

Welcome to Week 1

Cloud Accelerator Program

CloudFormation, IAM, and AWS SAM

 **Develop**Intelligence

A PLURALSIGHT COMPANY

Hello

HELLO
my name is

Allen Sanders
with DevelopIntelligence,
a Pluralsight Company.

About me...



- 26+ years in the industry
- 21+ years in teaching
- Certified Cloud architect
- Passionate about learning
- Also, passionate about Reese's Cups!



Why study these subjects?

In modern software engineering, our ability to quickly deploy incremental innovation, ensure its quality, and scale to meet customer demand proves critical to our success

- Cloud is everywhere and it's not going away
- As with many topics in technology, there are multiple options and multiple dimensions to those options
- Building a deeper understanding of Cloud and its offerings helps prepare you for modern IT
- Included in that is the importance of learning about key foundational concepts like Infrastructure-as-Code (IaC) and Identity & Access Management (IAM)



My pledge to you

I will...

- Make this interactive
- Ask you questions
- Ensure everyone can speak
- Use an on-screen timer



Agenda

- Speaking the language of Cloud
- CloudFormation – one of the Infrastructure-as-Code (IaC) options in AWS
- Identity & Access Management (IAM) – key to securing workloads in AWS
- The AWS SAM (Serverless Application Model) – one of the newer serverless offerings available in AWS



How we're going to work together

- Slides and words to highlight key concepts
- Demos to bring those concepts “to life”
- Lab work (which will take place in sandboxes provided by “A Cloud Guru”) for hands-on reinforcement
- NOTE: I welcome being interrupted – if you need more info, or clarification, or anything else, just break in and ask. I am here to help you.

Open Discussion

What is “the Cloud”?

How does “the Cloud” factor into modern IT?



Speaking the Language of Cloud

Infrastructure Options

Infrastructure Options



Infrastructure is the hardware & software that run our IT workloads and that provide our business users and customers a way to interface with the applications required to complete their daily jobs

What Are the Options?



On-Premise (in a Data Center)



Public Cloud



At the Edge



Hybrid Cloud

What do they all mean?

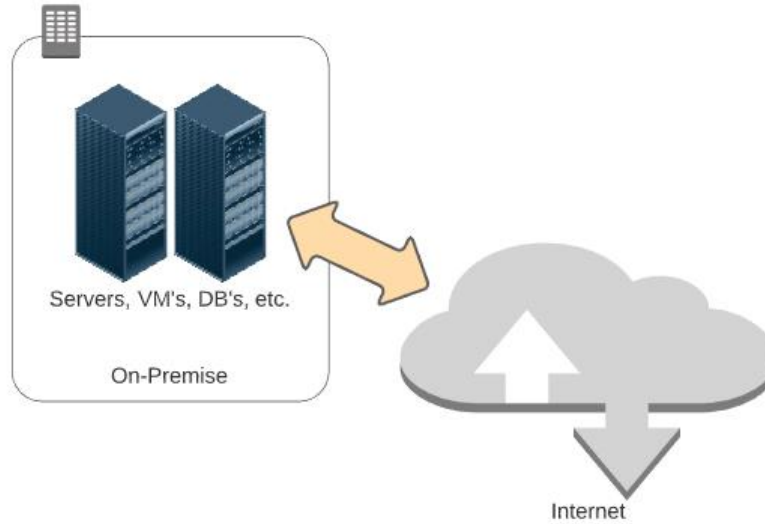
On-Premise

Can mean a few different things:

- In a wholly-owned Data Center
- In a COLO (or co-location Data Center)
- Sometimes called a “private cloud”



On-Premise



On-Premise



Why and What?

- How infrastructure has traditionally been done
- With this model, companies try and estimate current & future hardware capacity needed to support business operations



On-Premise

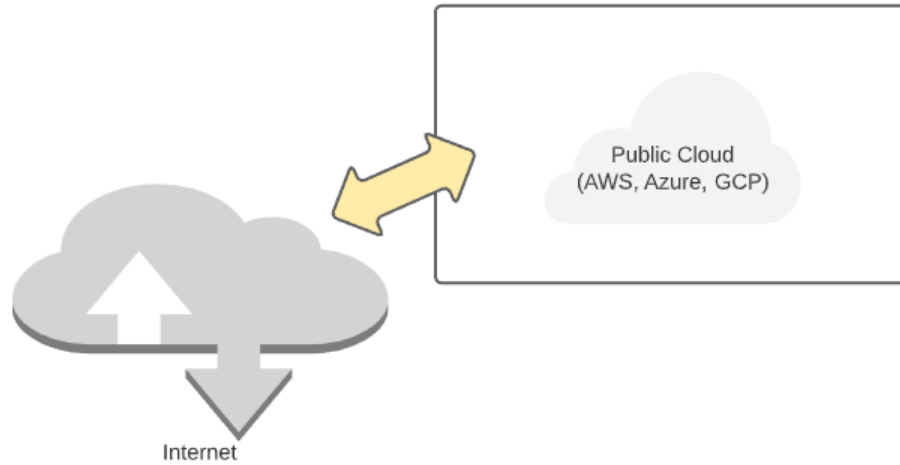


Why and What?

- Stakeholders plan out expected levels of consumption for the next 3 – 5 years (capacity to handle current volumes as well as expected growth)
- Some critical workloads may not be suitable for anything but a physical and directly-managed implementation (e.g., mainframe)



Public Cloud



Public Cloud



Why and What?

- Platform using the standard “Cloud computing model” to provide infrastructure and application services
- Accessed and integrated via the Internet
- May provide a few different types of services – IaaS, PaaS, etc.



Public Cloud

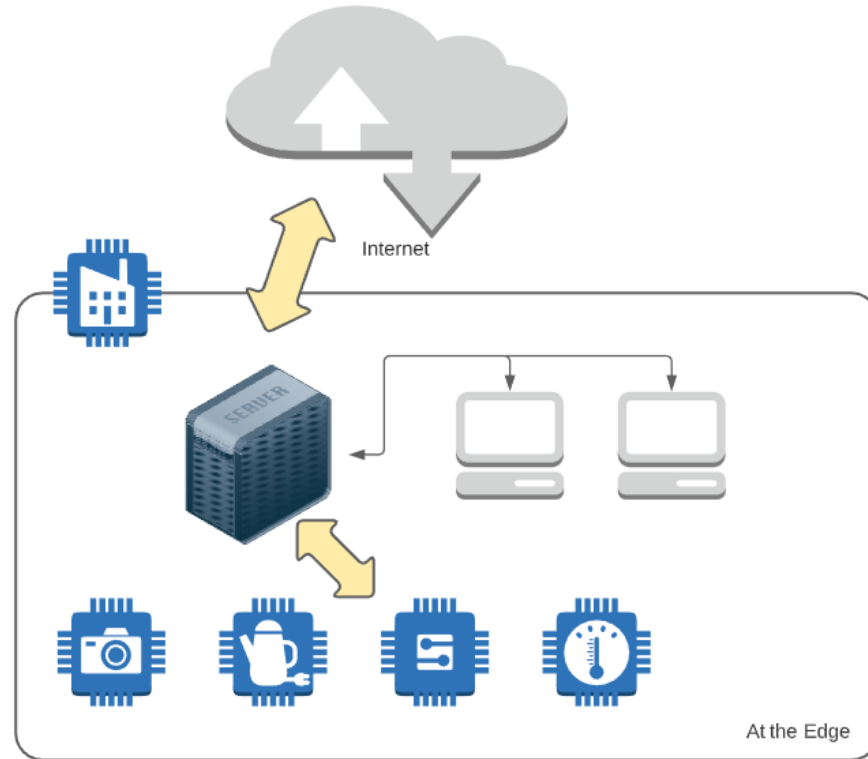


Why and What?

- Usually supports a subscription or “pay as you go” (on-demand) pricing model
- Largest players in this space include Azure, AWS and GCP



At the Edge



At the Edge

Can include 3 distinct layers:



Inner or Near Edge

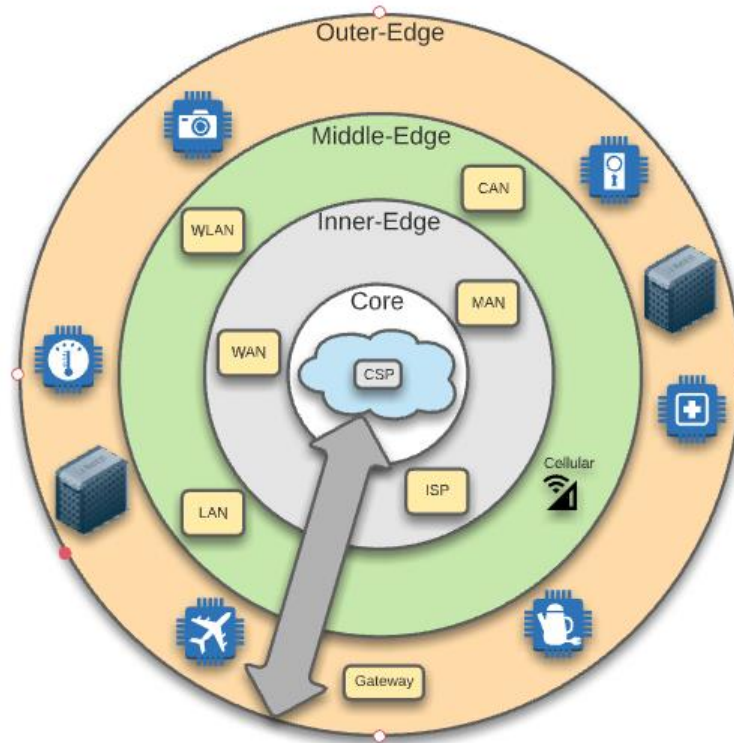


Middle Edge



Outer or Far Edge

At the Edge – Layers



CSP – Cloud Service Provider
WAN – Wide Area Network
ISP – Internet Service Provider
MAN – Metropolitan Area Network
LAN – Local Area Network
WLAN – Wireless Local Area Network
CAN – Campus Area Network

At the Edge



Why and What?

- It's about bringing the power of Cloud computing to you
- Enables additional processing closer to the sources of data while still supporting the offload of higher order processing to the Cloud
- Often involves setting up “Cloud-in-a-box” facilities on-premise



At the Edge



Why and What?

- IoT (Internet of Things) is a good example – devices in a facility reading massive amounts of data can incorporate processing at the edge to improve overall efficiency
- Helps inject lower latency, increased security and improved bandwidth into systems used to aggregate critical data for an enterprise



Hybrid Cloud



Why and What?

- In many ways, an amalgamation of the other options
- Supports distribution of system processing across on-premise infrastructure and the public Cloud



Hybrid Cloud

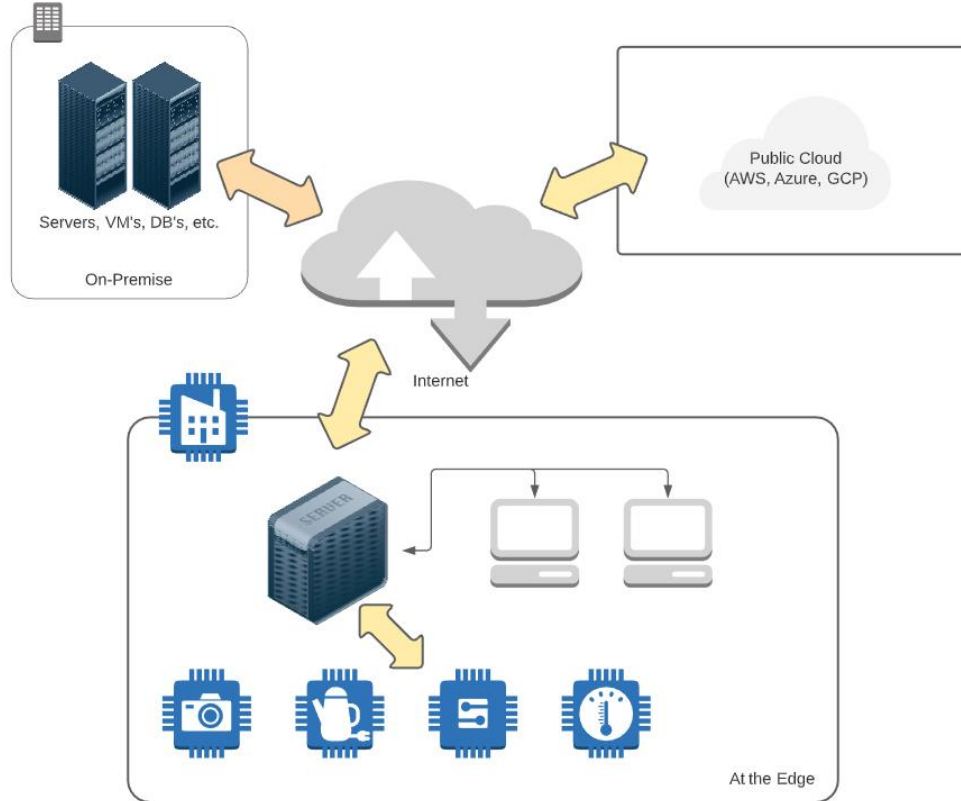


Why and What?

- Allows an enterprise to keep workloads that are best-suited for on-premise running on-premise while allowing migration of components that can move to the public Cloud
- Can help make an enterprise's move to the Cloud more gradual and planful



Hybrid Cloud



Application Hosting



Application Hosting

By Application Hosting, we mean the target infrastructure and runtime platform used for deployment and execution of an application or system; can include compute (CPU and server resources), storage, network, data and operating system



Application Hosting – An “Interesting” Example?

Here’s an example of someone thinking “outside-of-the-box” when it comes to application hosting!

<https://mashable.com/article/pregnancy-test-doom/>

What Are the Hosting Options with Cloud?

- ☐ IaaS
- ☐ PaaS
- ☐ Serverless / FaaS
- ☐ SaaS
- ☐ Containers



What do they all mean?



Infrastructure-as-a-Service (IaaS)

- Involves the building out (and management) of virtual instances of:
 - Compute
 - Network
 - Storage
- Akin to spinning up a server (physical or virtual) in your location or data center complete with disks and required network connectivity





Infrastructure-as-a-Service (IaaS)

- The difference is in the where – instead of in your data center, it is created in a data center managed by one of the public Cloud providers
- Your organization is responsible for patching the OS, ensuring all appropriate security updates are applied and that the right controls are in place to govern interaction between this set of components and other infrastructure





Platform-as-a-Service (PaaS)

- Involves leveraging managed services from a public Cloud provider
- With this model, an enterprise can focus on management of their application and data vs. focusing on management of the underlying infrastructure
- Patching and security of the infrastructure used to back the managed services falls to the CSP (Cloud Service Provider)





Platform-as-a-Service (PaaS)

- Many managed services support automatic scale up or down depending on demand to help ensure sufficient capacity is in place
- Can be considered synonymous with the term “Cloud native”





Serverless / Functions-as-a-Service (FaaS)

- Also represents a type of managed service provided by the CSP
- Cost structure is usually consumption-based (i.e., you only pay for what you use)
- Supports many different coding paradigms (C#/.NET, NodeJS, Python, etc.)





Serverless / Functions-as-a-Service (FaaS)

- Typically, with Serverless (and PaaS), the consumer is only concerned with the application code and data – elements of the CSP’s “backbone” used to support are managed by the CSP
- Includes more sophisticated automated scaling capabilities – built for Internet scale





Software-as-a-Service (SaaS)

- Subscription-based application services
- Licensed for utilization over the Internet / online rather than for download and install on a server or client machine
- Fully-hosted and fully-managed by a 3rd party

```
position:absolute;z-index:999;top:
width:0 1px 5px #ccc}.gbtl .gbm{-moz-b
color:#ccc;display:block;position:absol
line=1)*opacity:1;*top:-2px;*left:-5px;
opacity:1/0;top:-4px\0;left:-6px\0;rig
-moz-inline-box;display:inline-block;fo
e .gbm{display:block;list-style:none;
play:inline-block;line-height:27px;padd
q(cursor:pointer;display:block;text-de
ation:relative;z-index:1000).gbts(*disp
ad).gbts{padding-right:9px)#gbz .gbst
background:url(//
```



Software-as-a-Service (SaaS)

- Of those discussed, often the cheapest option for service consumers
- However, also offers minimal (or no) control, outside of exposed configuration capabilities

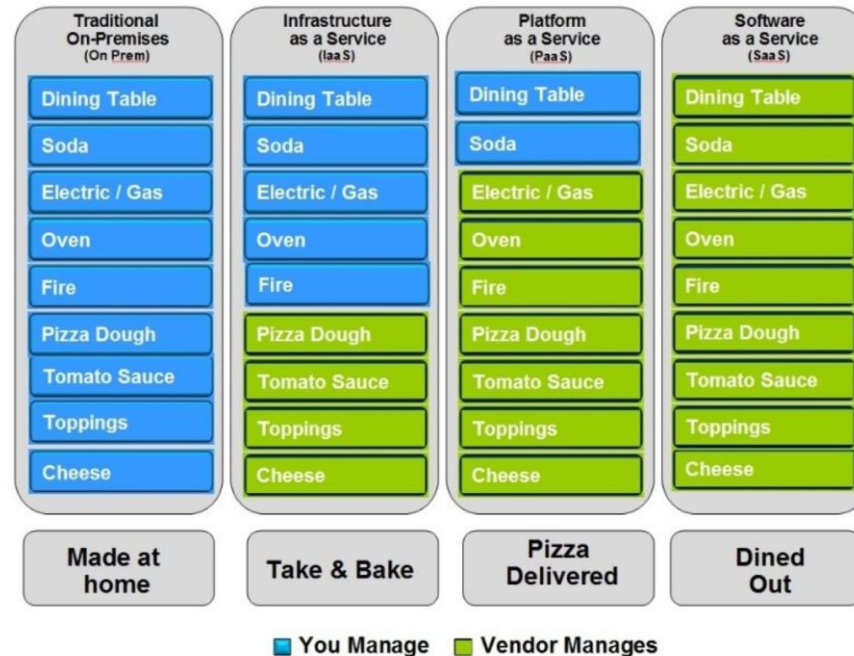
```
position:absolute;z-index:999;top:
width:0px 5px #ccc}.gbtl .gbm{-moz-be
color:#ccc;display:block;position:absol
line=1)*opacity:1;*top:-2px;*left:-5px;
opacity:1/0;top:-4px\0;left:-6px\0;rig
-moz-inline-box;display:inline-block;fo
e. gbm(display:block;list-style:none;
play:inline-block;line-height:27px;padd
q(cursor:pointer;display:block;text-de
ation:relative;z-index:1000).gbts(*disp
ad).gbts(padding-right:9px)#gbz .gbst
background:url(//
```

Pizza-as-a-Service

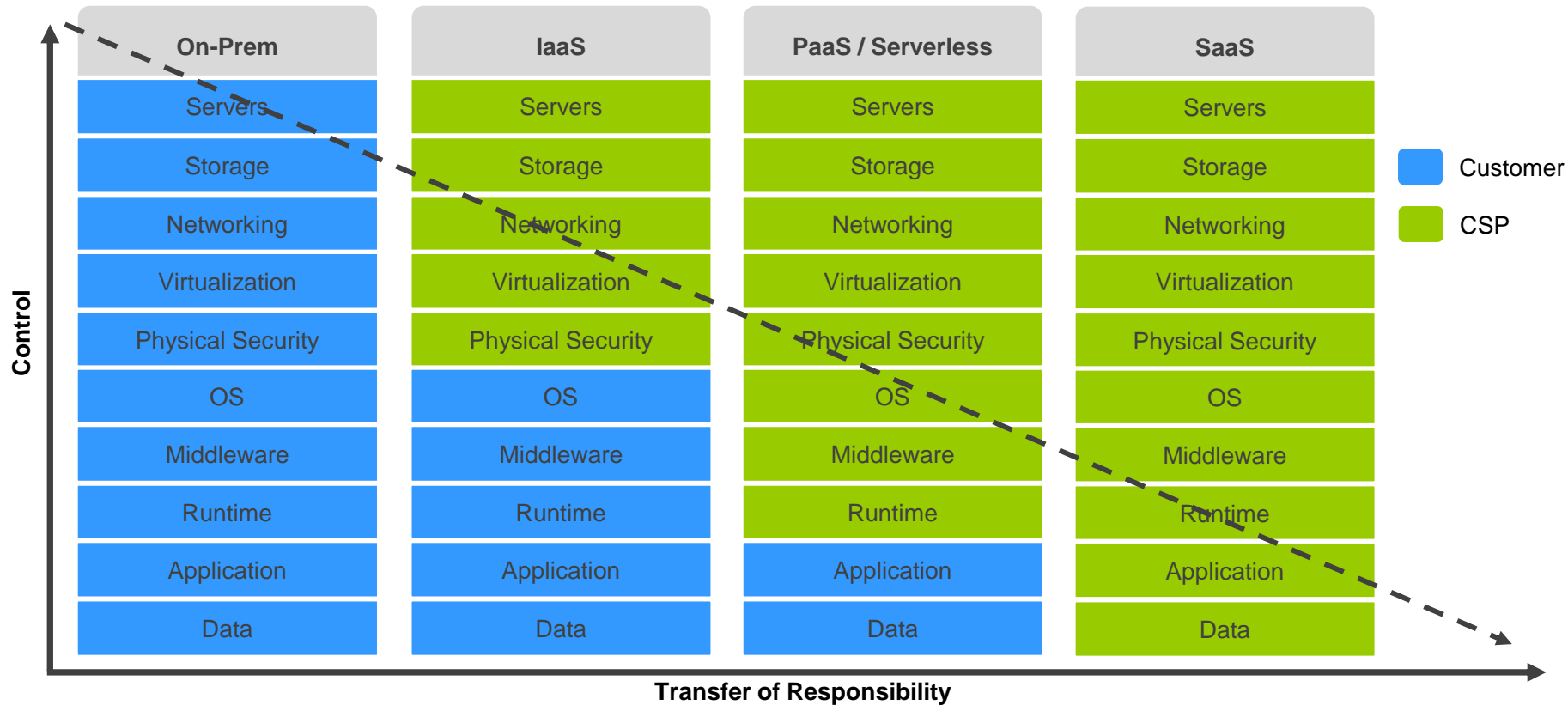
From a LinkedIn post by Albert Barron from IBM (<https://www.linkedin.com/pulse/20140730172610-9679881-pizza-as-a-service/>)



Pizza as a Service



Side-by-Side Comparison



Containerization in the Cloud

- One option includes standing up VM's (IaaS) and installing / managing a Kubernetes cluster on those machines or
- Another option includes leveraging a managed service (PaaS) provided by the CSP
- Options in AWS include Elastic Container Service (ECS), Elastic Container Registry (ECR), and EKS (Elastic Kubernetes Service)



Which One is Better?

- The answer is “it depends”
- It depends on the type of application
- It depends on the enterprise



Which One is Better?



- It depends on the skillset and expertise within the organization
- It depends on whether you have budget and opportunity to modernize an application environment (in some cases)
- The best option might be a combination of multiple approaches – right tool for the right job



Group Discussion:

Cloud Options

Scenario: Your company uses a sophisticated system for global scheduling of flights and flight reservations. The infrastructure used to power this critical system is currently hosted in an on-premise Data Center. This includes a mainframe for primary business functions (customer management, flight management, staff management, account management, etc.), several Web Apps (for customer and staff interaction), several Web APIs providing backend data and functionality to the UIs, and a system used to manage data feeds from several IoT devices present in the aircraft for reporting on equipment status.

As a member of the technical staff, you have been asked to provide thoughts and recommendations on moving from the Data Center to the Cloud.

In your assigned breakout room, discuss as a group and be prepared to provide the following: 1) Potential options for infrastructure in the Cloud for the different types of workload, 2) potential options for hosting of each component type, and 3) considerations that the company should keep in mind as they make the move to ensure awareness and proactive planning.

Nominate someone (or volunteer) to share your group's ideas.

Cloud Service Options in AWS

Cloud Native Services



Benefits

**Readily
Available**

**Relatively
Easy to
Configure**

**Cloud
Scale**

The  offers much in the way of capability and services

Cloud Native Services



Sophisticated services that bring business value



Enable expansion of the services ecosystem of your enterprise into new areas of differentiation and segmentation



Key thing to remember – just because a service is available does not mean that you must use it (or even should use it)




There should be an architectural vision in place for leverage of the Cloud that is directly aligned with business value

Cloud Native Services



Why? Because Cloud services will have  associated

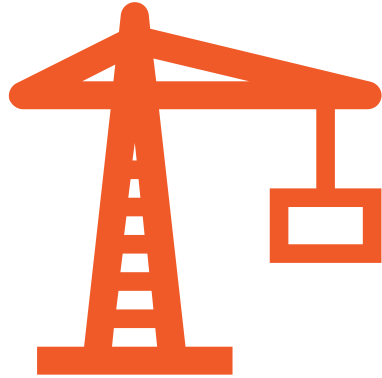


The  must be accounted for and justified as operating expense against business drivers



With good alignment and a good plan, sophisticated Cloud services can help accelerate business mission

Developing for Cloud



Compute



Storage



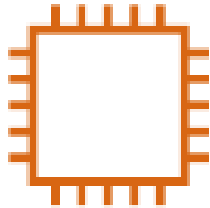
Networking



Database

Compute in AWS

Includes



EC2



AWS Lambda



Elastic Beanstalk

Storage in AWS

Includes



Simple
Storage
Service
(S3)



Elastic Block
Store (EBS)



AWS Snowball

Networking in AWS

Includes



Virtual Private
Cloud
(VPC)/Subnets



API Gateway



Route 53

Database in AWS

Includes



Relational
Database
Service (RDS)



DynamoDB



Aurora

Other in AWS

- Analytics
- Application Integration
- AR & VR
- AWS Cost Management
- Blockchain
- Business Applications
- Compute
- Containers
- Customer Enablement
- Database
- Developer Tools
- End User Computing
- Front-end Web & Mobile
- Game Development
- Internet of Things
- Machine Learning
- Management & Governance
- Media Services
- Migration & Transfer
- Networking & Content Delivery
- Quantum Technologies
- Robotics
- Satellite
- Security, Identity, & Compliance
- Storage



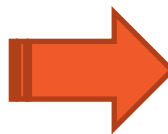
CloudFormation

Infrastructure-as-Code (IaC)



IaC – What is it?

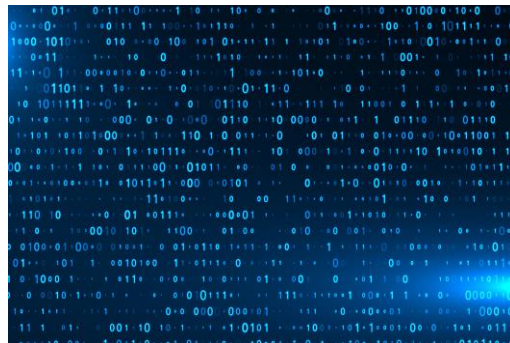
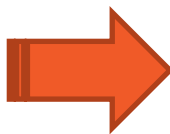
- As the name implies, the definition & configuration of our infrastructure IN code
- Instead of manually creating (inefficient) → automated in scripts that run “at the push of a button”





IaC – Why is it valuable?

- If only creating a handful of resources, manual is (probably) fine
- Creating hundreds (or even thousands), not so much!
- Modern DevOps is built around automation – quickly tearing down and rebuilding entire sets of infrastructure as and when required



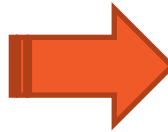
IaC – Advantages?



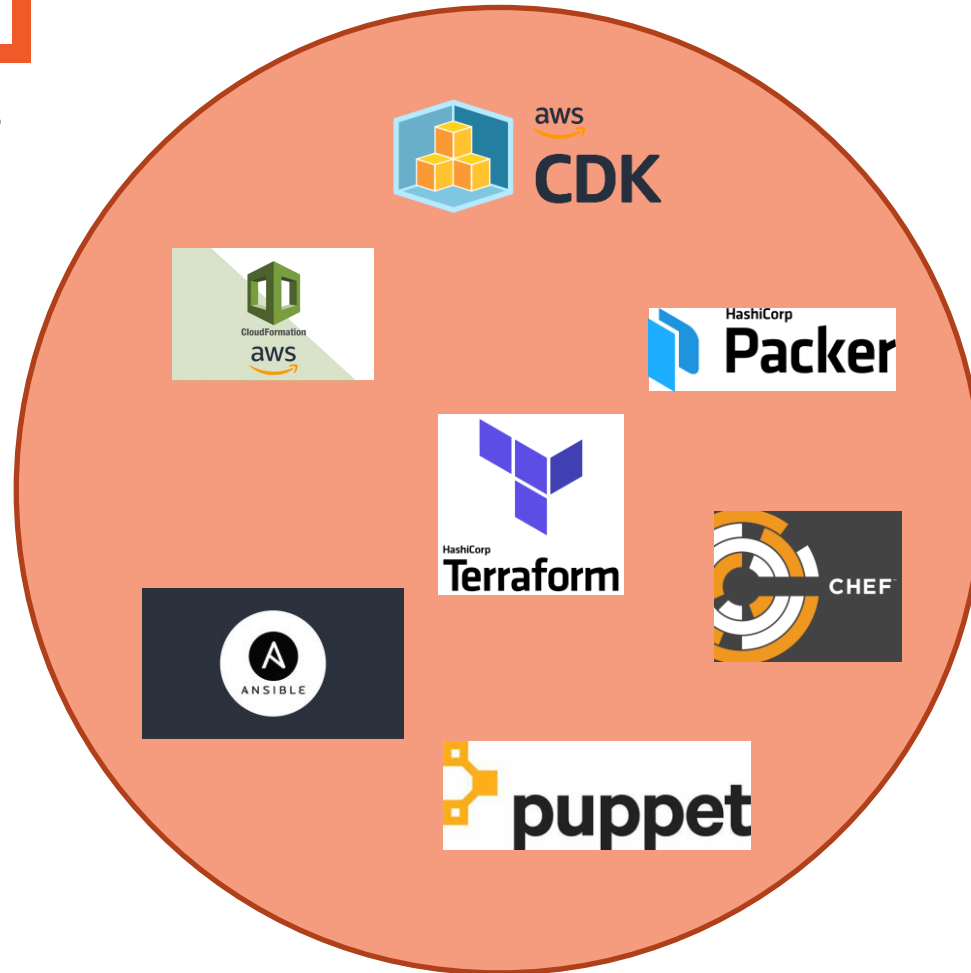
Testable

Repeatable

Auditable



IaC – Options?



AWS CloudFormation

AWS CloudFormation



Works off 3 main concepts:

Templates

Stacks

Change Sets

AWS CloudFormation



Works off 3 main concepts:

Formatted text files written in JSON or YAML that describe the “blueprint” for the AWS resources to be built

Templates

Stacks

Change Sets

AWS CloudFormation



Works off 3 main concepts:

Templates

Stacks

Change Sets

A grouping of the complete set of resources provisioned by execution of a CloudFormation template

AWS CloudFormation



Works off 3 main concepts:

Templates

Stacks

Change Sets

Provides a summary of proposed changes that will be made to a set of running resources through execution of an updated template – before those updates are made

LAB:

AWS CloudFormation

Execute the “Hands-On” lab available at

<https://learn.acloud.guru/hands-on/8a73c444-d5a3-461a-81fd-0cb4f0a56103>

LAB:

AWS CloudFormation

Execute the “Hands-On” lab available at

<https://learn.acloud.guru/handson/db9222f4-e0a0-4844-a110-d9225474c6e1>

Identity & Access Management (IAM)



IAM – What is it?



AWS Identity and Access Management

Apply fine-grained permissions to AWS services and resources



Who

Workforce users and workloads with IAM



Can access

Permissions with IAM policies

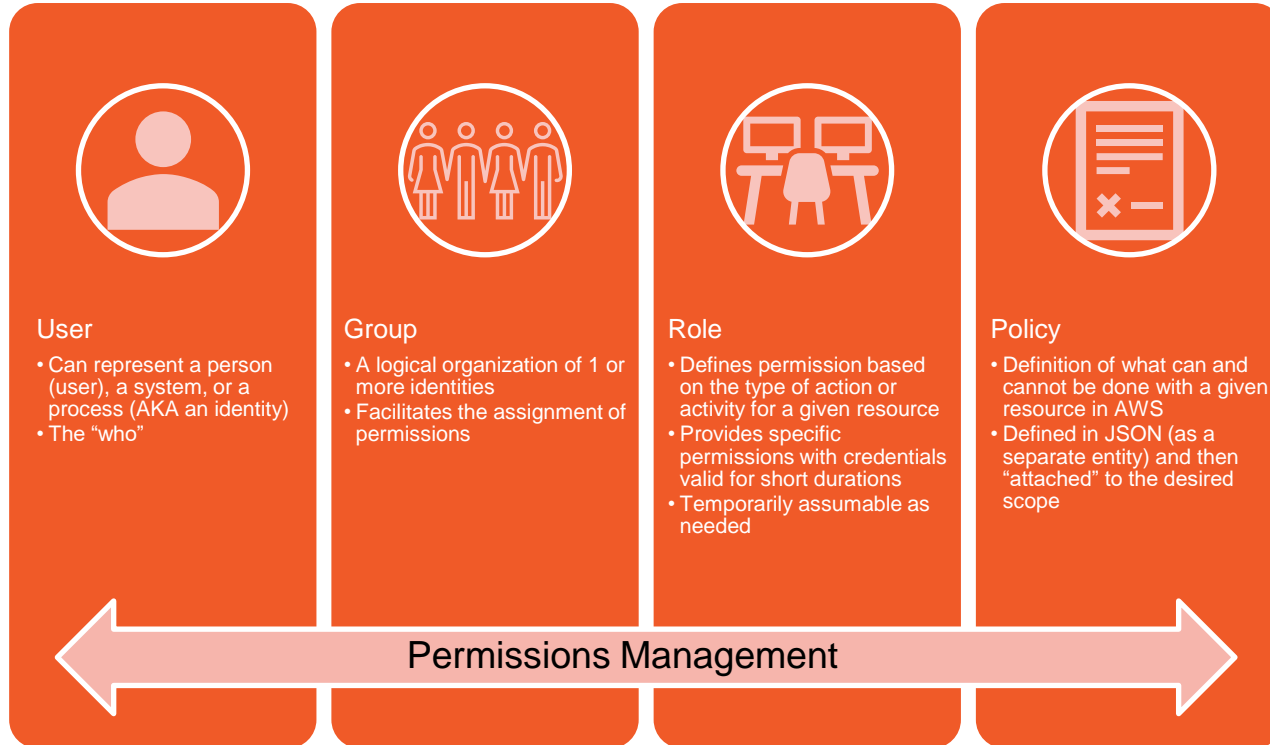


What

Resources within your AWS organization

Source: <https://aws.amazon.com/iam/>

IAM – What is it?



IAM – Users



jschmoe

Delete

Summary

ARN

[Redacted]

Console access

Disabled

Access key 1

Not enabled

Created

[Redacted]

Last console sign-in

-

Access key 2

Not enabled

Permissions

Groups (1)

Tags

Security credentials

Access Advisor

User groups membership (1)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users. A user can be a member of up to 10 groups at a time.



Remove

Add user to groups



Group name [↗](#)



Attached policies [↗](#)



Developers

[AmazonECS_FullAccess](#)

IAM – Groups



Developers

[Delete](#)

Summary

[Edit](#)

User group name
Developers

Creation time

ARN

[Users](#)[Permissions](#)[Access Advisor](#)

Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

[Simulate](#)[Remove](#)[Add permissions](#) ▼

< 1 >

<input type="checkbox"/>	Policy name	Type	Description
--------------------------	-------------	------	-------------

<input type="checkbox"/>	AmazonECS_FullAccess	AWS manag...	Provides administrative access to Amazon ECS resources and enables ECS features through access to other AWS service resources, including VPCs...
--------------------------	-----------------------------	--------------	--

AmazonECS_FullAccess

Provides administrative access to Amazon ECS resources and enables ECS features through access to other AWS service resources, including VPCs, Auto Scaling groups, and CloudFormation stacks.

[Copy](#)

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "application-autoscaling:DeleteScalingPolicy",
8         "application-autoscaling:DeregisterScalableTarget",
9         "application-autoscaling:DescribeScalableTargets",
10        "application-autoscaling:DescribeScalingActivities",
11      ]
12    }
13  ]
14 }
```


IAM – Roles



AWSServiceRoleForRDS

Allows Amazon RDS to manage AWS resources on your behalf

Delete

Summary

Edit

Creation date

ARN

Last activity

✓ 1 hour ago

Maximum session duration

1 hour

Permissions

Trust relationships

Tags

Access Advisor

Permissions policies (1) [Info](#)

Policy name [↗](#)

Type

Attached entities



AmazonRDSServiceRolePolicy

AWS managed

1

AmazonRDSServiceRolePolicy

Allows Amazon RDS to manage AWS resources on your behalf.

[Copy](#)

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "rds:CrossRegionCommunication"  
8       ],  
9       "Resource": "*"

```

IAM – Policies



AWSCloudFormationReadOnlyAccess

Provides access to AWS CloudFormation via the AWS Management Console.

Policy details

Type	Creation time	Edited time	ARN
AWS managed			

Permissions

Entities attached

Policy versions

Access Advisor

Permissions defined in this policy [Info](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Copy

Summary

JSON

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "cloudformation:Describe*",  
8         "cloudformation:EstimateTemplateCost",  
9         "cloudformation:Get*",  
10        "cloudformation:List*",  
11        "cloudformation:ValidateTemplate",  
12        "cloudformation:Detect*",  
13      ],  
14      "Resource": "*"   
15    }  
16  ]  
17 }
```

IAM – Policies



AWSCloudFormationFullAccess

Provides full access to AWS CloudFormation.

Policy details

Type	Creation time	Edited time	ARN
AWS managed			

Permissions

Entities attached

Policy versions

Access Advisor

Permissions defined in this policy [Info](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

[Copy](#)

[Summary](#)

[JSON](#)

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "cloudformation:*"
8       ],
9       "Resource": "*"
10    }
11  ]
12 }
```

LAB:

AWS IAM

Execute the “Hands-On” lab available at
<https://learn.acloud.guru/handson/2b676662-301f-4797-a22a-e13d48d4ca92>

DEMO:

AWS CloudFormation

Review the examples at

<https://github.com/KernelGamut32/Mastering-AWS-CloudFormation>

DEMO:

AWS CloudFormation – Nested Stacks

Review the examples at

<https://learn.acloud.guru/handson/7e6eeca-283a-46d2-a1ad-8ec41c198250>

AWS SAM (Serverless Application Model)

AWS SAM – What is it?



AWS SAM Template Specification

AWS SAM CLI (Command-Line Interface)



AWS SAM – What is it?

- Open-source framework
- An extension of CloudFormation
- Enables use of abstract, short-hand syntax to define infrastructure
- Transforms short-hand syntax into code to define and create resources

AWS SAM Template Specification

AWS SAM CLI (Command-Line Interface)

AWS SAM – What is it?



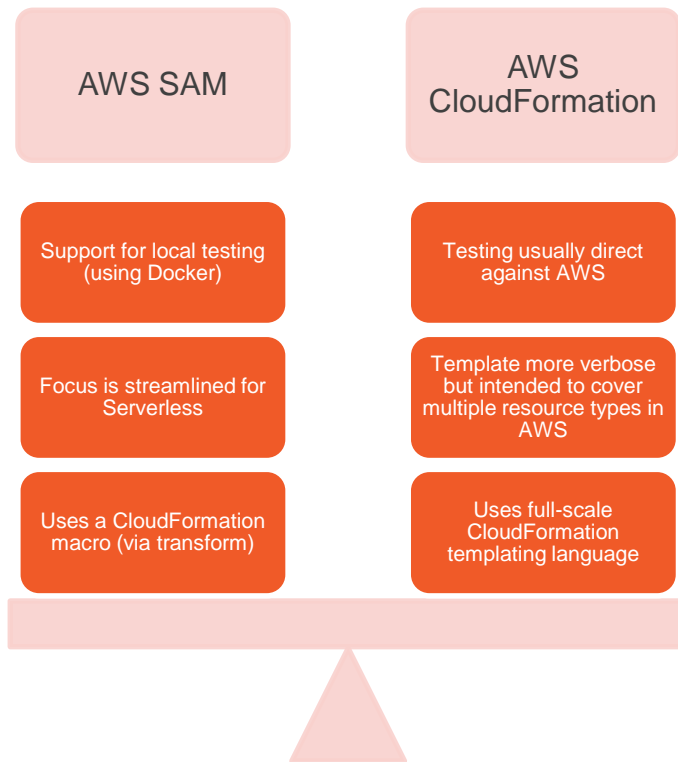
AWS SAM Template Specification

AWS SAM CLI (Command-Line Interface)

- Separately installed command line tool
- Used to initialize a new project, build, test, deploy, and monitor
- Supports sync of local changes to the Cloud
- Can be used (alongside a Docker installation) to test the application locally!



“Differences” Between AWS SAM and CloudFormation





DEMO:

AWS SAM



Thank you!

If you have additional questions,
please reach out to me at:
asanders@gamuttechnologysvcs.com