Welcome to Week 1

Cloud Accelerator Program

CloudFormation, IAM, and S3

DevelopIntelligence

A PLURALSIGHT COMPANY

Hello

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?

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/

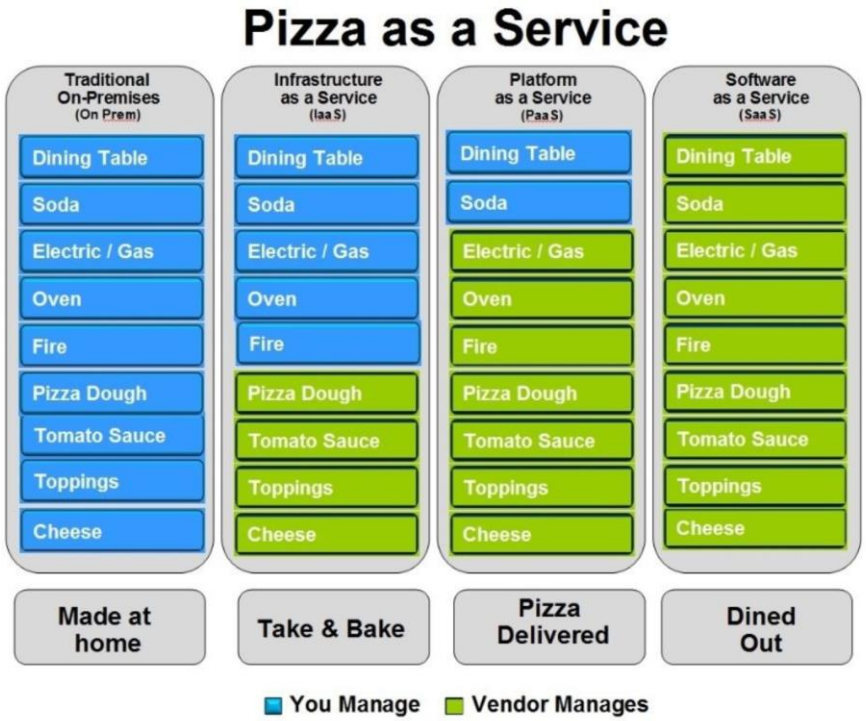
What Are the Hosting Options with Cloud?

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

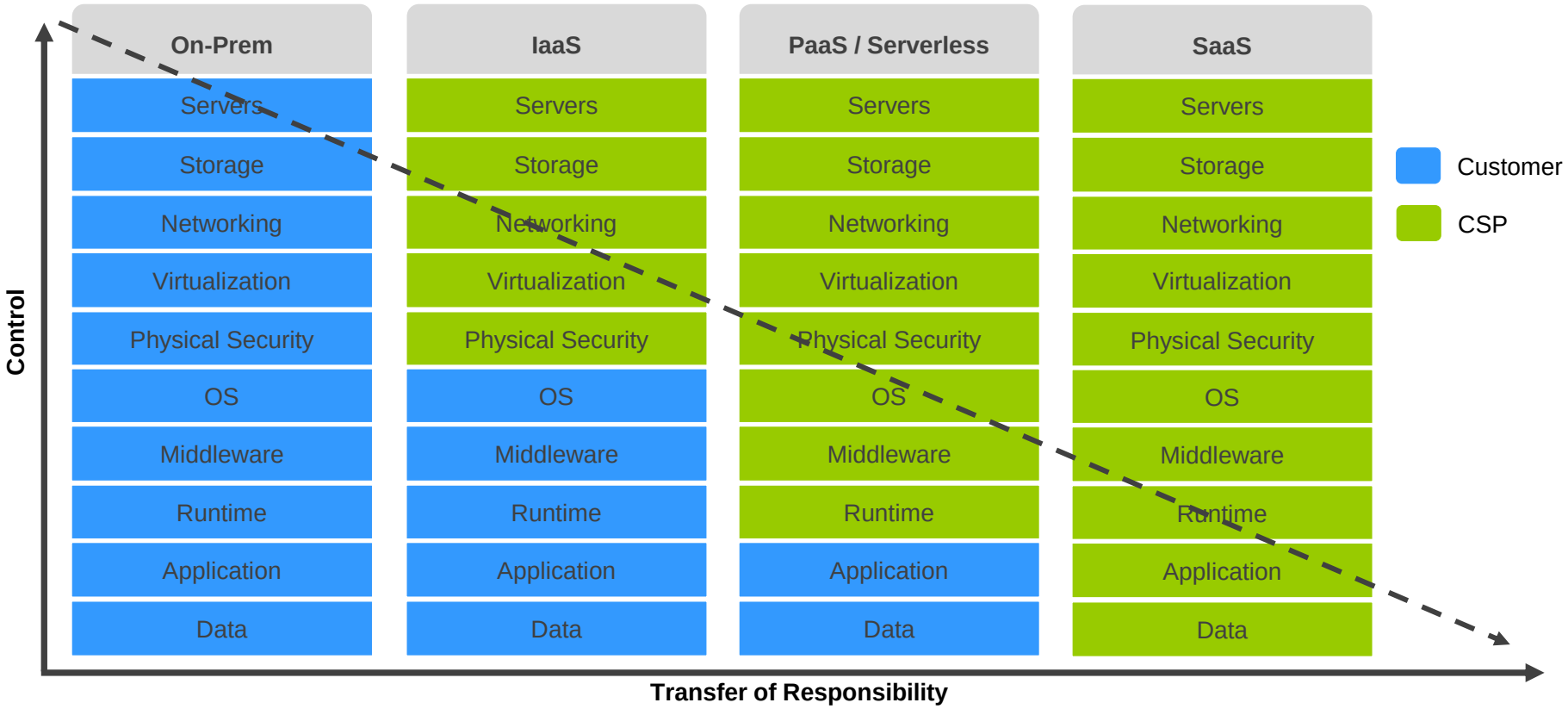
What do they all mean?

Pizza-as-a-Service

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



Side-by-Side Comparison



CloudFormation

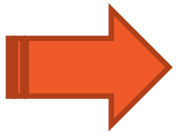
Infrastructure-as-Code (IaC)

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



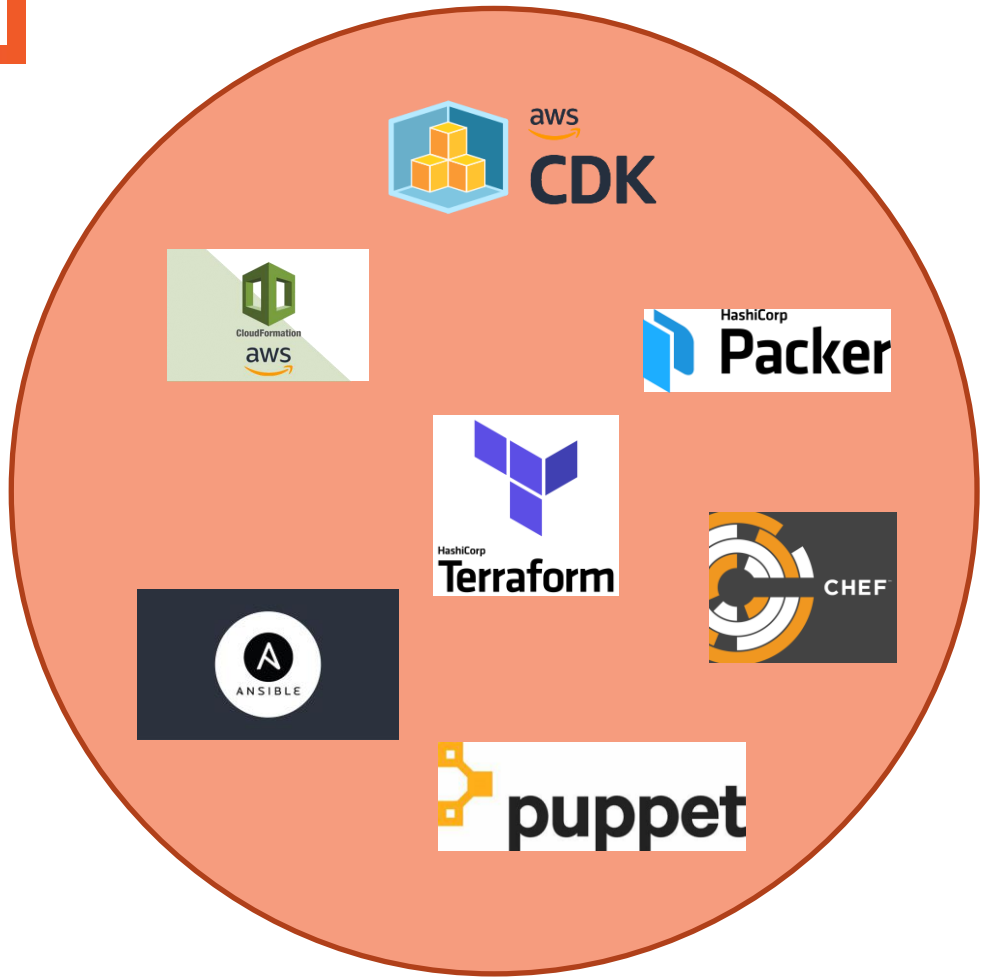
IaC – Advantages?

Testable

Repeatable

Auditable

IaC – Options?


aws
CDK
CloudFormation
aws
HashiCorp
Packer
HashiCorp
Terraform
CHEF
ANSIBLE
puppet

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

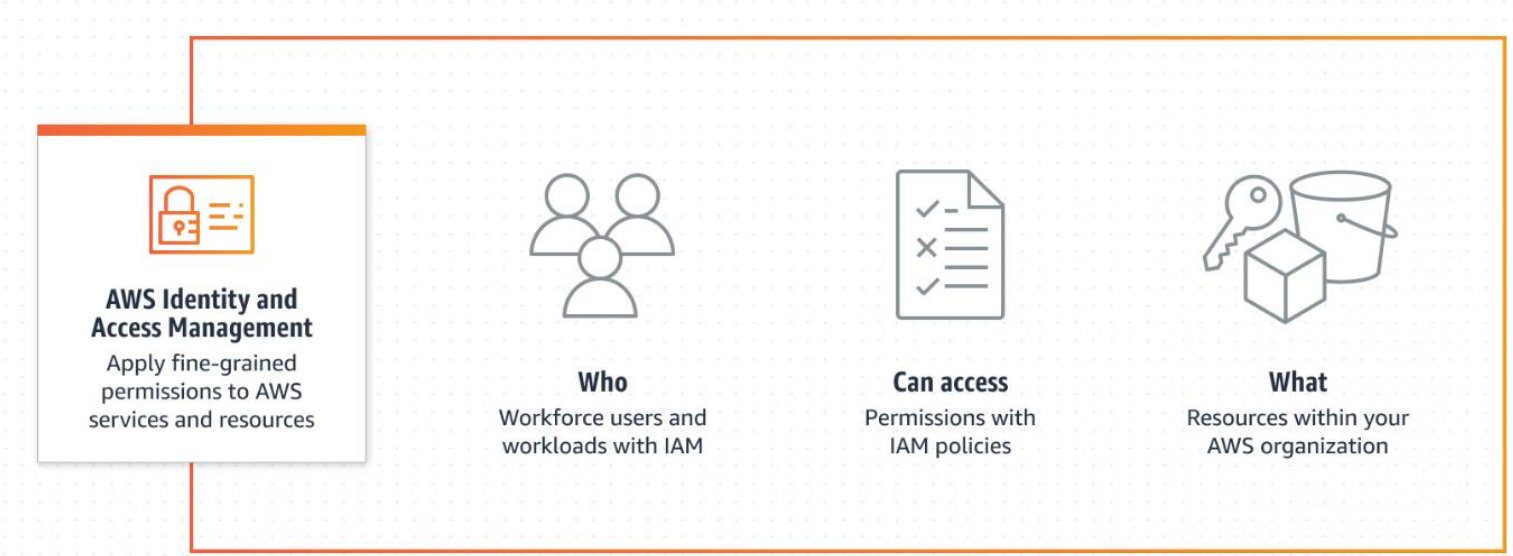
Stacks

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?



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

IAM – What is it?

User

- Can represent a person (user), a system, or a process (AKA an identity)
- The “who”

Group

- A logical organization of 1 or more identities
- Facilitates the assignment of permissions

Role

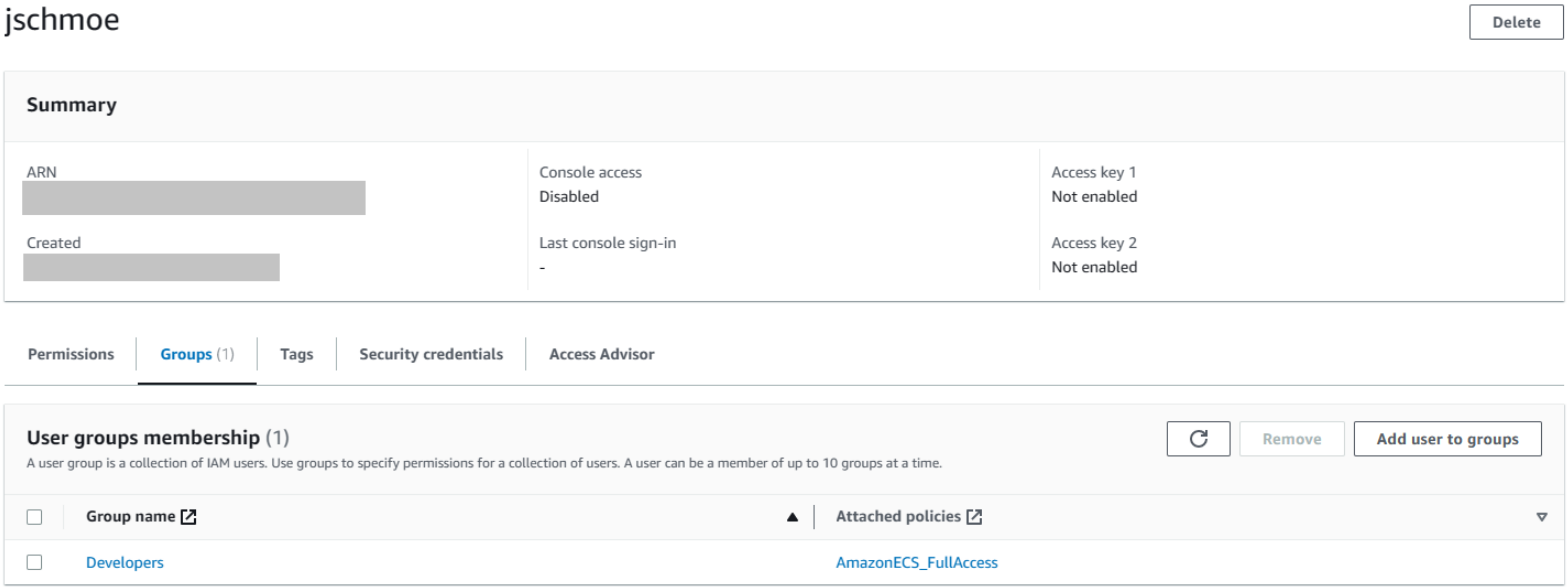
- Defines permission based on the type of action or activity for a given resource
- Provides specific permissions with credentials valid for short durations
- Temporarily assumable as needed

Policy

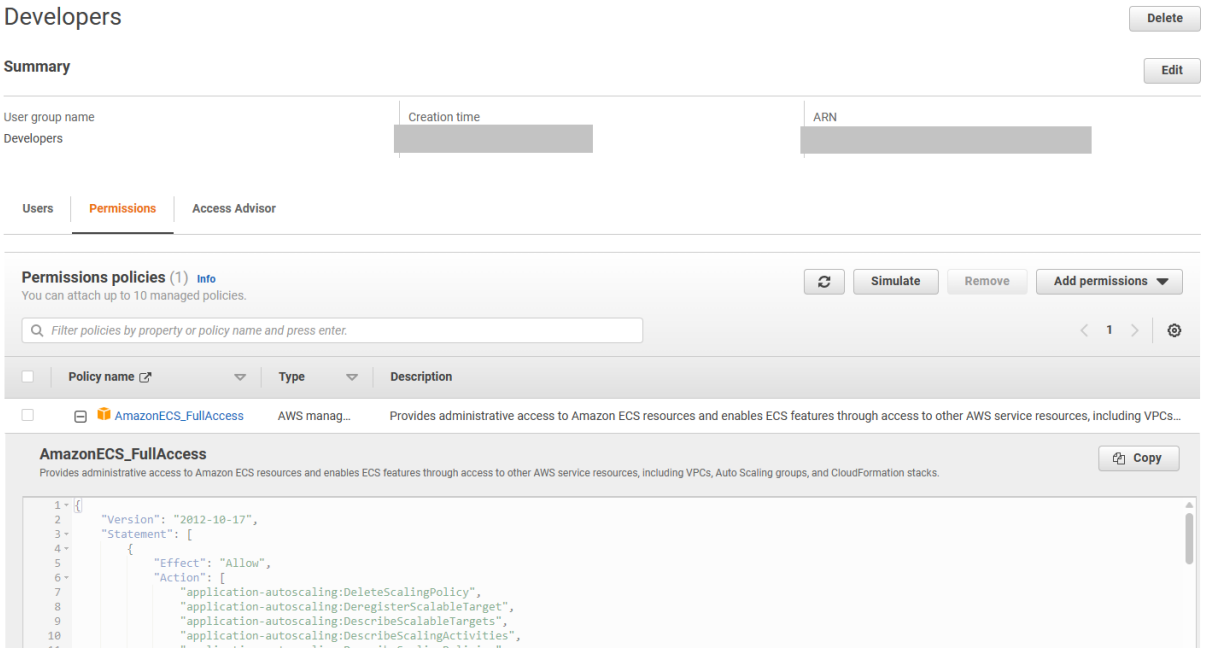
- Definition of what can and cannot be done with a given resource in AWS
- Defined in JSON (as a separate entity) and then “attached” to the desired scope

Permissions Management

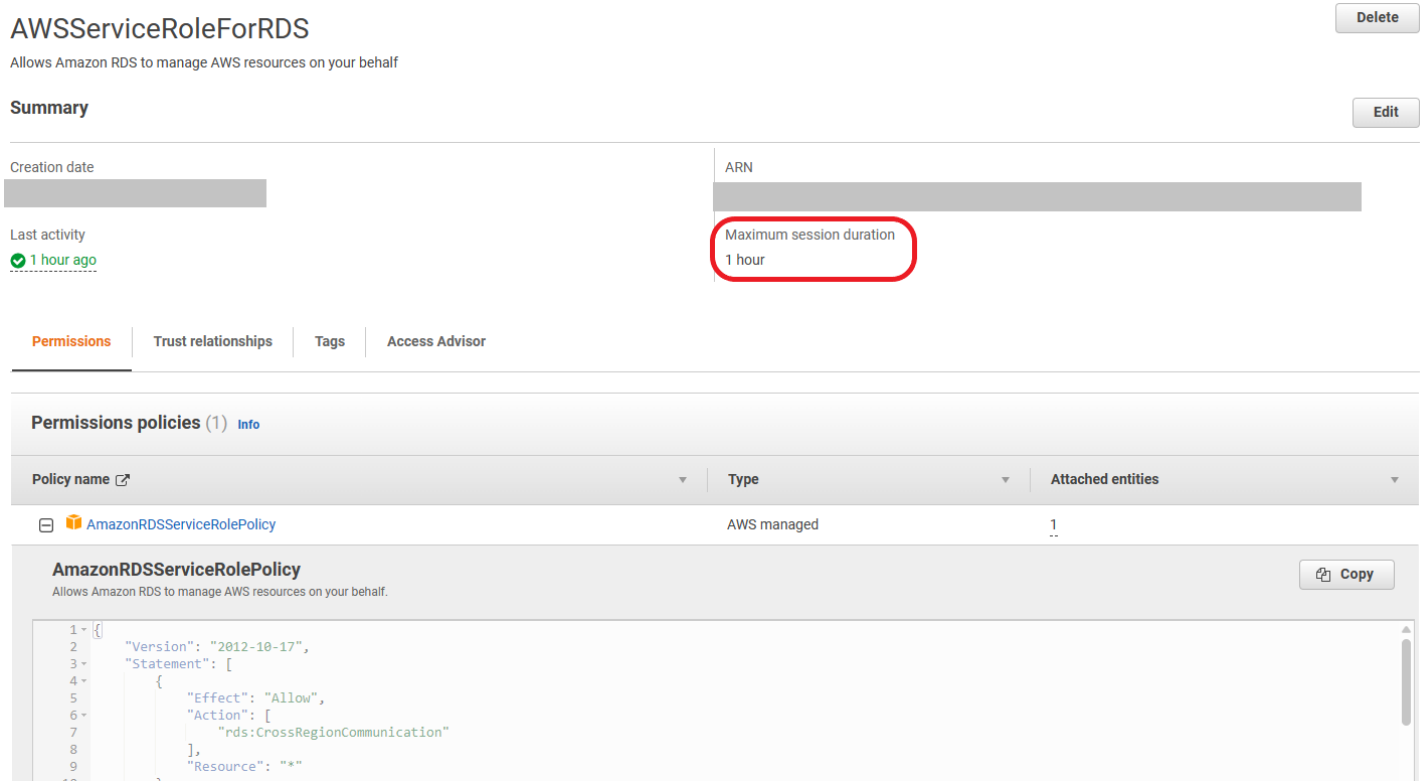
IAM – Users


jschmoe
Delete
Summary
ARN
Console access
Disabled
Access key 1
Not enabled
Created
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
Filter policies by property or policy name and press enter.
1
Policy name
Type
Description
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
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"application-autoscaling:DeleteScalingPolicy",
"application-autoscaling:DeregisterScalableTarget",
"application-autoscaling:DescribeScalableTargets",
"application-autoscaling:DescribeScalingActivities",

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
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"rds:CrossRegionCommunication"
],
"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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:Describe*",
                "cloudformation:EstimateTemplateCost",
                "cloudformation:Get*",
                "cloudformation:List*",
                "cloudformation:ValidateTemplate",
                "cloudformation:Detect*"
            ],
            "Resource": "*"
        }
    ]
}
```

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:*"
            ],
            "Resource": "*"
        }
    ]
}
```

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

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

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

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

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

Thank you!

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

DevelopIntelligence
A PLURALSIGHT COMPANY