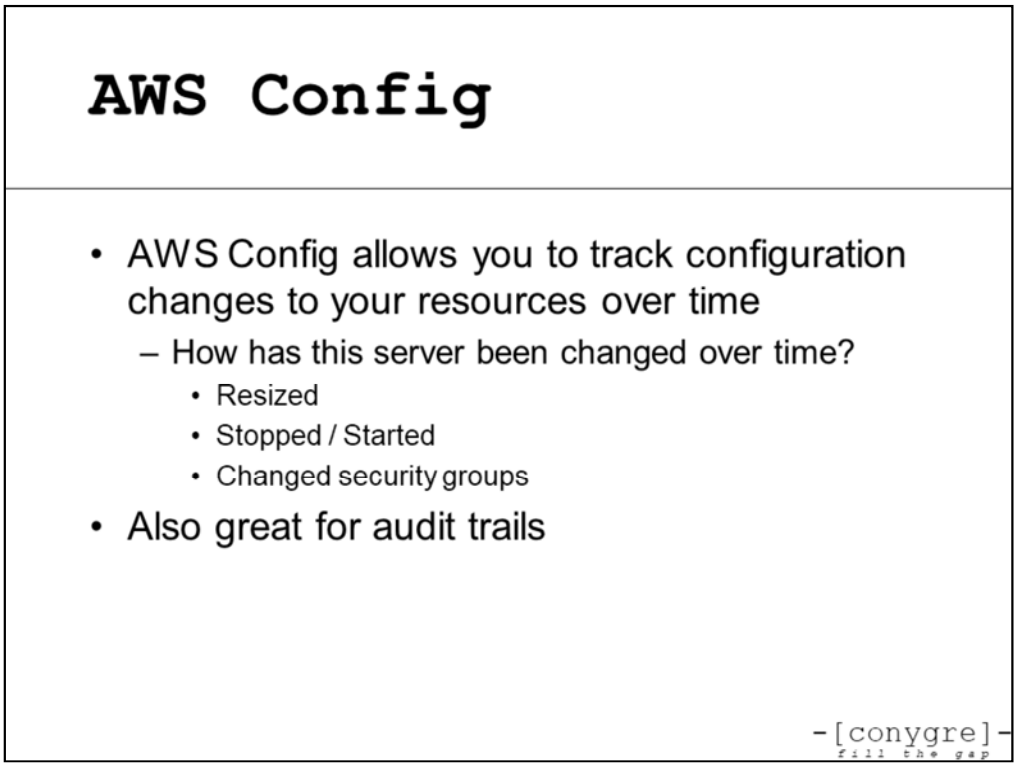
Security



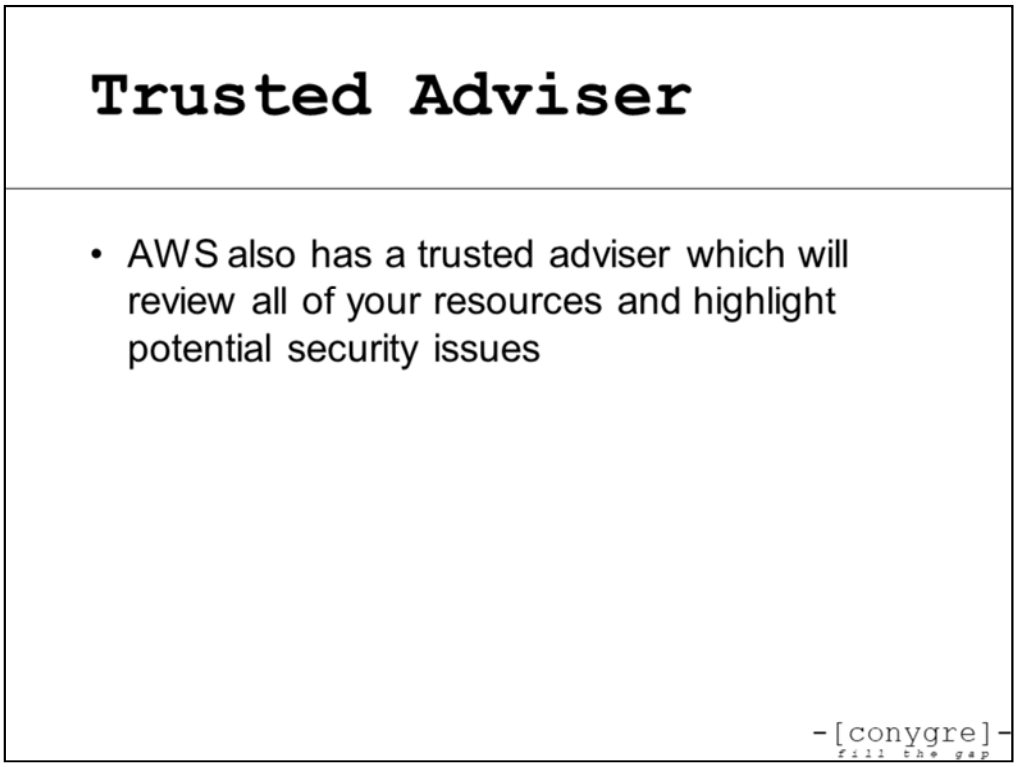
Security



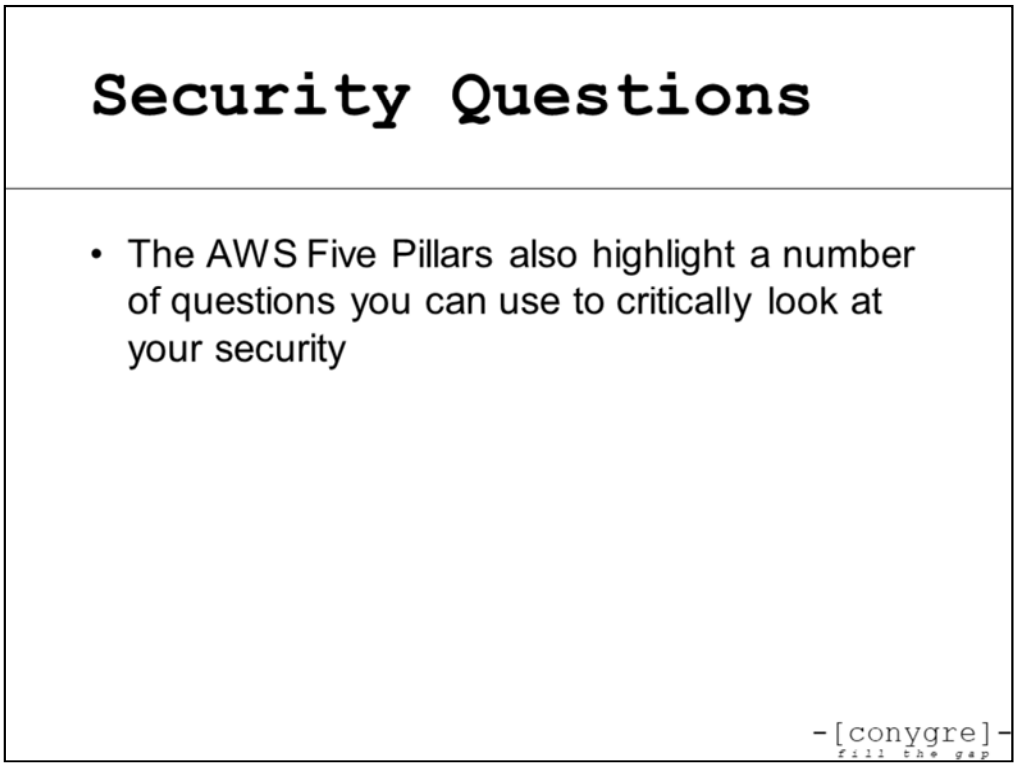
Security



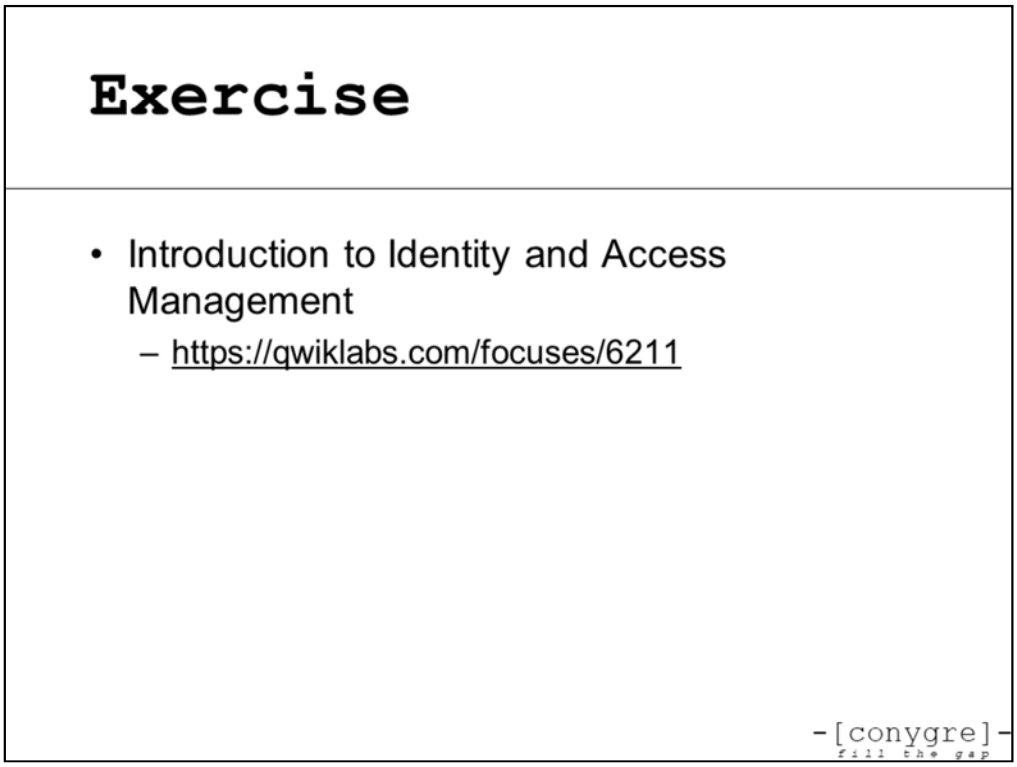
Security



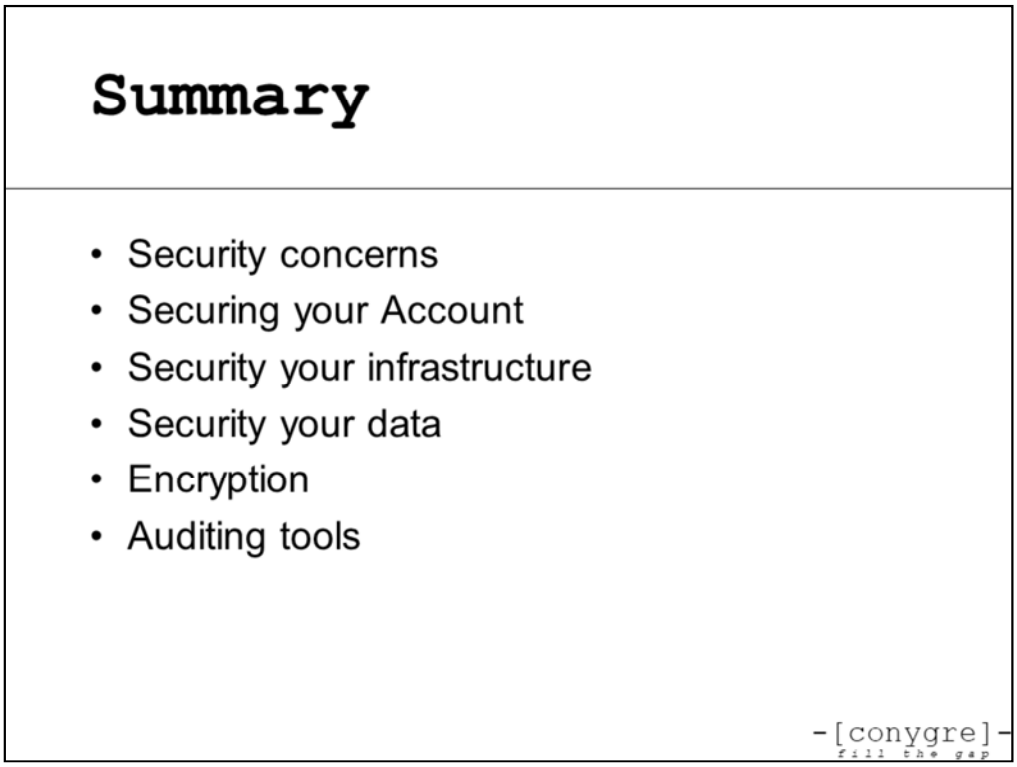
Security



Security

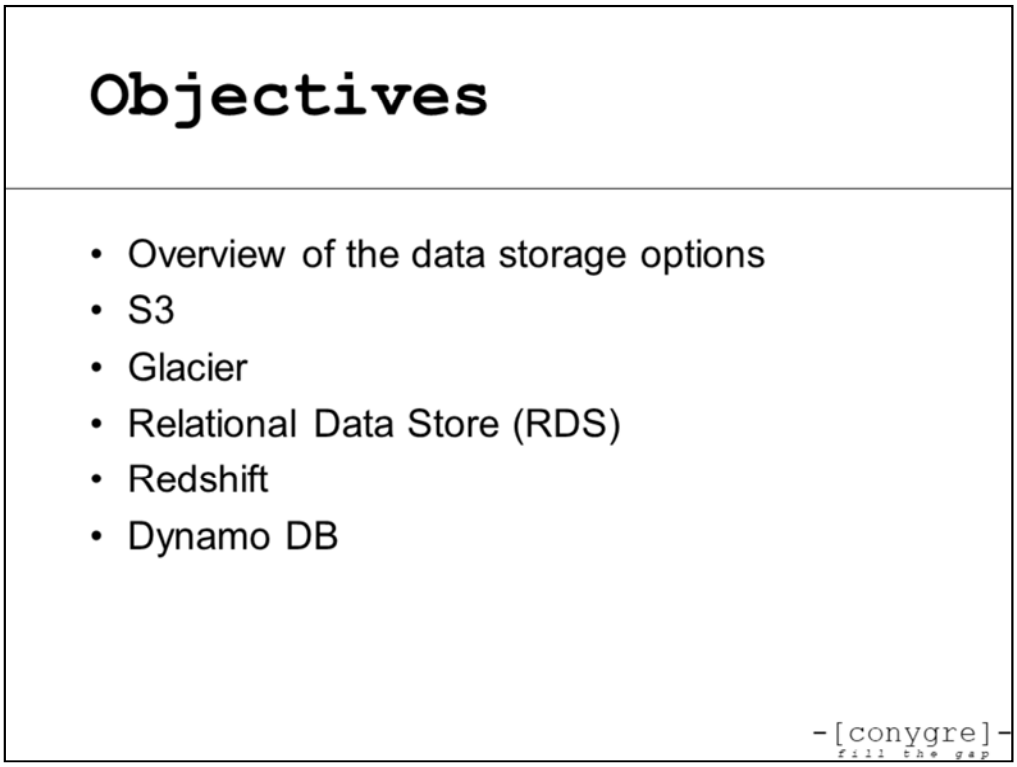


Security

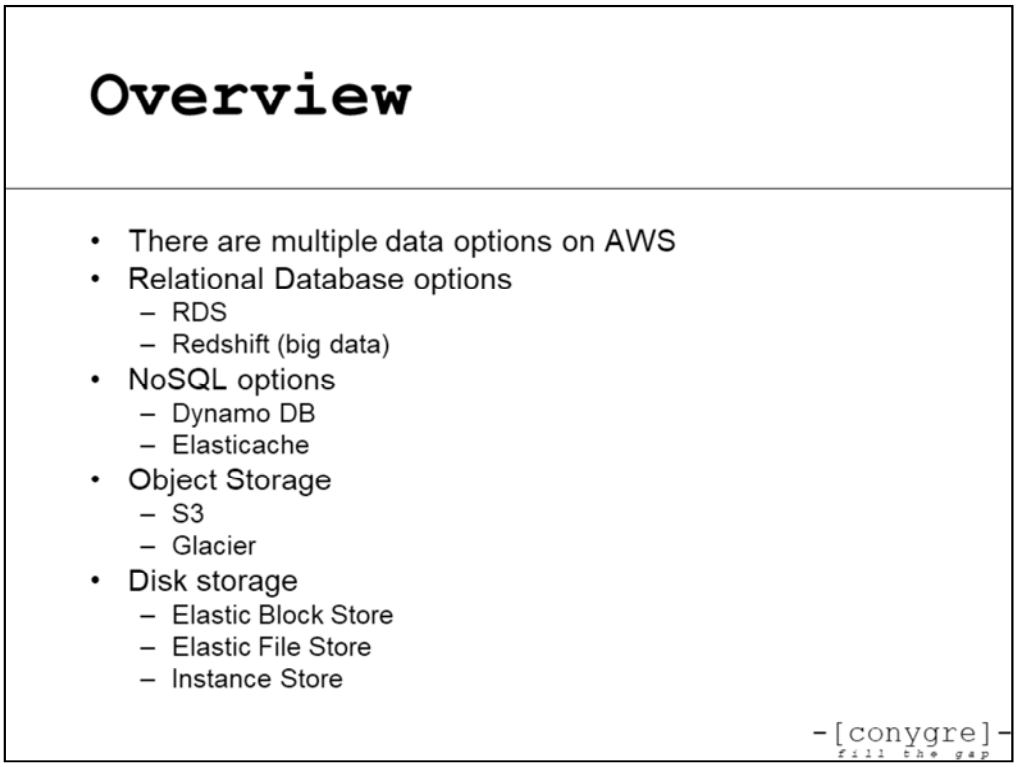


Storage Options

Storage Options



Storage Options



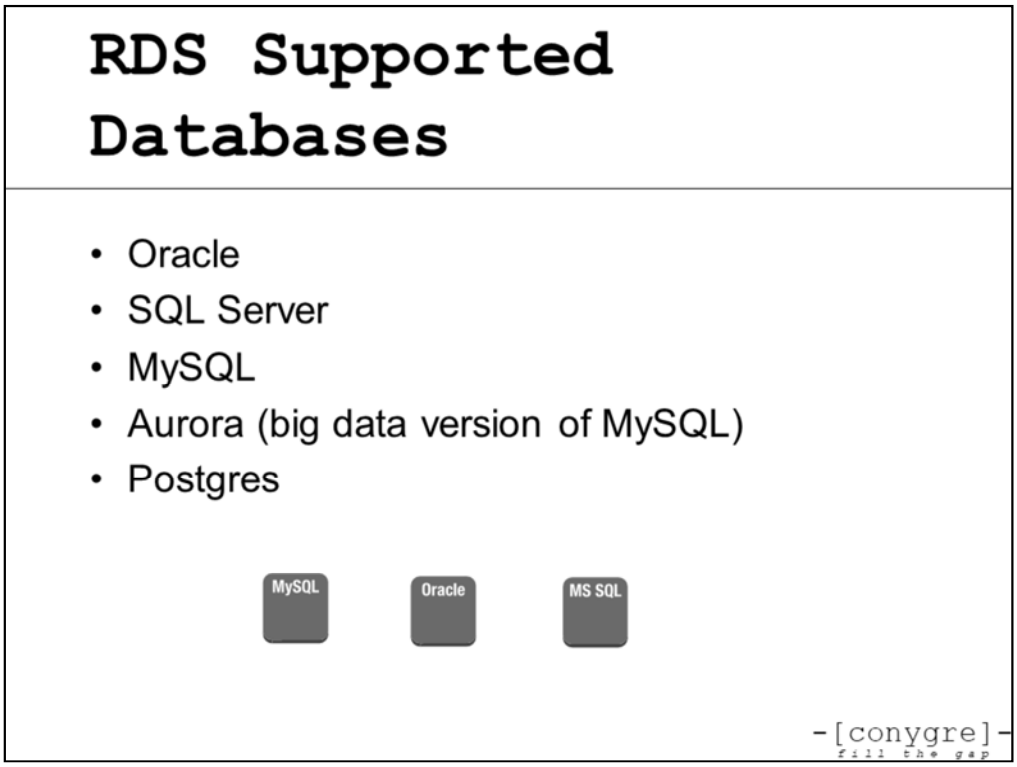
Storage Options

Relational Data Store (RDS)

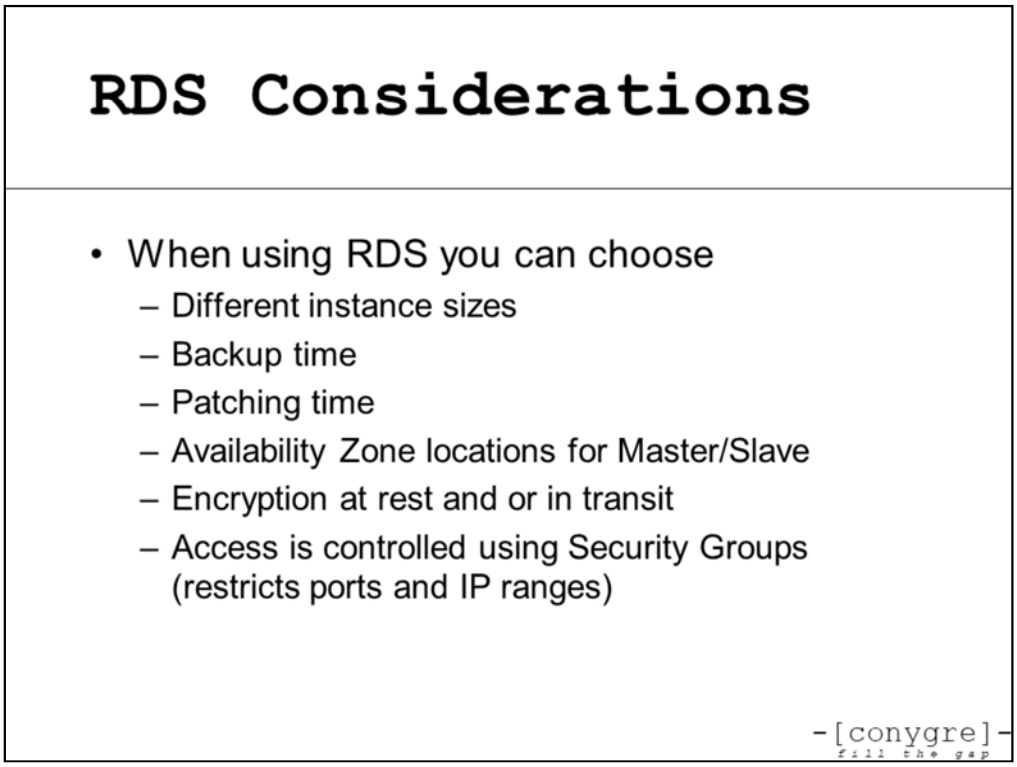
- RDS is where AWS provide the database instance for you so you don't have to deal with
  - Installation
  - Patching
  - Backups
  - Master / Slave configuration
  - Read Replica configuration (on some databases)
  - Complexities around resizing a live database instance

-[conygre]-
fill the gap

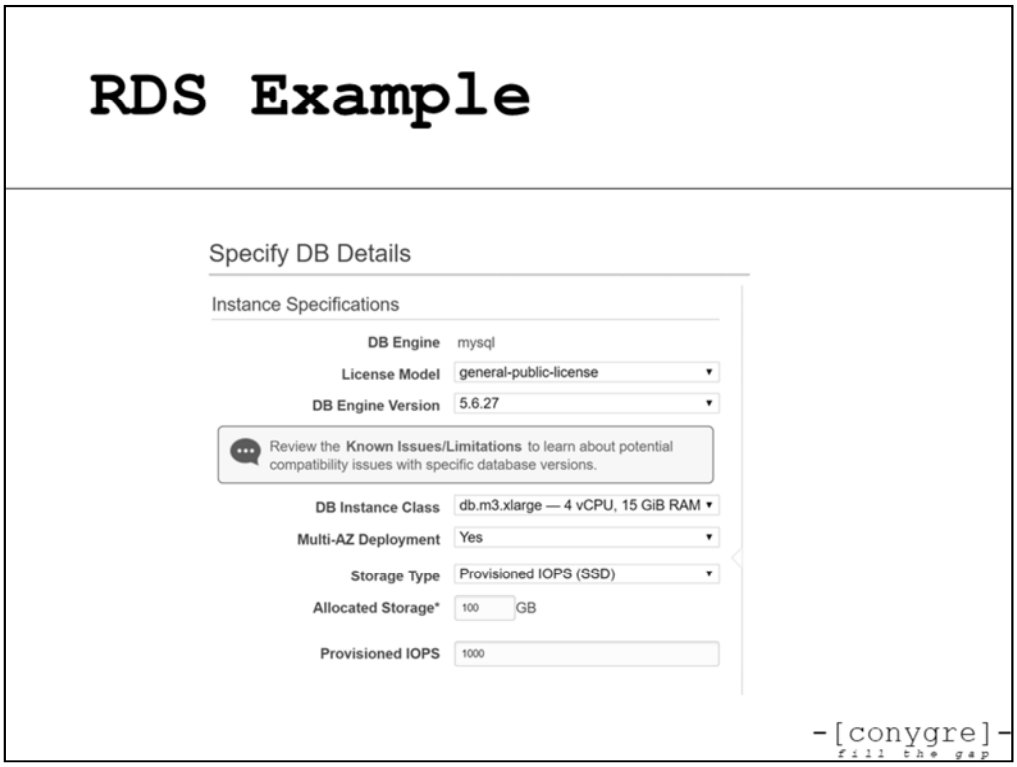
Storage Options



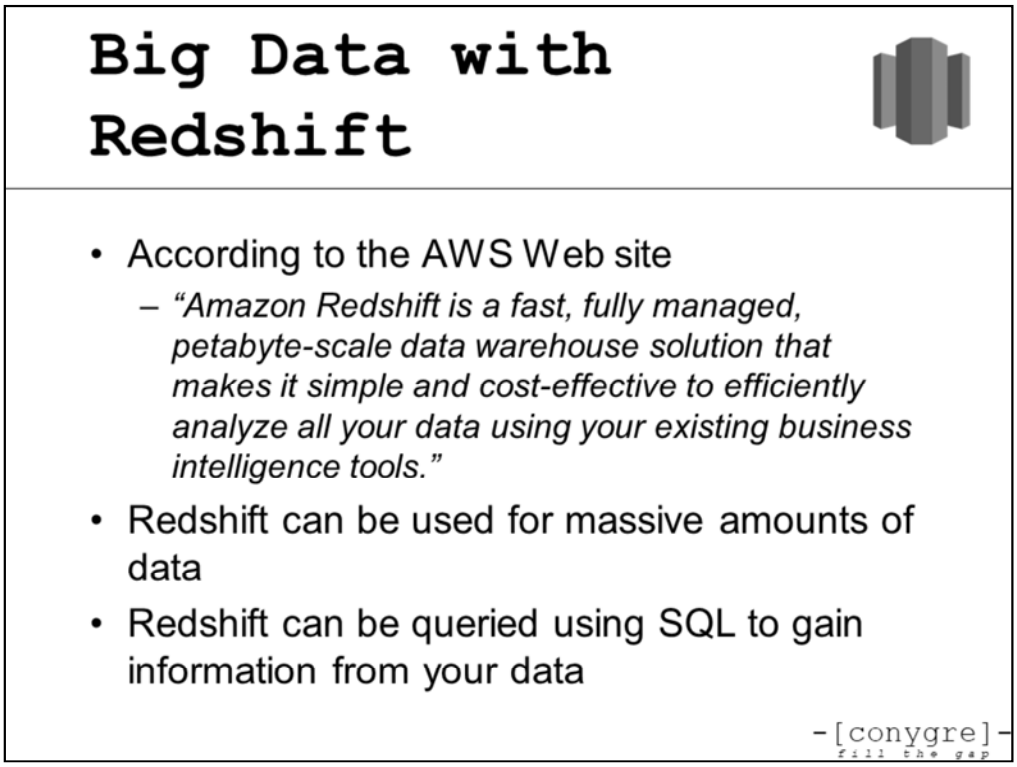
Storage Options



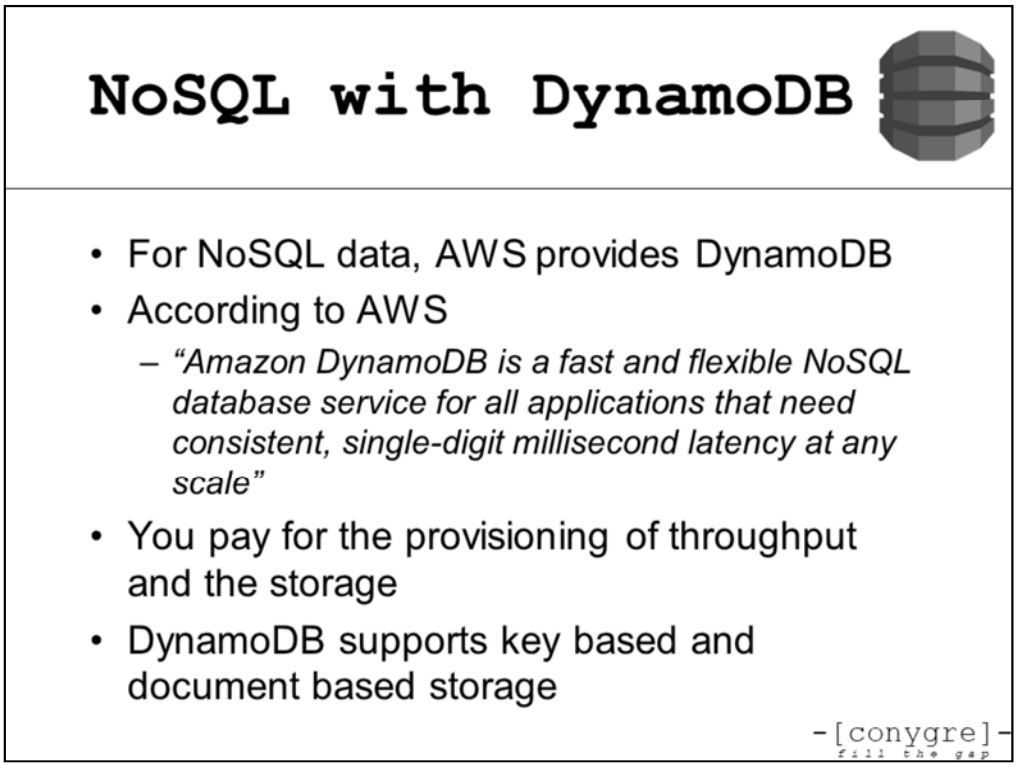
Storage Options



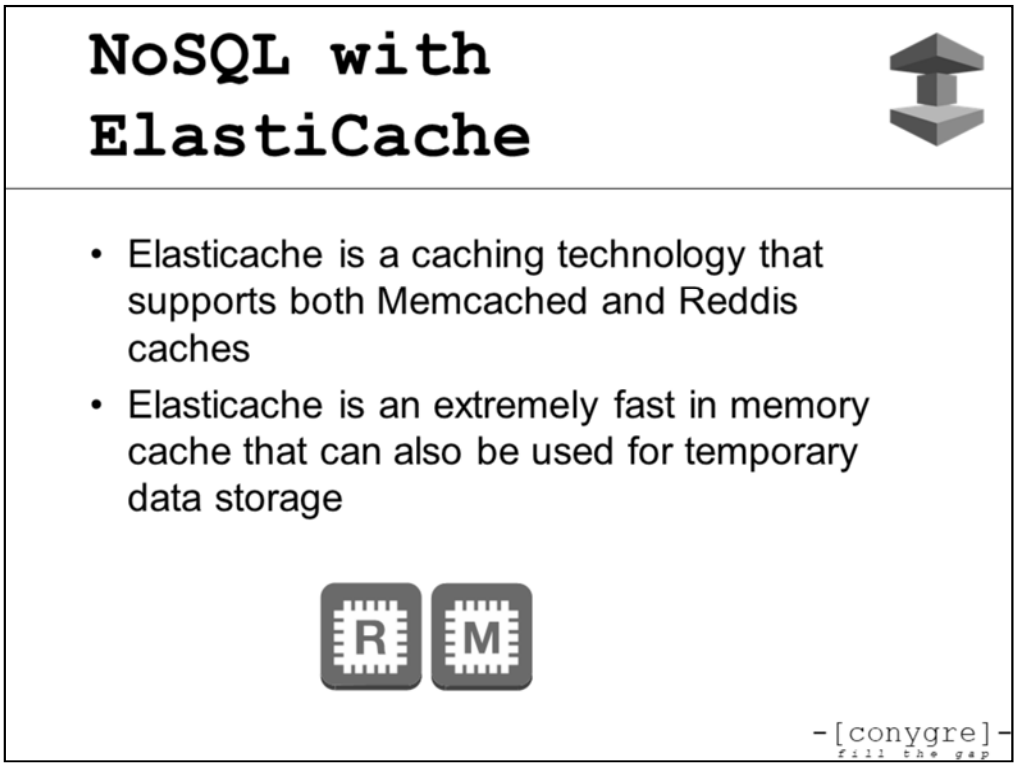
Storage Options



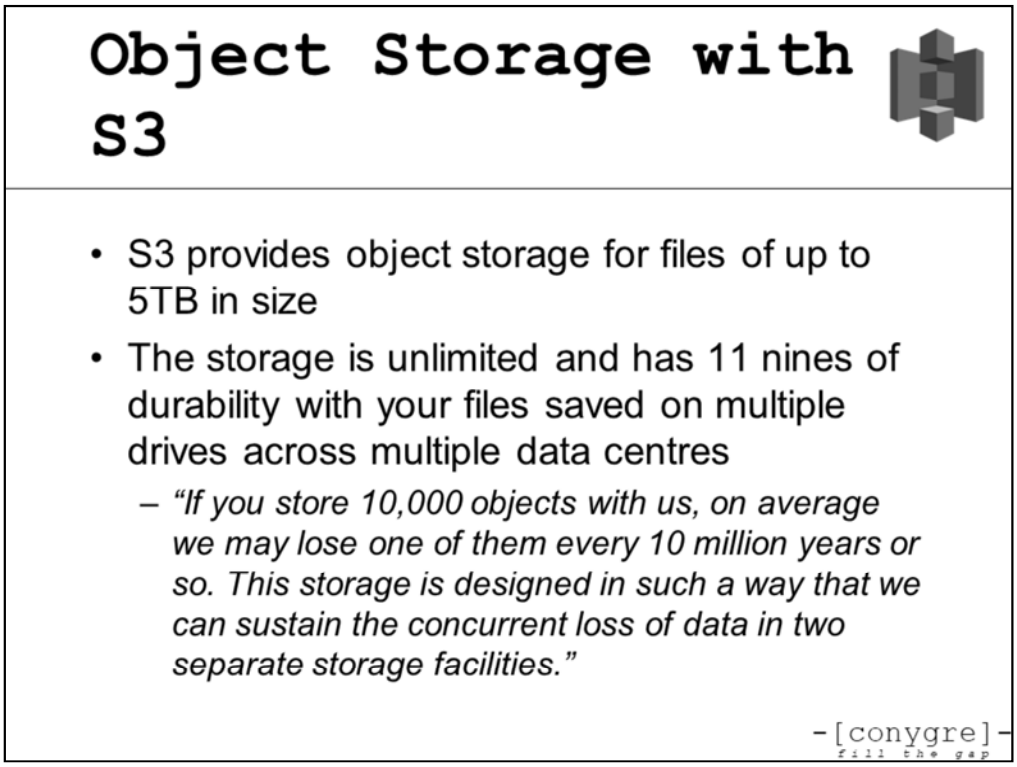
Storage Options



Storage Options



Storage Options



Storage Options

S3 Buckets

- When using S3 you create buckets into which you place objects
- These objects then have a key which is what is used to retrieve the object
- Buckets can be made available over the Internet
  - Static Web sites can be hosted from buckets
  - CSS / JS / Images can be hosted from buckets

-[conygre]-
fill the gap

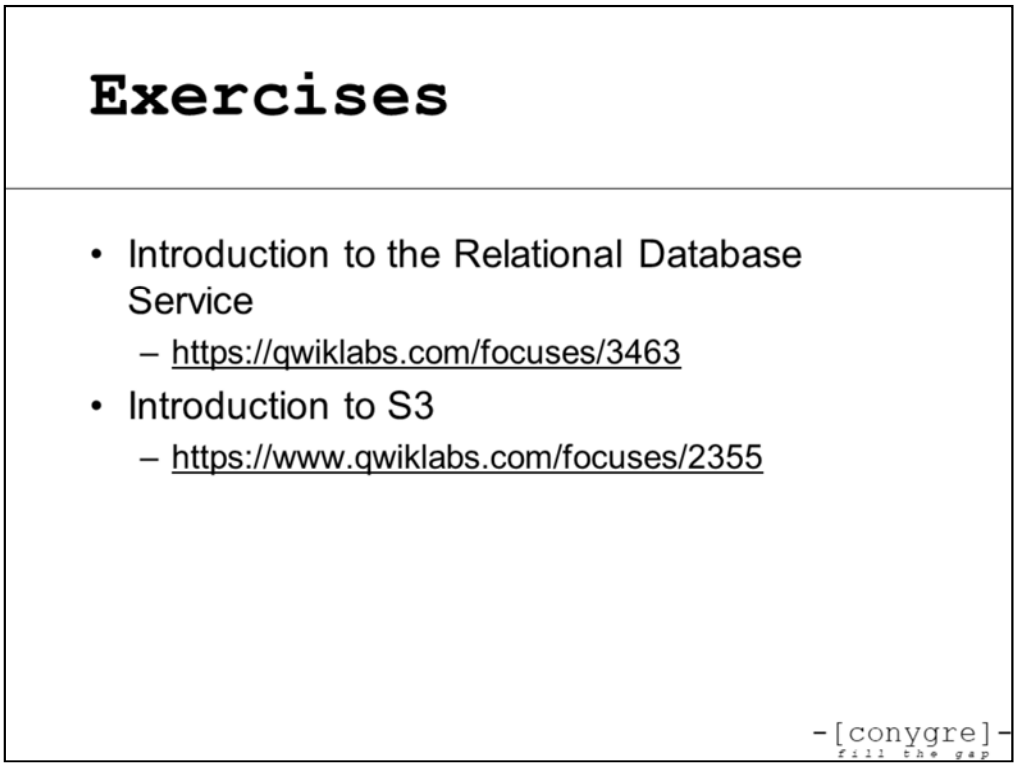
Storage Options

Glacier

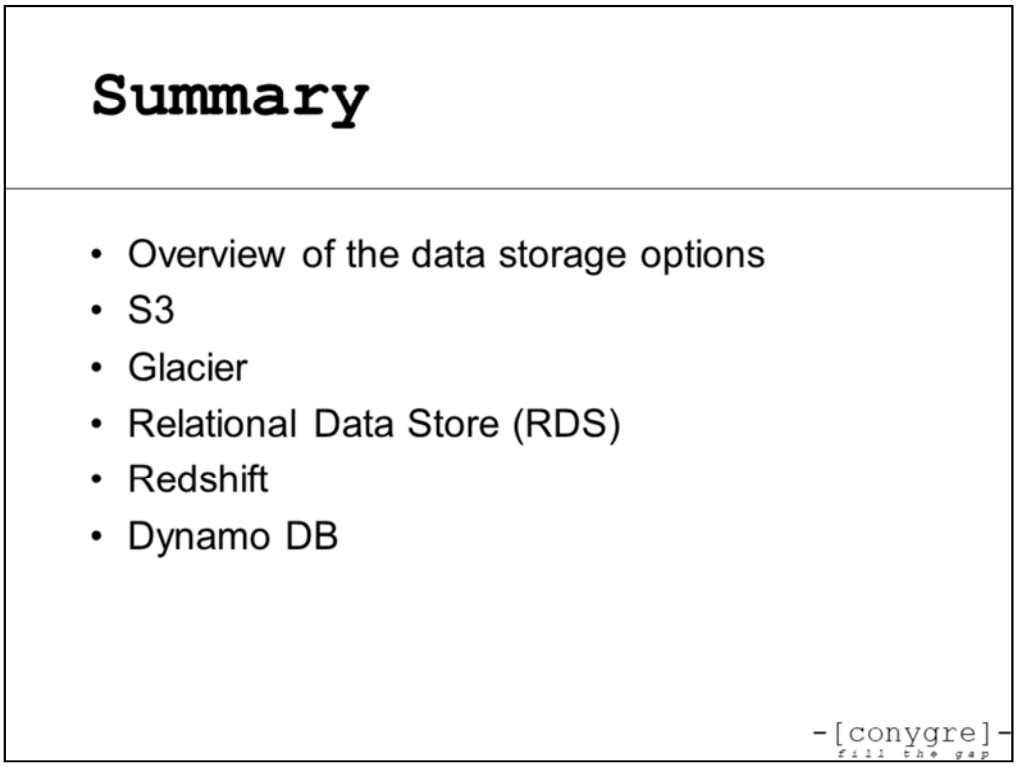
- Glacier is the data archiving service
- It is ideal for data that you have to store but are unlikely to want to access
  - Historical logs
  - Archives
  - Old Backups
  - Regulatory compliance
- Glacier is similar to S3 with 11 9's of durability
- S3 objects can be put into a lifecycle automating a transition to Glacier

-[conygre]-
fill the gap

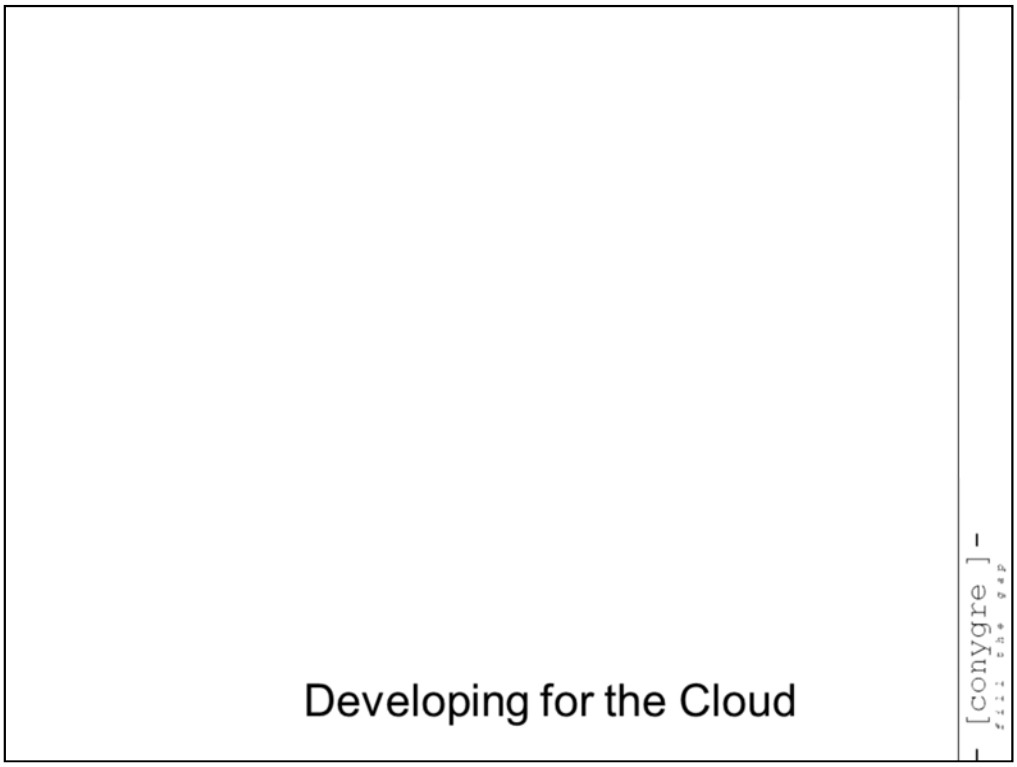
Storage Options



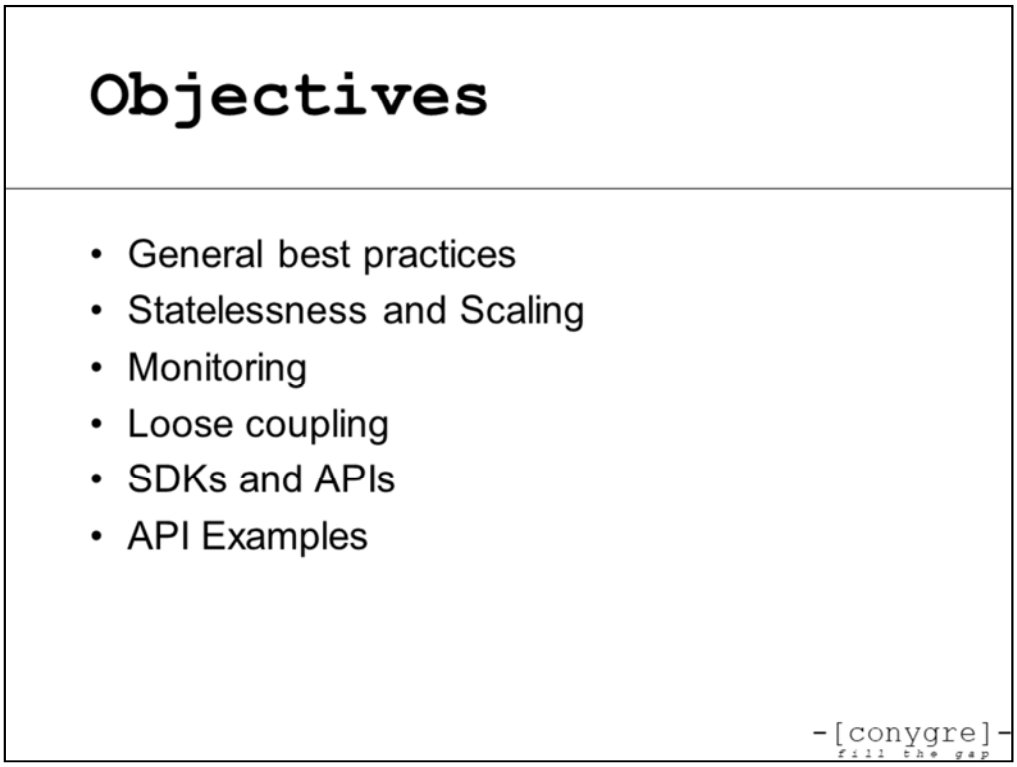
Storage Options



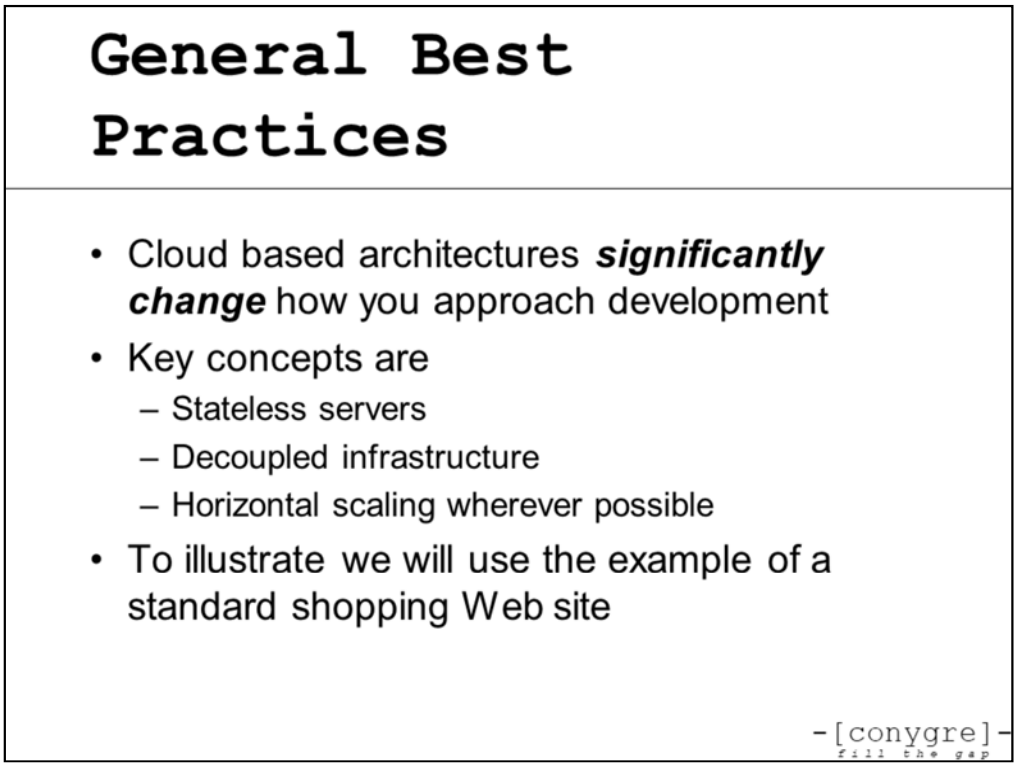
Development in the Cloud



Development in the Cloud



Development in the Cloud



Standard Web Site

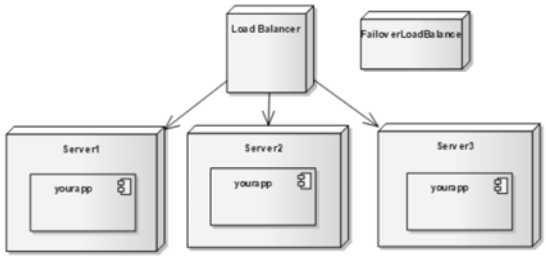
- Many Web sites store session state
  - Where do you keep it?
- If you keep it on the server, this prevents elasticity
  - Servers cannot be stopped and started automatically in response to load
    - Stopping servers will result in the loss of session state
- **Cloud based servers should be stateless wherever possible**

-[conygre]-
fill the gap

Development in the Cloud

Horizontal / Vertical Scaling

- Vertical scaling always has limits
- Horizontal scaling is far less limiting
  - Will your application horizontally scale?
- Building components that cannot be horizontally scaled lacks flexibility in the cloud

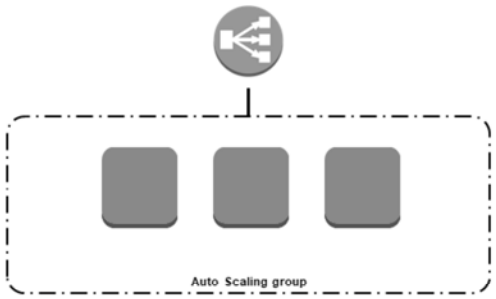


-[conygre]-
fill the gap

Development in the Cloud

Horizontal Scaling on AWS

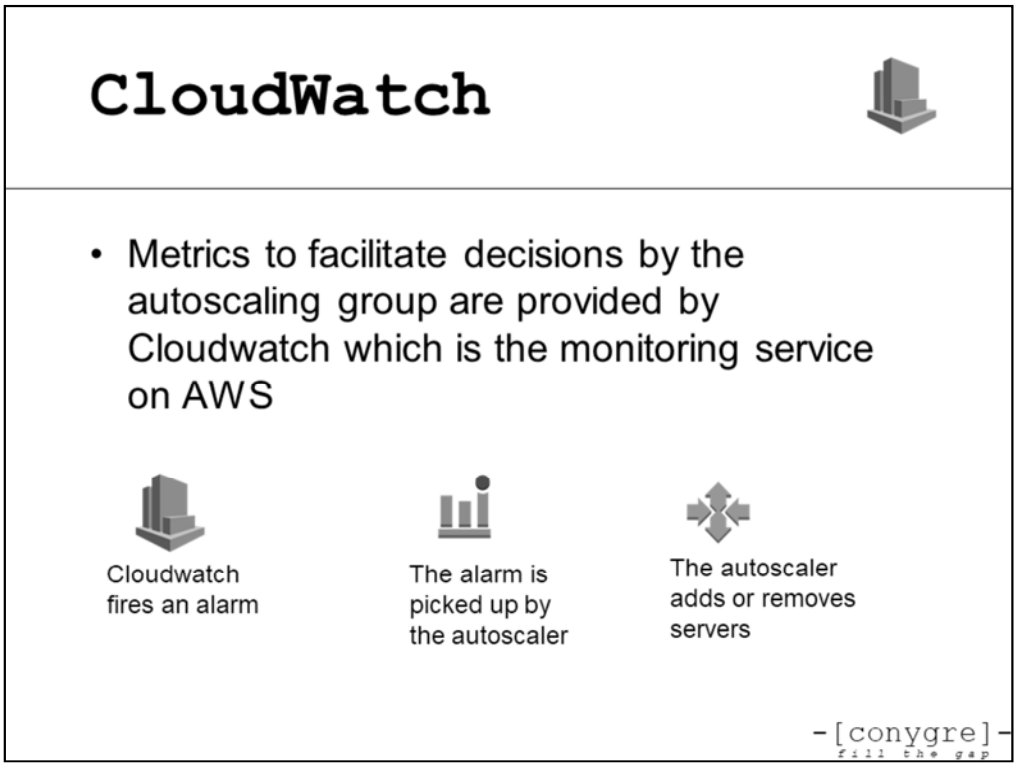
- The Elastic Load Balancer and the AutoScaling Group facilitate horizontal scaling



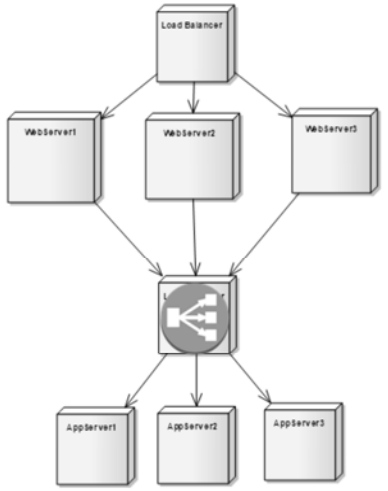
Number of servers Increases and decreases based on metrics decided by you

-[conygre]-
fill the gap

Development in the Cloud



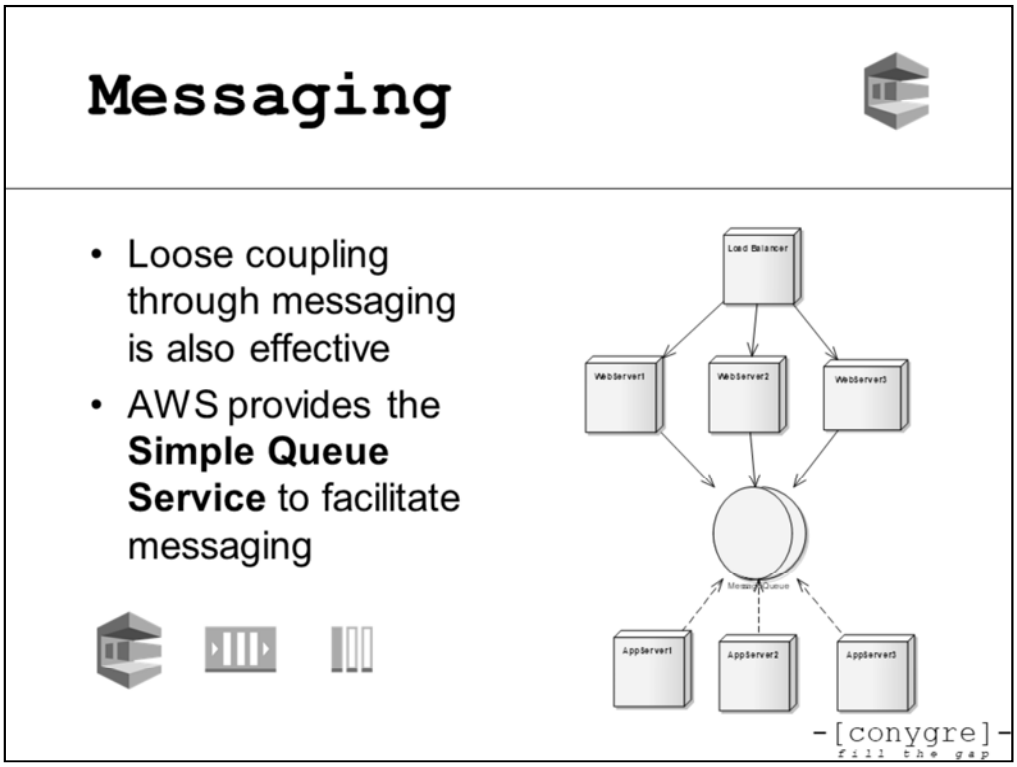
Loose Coupling



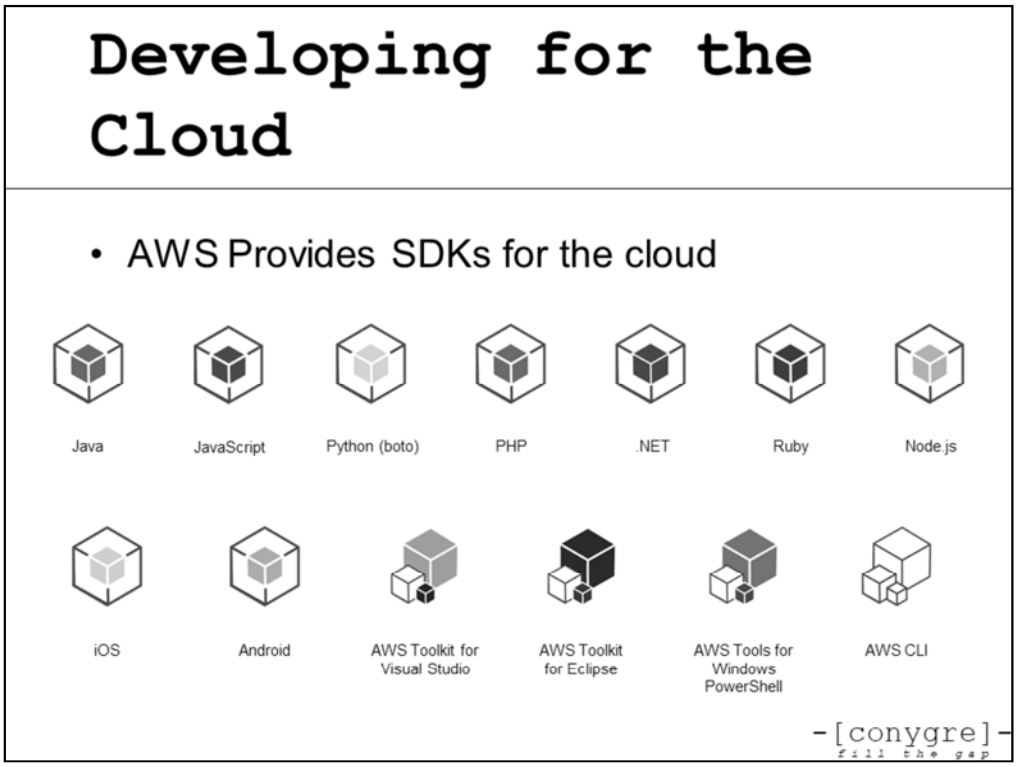
- Tightly coupled servers are unnecessarily inflexible
- Direct servers to load balancers NOT server IP addresses

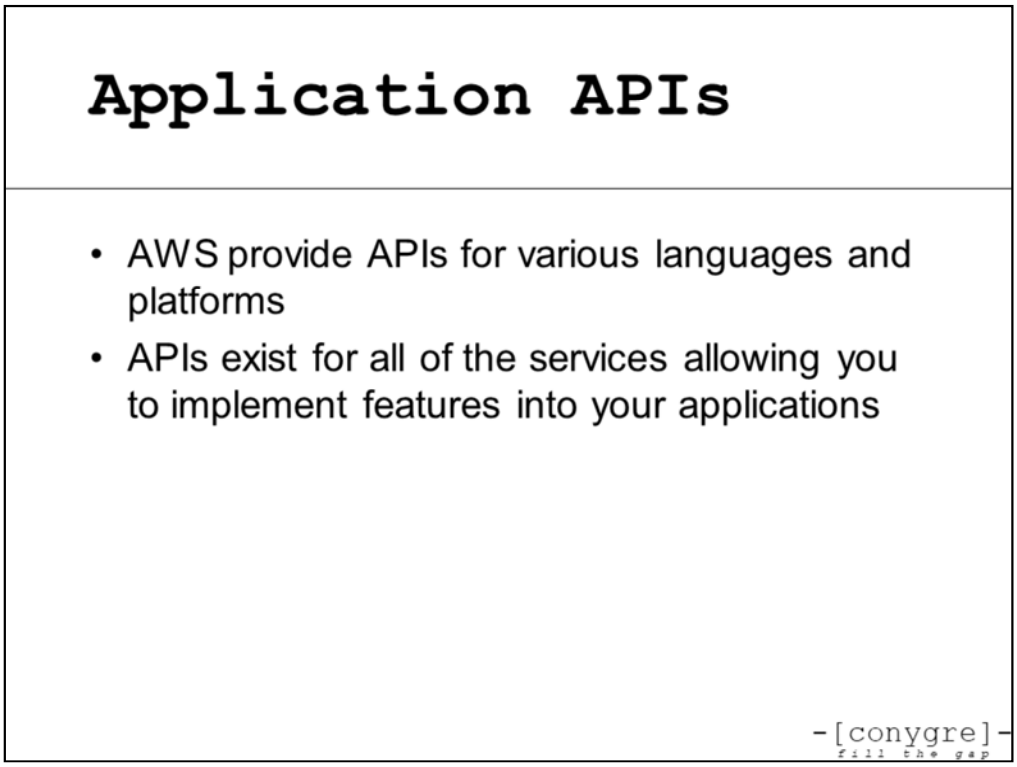
-[conygre]-
fill the gap

Development in the Cloud



Development in the Cloud





Development in the Cloud

Example S3 Code to List Bucket Contents

- Below is an S3 code snippet in Java

```
BasicAWSCredentials awsCreds = new BasicAWSCredentials(accessKey, secretKey);
s3client = new AmazonS3Client(awsCreds);
List<String> keyNames = new ArrayList<String>();
System.out.println("Listing objects");
ListObjectsRequest listObjectsRequest = new ListObjectsRequest()
ObjectListing objectListing;
do {
        objectListing = s3client.listObjects(listObjectsRequest);
        for (S3ObjectSummary objectSummary : objectListing.getObjectSummaries()) {
                String keyName = objectSummary.getKey();
                System.out.println(" - " + keyName + "  " + "(size = "
                        + objectSummary.getSize() + ")");
        if (!keyName.endsWith("/")) {
                keyNames.add(keyName);
        }
}
listObjectsRequest.setMarker(objectListing.getNextMarker());
```

-[conygre]-
fill the gap

Development in the Cloud

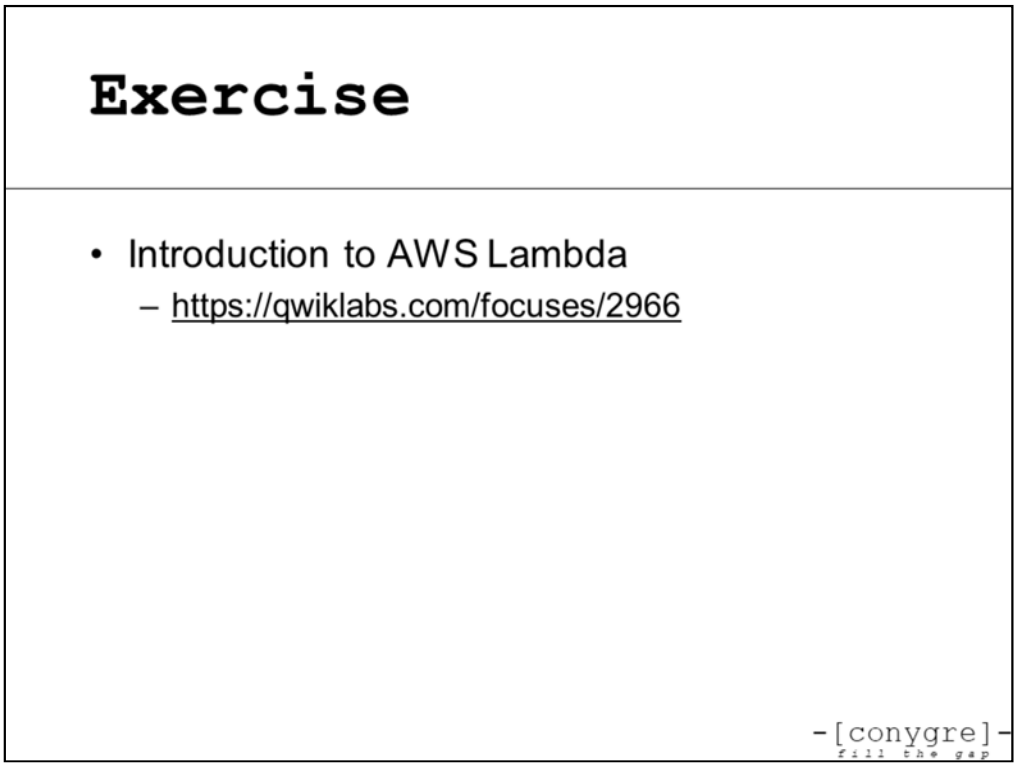
Example Lambda for Stopping Instances

- Below is a Lambda Function in Python

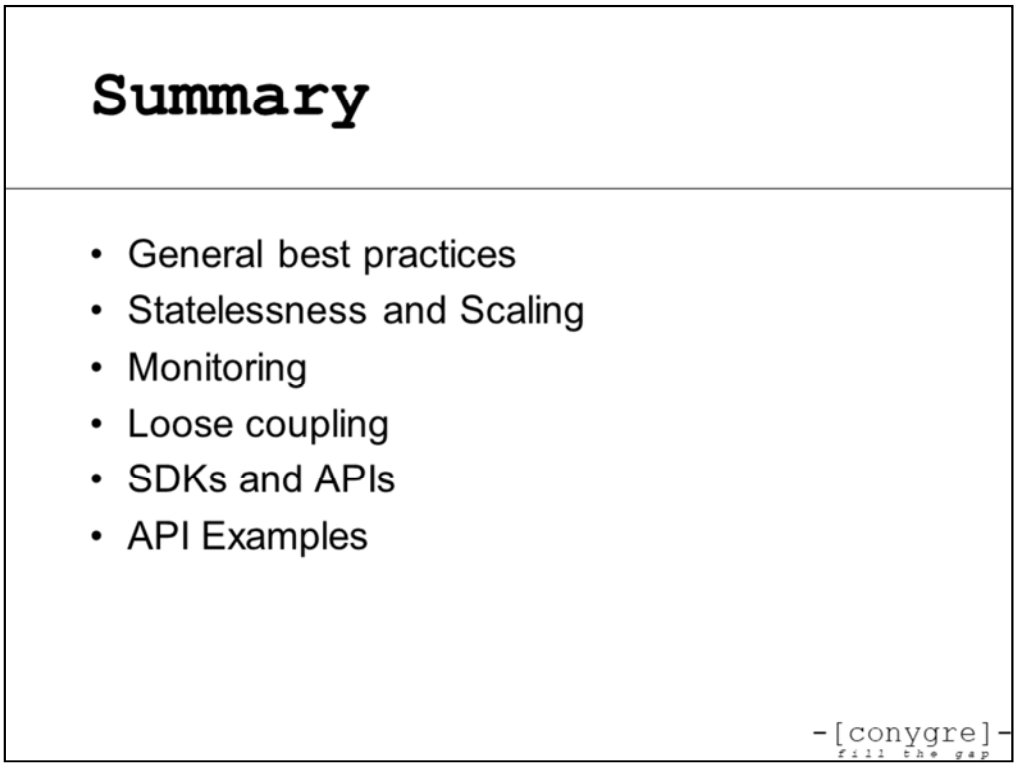
```
import boto3
import logging
ec2 = boto3.resource('ec2')

def lambda_handler(event, context):
filters = [{
        'Name': 'tag:Role',
        'Values': ['MyRole']
    },
    {
        'Name': 'instance-state-name',
        'Values': ['stopped']
    }
  ]
instances = ec2.instances.filter(Filters=filters)
StoppedInstances = [instance.id for instance in instances]
if len(StoppedInstances) > 0:
startingUp = ec2.instances.filter(InstanceIds=StoppedInstances).start()
```

-[conygre]-
fill the gap

Development in the Cloud

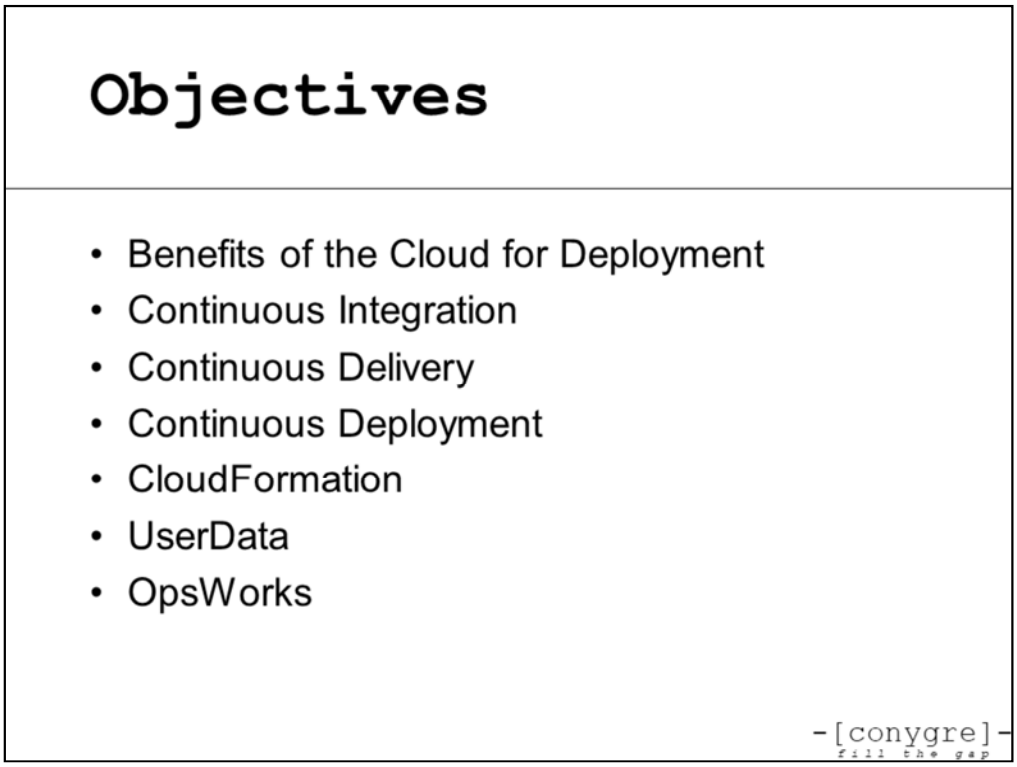


Development in the Cloud

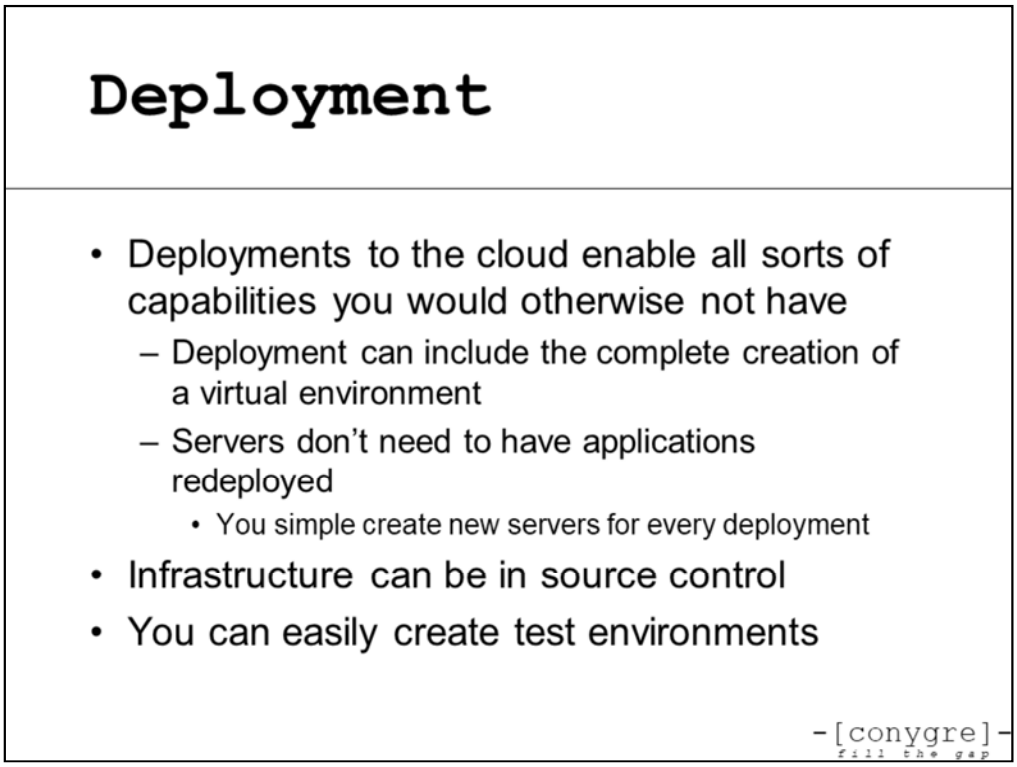


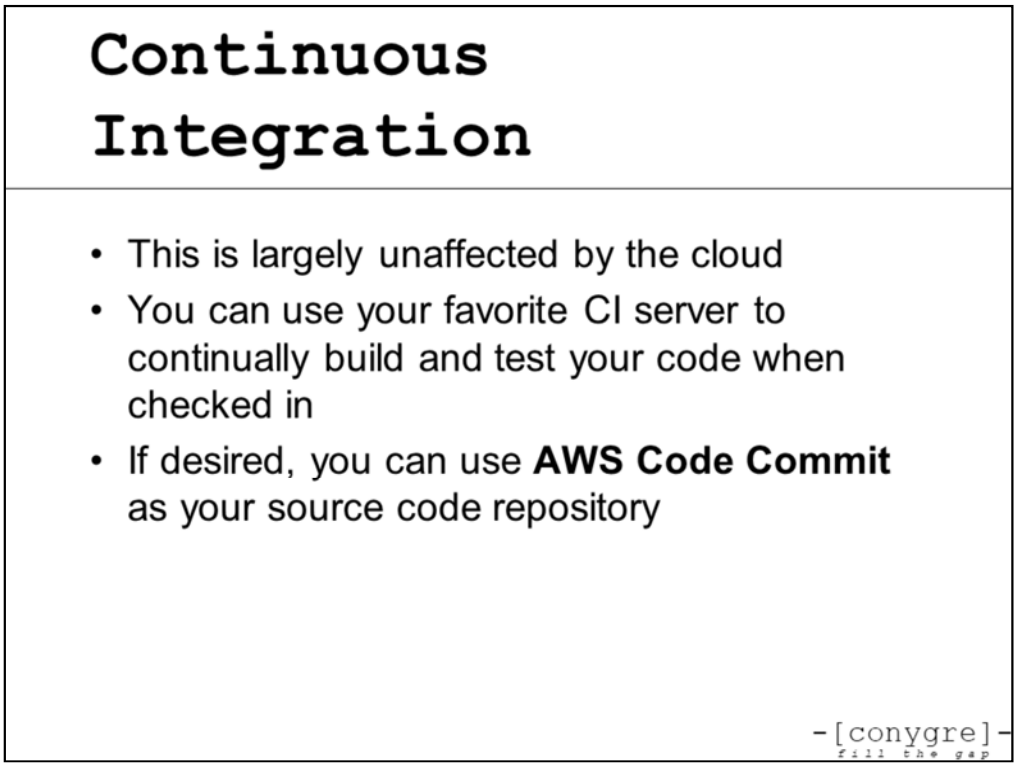
Deployment and Devops

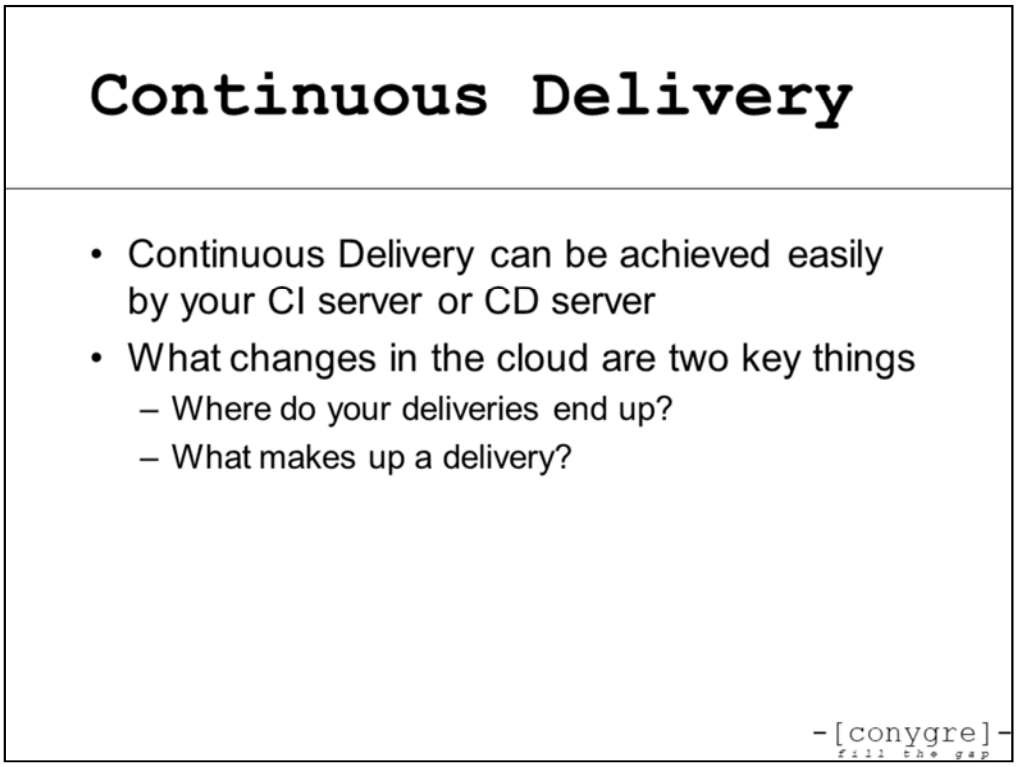
Deployment and Devops

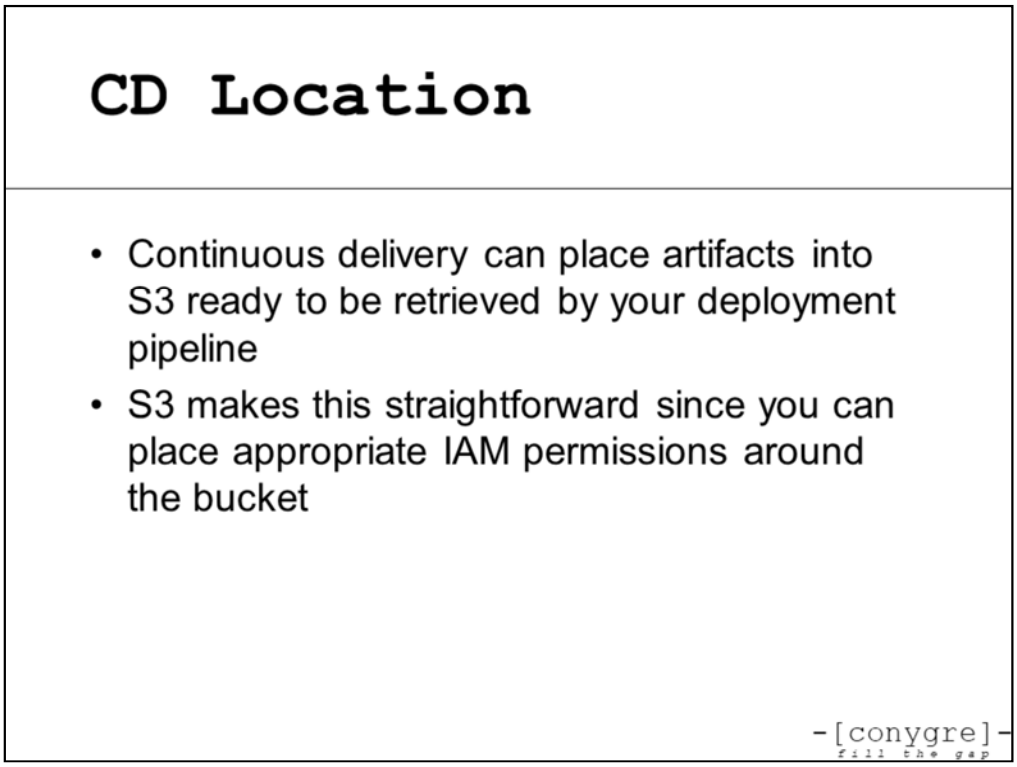


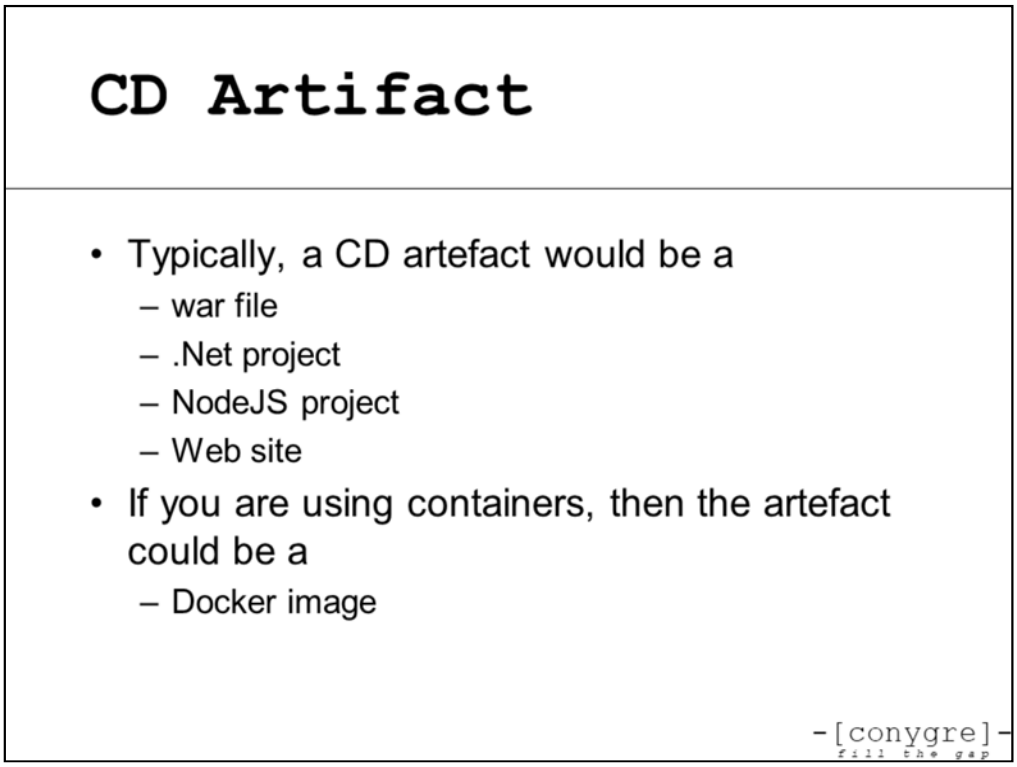
Deployment and Devops







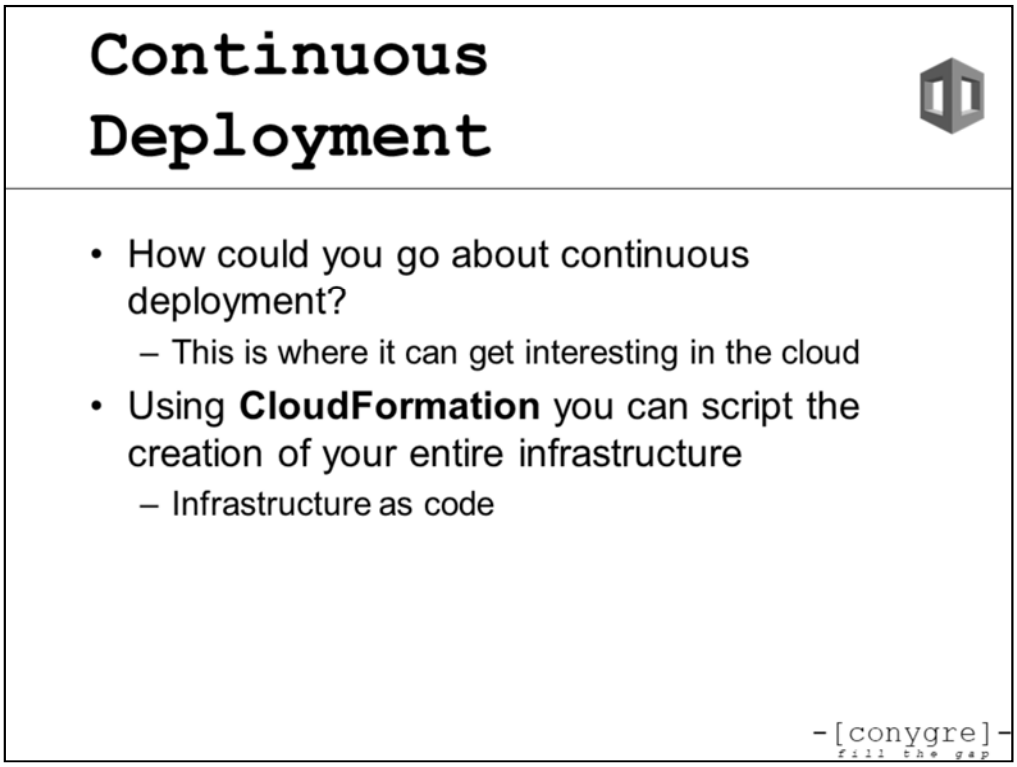




AMIs as Artifacts

- When using AWS, you can also build an AMI as part of your CD process
- The AMI contains all of the software and configurations of the server so it is ready to launch
  - Resulting in a fast launch time
- Netflix outsourced a utility to help with this
  - **Aminator**

-[conygre]-
fill the gap



Infrastructure Creation

- To automate the creation of infrastructure, AWS provide **Cloudformation**
- Cloudformation allows you to maintain ***infrastructure as code***
- JSON files are maintained in version control that define all the resources you need to deploy
  - This can then be run as a script whenever you need to

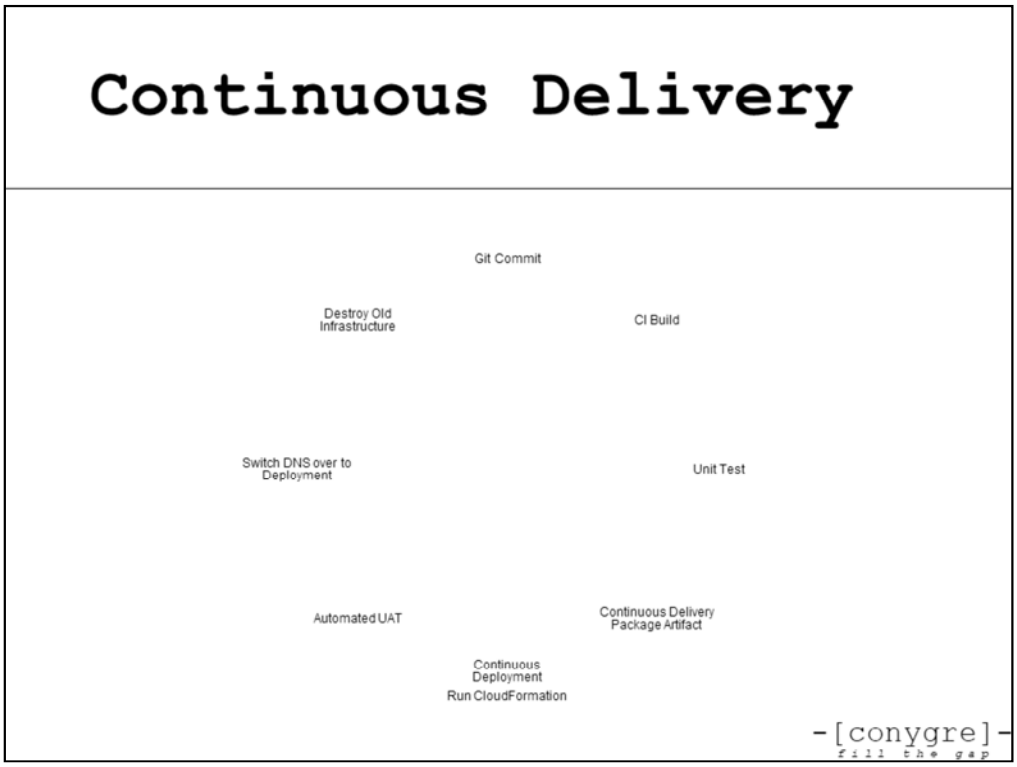
-[conygre]-
fill the gap

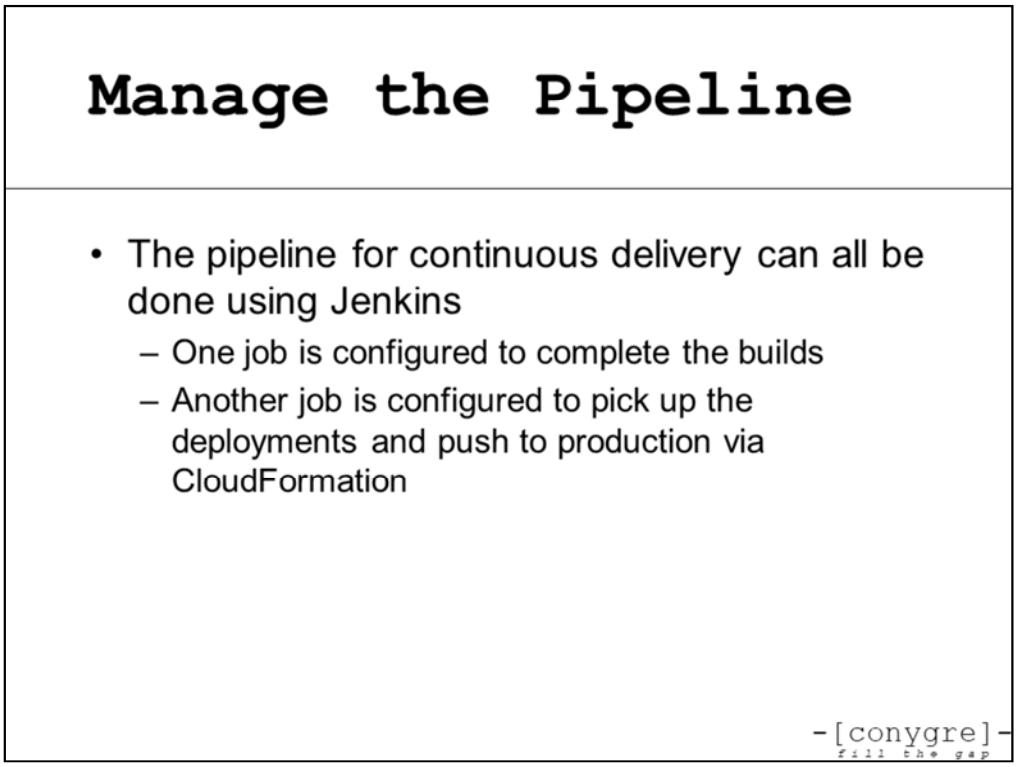
CloudFormation Templates

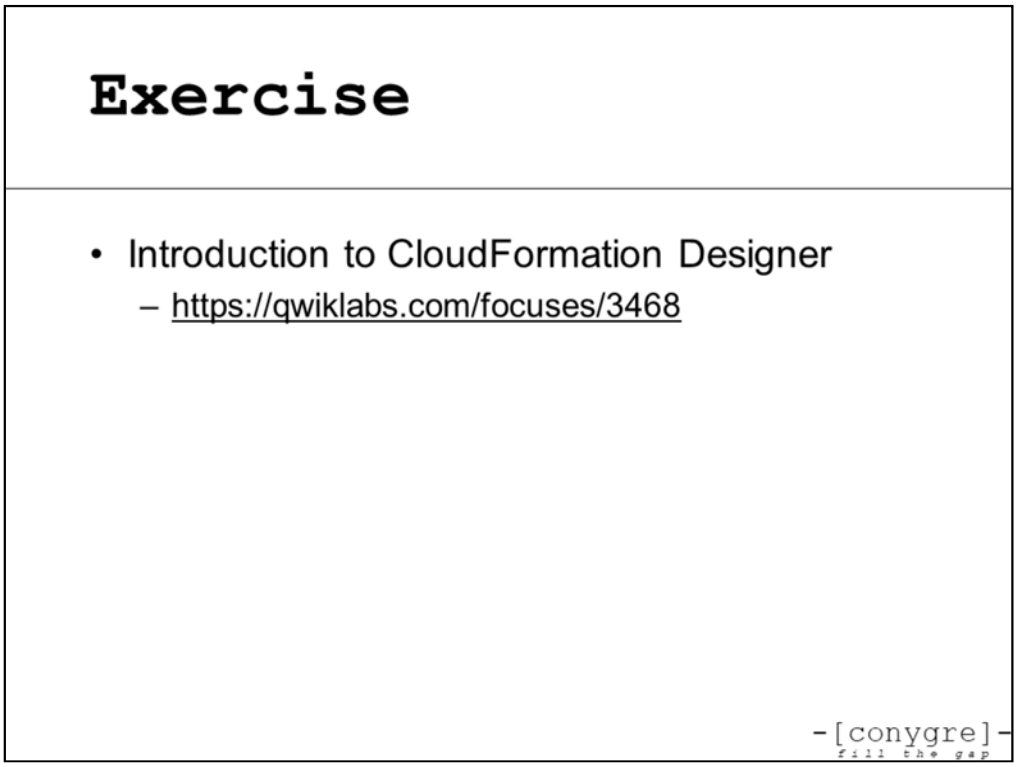
- A CloudFormation Template can be used to
  - Create servers
  - Create network infrastructure
  - Create autoscaling groups
  - Create IAM users
- This facilitiates Continuous Delivery with a new infrastructure every time

-[conygre]-
fill the gap

Deployment and Devops





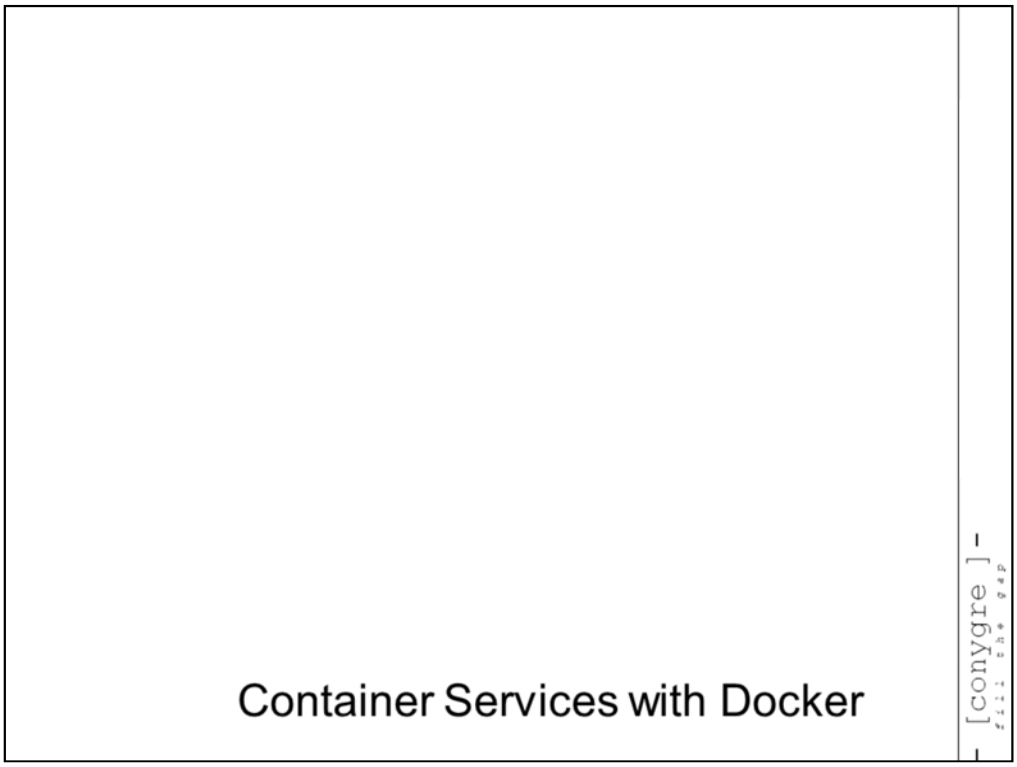


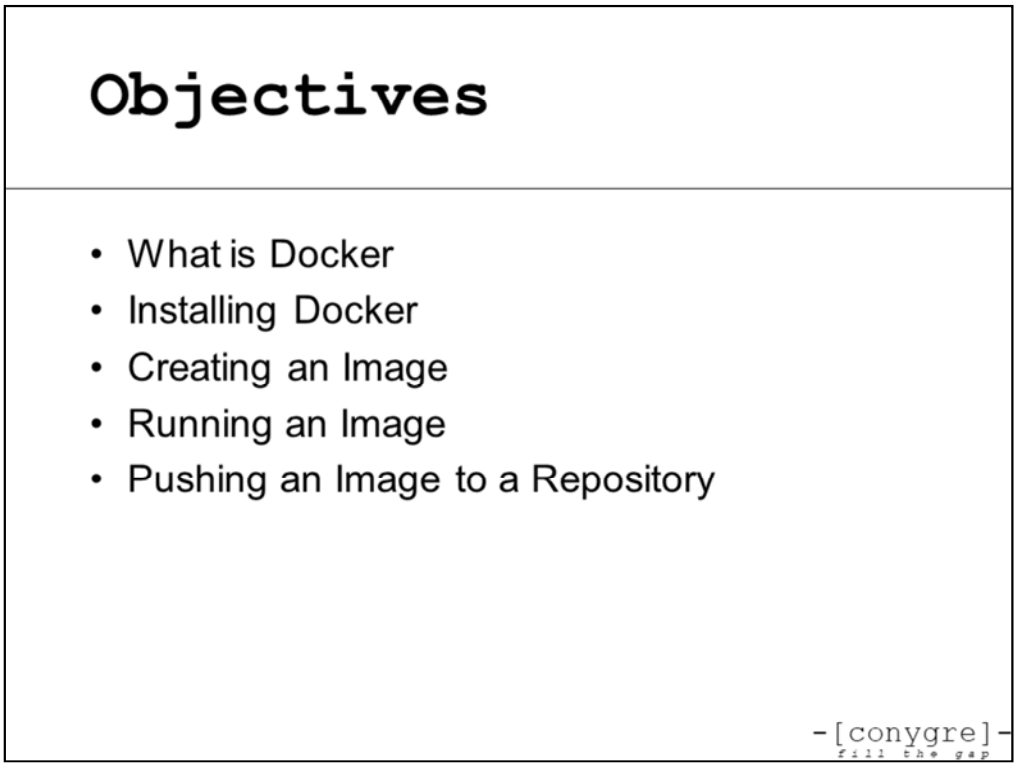
Summary

- What do we mean by 'the cloud'?
- Benefits of the Cloud
- Corporate Approaches to the Cloud
- How does the Cloud affect Development

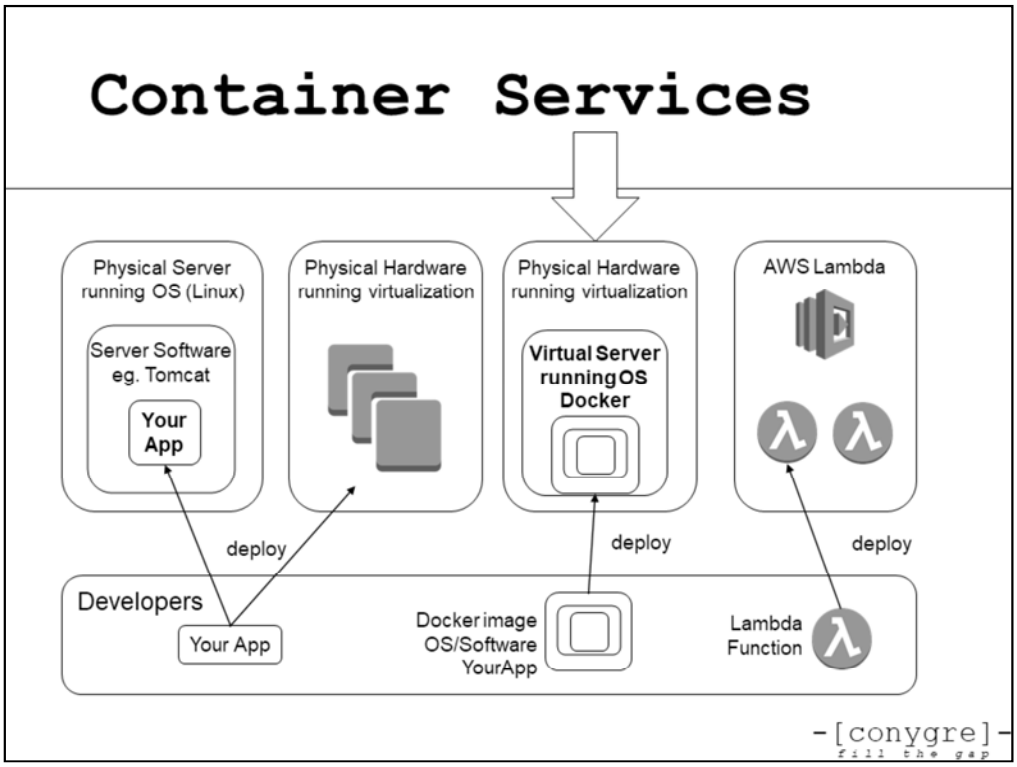
-[conygre]-
fill the gap

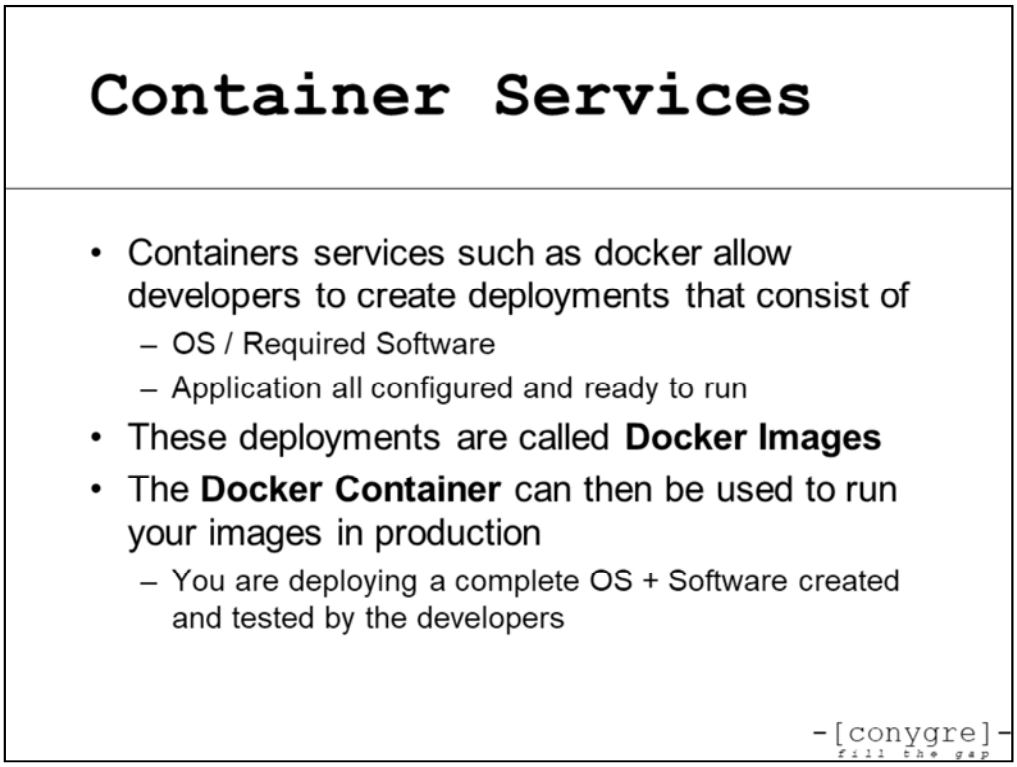
Docker

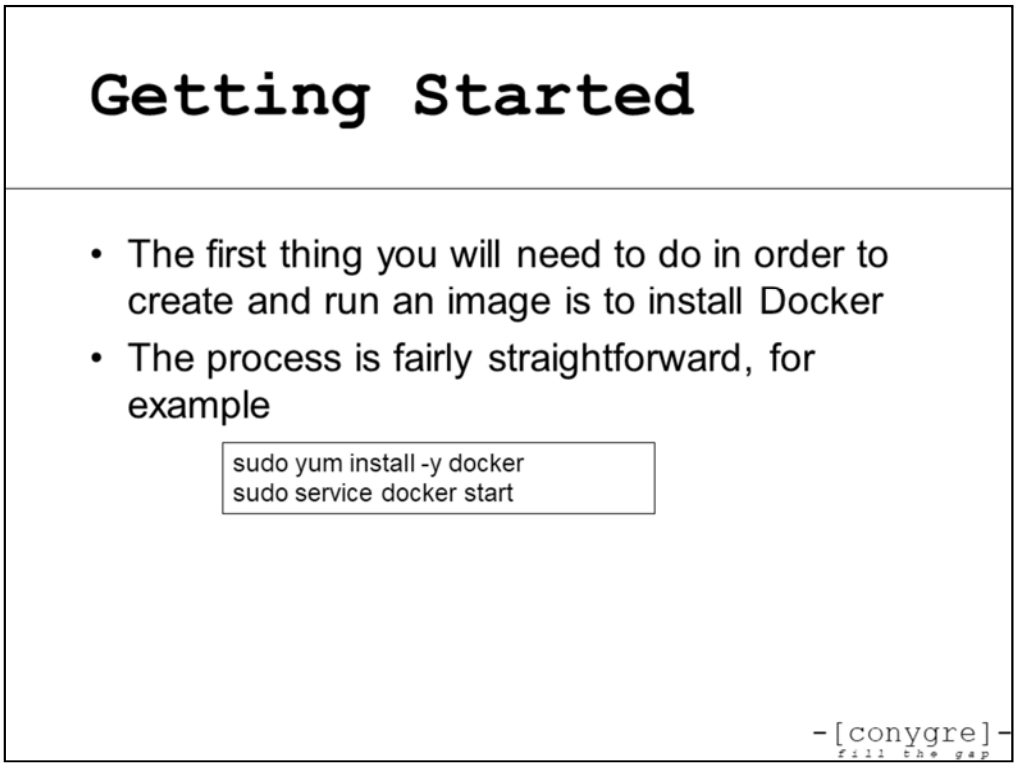


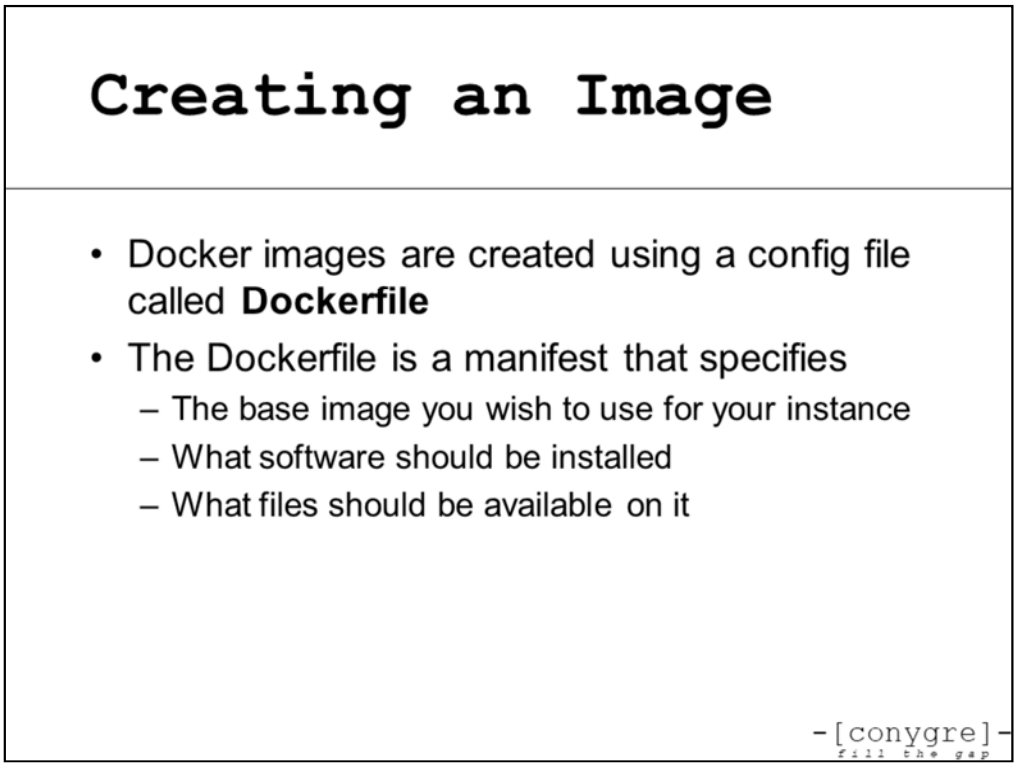


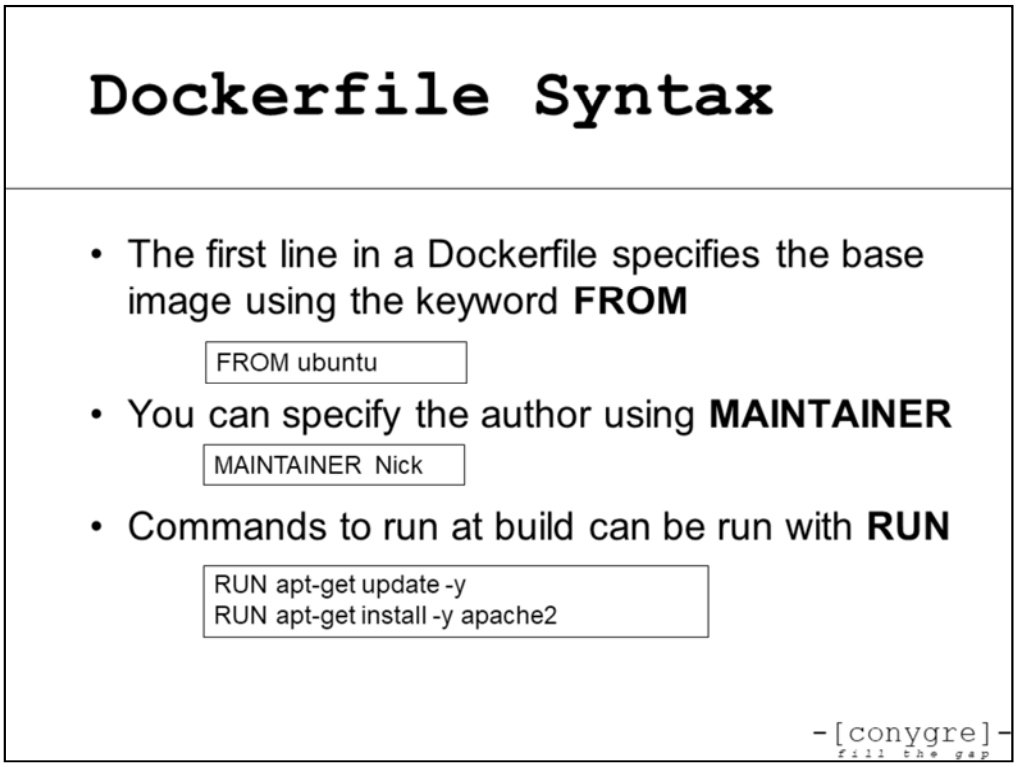
Docker

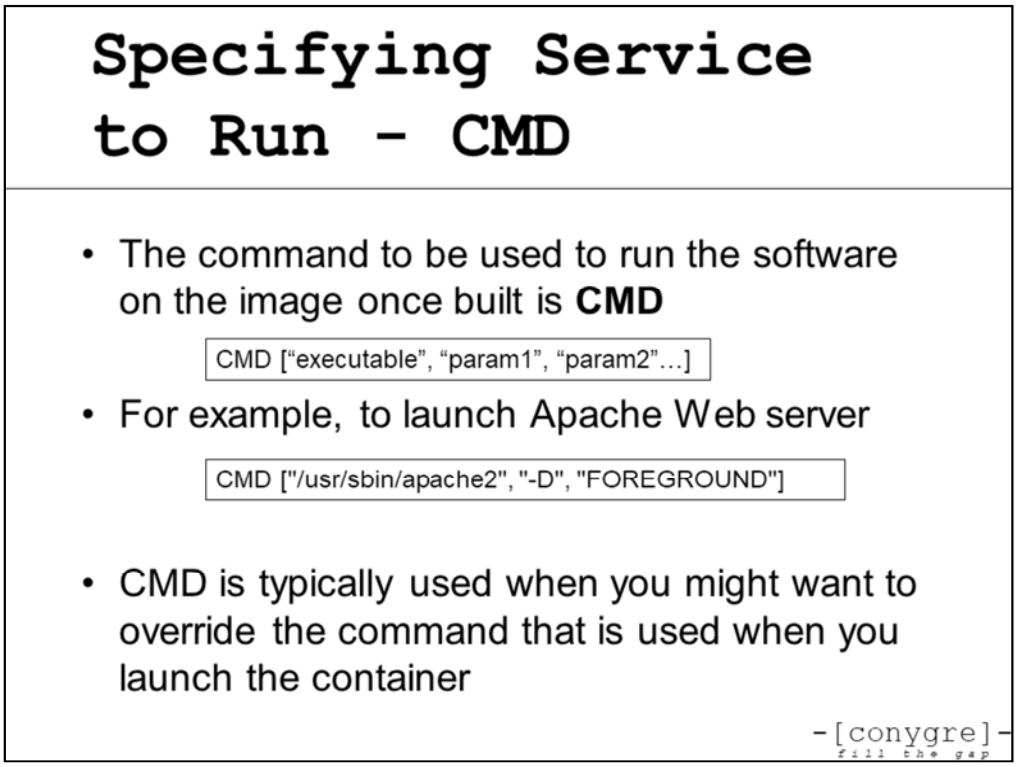


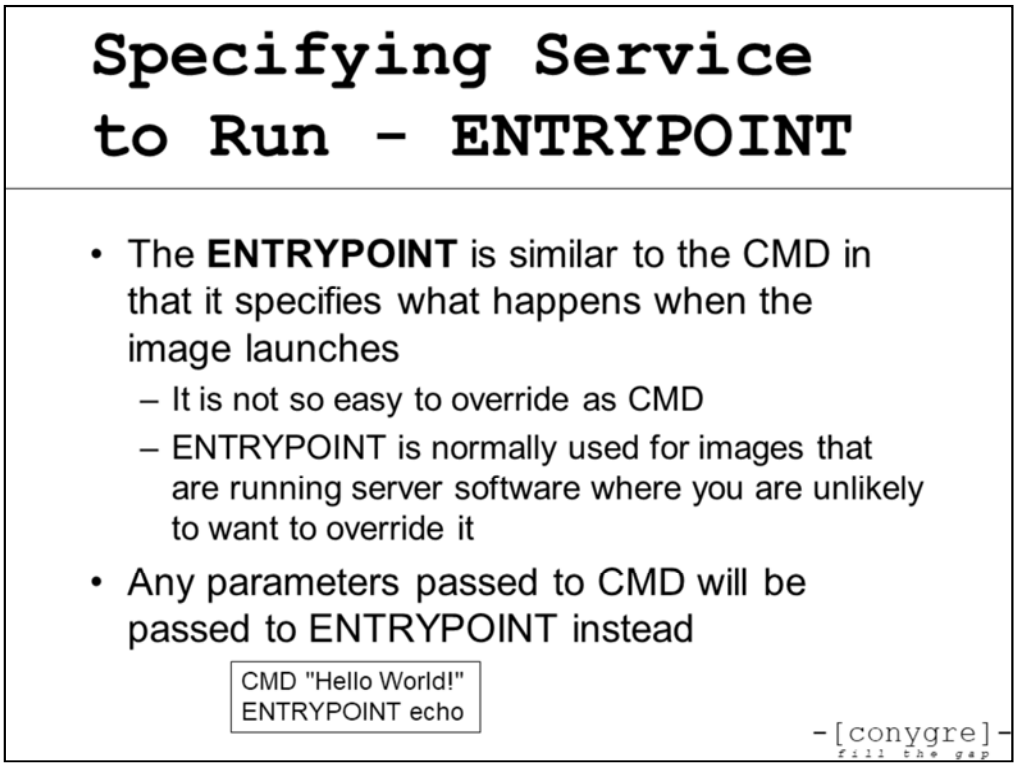










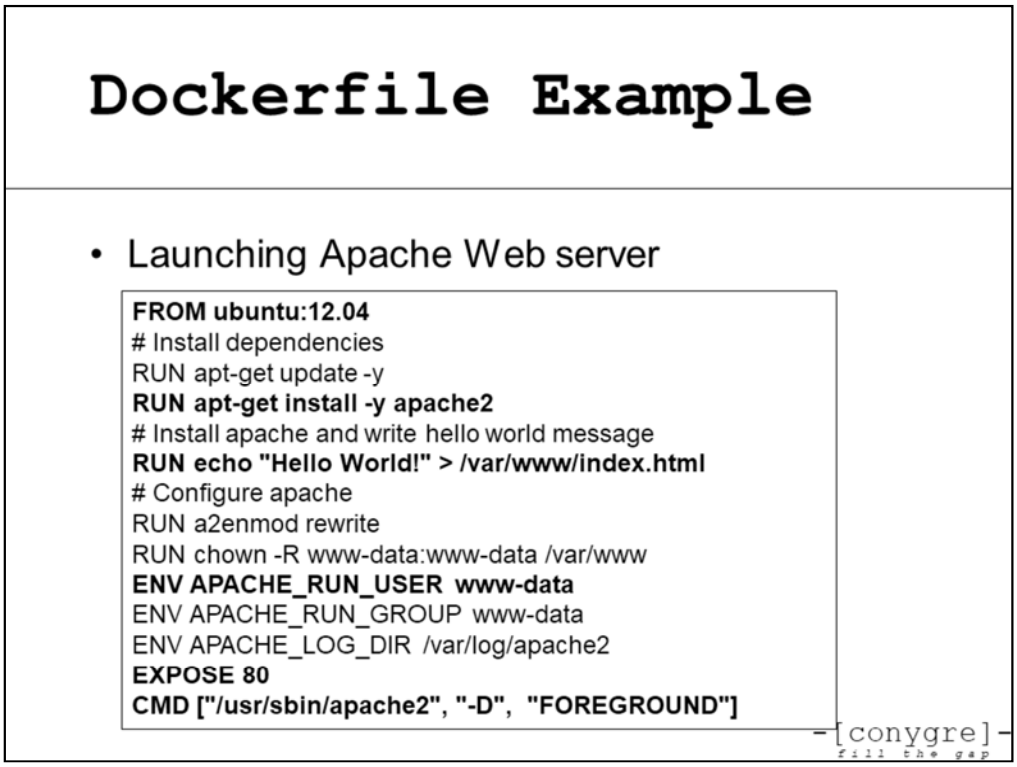


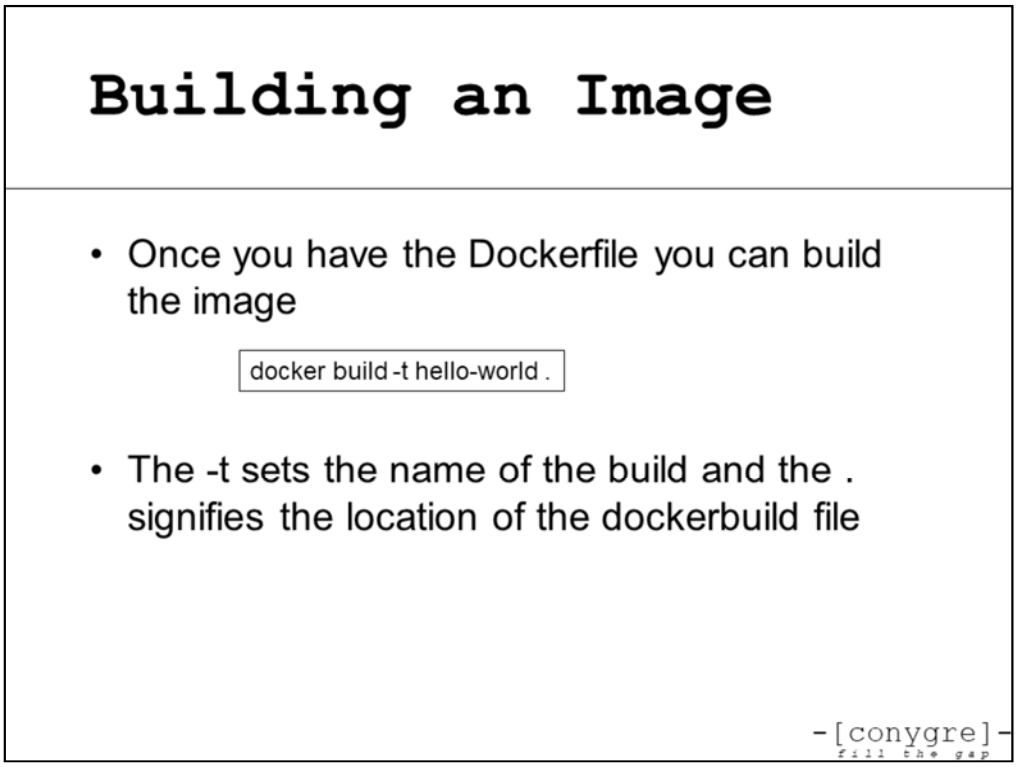
Other Dockerfile Keywords

Keyword	Role
LABEL	Adds meta data. Each LABEL creates a new layer, so don't have too many!
EXPOSE	Which ports to open from the image
COPY	Copy files into the image
VOLUME	Mount volumes on the host into the image
USER	Specify the user that the image command runs as

-[conygre]-
fill the gap

Docker

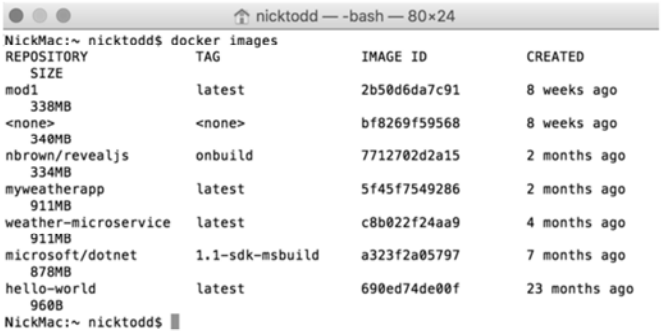




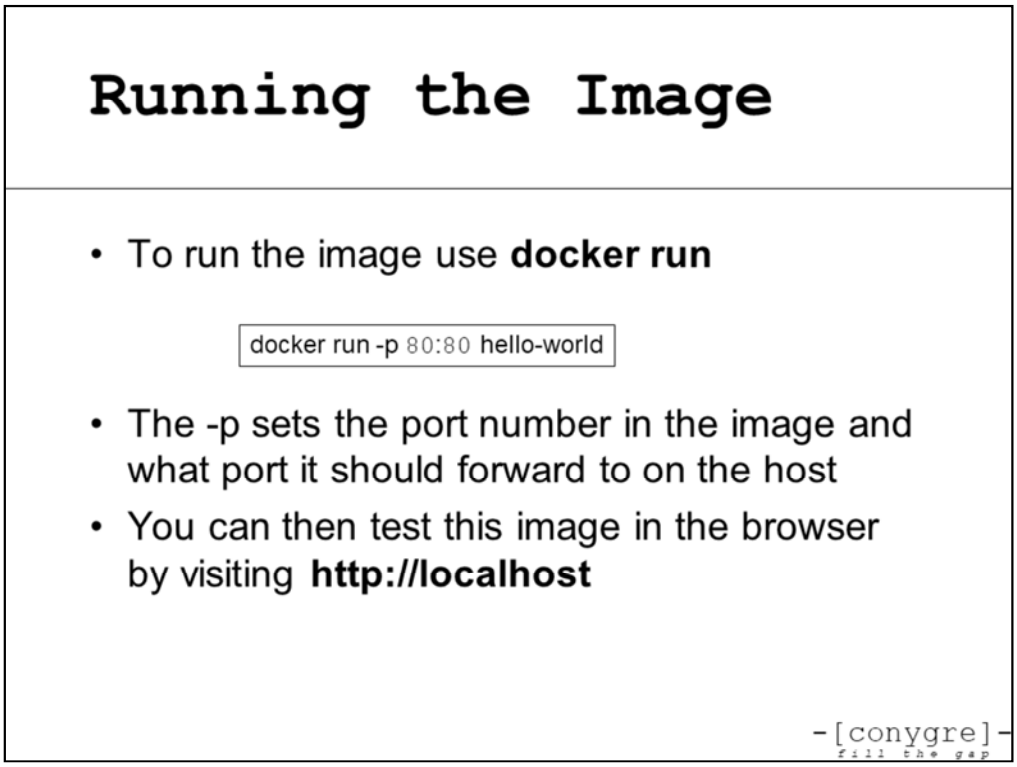
Docker

Viewing your Images

- You can view all of your images using the **docker images** command



-[conygre]-
fill the gap



EC2 Container Registry

- Docker images can be registered in the **Amazon EC2 Container Registry**
  - A managed container registry service
- Docker provides a CLI for pushing images and managing images in the registry
- A registry can be created through the AWS CLI or the AWS Console

-[conygre]-
fill the gap