

Welcome to Week 1

Cloud Accelerator Program

CloudFormation, IAM, and S3

 **Develop**Intelligence

A PLURALSIGHT COMPANY

Hello

HELLO
my name is

Allen Sanders
with DevelopIntelligence,
a Pluralsight Company.

About me...



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



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
- S3 – Cloud Storage 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?



A decorative graphic consisting of a thick L-shaped line, with the top horizontal segment in orange and the left vertical segment in pink. To the right of this line, the background is filled with a grid of small, light gray dots.

Speaking the Language of Cloud



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



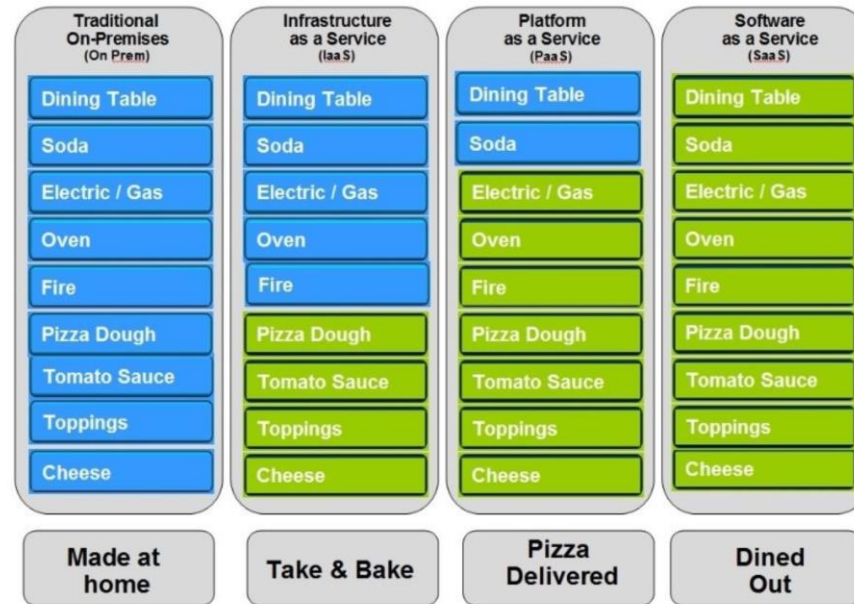
What do they all mean?

Pizza-as-a-Service

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

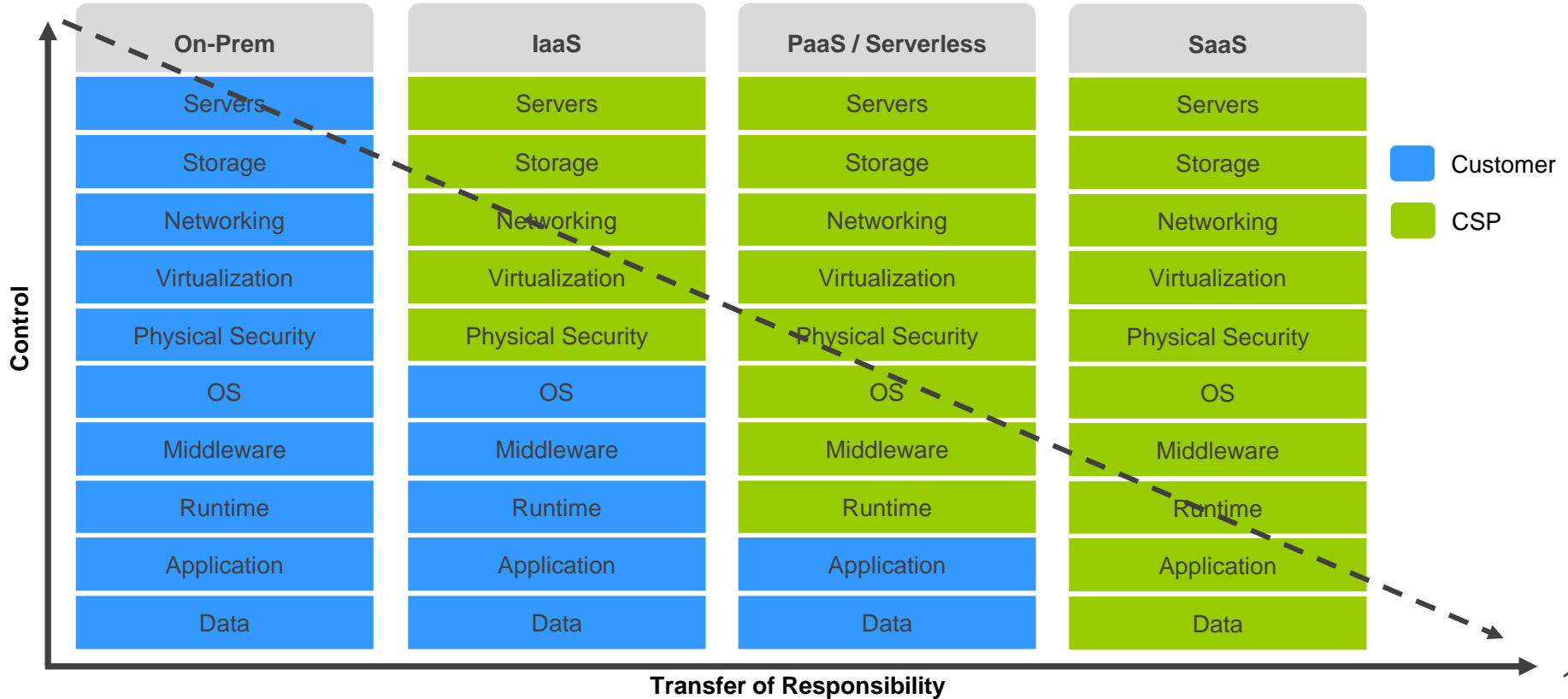


Pizza as a Service



■ You Manage ■ Vendor Manages

Side-by-Side Comparison





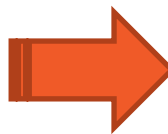
CloudFormation

Infrastructure-as-Code (IaC)



IaC – What is it?

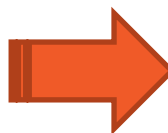
- As the name implies, the definition & configuration of our infrastructure IN code
- Instead of manually creating (inefficient) → automated in scripts that run “at the push of a button”





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



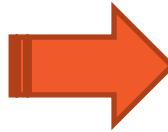
laC – Advantages?



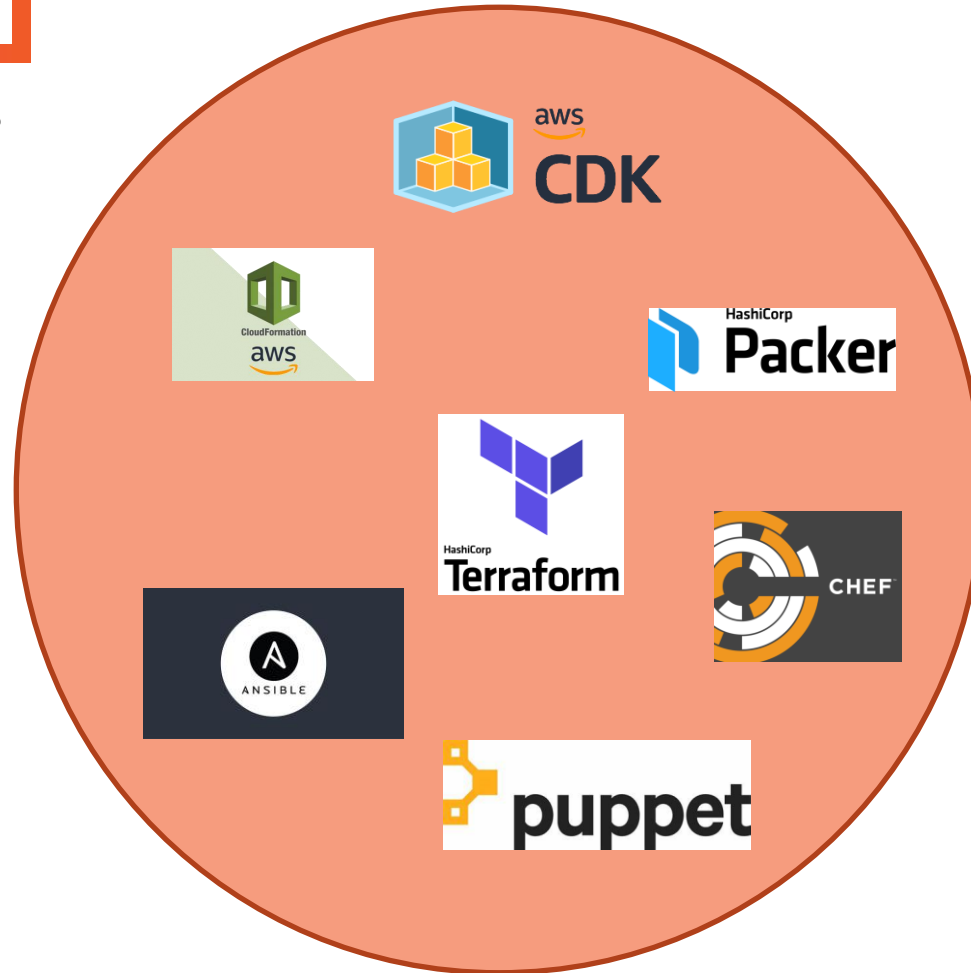
Testable

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

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

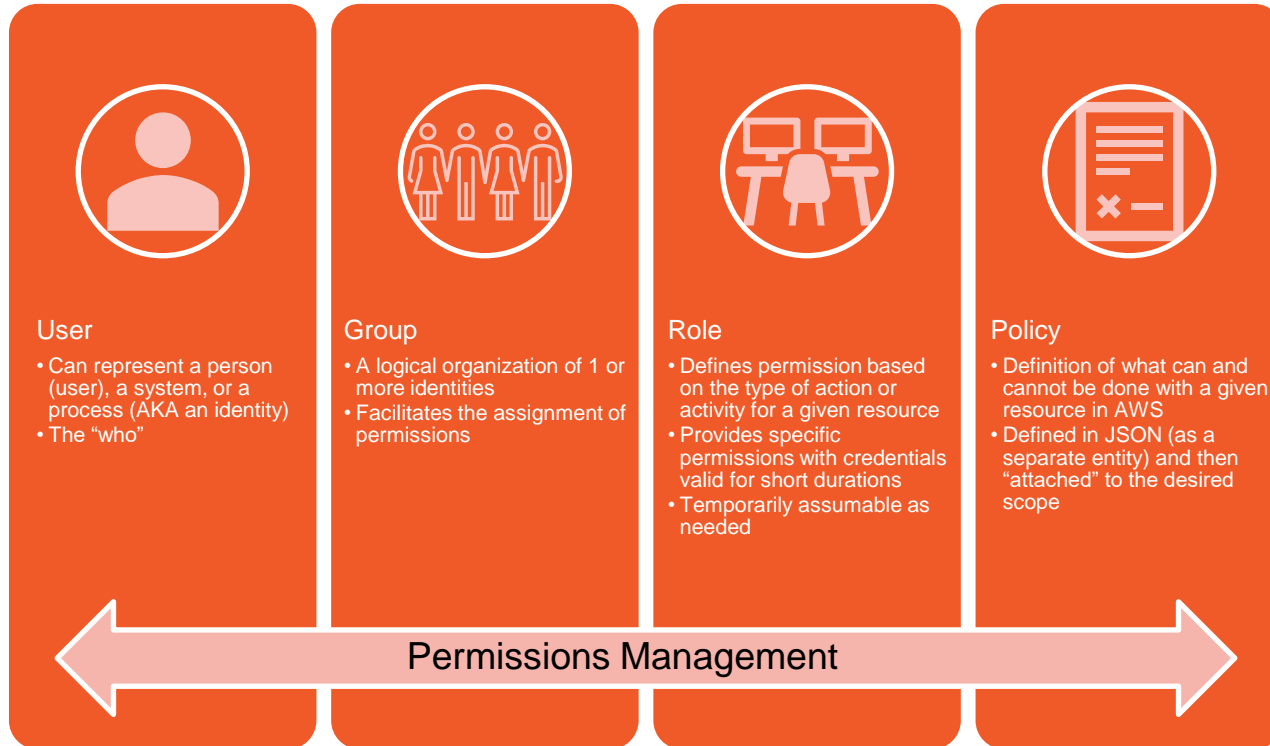


What

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": "*"
10    }
11  ]
12 }
```

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 }
```

S3 (Simple Storage Service)



S3

<https://cloudacademy.com/blog/s3-lifecycle-policies-versioning-encryption-aws-security/>

<https://aws.amazon.com/s3/storage-classes/>

LAB:

AWS CloudFormation

Execute the “Hands-On” lab available at
<https://github.com/KernelGamut32/cloud-accel-aws-2024-public/tree/main/week01/labs/lab01>

LAB:

AWS CloudFormation
(Condition Functions)

Execute the “Hands-On” lab available at
<https://github.com/KernelGamut32/cloud-accel-aws-2024-public/tree/main/week01/labs/lab02>

DEMO:

AWS CloudFormation
(Template Anatomy)

Review the template available at

<https://github.com/PacktPublishing/Mastering-AWS-CloudFormation/blob/master/Chapter2/core.yaml>

Also, see

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/mapping-section-structure.html>,

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/outputs-section-structure.html>, and

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/getting-started.templatebasics.html#gettingstarted.templatebasics.mappings>

LAB:

AWS CloudFormation
(Looping)

Execute the “Hands-On” lab available at
[https://github.com/KernelGamut32/cloud-accel-aws-2024-
public/tree/main/week01/labs/lab03](https://github.com/KernelGamut32/cloud-accel-aws-2024-public/tree/main/week01/labs/lab03)

LAB:

AWS CloudFormation
(Working with Roles)

Execute the “Hands-On” lab available at
[https://github.com/KernelGamut32/cloud-accel-aws-2024-
public/tree/main/week01/labs/lab04](https://github.com/KernelGamut32/cloud-accel-aws-2024-public/tree/main/week01/labs/lab04)

LAB:

AWS CloudFormation
(Drift Detection)

Execute the “Hands-On” lab available at
[https://github.com/KernelGamut32/cloud-accel-aws-2024-
public/tree/main/week01/labs/lab05](https://github.com/KernelGamut32/cloud-accel-aws-2024-public/tree/main/week01/labs/lab05)

LAB:

AWS CloudFormation
(Nested Stacks)

Execute the “Hands-On” lab available at
[https://github.com/KernelGamut32/cloud-accel-aws-2024-
public/tree/main/week01/labs/lab06](https://github.com/KernelGamut32/cloud-accel-aws-2024-public/tree/main/week01/labs/lab06)

LAB:

S3 Bucket Versioning

Execute the “Hands-On” lab available at
<https://github.com/KernelGamut32/cloud-accel-aws-2024-public/tree/main/week01/labs/lab07>

LAB:

S3 Lifecycle Rules

Execute the “Hands-On” lab available at
<https://github.com/KernelGamut32/cloud-accel-aws-2024-public/tree/main/week01/labs/lab08>



Knowledge Check



Question #1

Q: This hosting option provides a “function” hosted in the Cloud that can be used to expose functionality using multiple languages, can be triggered in multiple ways, and provides a consumption-based costing model. Your choice?

1. IaaS
2. PaaS
3. Serverless
4. SaaS

Enter your answer in the chat...



Question #2

Q: This hosting option requires a higher degree of operational management on the part of the organization that chooses to use it for hosting resources in the Cloud. Your choice?

1. IaaS
2. PaaS
3. Serverless
4. SaaS

Enter your answer in the chat...



Question #3

Q: Which of the following is an advantage of IaC (Infrastructure-as-Code)?

1. Testability
2. Repeatability
3. Auditability
4. All of the above

Enter your answer in the chat...



Question #4

Q: Which of the following in CloudFormation represents a “what if” assessment of the changes to be made in AWS from applying an updated template without actually applying the changes to the Cloud?

1. Template
2. Stack
3. CDK
4. Change set

Enter your answer in the chat...



Question #5

Q: Which of the following in CloudFormation represents a logical grouping of resources that will be deployed together as part of the application of a CFT?

1. Template
2. Stack
3. CDK
4. Change set

Enter your answer in the chat...



Question #6

Q: Which of the following constructs in IAM is used to organize users to facilitate the application of permissions to all of them?

1. User
2. Group
3. Role
4. Policy

Enter your answer in the chat...



Question #7

Q: Which of the following constructs in IAM is used to associate a set of permissions to a service (like a Lambda) to give that service the context needed to complete a specific set of actions?

1. User
2. Group
3. Role
4. Policy

Enter your answer in the chat...



Question #8

Q: True or False? Policies in AWS give you the ability to control access at a very granular level.

1. True
2. False

Enter your answer in the chat...



Thank you!

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