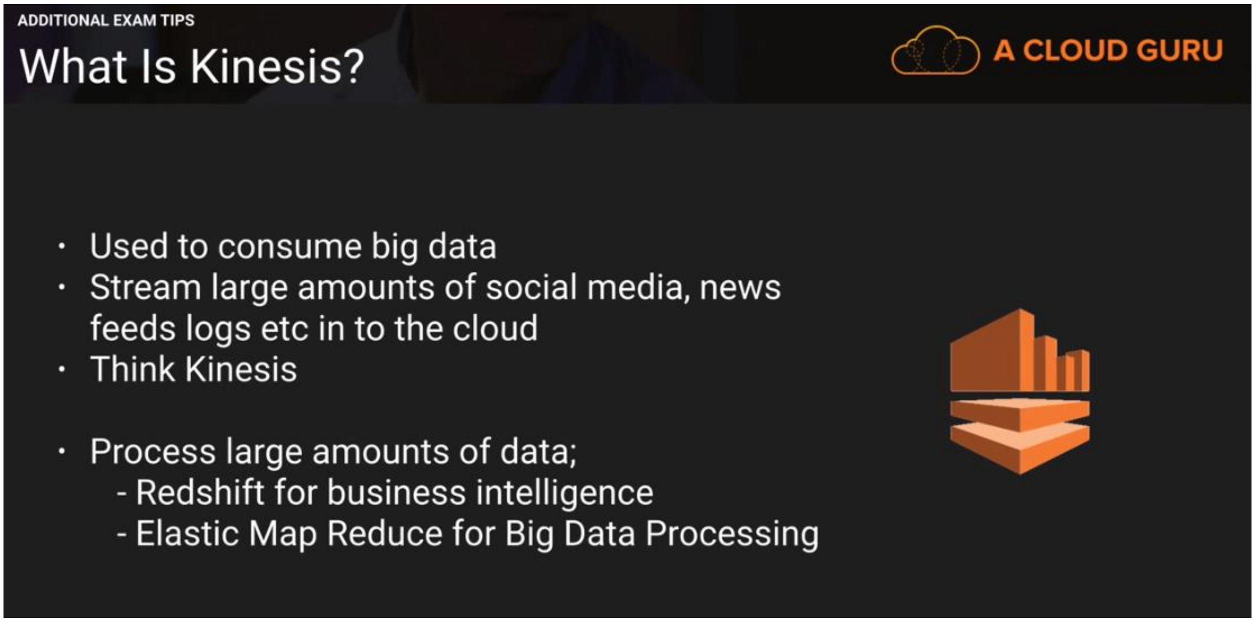


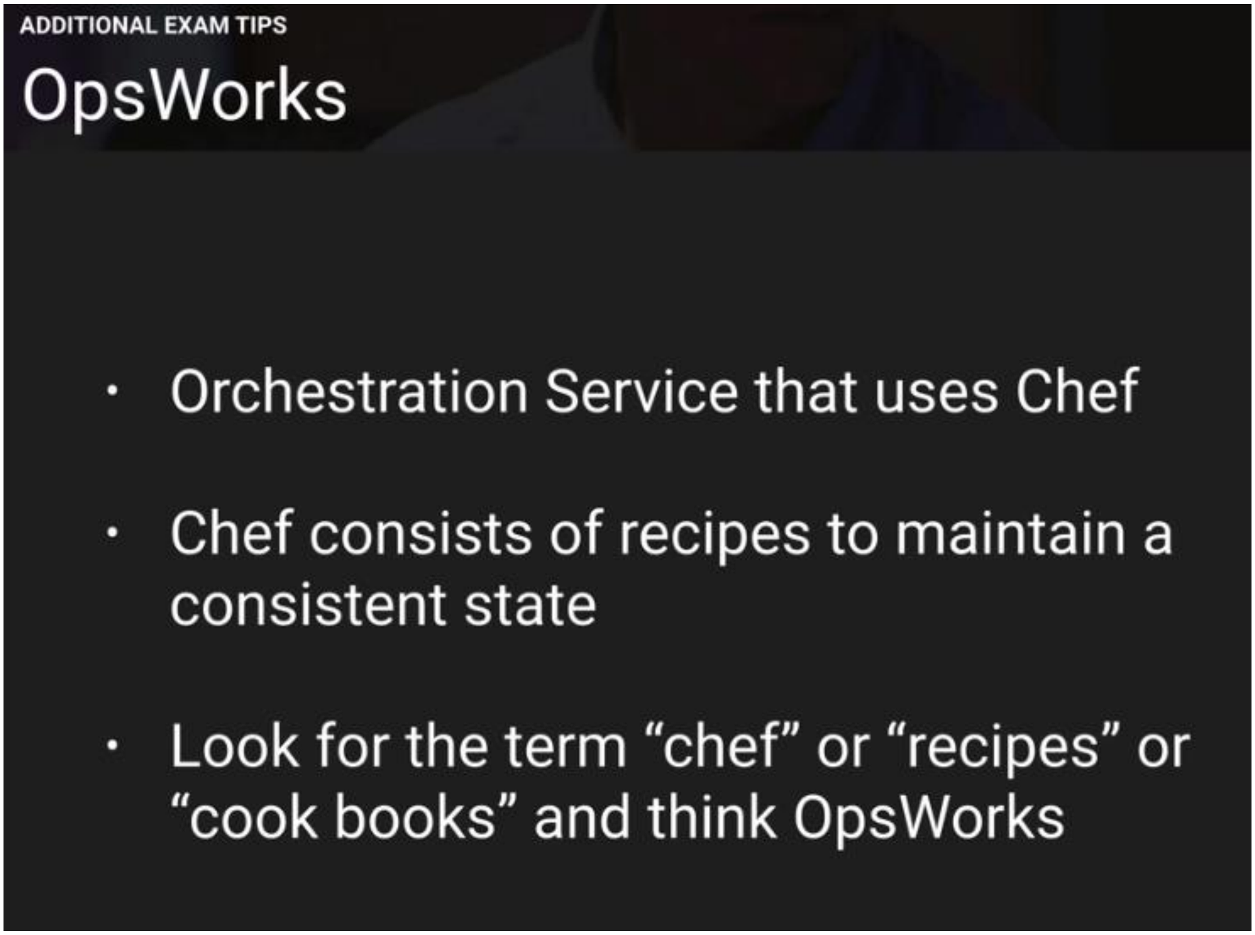
ADDITIONAL EXAM TIPS

What Is Kinesis?

A CLOUD GURU

- Used to consume big data
- Stream large amounts of social media, news feeds logs etc in to the cloud
- Think Kinesis

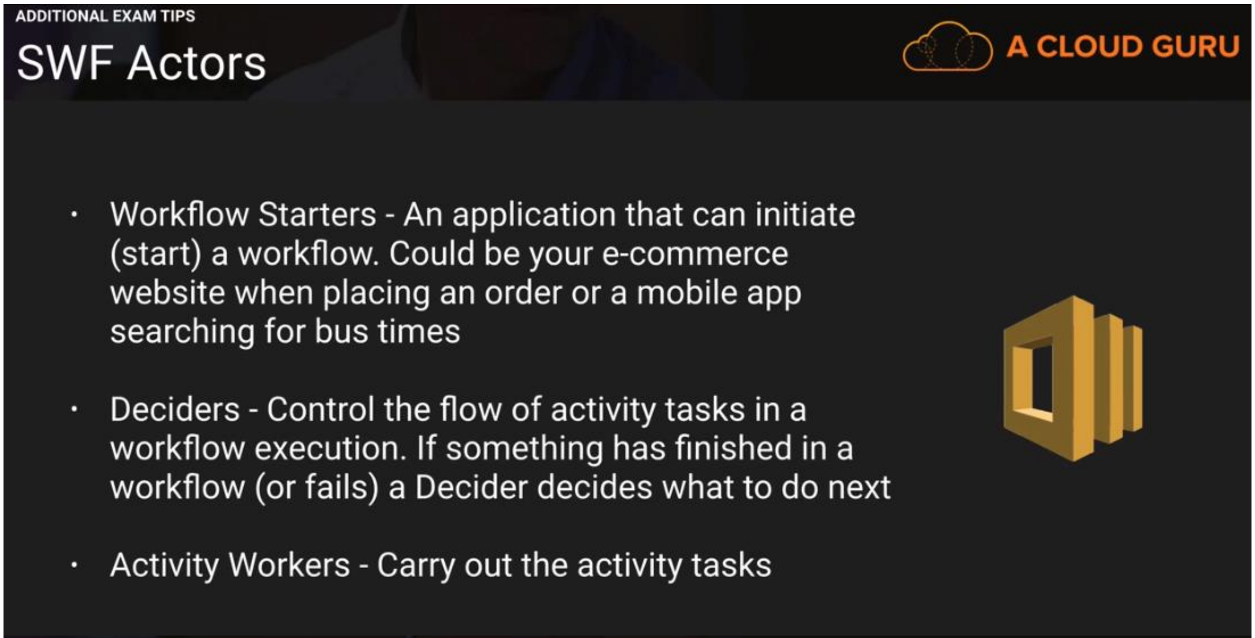
- Process large amounts of data;
  - Redshift for business intelligence
  - Elastic Map Reduce for Big Data Processing



ADDITIONAL EXAM TIPS

OpsWorks

- Orchestration Service that uses Chef
- Chef consists of recipes to maintain a consistent state
- Look for the term “chef” or “recipes” or “cook books” and think OpsWorks

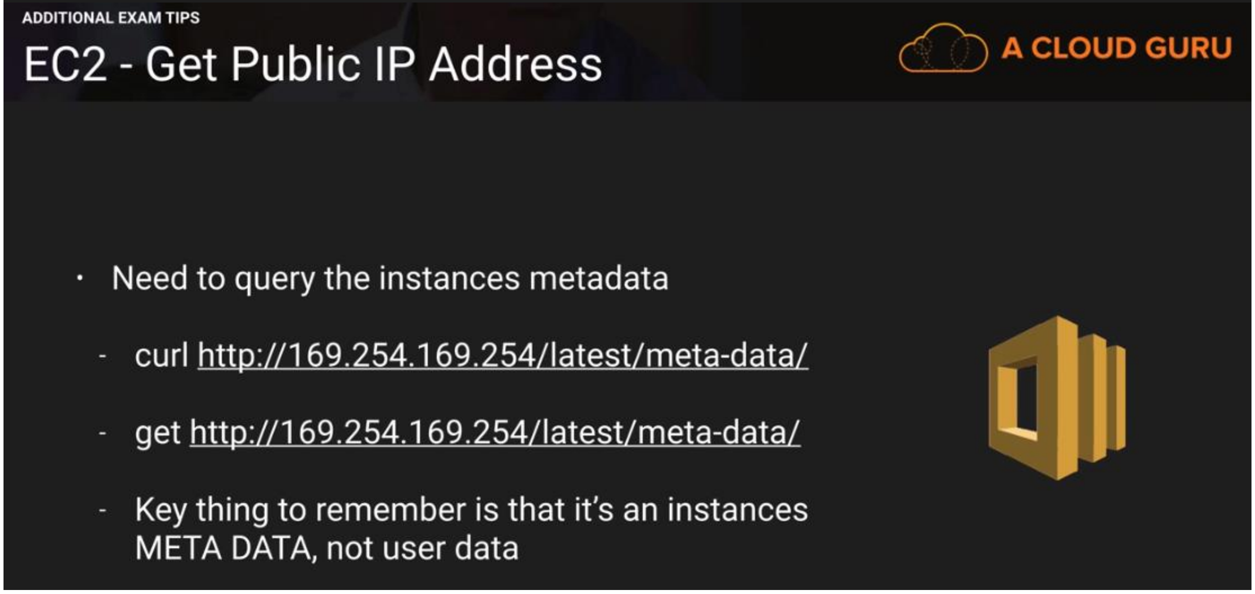


ADDITIONAL EXAM TIPS

SWF Actors

A CLOUD GURU

- Workflow Starters - An application that can initiate (start) a workflow. Could be your e-commerce website when placing an order or a mobile app searching for bus times
- Deciders - Control the flow of activity tasks in a workflow execution. If something has finished in a workflow (or fails) a Decider decides what to do next
- Activity Workers - Carry out the activity tasks



ADDITIONAL EXAM TIPS

EC2 - Get Public IP Address

A CLOUD GURU

- Need to query the instances metadata
  - curl http://169.254.169.254/latest/meta-data/
  - get http://169.254.169.254/latest/meta-data/
  - Key thing to remember is that it's an instances META DATA, not user data

AWS Organizations & Consolidated Billing

A CLOUD GURU

AWS Organizations & Consolidated Billing

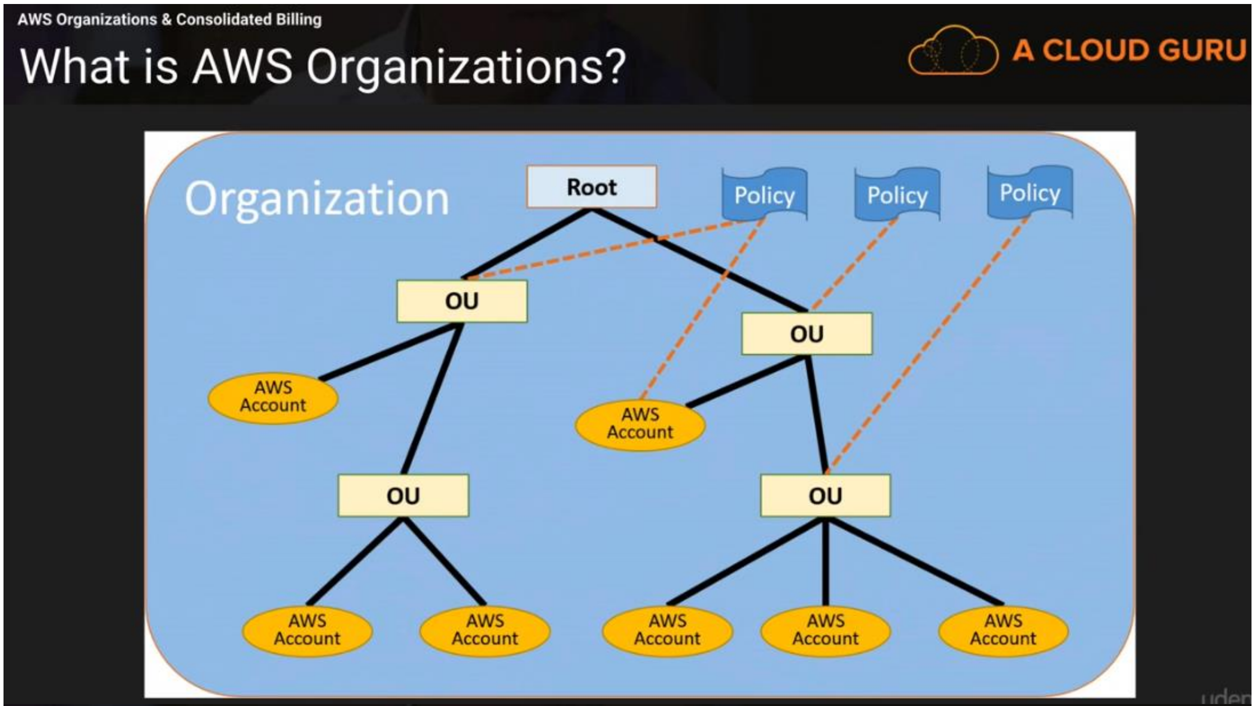
What is AWS Organizations?

A CLOUD GURU

AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage.

Available in two feature sets;

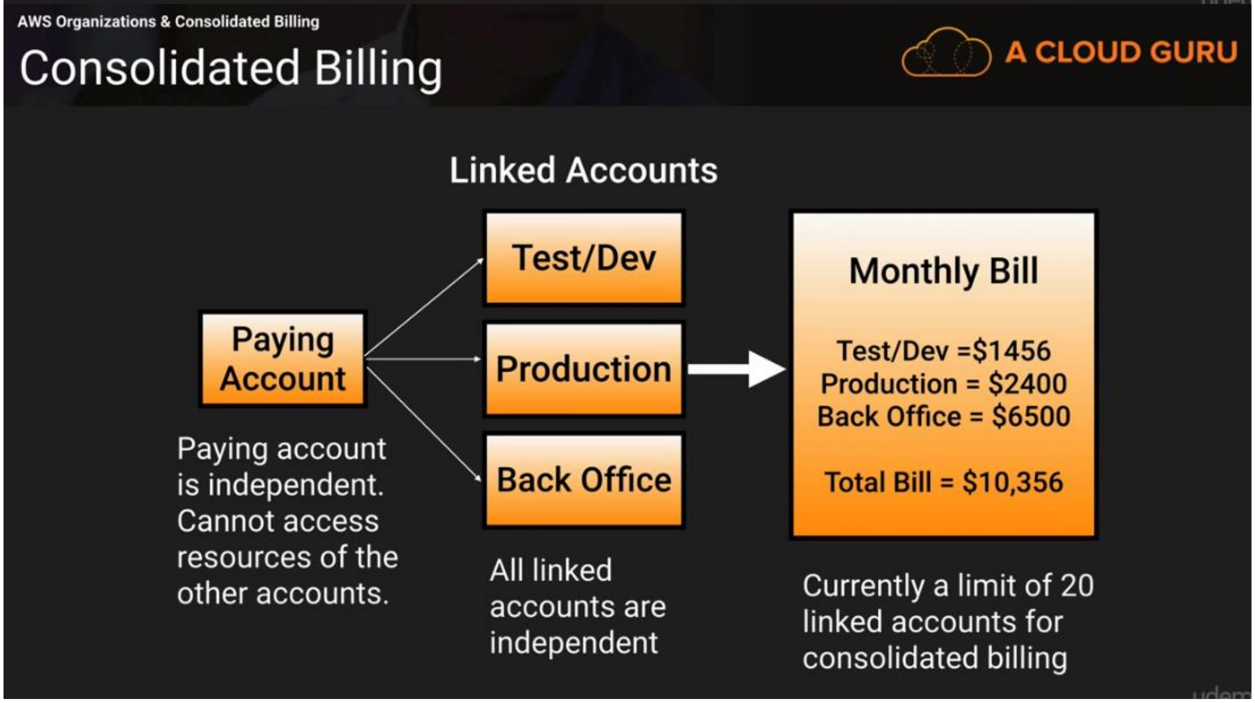
- Consolidated Billing
- All Features



AWS Organizations & Consolidated Billing

What is AWS Organizations?

A CLOUD GURU



AWS Organizations & Consolidated Billing

Consolidated Billing

A CLOUD GURU

Linked Accounts

Paying Account

Test/Dev

Production

Back Office

Monthly Bill

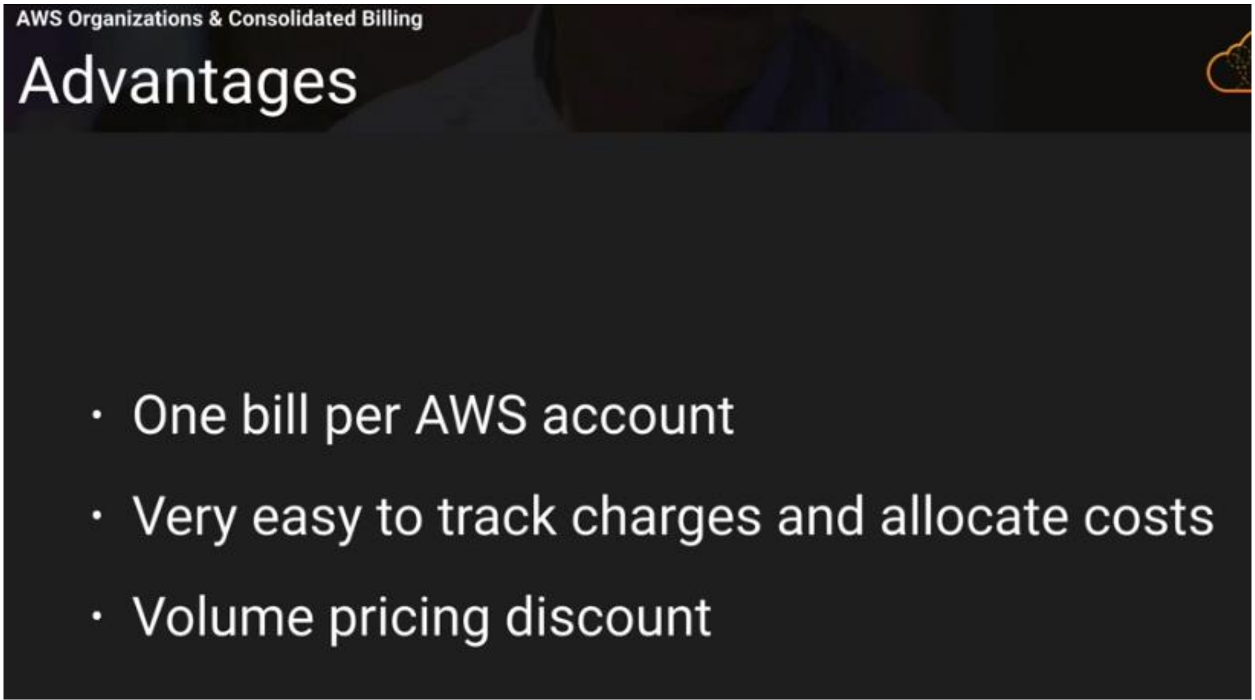
Test/Dev =$1456
Production = $2400
Back Office = $6500

Total Bill = $10,356

Paying account is independent. Cannot access resources of the other accounts.

All linked accounts are independent

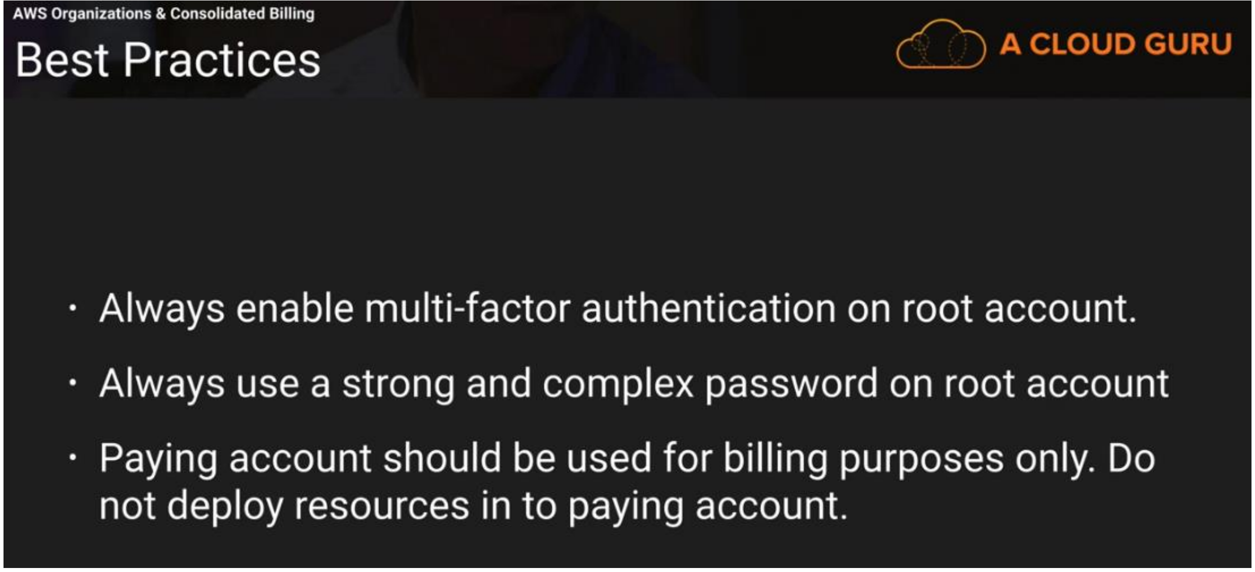
Currently a limit of 20 linked accounts for consolidated billing



AWS Organizations & Consolidated Billing

Advantages

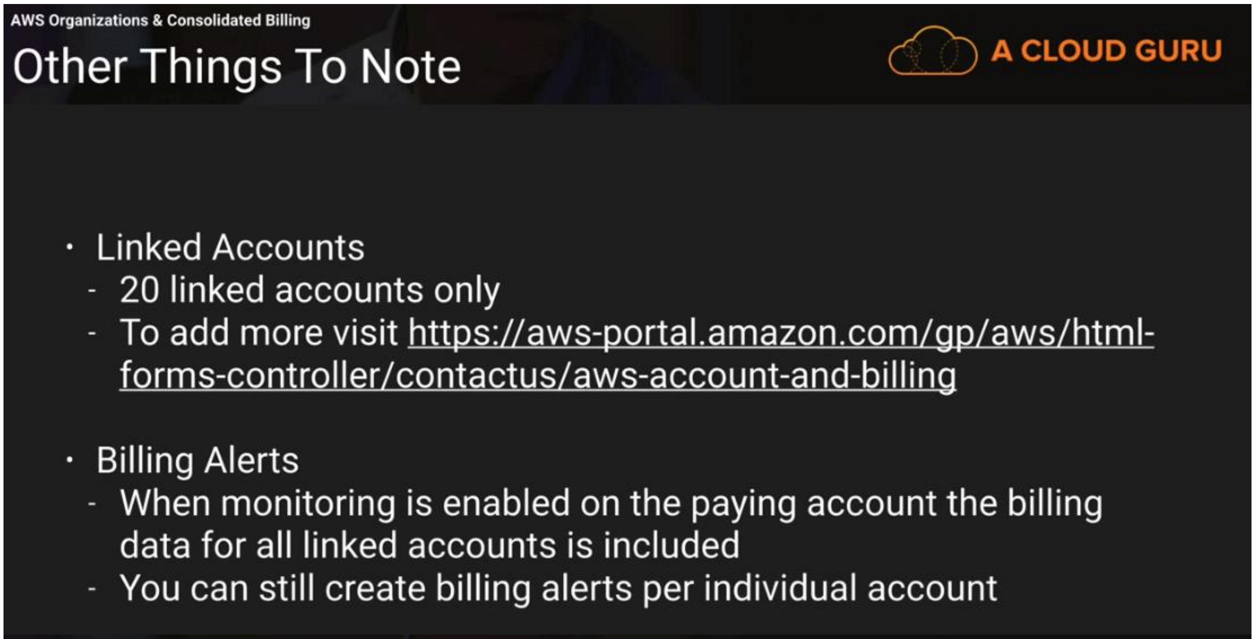
- One bill per AWS account
- Very easy to track charges and allocate costs
- Volume pricing discount



AWS Organizations & Consolidated Billing

Best Practices

- Always enable multi-factor authentication on root account.
- Always use a strong and complex password on root account
- Paying account should be used for billing purposes only. Do not deploy resources in to paying account.

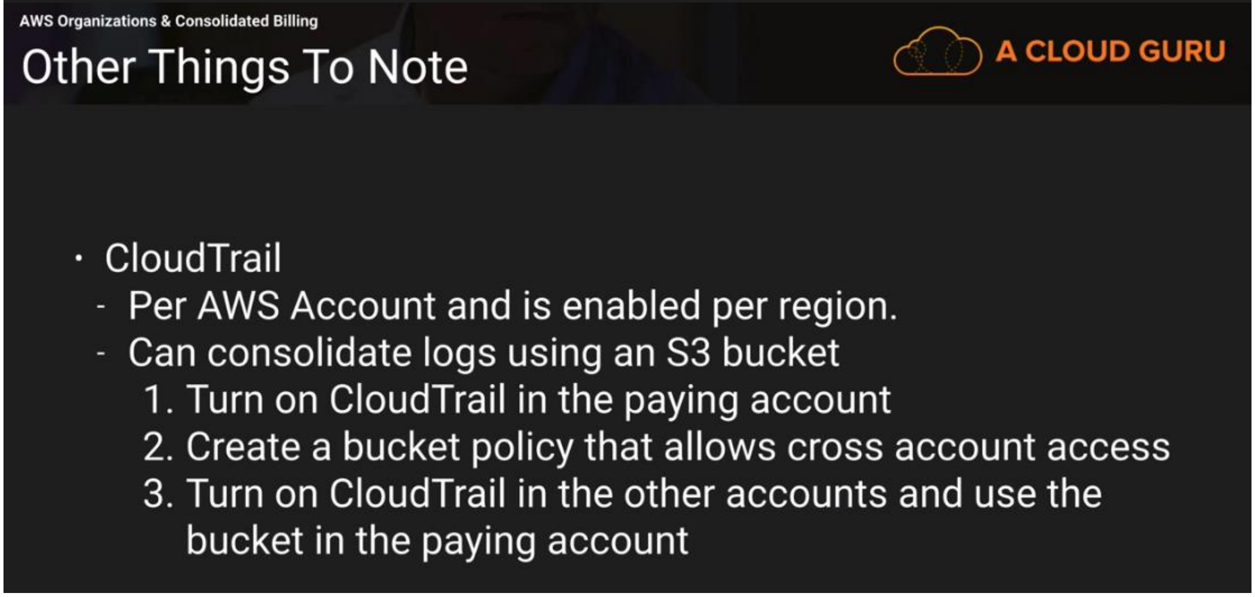


AWS Organizations & Consolidated Billing

Other Things To Note

A CLOUD GURU

- Linked Accounts
  - 20 linked accounts only
  - To add more visit https://aws-portal.amazon.com/gp/aws/html-forms-controller/contactus/aws-account-and-billing
- Billing Alerts
  - When monitoring is enabled on the paying account the billing data for all linked accounts is included
  - You can still create billing alerts per individual account

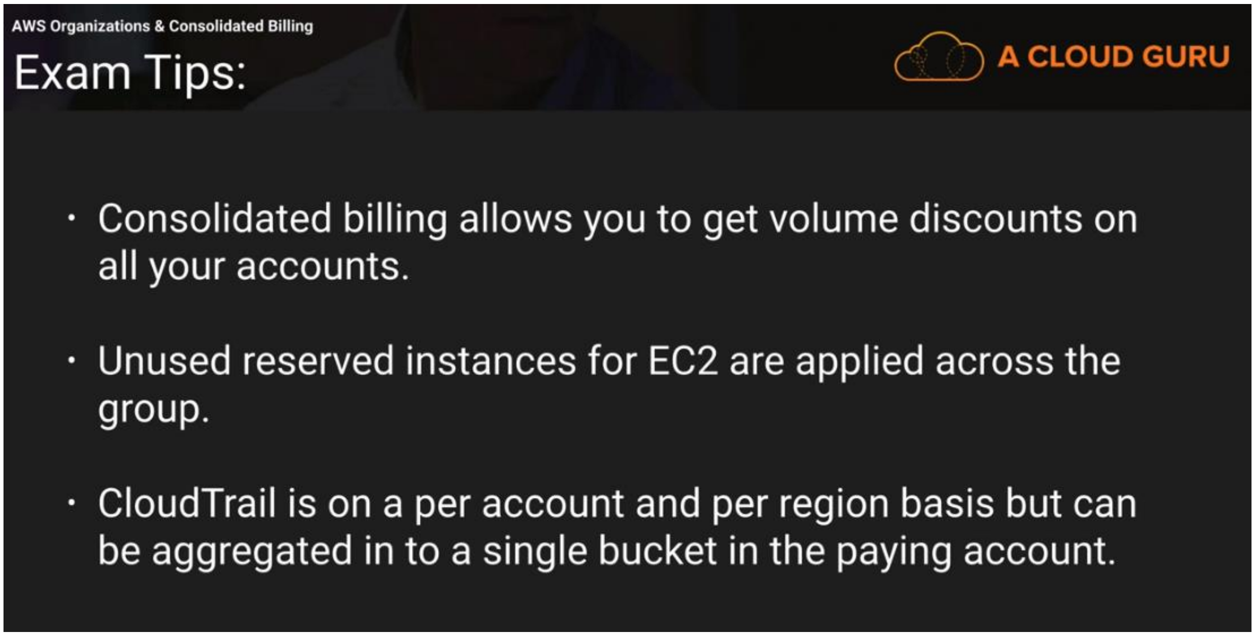


AWS Organizations & Consolidated Billing

Other Things To Note

A CLOUD GURU

- CloudTrail
  - Per AWS Account and is enabled per region.
  - Can consolidate logs using an S3 bucket
    1. Turn on CloudTrail in the paying account
    2. Create a bucket policy that allows cross account access
    3. Turn on CloudTrail in the other accounts and use the bucket in the paying account

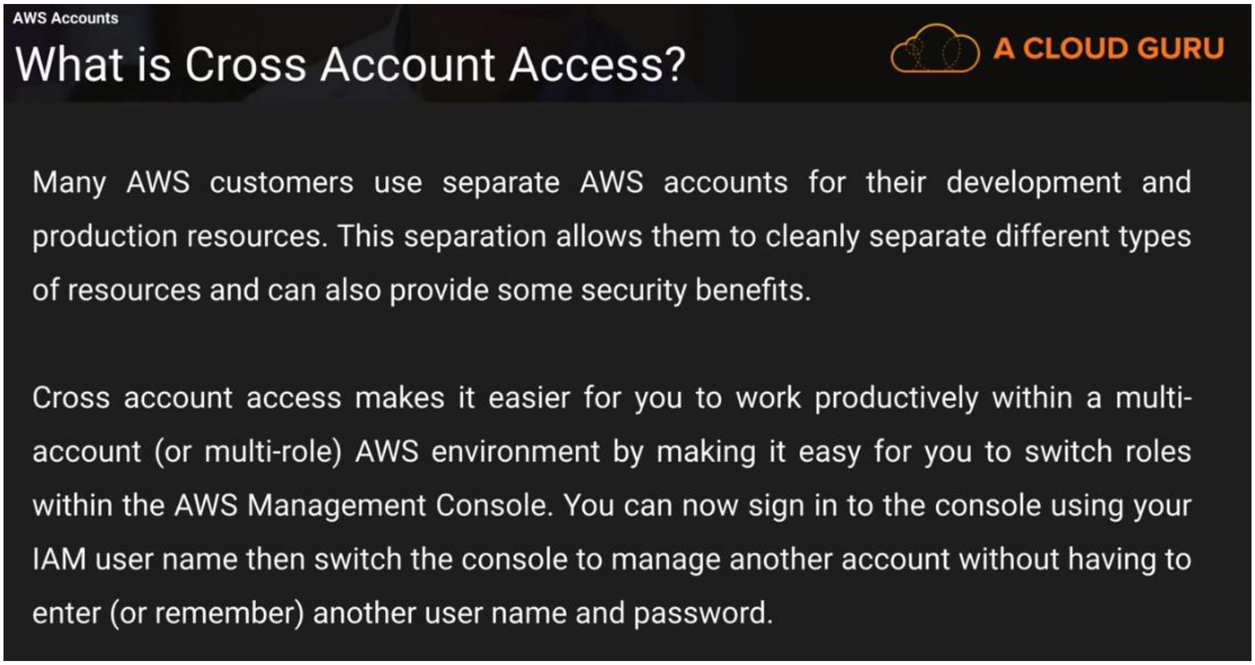


AWS Organizations & Consolidated Billing

Exam Tips:

A CLOUD GURU

- Consolidated billing allows you to get volume discounts on all your accounts.
- Unused reserved instances for EC2 are applied across the group.
- CloudTrail is on a per account and per region basis but can be aggregated in to a single bucket in the paying account.



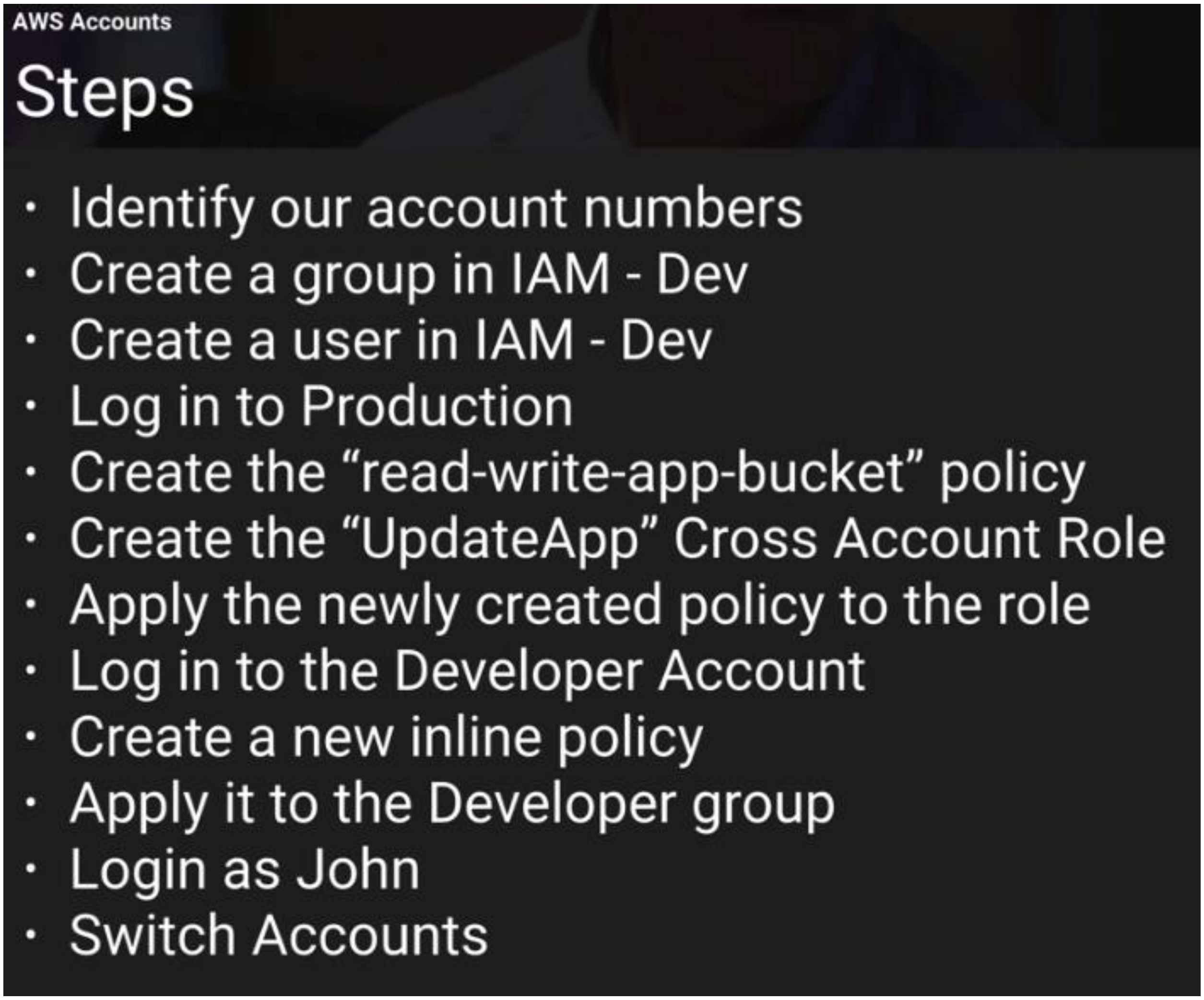
AWS Accounts

What is Cross Account Access?

A CLOUD GURU

Many AWS customers use separate AWS accounts for their development and production resources. This separation allows them to cleanly separate different types of resources and can also provide some security benefits.

Cross account access makes it easier for you to work productively within a multi-account (or multi-role) AWS environment by making it easy for you to switch roles within the AWS Management Console. You can now sign in to the console using your IAM user name then switch the console to manage another account without having to enter (or remember) another user name and password.



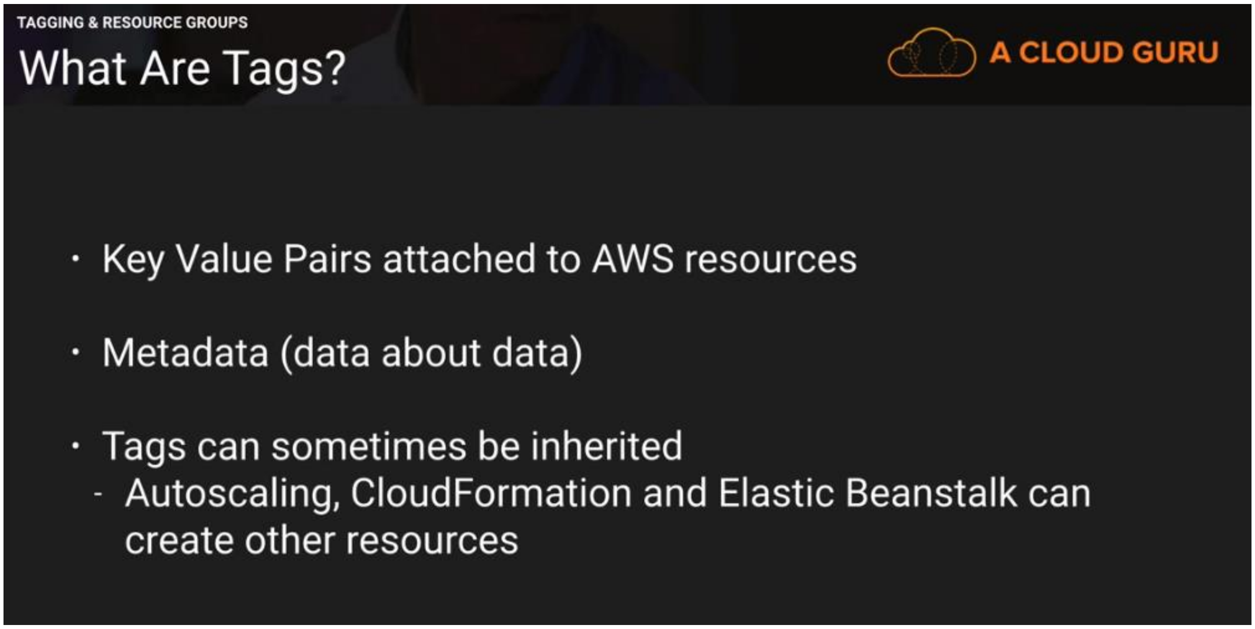
AWS Accounts

Steps

- Identify our account numbers
- Create a group in IAM - Dev
- Create a user in IAM - Dev
- Log in to Production
- Create the “read-write-app-bucket” policy
- Create the “UpdateApp” Cross Account Role
- Apply the newly created policy to the role
- Log in to the Developer Account
- Create a new inline policy
- Apply it to the Developer group
- Login as John
- Switch Accounts

Tagging & Resource Groups

A CLOUD GURU

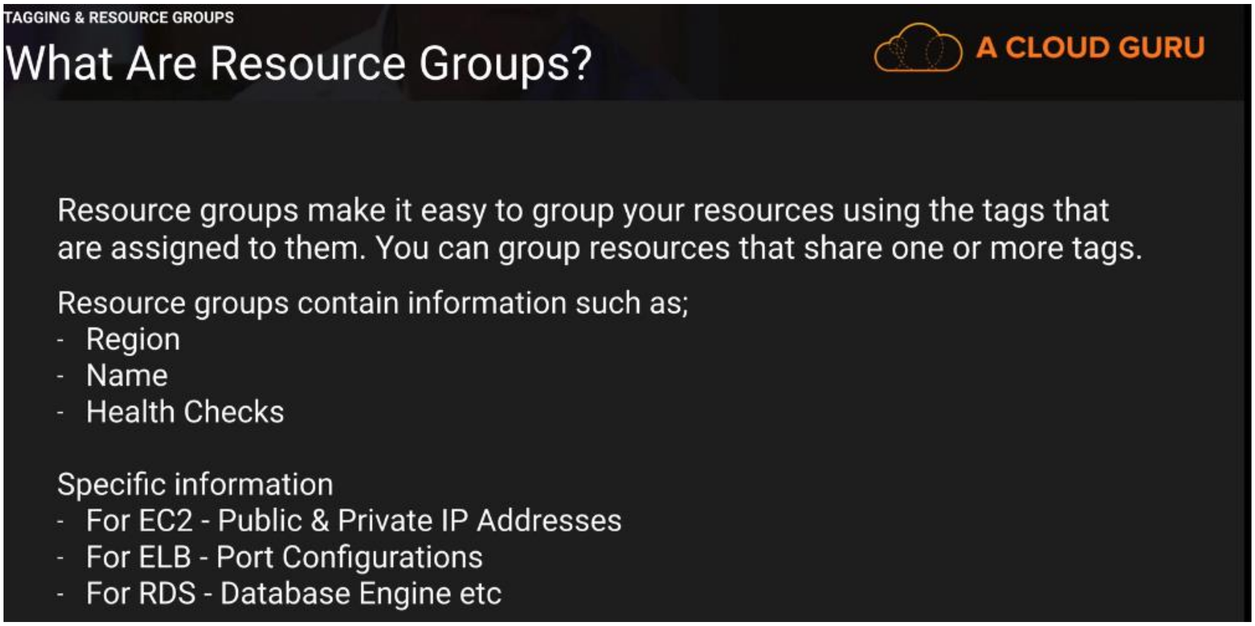


TAGGING & RESOURCE GROUPS

What Are Tags?

A CLOUD GURU

- Key Value Pairs attached to AWS resources
- Metadata (data about data)
- Tags can sometimes be inherited
  - Autoscaling, CloudFormation and Elastic Beanstalk can create other resources



TAGGING & RESOURCE GROUPS

What Are Resource Groups?

A CLOUD GURU

Resource groups make it easy to group your resources using the tags that are assigned to them. You can group resources that share one or more tags.

Resource groups contain information such as;

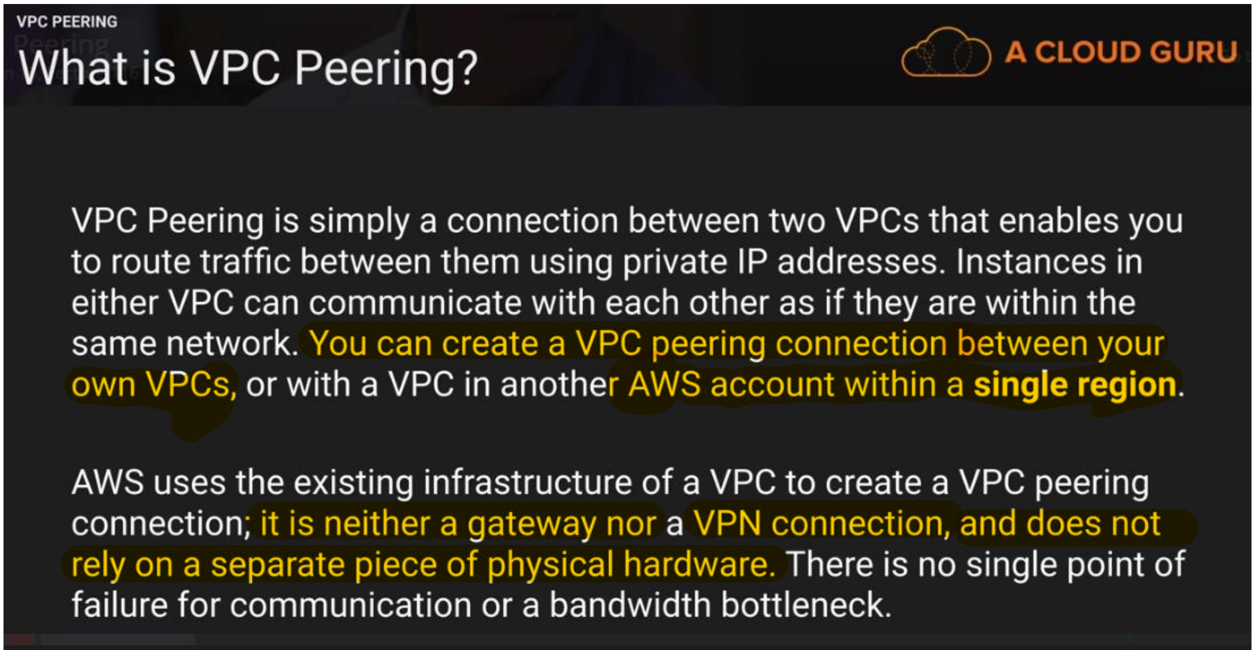
- Region
- Name
- Health Checks

Specific information

- For EC2 - Public & Private IP Addresses
- For ELB - Port Configurations
- For RDS - Database Engine etc

VPC Peering

A CLOUD GURU



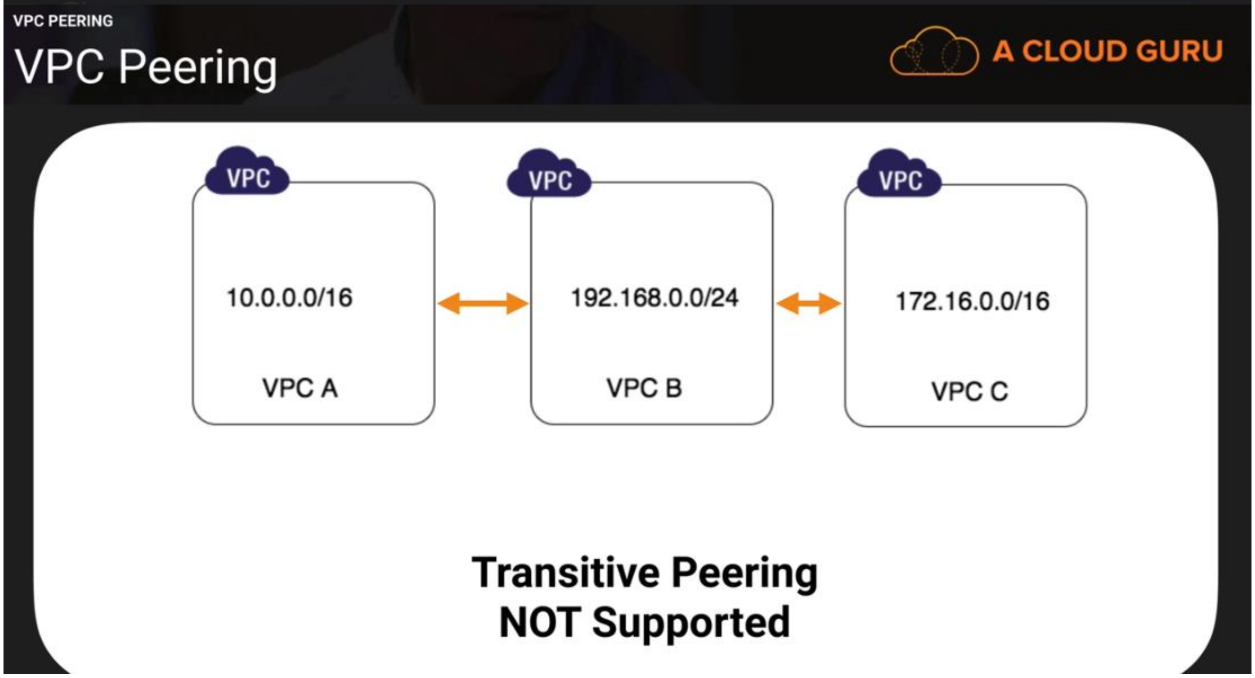
VPC PEERING

What is VPC Peering?

A CLOUD GURU

VPC Peering is simply a connection between two VPCs that enables you to route traffic between them using private IP addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account within a **single region**.

AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

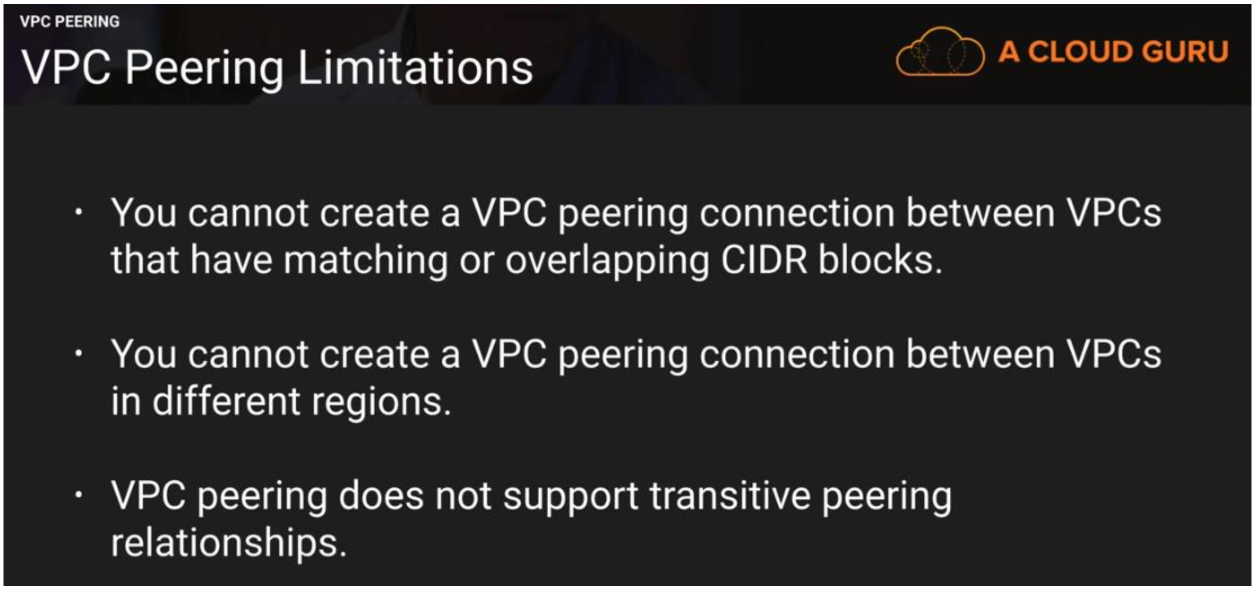


VPC PEERING

VPC Peering

A CLOUD GURU

**Transitive Peering
NOT Supported**



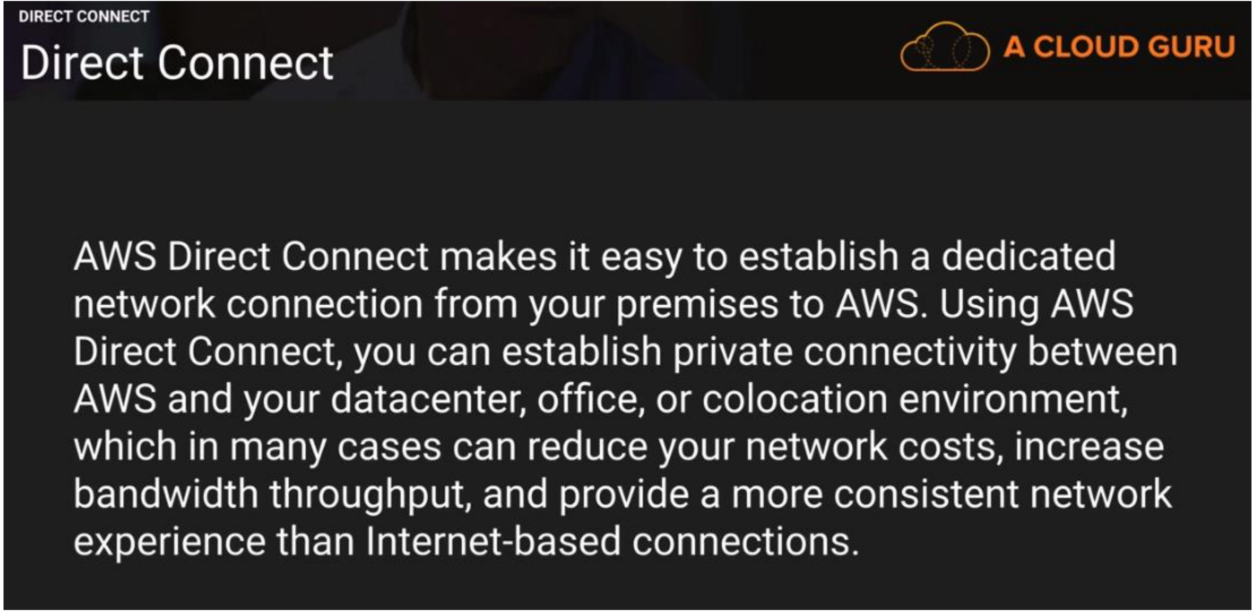
VPC PEERING

VPC Peering Limitations

- You cannot create a VPC peering connection between VPCs that have matching or overlapping CIDR blocks.
- You cannot create a VPC peering connection between VPCs in different regions.
- VPC peering does not support transitive peering relationships.

Direct Connect

A CLOUD GURU

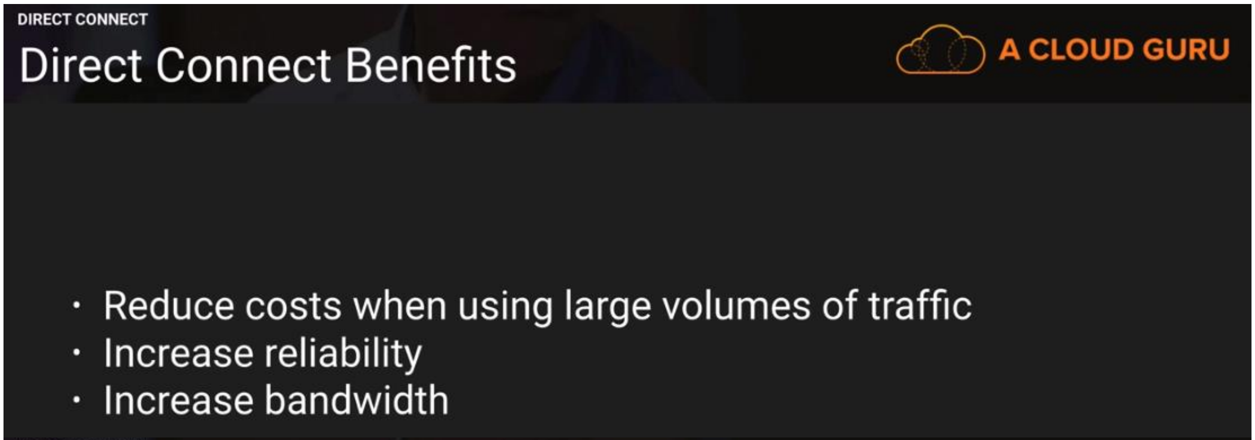


DIRECT CONNECT

Direct Connect

A CLOUD GURU

AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

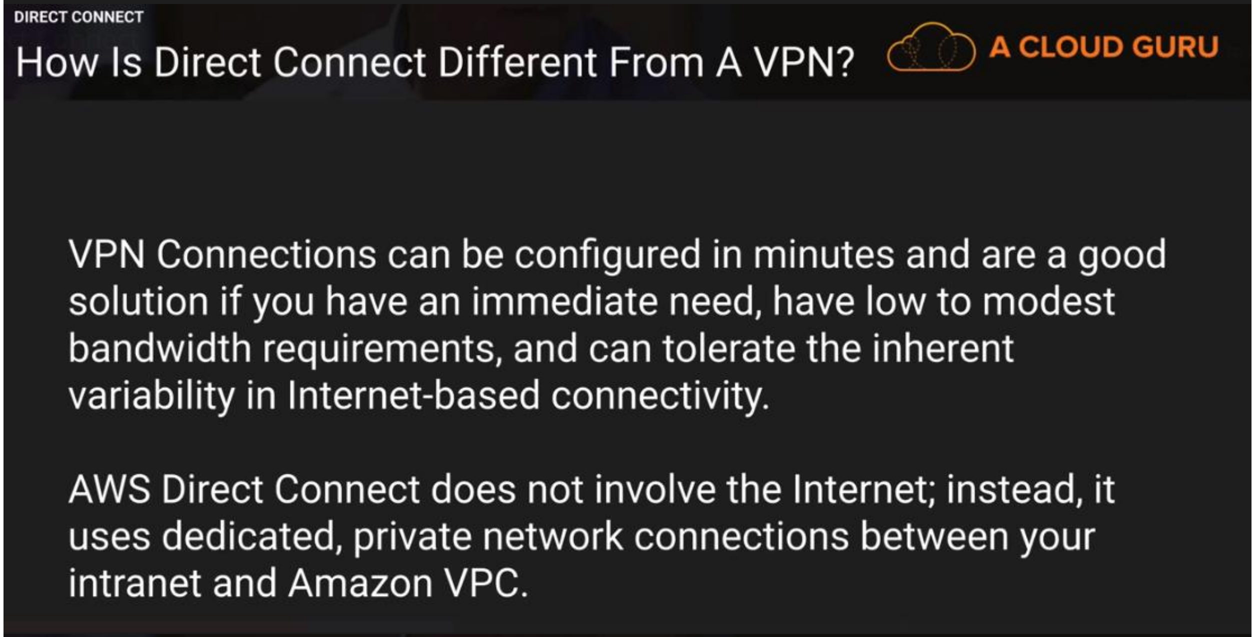


DIRECT CONNECT

Direct Connect Benefits

A CLOUD GURU

- Reduce costs when using large volumes of traffic
- Increase reliability
- Increase bandwidth



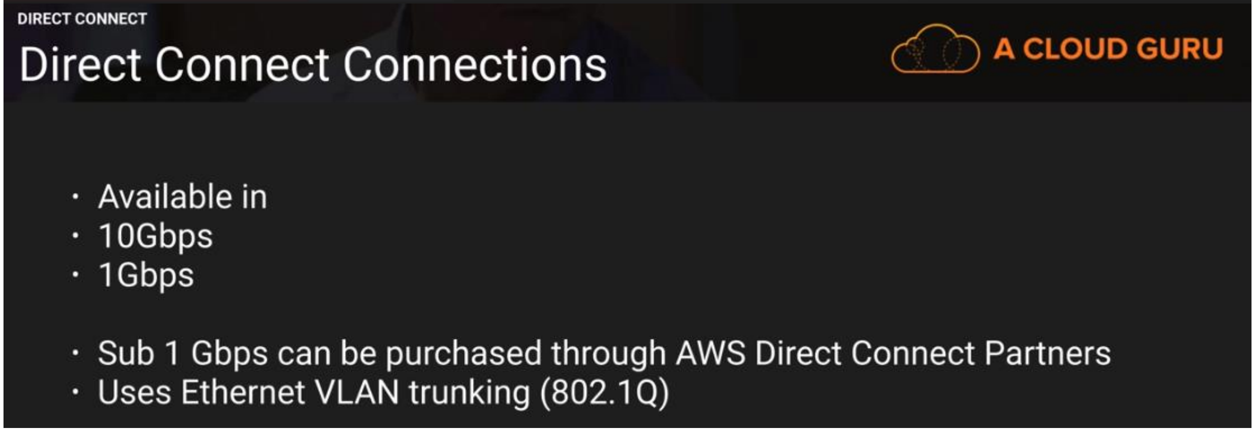
DIRECT CONNECT

How Is Direct Connect Different From A VPN?

A CLOUD GURU

VPN Connections can be configured in minutes and are a good solution if you have an immediate need, have low to modest bandwidth requirements, and can tolerate the inherent variability in Internet-based connectivity.

AWS Direct Connect does not involve the Internet; instead, it uses dedicated, private network connections between your intranet and Amazon VPC.



DIRECT CONNECT

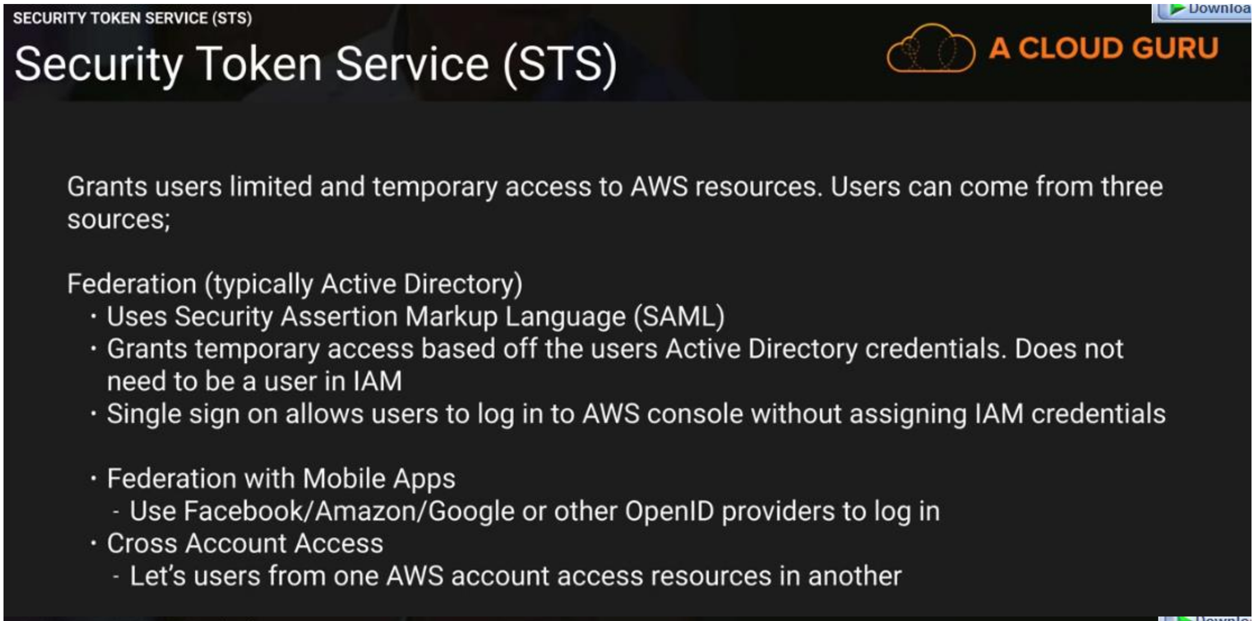
Direct Connect Connections

A CLOUD GURU

- Available in
- 10Gbps
- 1Gbps

- Sub 1 Gbps can be purchased through AWS Direct Connect Partners
- Uses Ethernet VLAN trunking (802.1Q)

Security Token Service (STS)



SECURITY TOKEN SERVICE (STS)

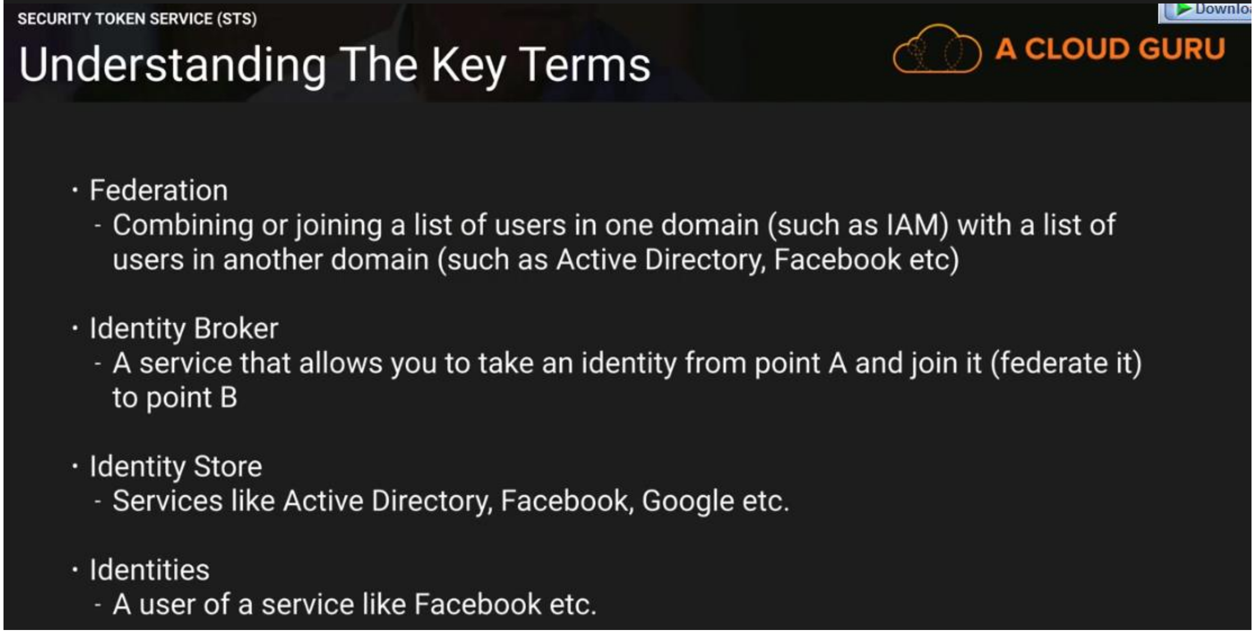
Security Token Service (STS)

Grants users limited and temporary access to AWS resources. Users can come from three sources;

Federation (typically Active Directory)

- Uses Security Assertion Markup Language (SAML)
- Grants temporary access based off the users Active Directory credentials. Does not need to be a user in IAM
- Single sign on allows users to log in to AWS console without assigning IAM credentials

- Federation with Mobile Apps
  - Use Facebook/Amazon/Google or other OpenID providers to log in
- Cross Account Access
  - Let's users from one AWS account access resources in another



SECURITY TOKEN SERVICE (STS)

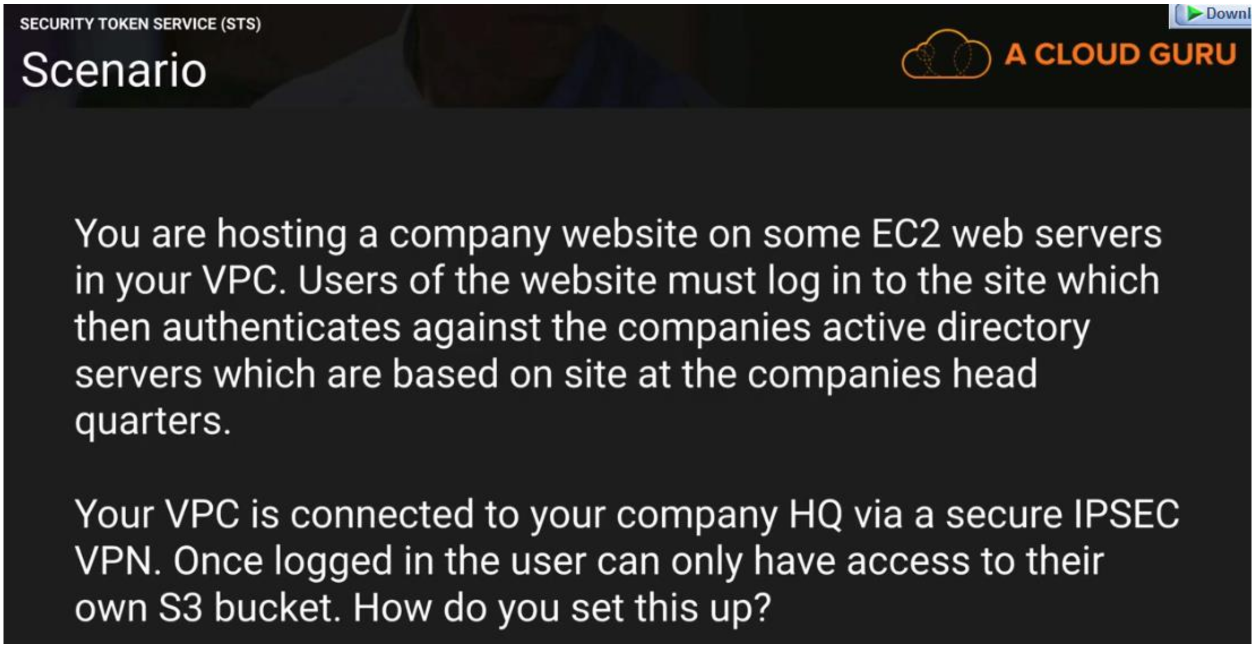
Understanding The Key Terms

- Federation
  - Combining or joining a list of users in one domain (such as IAM) with a list of users in another domain (such as Active Directory, Facebook etc)

- Identity Broker
  - A service that allows you to take an identity from point A and join it (federate it) to point B

- Identity Store
  - Services like Active Directory, Facebook, Google etc.

- Identities
  - A user of a service like Facebook etc.

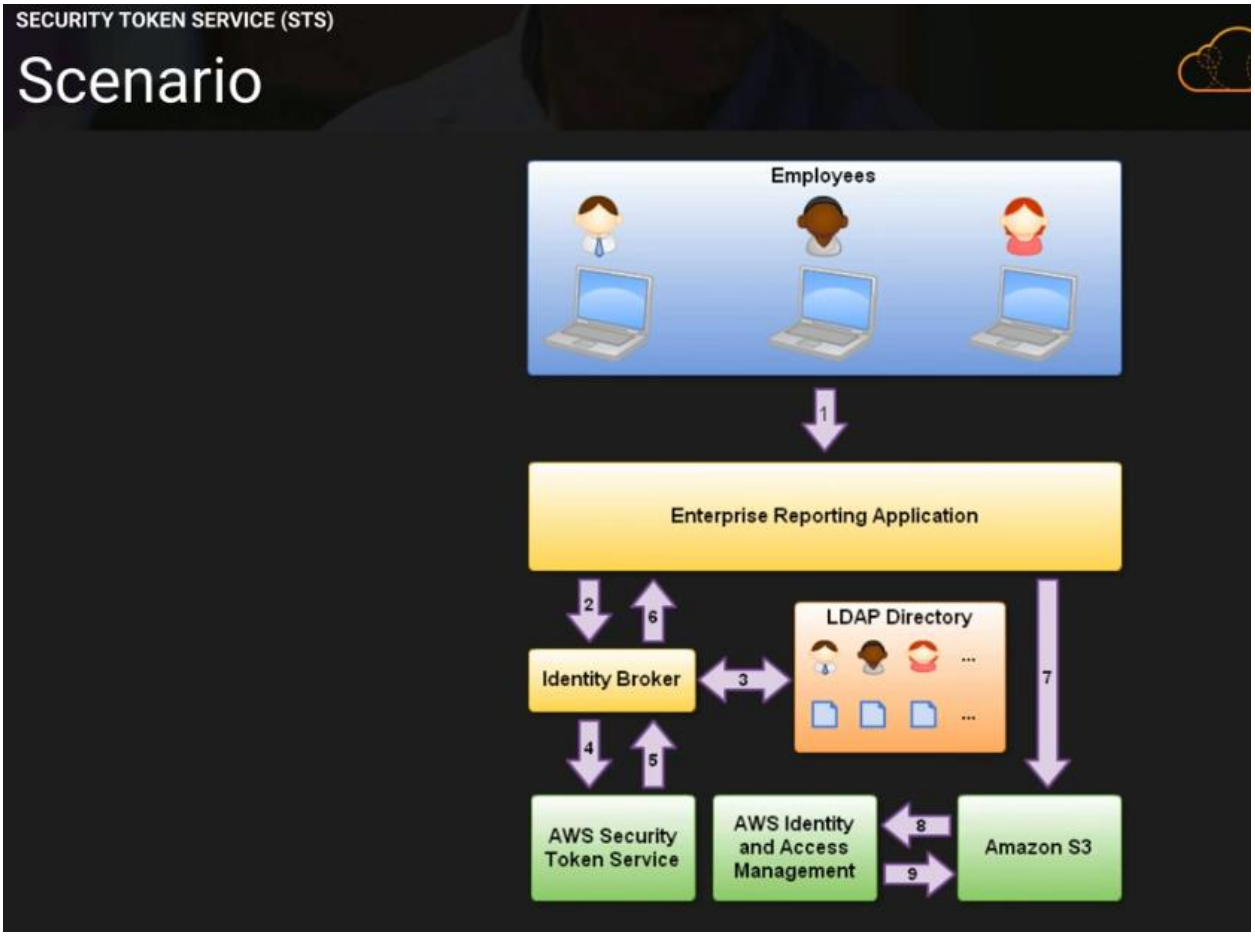


SECURITY TOKEN SERVICE (STS)

Scenario

You are hosting a company website on some EC2 web servers in your VPC. Users of the website must log in to the site which then authenticates against the companies active directory servers which are based on site at the companies head quarters.

Your VPC is connected to your company HQ via a secure IPSEC VPN. Once logged in the user can only have access to their own S3 bucket. How do you set this up?



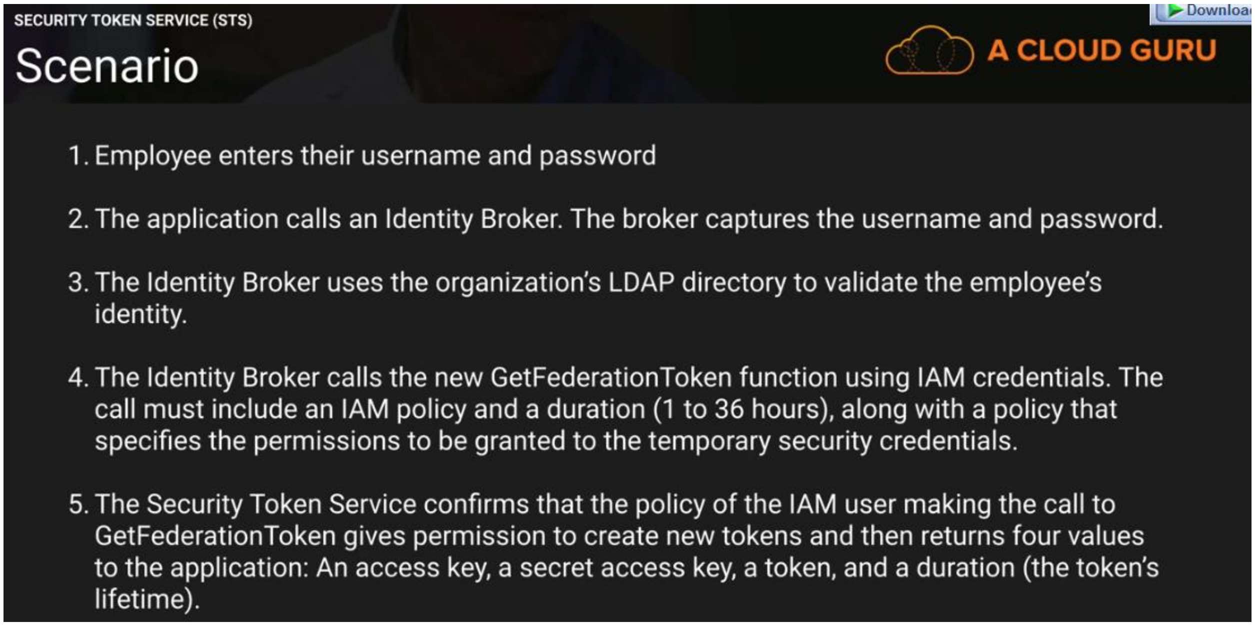
SECURITY TOKEN SERVICE (STS)

Scenario

Employees
1
Enterprise Reporting Application
2
6
Identity Broker
3
LDAP Directory
...
...
7
4
5
AWS Security Token Service
AWS Identity and Access Management
8
9
Amazon S3

AWS Security Token Service returns four things (Important to remember before going to exam):

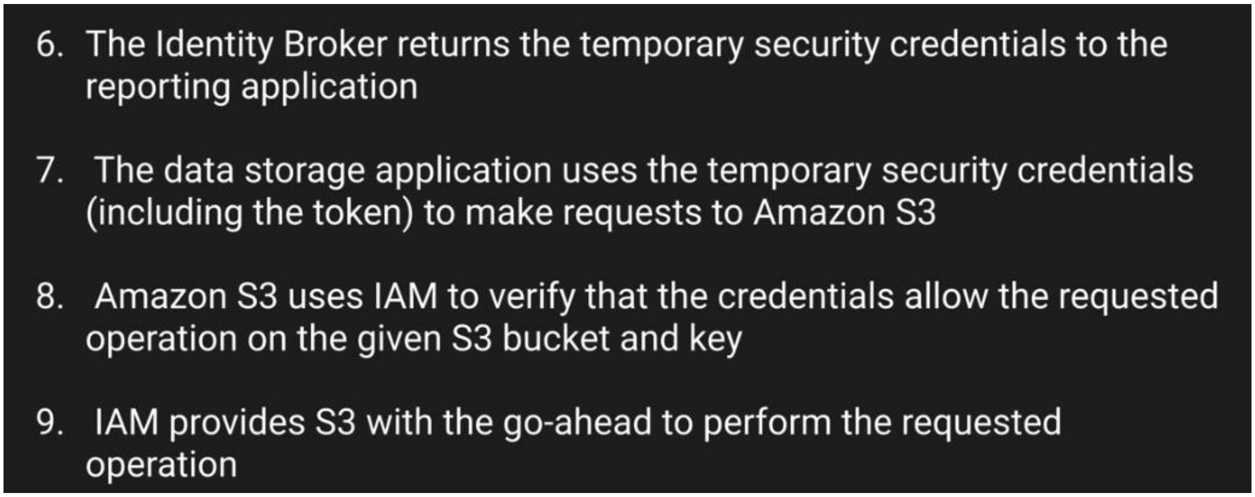
Access Key id, secret access key, a token and duration.



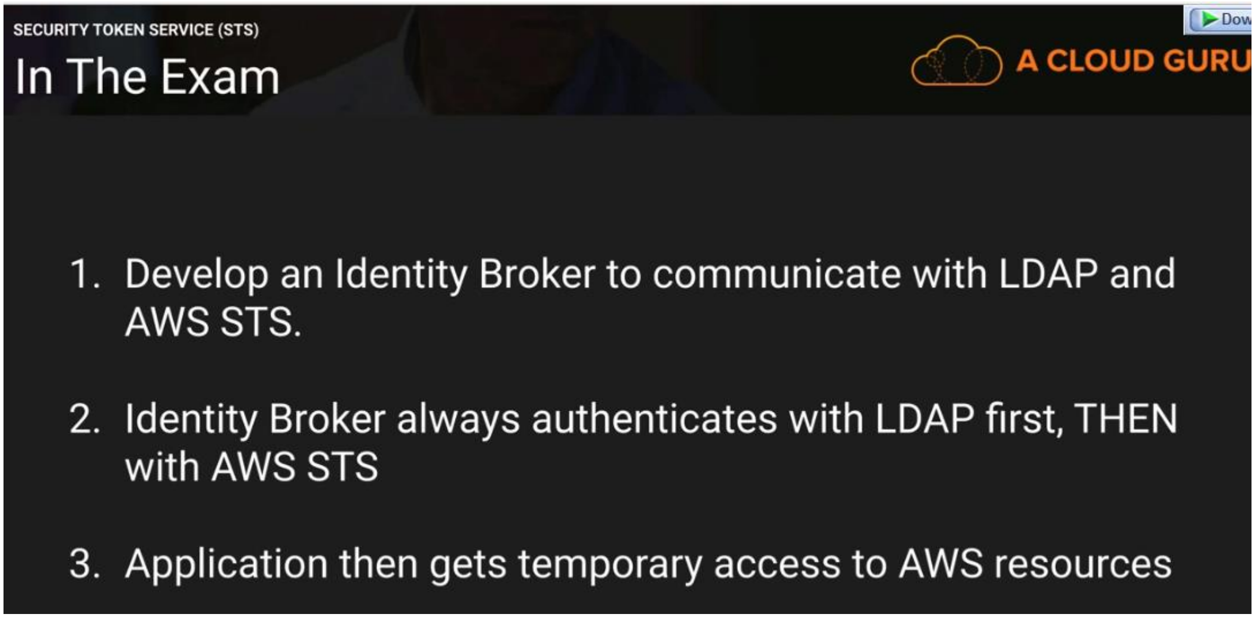
SECURITY TOKEN SERVICE (STS)

Scenario

1. Employee enters their username and password
2. The application calls an Identity Broker. The broker captures the username and password.
3. The Identity Broker uses the organization's LDAP directory to validate the employee's identity.
4. The Identity Broker calls the new GetFederationToken function using IAM credentials. The call must include an IAM policy and a duration (1 to 36 hours), along with a policy that specifies the permissions to be granted to the temporary security credentials.
5. The Security Token Service confirms that the policy of the IAM user making the call to GetFederationToken gives permission to create new tokens and then returns four values to the application: An access key, a secret access key, a token, and a duration (the token's lifetime).



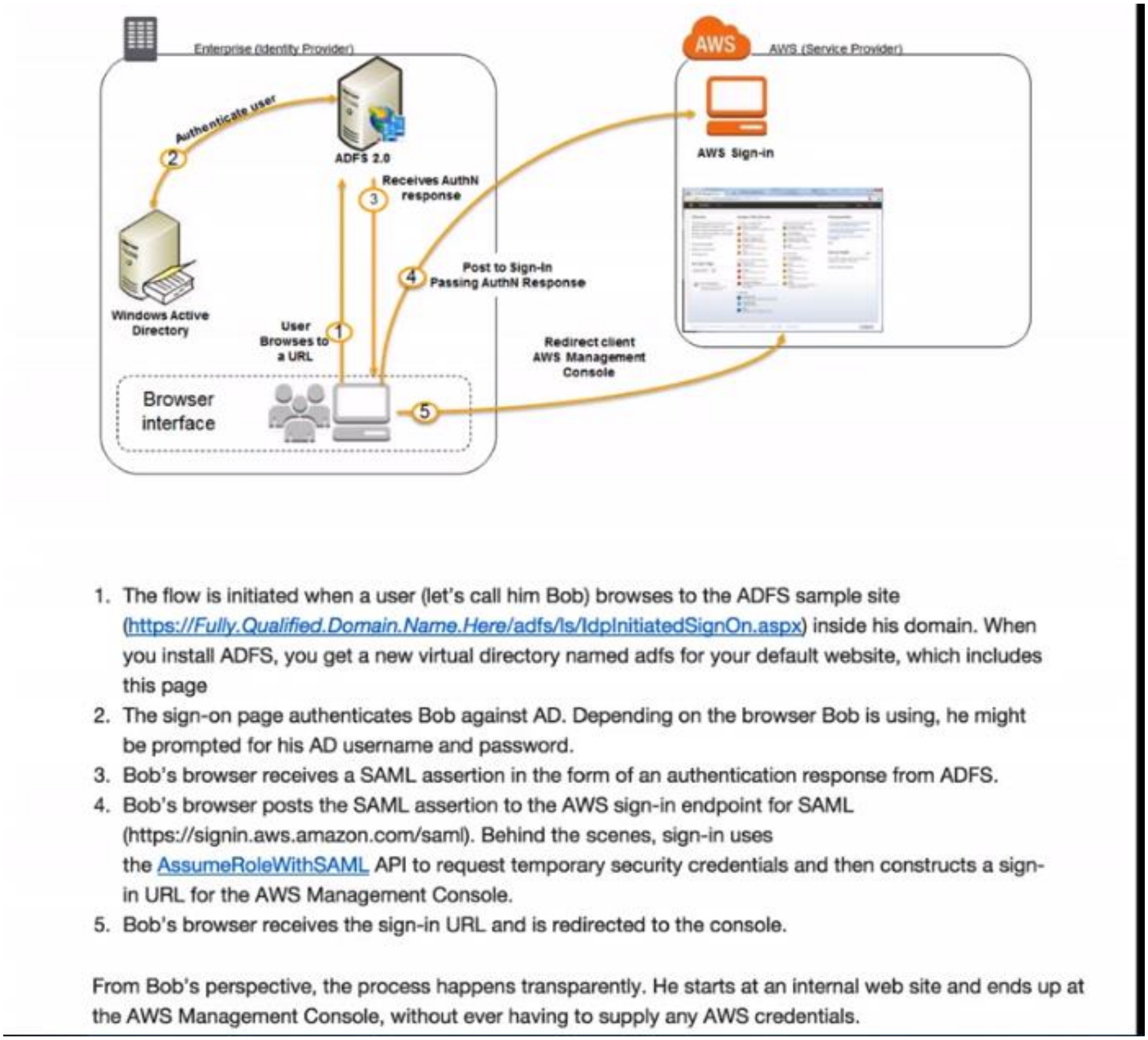
6. The Identity Broker returns the temporary security credentials to the reporting application
7. The data storage application uses the temporary security credentials (including the token) to make requests to Amazon S3
8. Amazon S3 uses IAM to verify that the credentials allow the requested operation on the given S3 bucket and key
9. IAM provides S3 with the go-ahead to perform the requested operation



SECURITY TOKEN SERVICE (STS)

In The Exam

1. Develop an Identity Broker to communicate with LDAP and AWS STS.
2. Identity Broker always authenticates with LDAP first, THEN with AWS STS
3. Application then gets temporary access to AWS resources

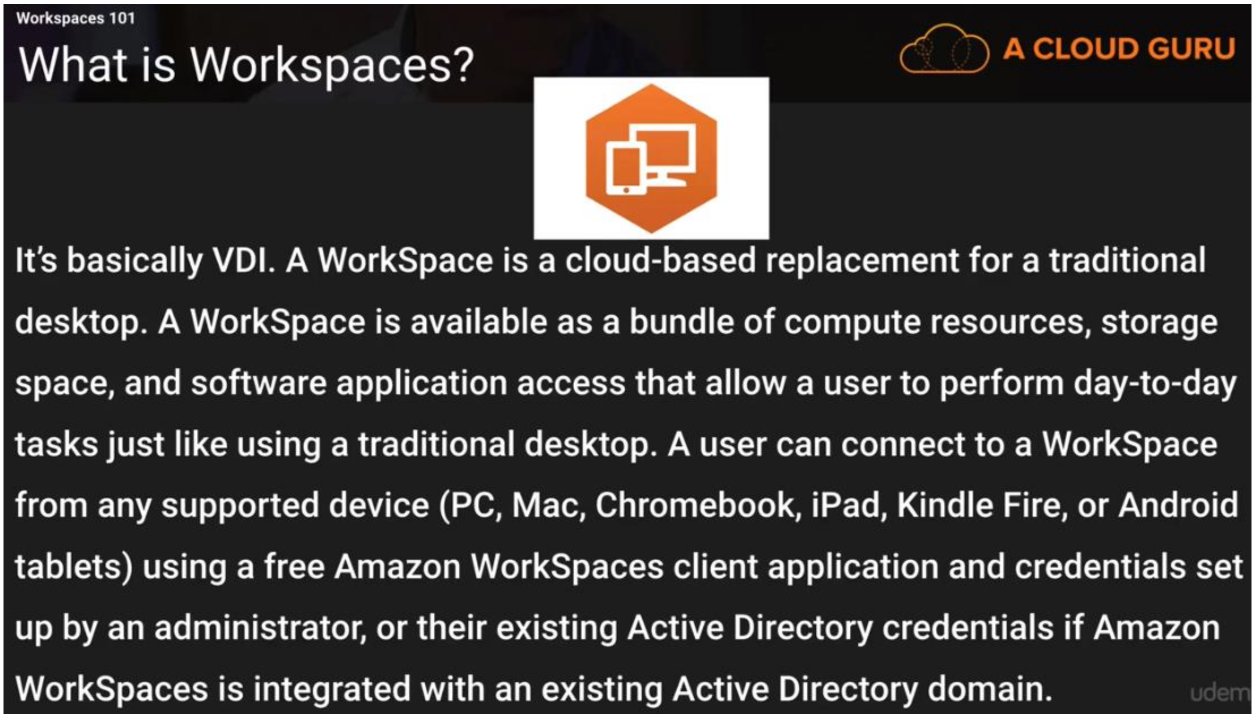


1. The flow is initiated when a user (let's call him Bob) browses to the ADFS sample site (https://*Fully.Qualified.Domain.Name.Here*/adfs/ls/IdpInitiatedSignOn.aspx) inside his domain. When you install ADFS, you get a new virtual directory named adfs for your default website, which includes this page
2. The sign-on page authenticates Bob against AD. Depending on the browser Bob is using, he might be prompted for his AD username and password.
3. Bob's browser receives a SAML assertion in the form of an authentication response from ADFS.
4. Bob's browser posts the SAML assertion to the AWS sign-in endpoint for SAML (https://signin.aws.amazon.com/saml). Behind the scenes, sign-in uses the AssumeRoleWithSAML API to request temporary security credentials and then constructs a sign-in URL for the AWS Management Console.
5. Bob's browser receives the sign-in URL and is redirected to the console.

From Bob's perspective, the process happens transparently. He starts at an internal web site and ends up at the AWS Management Console, without ever having to supply any AWS credentials.

Workspaces

A CLOUD GURU



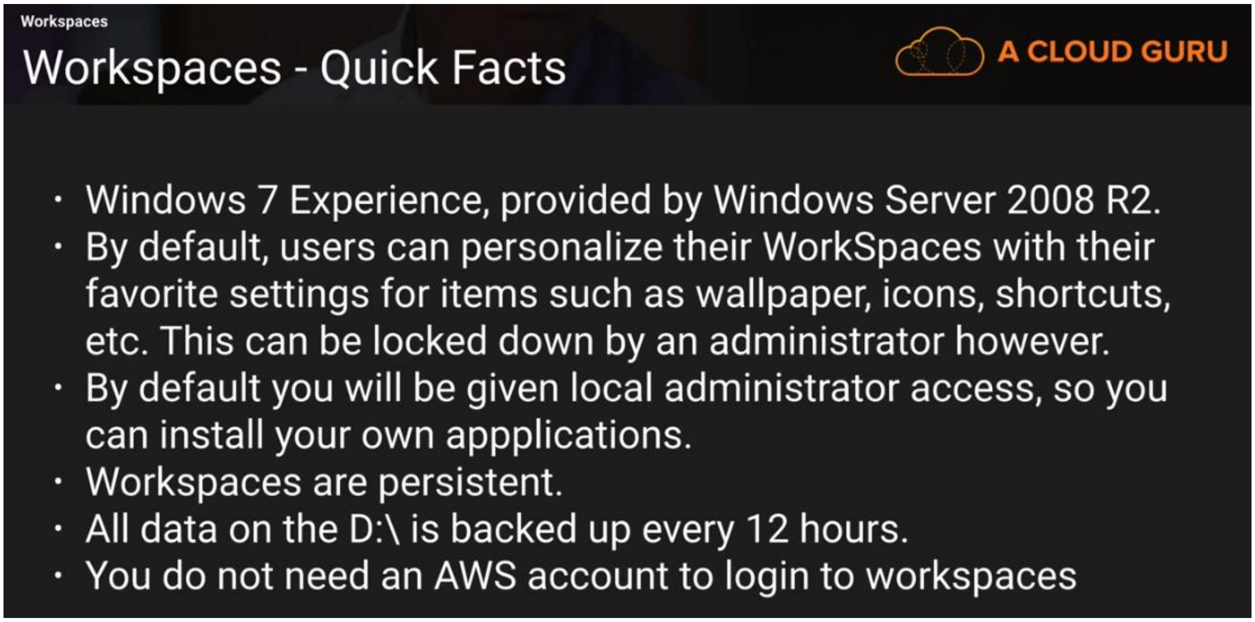
Workspaces 101

What is Workspaces?

A CLOUD GURU

It’s basically VDI. A WorkSpace is a cloud-based replacement for a traditional desktop. A WorkSpace is available as a bundle of compute resources, storage space, and software application access that allow a user to perform day-to-day tasks just like using a traditional desktop. A user can connect to a WorkSpace from any supported device (PC, Mac, Chromebook, iPad, Kindle Fire, or Android tablets) using a free Amazon WorkSpaces client application and credentials set up by an administrator, or their existing Active Directory credentials if Amazon WorkSpaces is integrated with an existing Active Directory domain.

udem

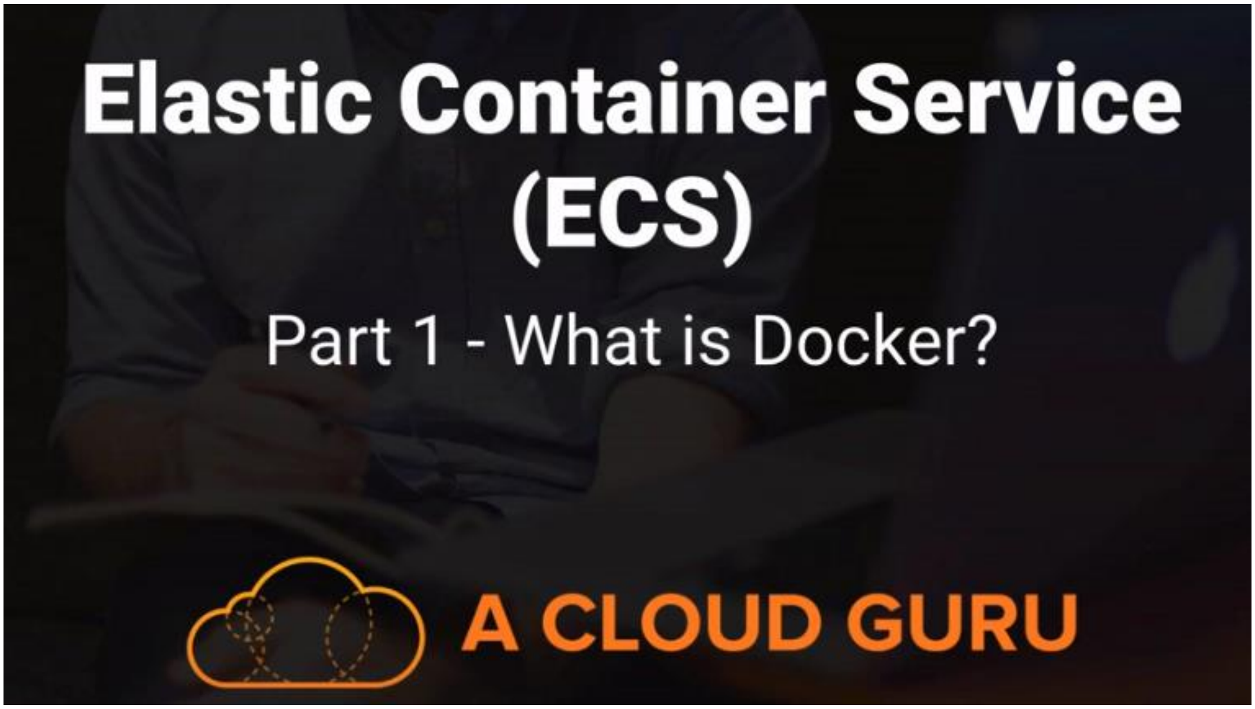


Workspaces

Workspaces - Quick Facts

A CLOUD GURU

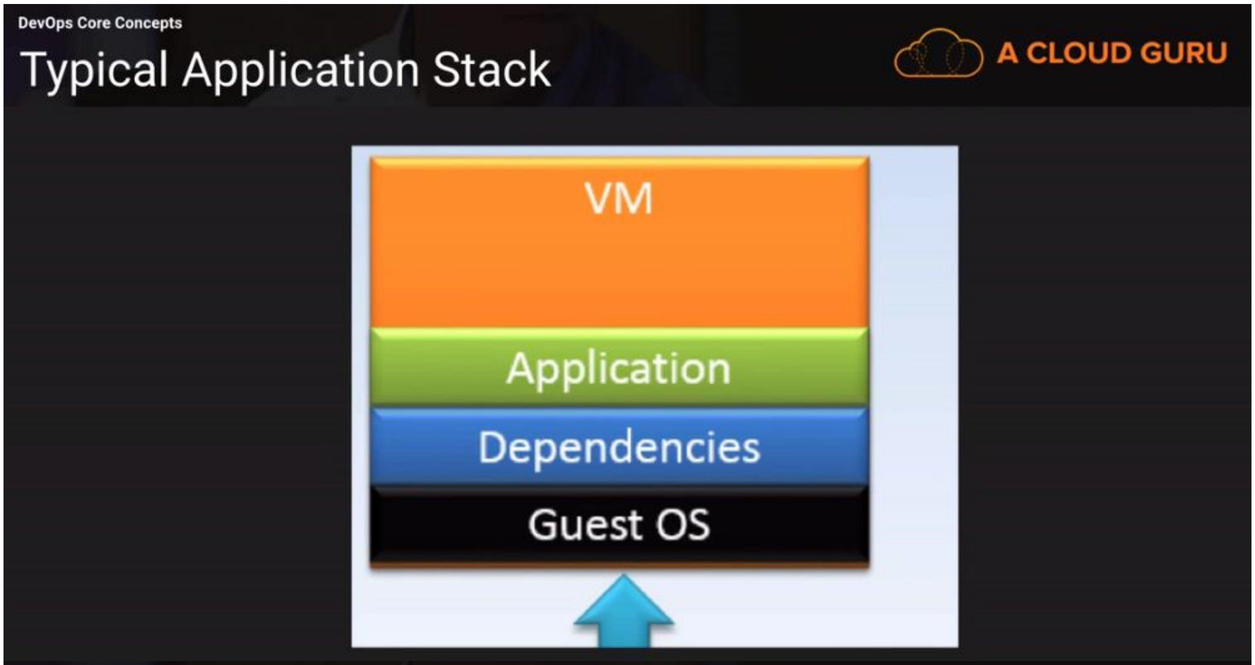
- Windows 7 Experience, provided by Windows Server 2008 R2.
- By default, users can personalize their WorkSpaces with their favorite settings for items such as wallpaper, icons, shortcuts, etc. This can be locked down by an administrator however.
- By default you will be given local administrator access, so you can install your own appplications.
- Workspaces are persistent.
- All data on the D:\ is backed up every 12 hours.
- You do not need an AWS account to login to workspaces



Elastic Container Service (ECS)

Part 1 - What is Docker?

A CLOUD GURU



DevOps Core Concepts

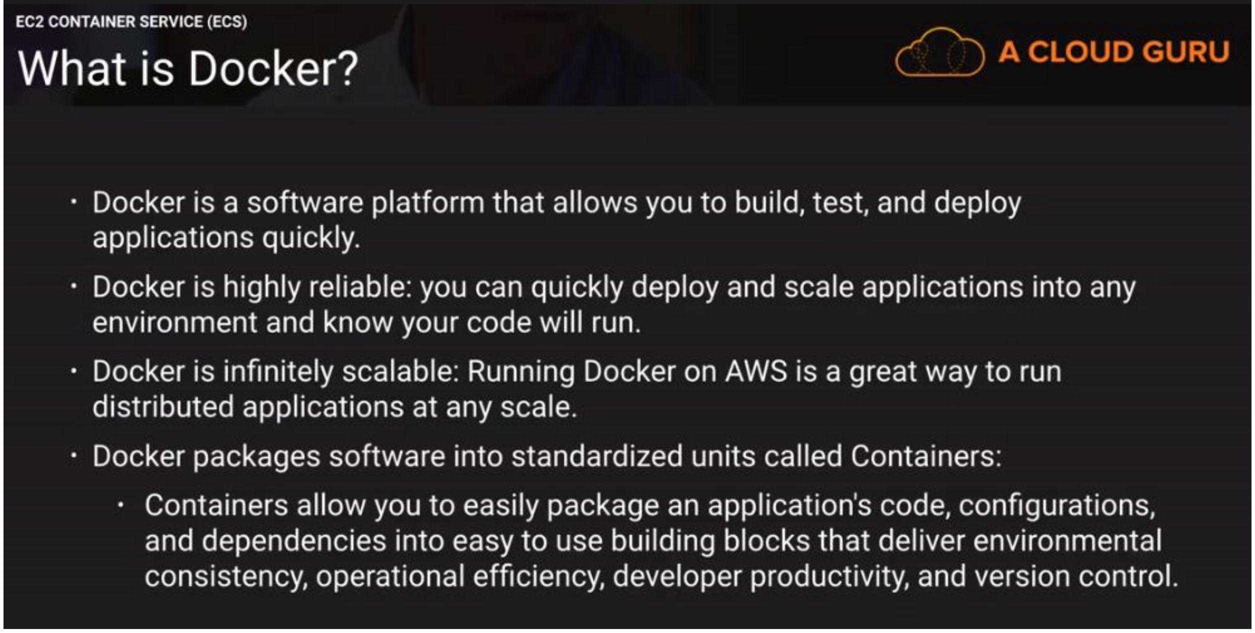
Typical Application Stack

VM

Application

Dependencies

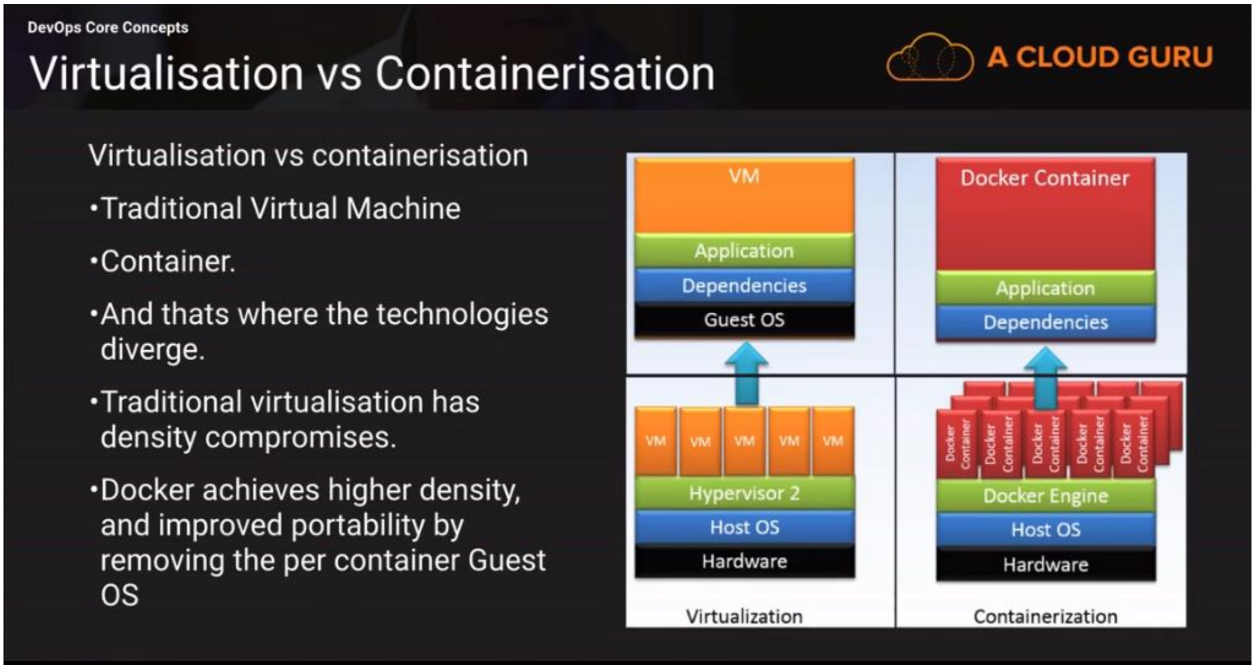
Guest OS



EC2 CONTAINER SERVICE (ECS)

What is Docker?

- Docker is a software platform that allows you to build, test, and deploy applications quickly.
- Docker is highly reliable: you can quickly deploy and scale applications into any environment and know your code will run.
- Docker is infinitely scalable: Running Docker on AWS is a great way to run distributed applications at any scale.
- Docker packages software into standardized units called Containers:
  - Containers allow you to easily package an application's code, configurations, and dependencies into easy to use building blocks that deliver environmental consistency, operational efficiency, developer productivity, and version control.



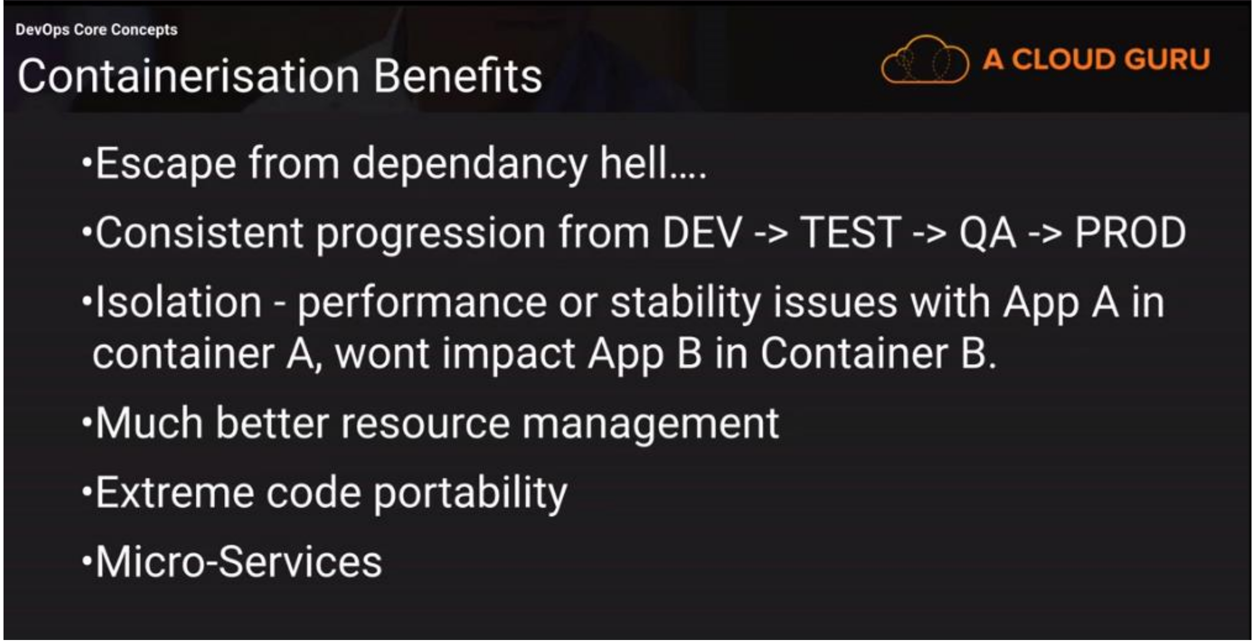
DevOps Core Concepts

Virtualisation vs Containerisation

A CLOUD GURU

Virtualisation vs containerisation

- Traditional Virtual Machine
- Container.
- And thats where the technologies diverge.
- Traditional virtualisation has density compromises.
- Docker achieves higher density, and improved portability by removing the per container Guest OS

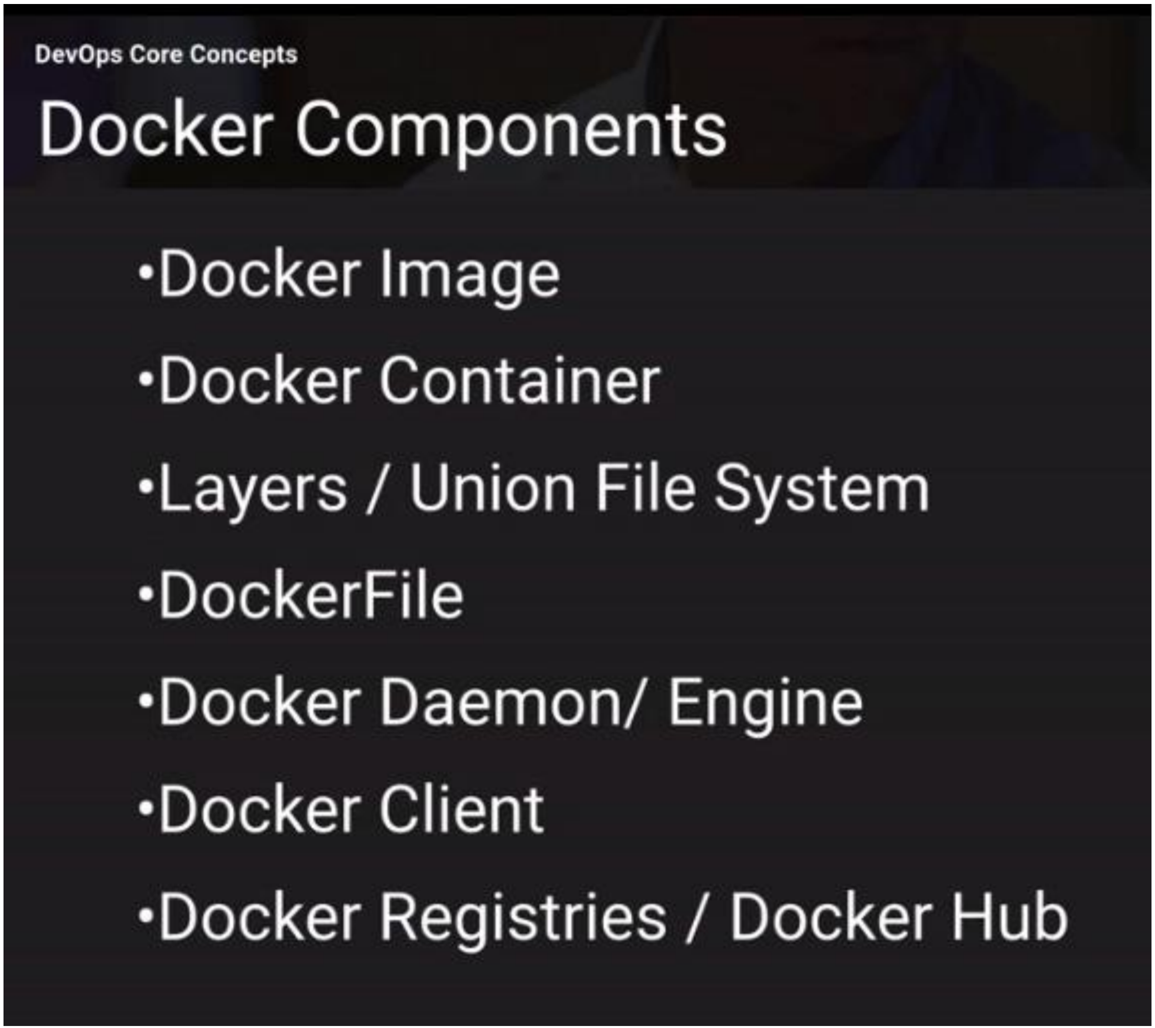


DevOps Core Concepts

Containerisation Benefits

A CLOUD GURU

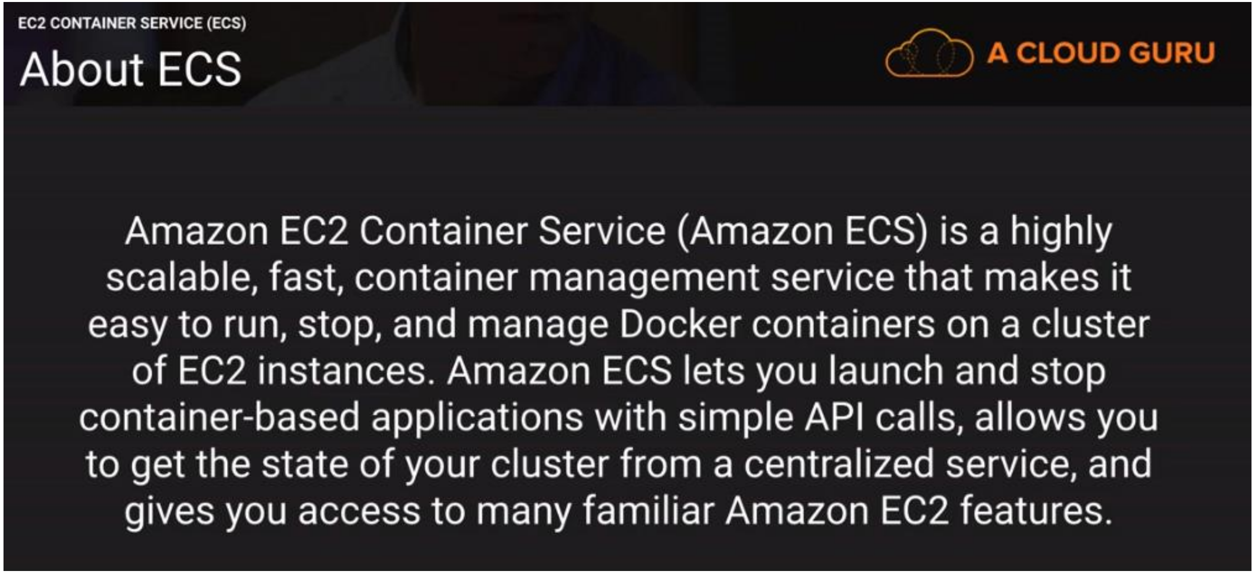
- Escape from dependancy hell....
- Consistent progression from DEV -> TEST -> QA -> PROD
- Isolation - performance or stability issues with App A in container A, wont impact App B in Container B.
- Much better resource management
- Extreme code portability
- Micro-Services



DevOps Core Concepts

Docker Components

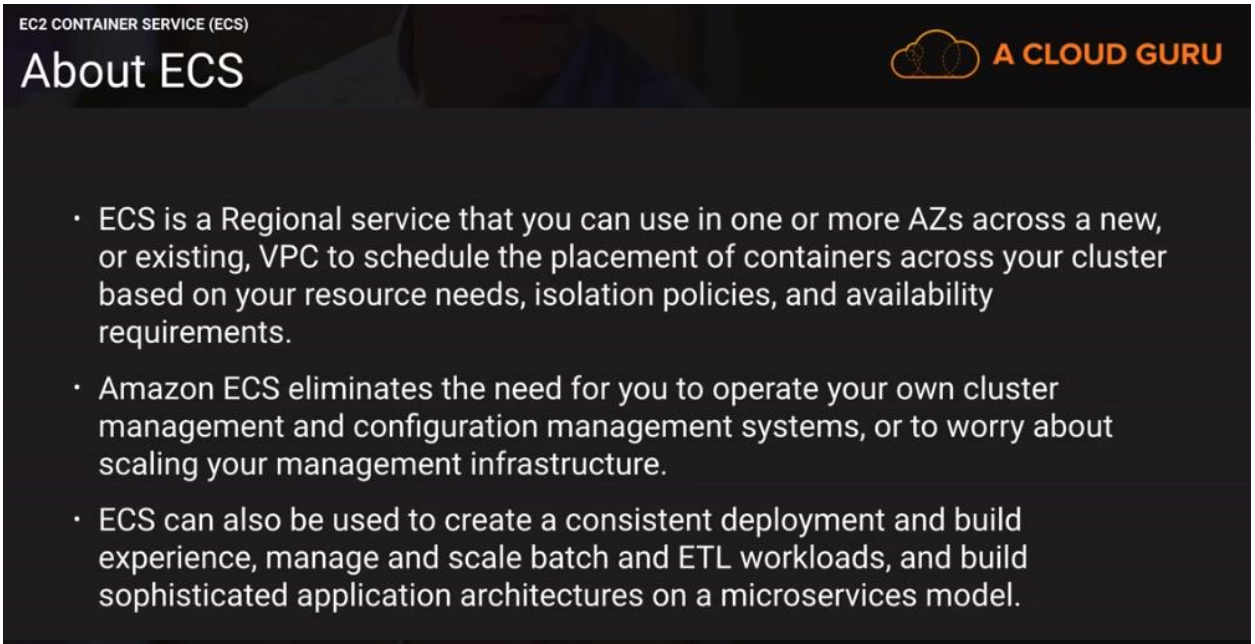
- Docker Image
- Docker Container
- Layers / Union File System
- DockerFile
- Docker Daemon/ Engine
- Docker Client
- Docker Registries / Docker Hub



EC2 CONTAINER SERVICE (ECS)

About ECS

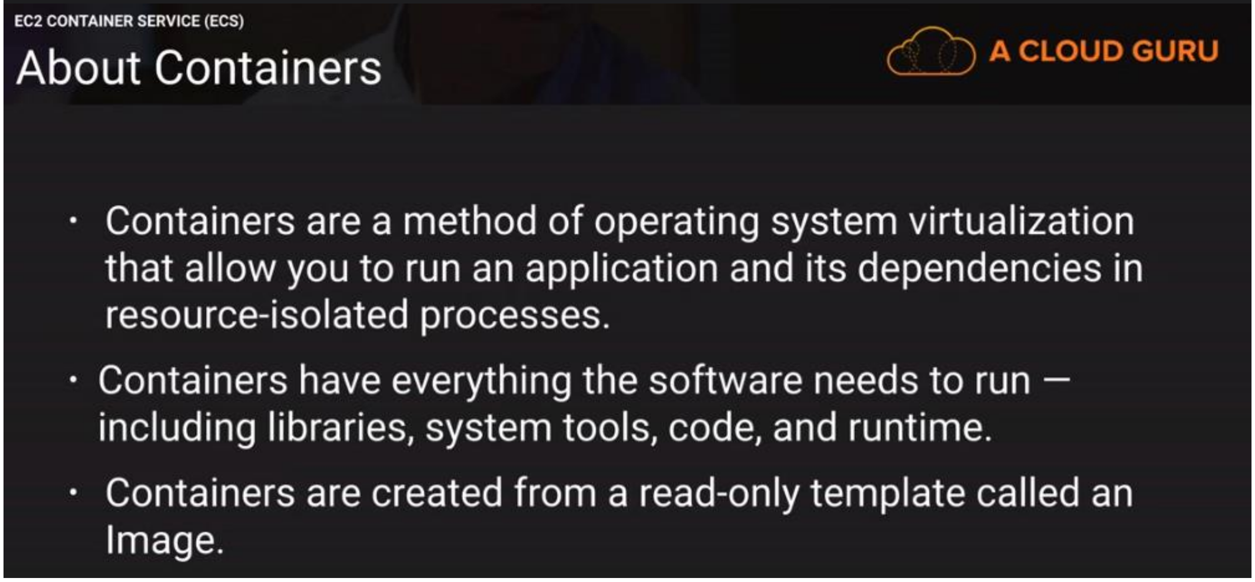
Amazon EC2 Container Service (Amazon ECS) is a highly scalable, fast, container management service that makes it easy to run, stop, and manage Docker containers on a cluster of EC2 instances. Amazon ECS lets you launch and stop container-based applications with simple API calls, allows you to get the state of your cluster from a centralized service, and gives you access to many familiar Amazon EC2 features.



EC2 CONTAINER SERVICE (ECS)

About ECS

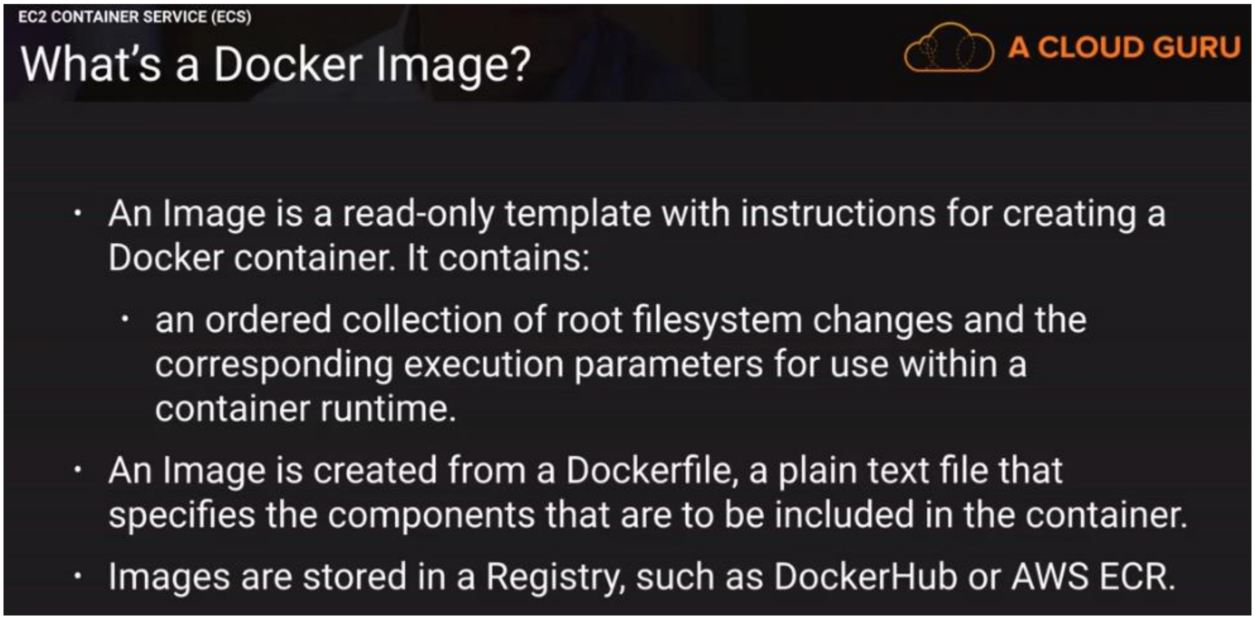
- ECS is a Regional service that you can use in one or more AZs across a new, or existing, VPC to schedule the placement of containers across your cluster based on your resource needs, isolation policies, and availability requirements.
- Amazon ECS eliminates the need for you to operate your own cluster management and configuration management systems, or to worry about scaling your management infrastructure.
- ECS can also be used to create a consistent deployment and build experience, manage and scale batch and ETL workloads, and build sophisticated application architectures on a microservices model.



EC2 CONTAINER SERVICE (ECS)

About Containers

- Containers are a method of operating system virtualization that allow you to run an application and its dependencies in resource-isolated processes.
- Containers have everything the software needs to run — including libraries, system tools, code, and runtime.
- Containers are created from a read-only template called an Image.

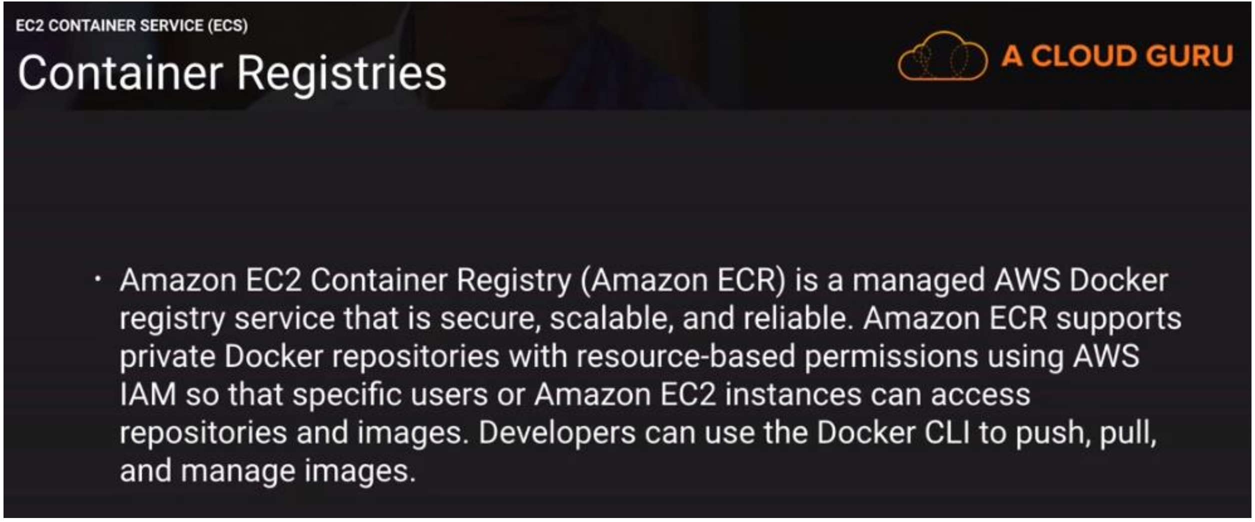


EC2 CONTAINER SERVICE (ECS)

What's a Docker Image?

A CLOUD GURU

- An Image is a read-only template with instructions for creating a Docker container. It contains:
  - an ordered collection of root filesystem changes and the corresponding execution parameters for use within a container runtime.
- An Image is created from a Dockerfile, a plain text file that specifies the components that are to be included in the container.
- Images are stored in a Registry, such as DockerHub or AWS ECR.

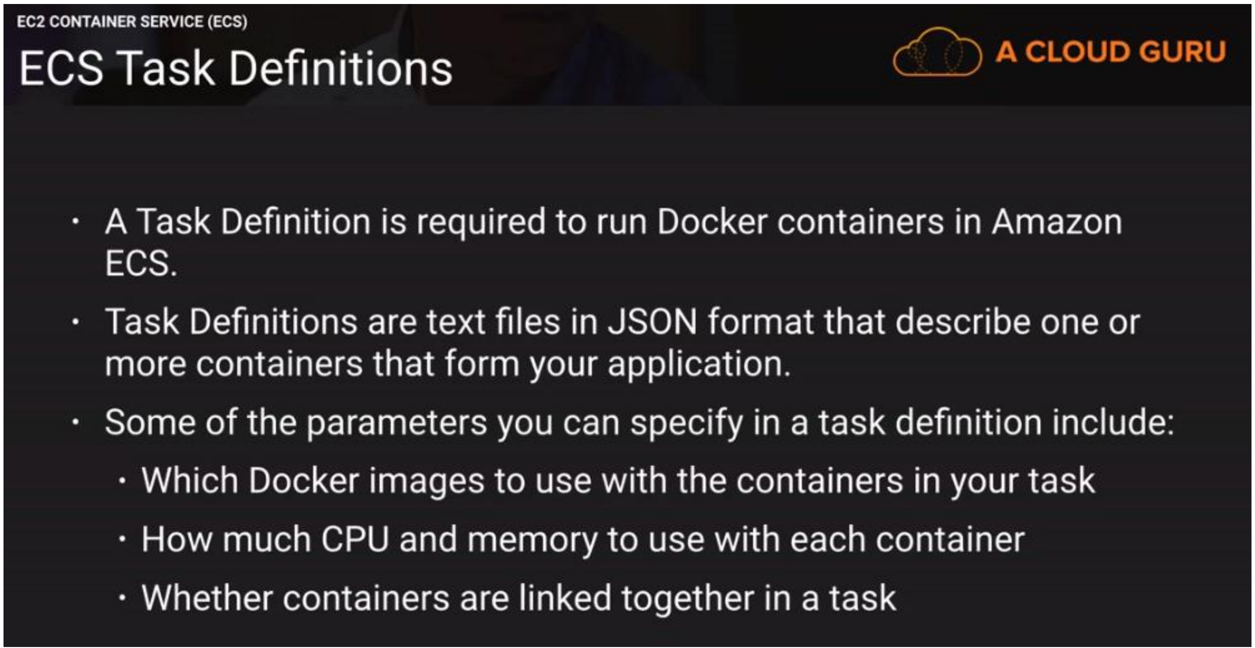


EC2 CONTAINER SERVICE (ECS)

Container Registries

A CLOUD GURU

- Amazon EC2 Container Registry (Amazon ECR) is a managed AWS Docker registry service that is secure, scalable, and reliable. Amazon ECR supports private Docker repositories with resource-based permissions using AWS IAM so that specific users or Amazon EC2 instances can access repositories and images. Developers can use the Docker CLI to push, pull, and manage images.

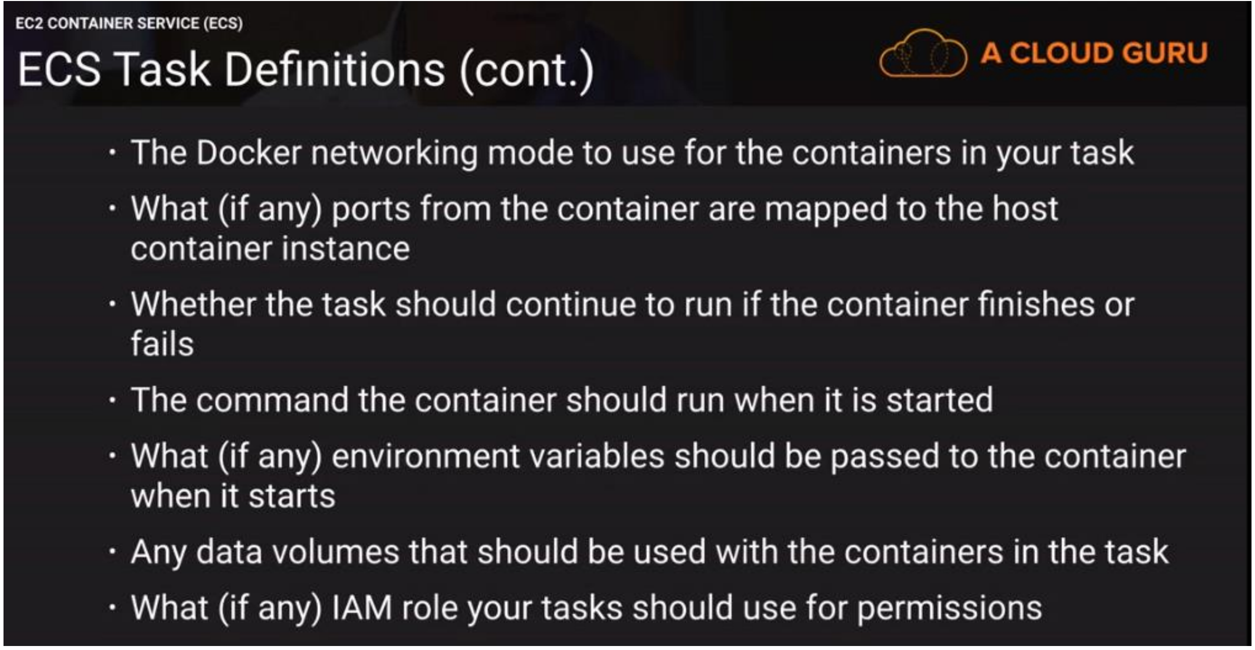


EC2 CONTAINER SERVICE (ECS)

ECS Task Definitions

A CLOUD GURU

- A Task Definition is required to run Docker containers in Amazon ECS.
- Task Definitions are text files in JSON format that describe one or more containers that form your application.
- Some of the parameters you can specify in a task definition include:
  - Which Docker images to use with the containers in your task
  - How much CPU and memory to use with each container
  - Whether containers are linked together in a task

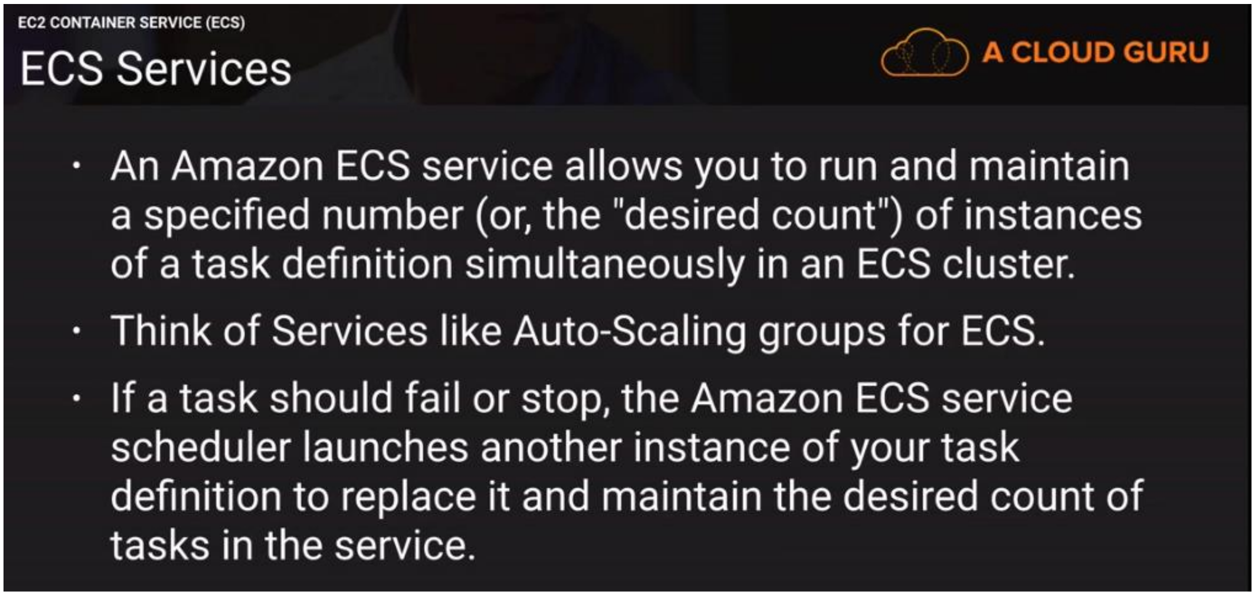


EC2 CONTAINER SERVICE (ECS)

ECS Task Definitions (cont.)

A CLOUD GURU

- The Docker networking mode to use for the containers in your task
- What (if any) ports from the container are mapped to the host container instance
- Whether the task should continue to run if the container finishes or fails
- The command the container should run when it is started
- What (if any) environment variables should be passed to the container when it starts
- Any data volumes that should be used with the containers in the task
- What (if any) IAM role your tasks should use for permissions

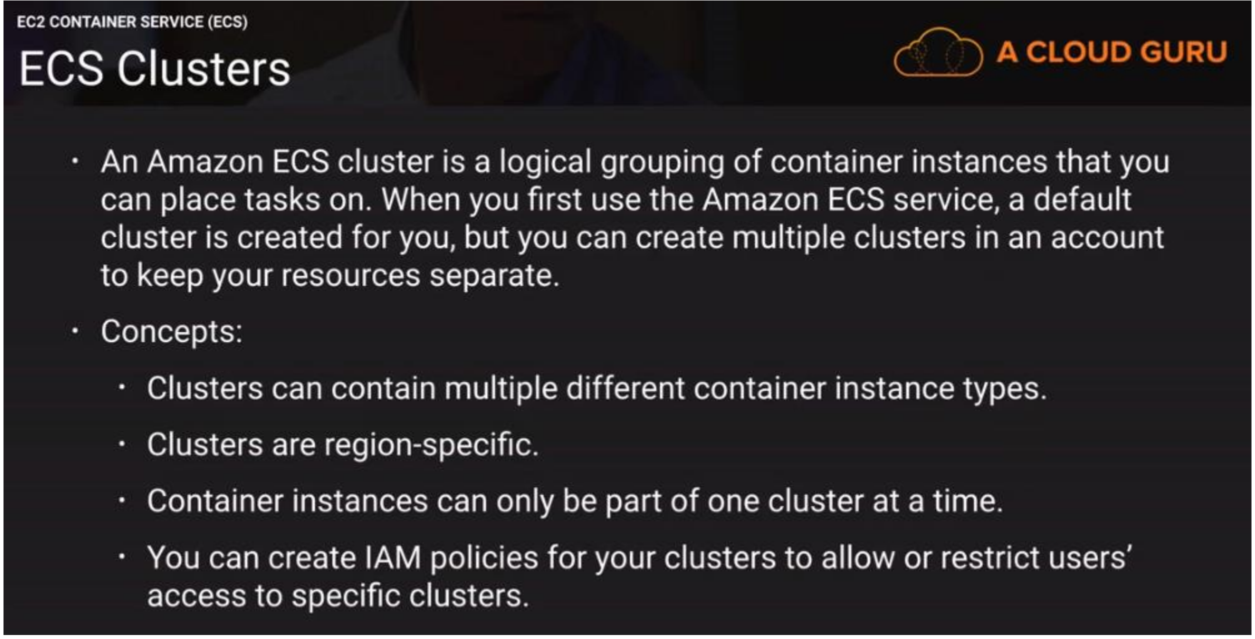


EC2 CONTAINER SERVICE (ECS)

ECS Services

A CLOUD GURU

- An Amazon ECS service allows you to run and maintain a specified number (or, the "desired count") of instances of a task definition simultaneously in an ECS cluster.
- Think of Services like Auto-Scaling groups for ECS.
- If a task should fail or stop, the Amazon ECS service scheduler launches another instance of your task definition to replace it and maintain the desired count of tasks in the service.

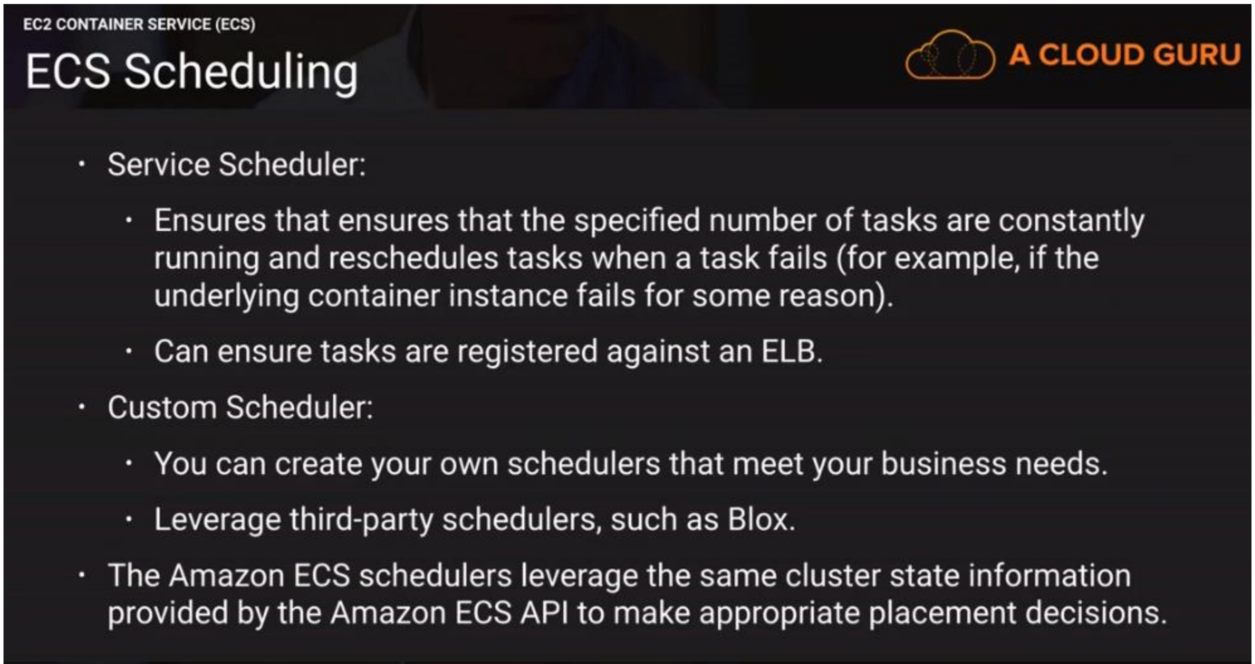


EC2 CONTAINER SERVICE (ECS)

ECS Clusters

A CLOUD GURU

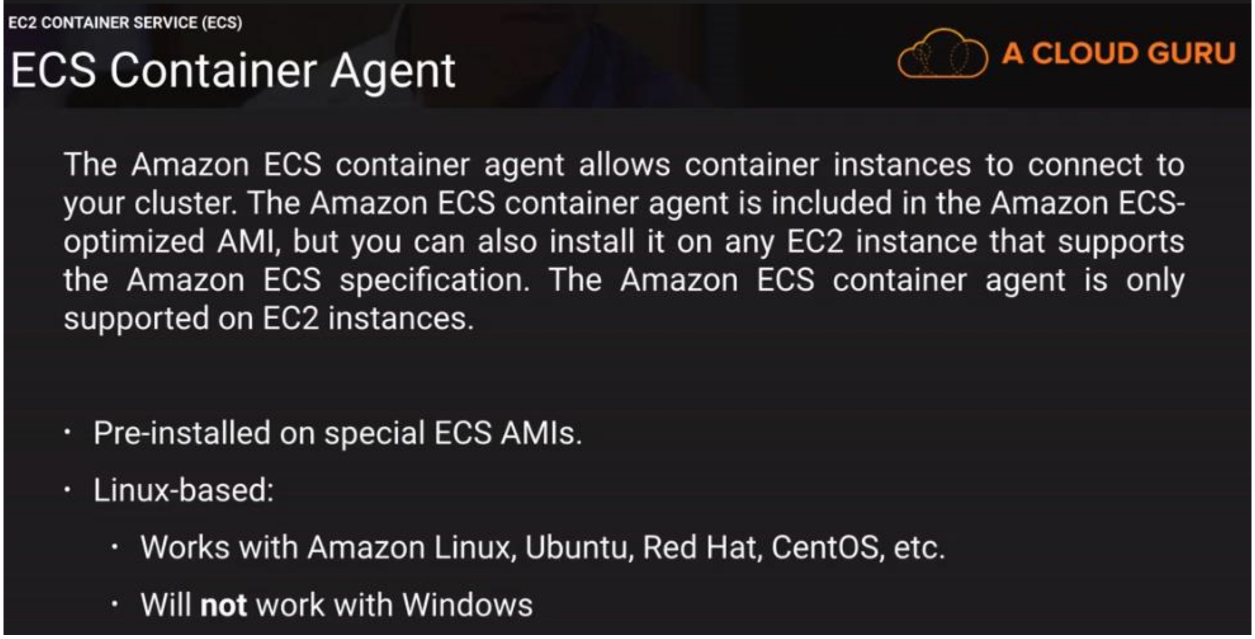
- An Amazon ECS cluster is a logical grouping of container instances that you can place tasks on. When you first use the Amazon ECS service, a default cluster is created for you, but you can create multiple clusters in an account to keep your resources separate.
- Concepts:
  - Clusters can contain multiple different container instance types.
  - Clusters are region-specific.
  - Container instances can only be part of one cluster at a time.
  - You can create IAM policies for your clusters to allow or restrict users' access to specific clusters.



EC2 CONTAINER SERVICE (ECS)

ECS Scheduling

- Service Scheduler:
  - Ensures that ensures that the specified number of tasks are constantly running and reschedules tasks when a task fails (for example, if the underlying container instance fails for some reason).
  - Can ensure tasks are registered against an ELB.
- Custom Scheduler:
  - You can create your own schedulers that meet your business needs.
  - Leverage third-party schedulers, such as Blox.
- The Amazon ECS schedulers leverage the same cluster state information provided by the Amazon ECS API to make appropriate placement decisions.

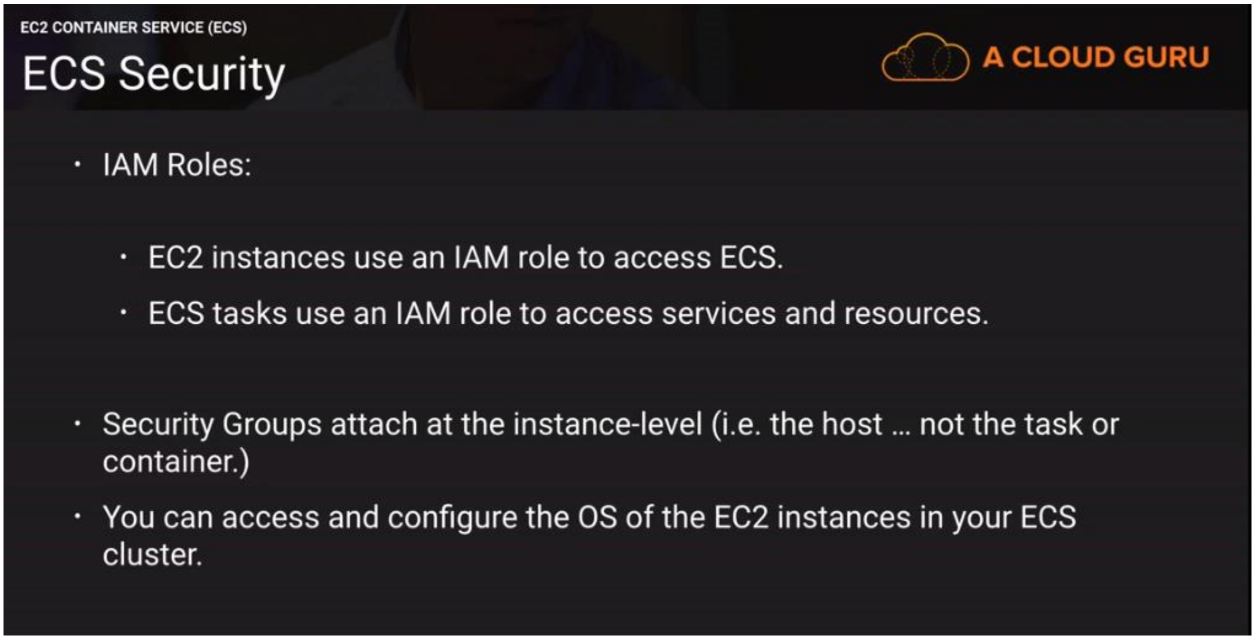


EC2 CONTAINER SERVICE (ECS)

ECS Container Agent

The Amazon ECS container agent allows container instances to connect to your cluster. The Amazon ECS container agent is included in the Amazon ECS-optimized AMI, but you can also install it on any EC2 instance that supports the Amazon ECS specification. The Amazon ECS container agent is only supported on EC2 instances.

- Pre-installed on special ECS AMIs.
- Linux-based:
  - Works with Amazon Linux, Ubuntu, Red Hat, CentOS, etc.
  - Will **not** work with Windows

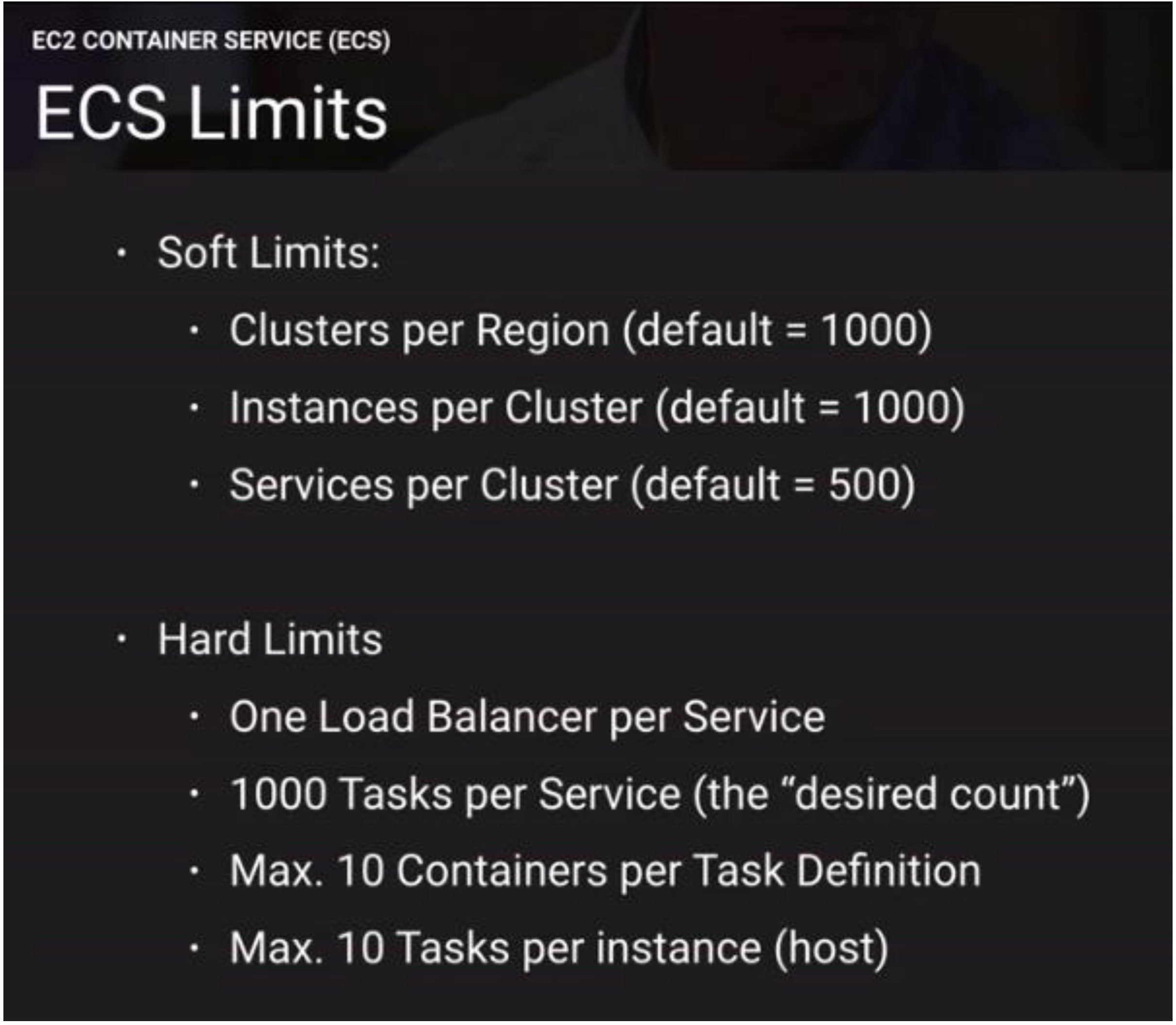


EC2 CONTAINER SERVICE (ECS)

ECS Security

A CLOUD GURU

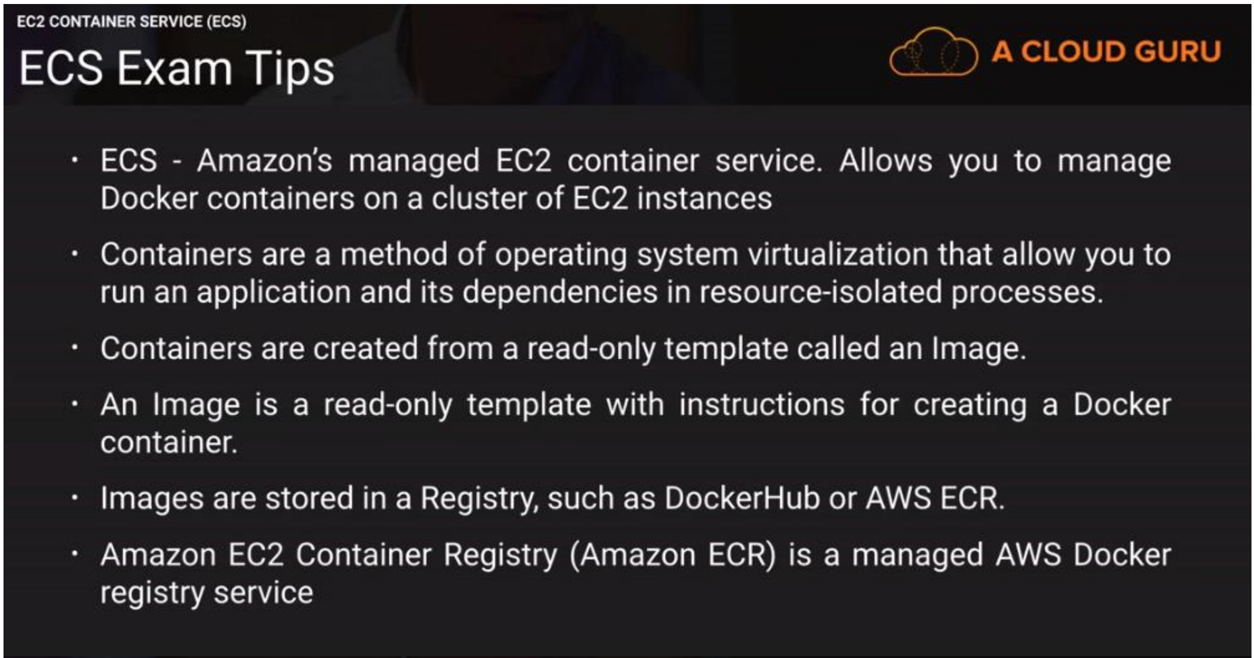
- IAM Roles:
  - EC2 instances use an IAM role to access ECS.
  - ECS tasks use an IAM role to access services and resources.
- Security Groups attach at the instance-level (i.e. the host … not the task or container.)
- You can access and configure the OS of the EC2 instances in your ECS cluster.



EC2 CONTAINER SERVICE (ECS)

ECS Limits

- Soft Limits:
  - Clusters per Region (default = 1000)
  - Instances per Cluster (default = 1000)
  - Services per Cluster (default = 500)
- Hard Limits
  - One Load Balancer per Service
  - 1000 Tasks per Service (the “desired count”)
  - Max. 10 Containers per Task Definition
  - Max. 10 Tasks per instance (host)

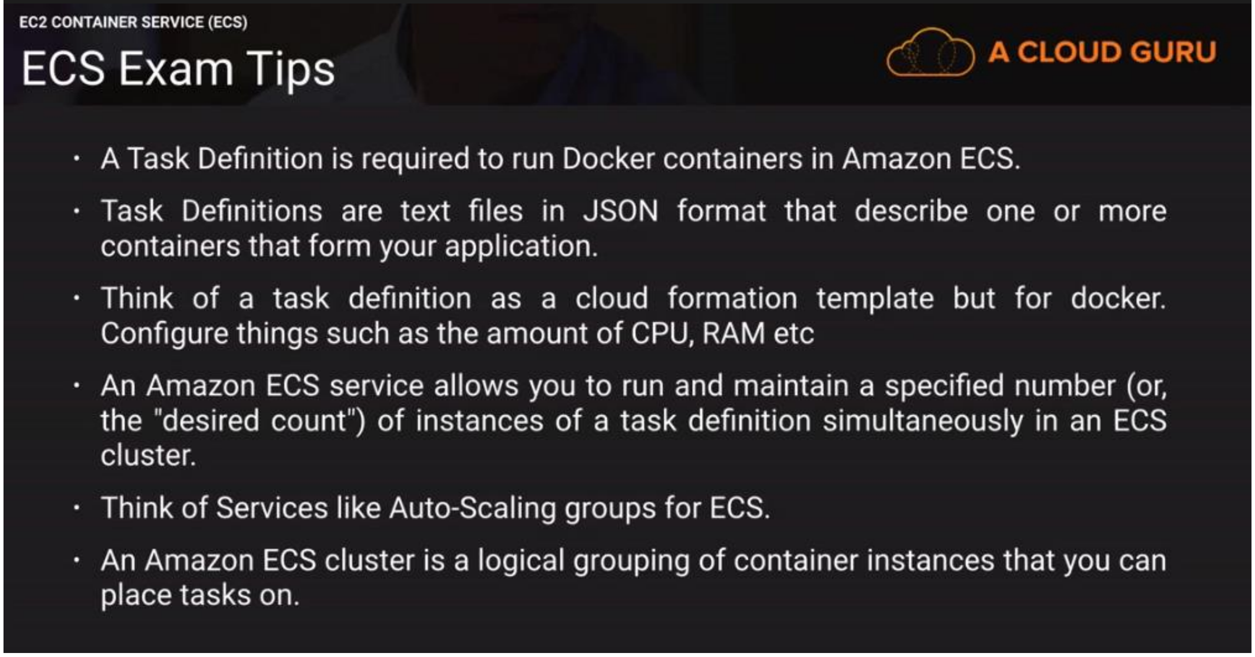


EC2 CONTAINER SERVICE (ECS)

ECS Exam Tips

A CLOUD GURU

- ECS - Amazon's managed EC2 container service. Allows you to manage Docker containers on a cluster of EC2 instances
- Containers are a method of operating system virtualization that allow you to run an application and its dependencies in resource-isolated processes.
- Containers are created from a read-only template called an Image.
- An Image is a read-only template with instructions for creating a Docker container.
- Images are stored in a Registry, such as DockerHub or AWS ECR.
- Amazon EC2 Container Registry (Amazon ECR) is a managed AWS Docker registry service

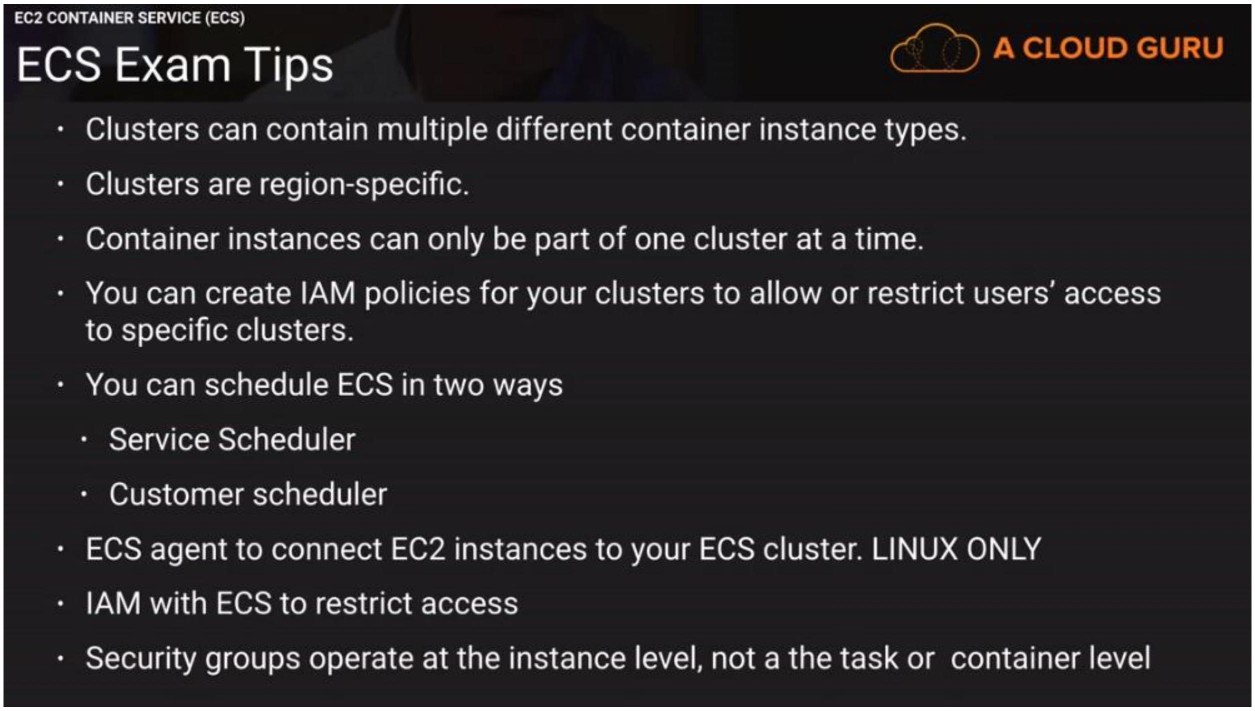


EC2 CONTAINER SERVICE (ECS)

ECS Exam Tips

A CLOUD GURU

- A Task Definition is required to run Docker containers in Amazon ECS.
- Task Definitions are text files in JSON format that describe one or more containers that form your application.
- Think of a task definition as a cloud formation template but for docker. Configure things such as the amount of CPU, RAM etc
- An Amazon ECS service allows you to run and maintain a specified number (or, the "desired count") of instances of a task definition simultaneously in an ECS cluster.
- Think of Services like Auto-Scaling groups for ECS.
- An Amazon ECS cluster is a logical grouping of container instances that you can place tasks on.



EC2 CONTAINER SERVICE (ECS)

ECS Exam Tips

A CLOUD GURU

- Clusters can contain multiple different container instance types.
- Clusters are region-specific.
- Container instances can only be part of one cluster at a time.
- You can create IAM policies for your clusters to allow or restrict users' access to specific clusters.
- You can schedule ECS in two ways
  - Service Scheduler
  - Customer scheduler
- ECS agent to connect EC2 instances to your ECS cluster. LINUX ONLY
- IAM with ECS to restrict access
- Security groups operate at the instance level, not a the task or container level