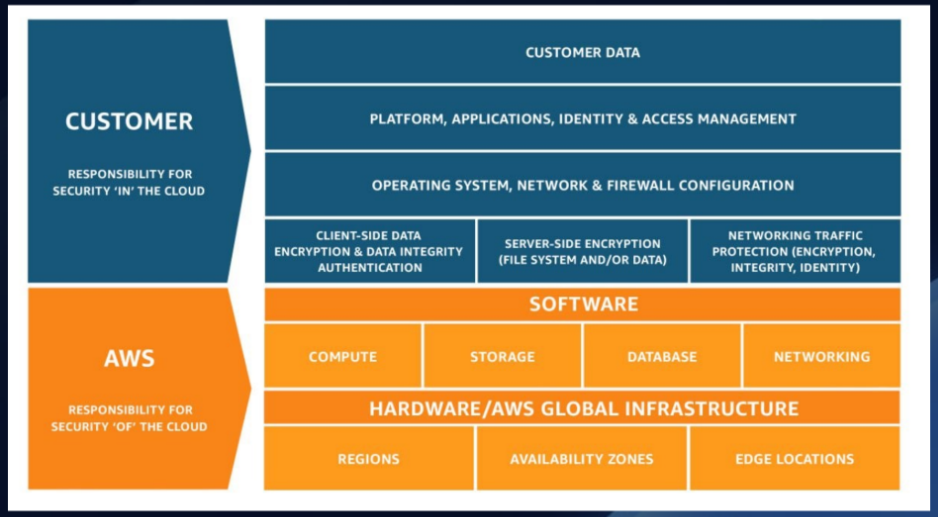
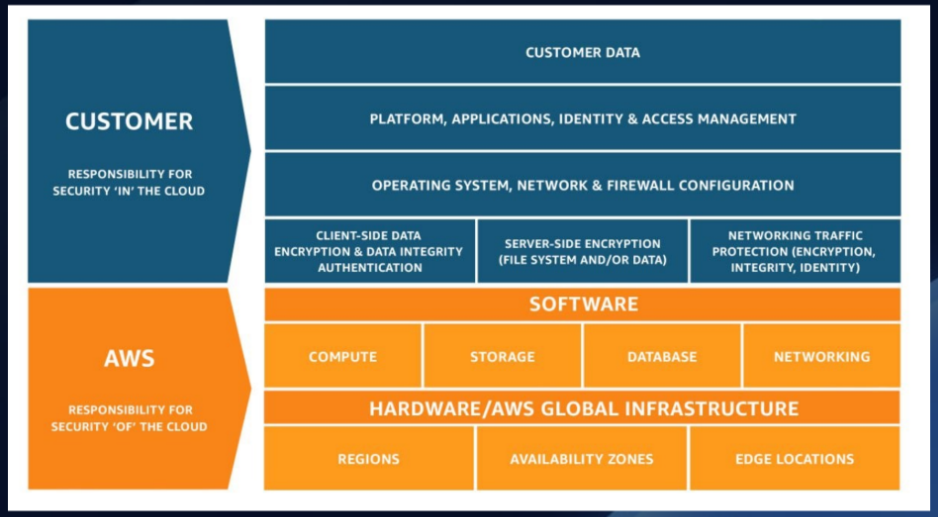
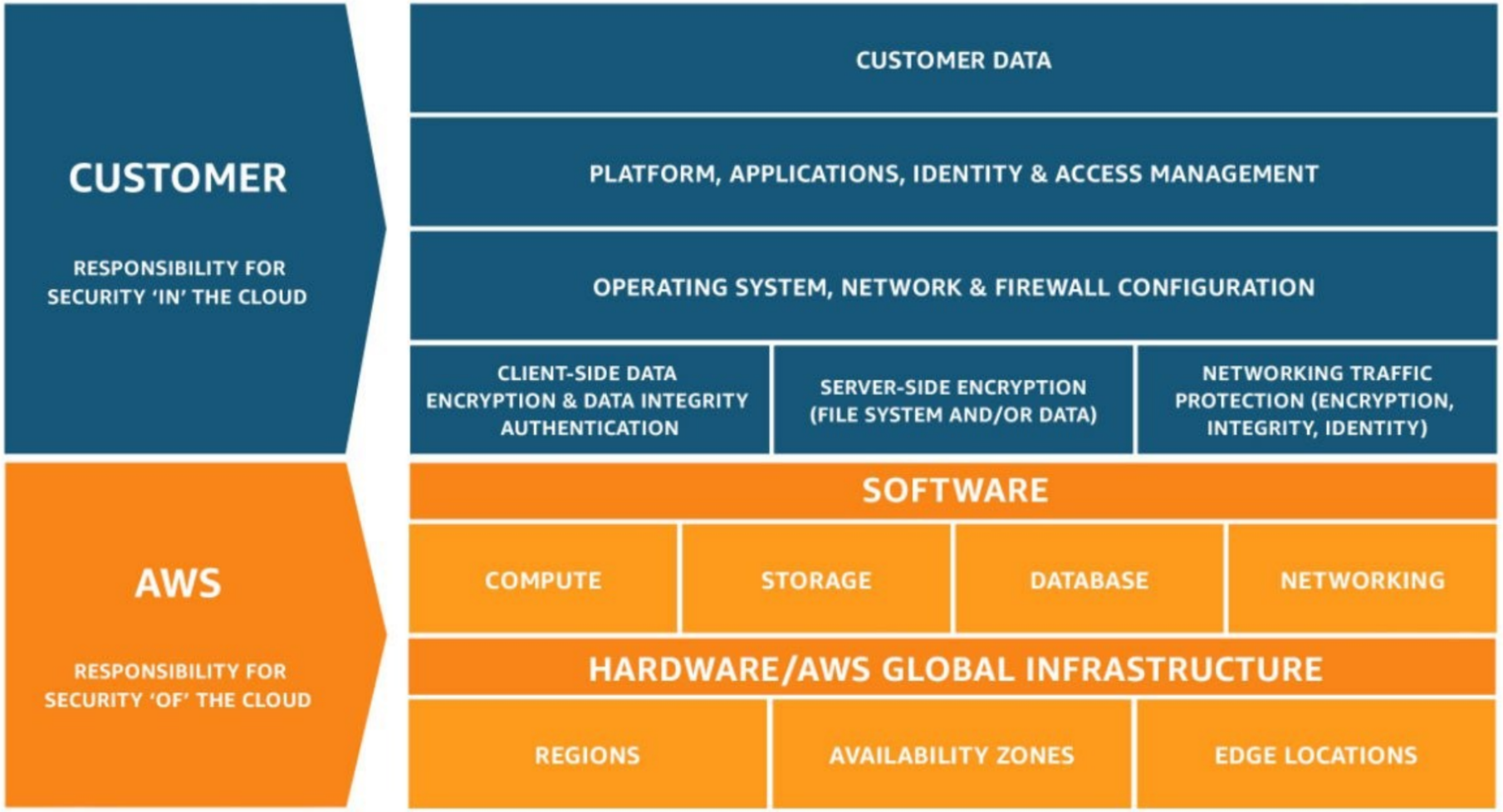

aws certified
Cloud Practitioner
IAM, Organisations, & CloudTrail
AWS Certification Preparation
1
Shared Responsibility Model
2
Users, Groups & Roles
3
AWS Organisations
4
IAM Policies
5
Identity Federation
6
AWS CloudTrail
© BackSpace Technology LLC
BackSpace

# AWS Shared Responsibility Model

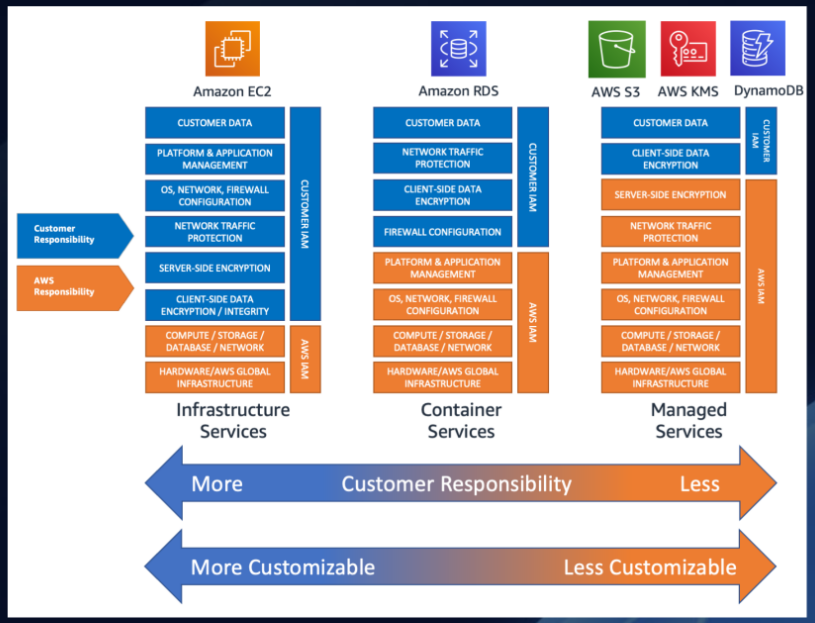


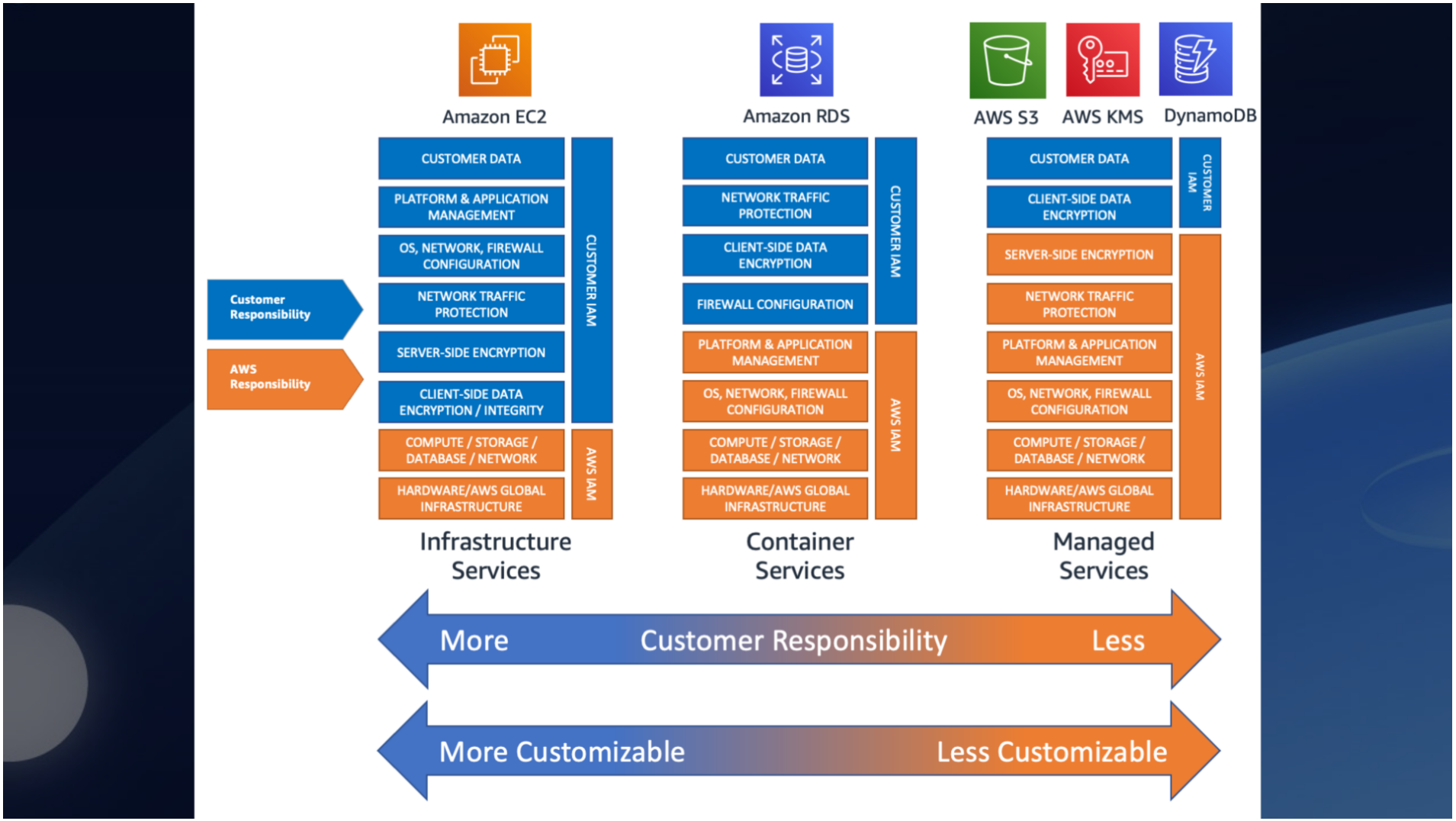
# AWS Shared Responsibility Model



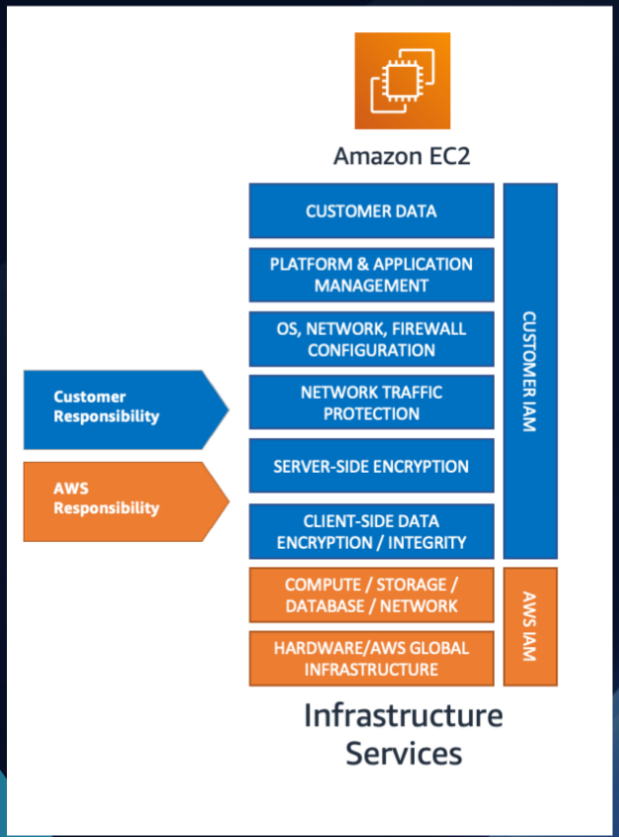

CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

# AWS Shared Responsibility Model




Amazon EC2
Amazon RDS
AWS S3
AWS KMS
DynamoDB
Customer Responsibility
AWS Responsibility
CUSTOMER DATA
PLATFORM & APPLICATION MANAGEMENT
OS, NETWORK, FIREWALL CONFIGURATION
NETWORK TRAFFIC PROTECTION
SERVER-SIDE ENCRYPTION
CLIENT-SIDE DATA ENCRYPTION / INTEGRITY
COMPUTE / STORAGE / DATABASE / NETWORK
HARDWARE/AWS GLOBAL INFRASTRUCTURE
CUSTOMER IAM
AWS IAM
CUSTOMER DATA
NETWORK TRAFFIC PROTECTION
CLIENT-SIDE DATA ENCRYPTION
FIREWALL CONFIGURATION
PLATFORM & APPLICATION MANAGEMENT
OS, NETWORK, FIREWALL CONFIGURATION
COMPUTE / STORAGE / DATABASE / NETWORK
HARDWARE/AWS GLOBAL INFRASTRUCTURE
CUSTOMER IAM
AWS IAM
CUSTOMER DATA
CLIENT-SIDE DATA ENCRYPTION
SERVER-SIDE ENCRYPTION
NETWORK TRAFFIC PROTECTION
PLATFORM & APPLICATION MANAGEMENT
OS, NETWORK, FIREWALL CONFIGURATION
COMPUTE / STORAGE / DATABASE / NETWORK
HARDWARE/AWS GLOBAL INFRASTRUCTURE
CUSTOMER IAM
AWS IAM
Infrastructure Services
Container Services
Managed Services
More
Customer Responsibility
Less
More Customizable
Less Customizable

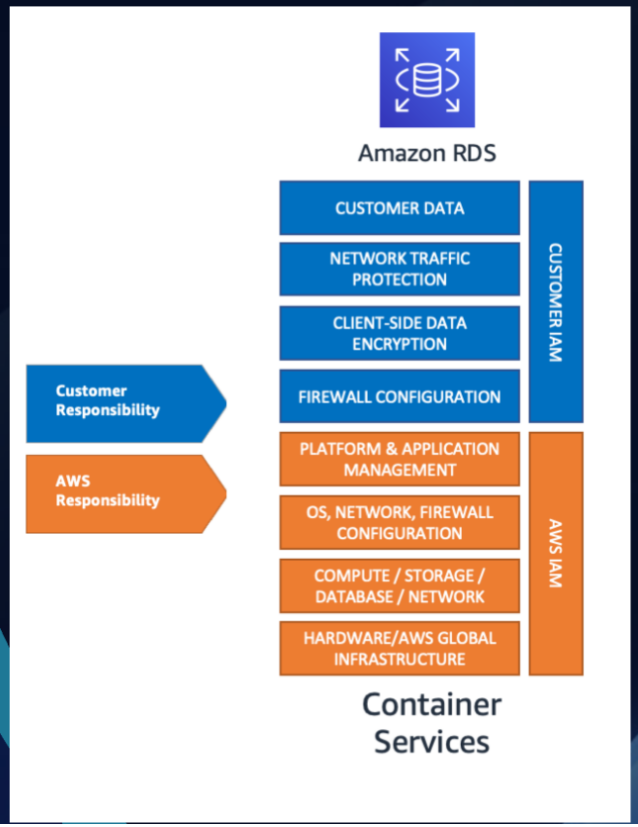
# Infrastructure Services




Infrastructure Services e.g.

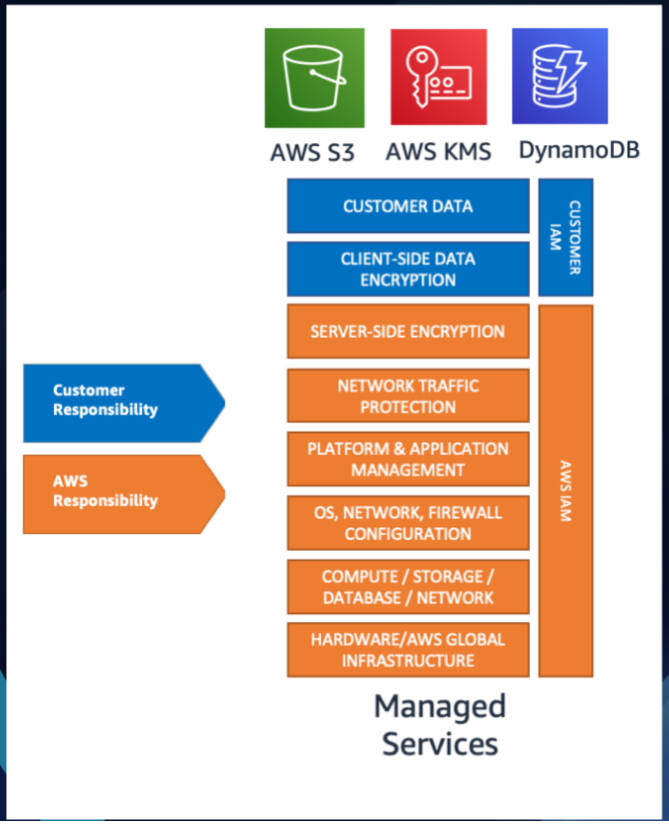
- Amazon EC2, and related services, such as:
  - Amazon EBS,
  - Auto Scaling, and
  - Amazon VPC.
- **You** control the operating system,
- **You** configure and operate IAM

# Container Services




- Container Services e.g.
  - Amazon RDS
  - Amazon EMR,
  - AWS Elastic Beanstalk
- AWS provides a managed service
- **You** are responsible for:
  - network controls eg firewall rules
  - platform-level security separate from IAM

# Managed Services




- High-level storage, database, and messaging services:
  - Amazon S3,
  - Amazon Glacier,
  - DynamoDB,
  - AWS Lambda,
  - Amazon SQS, and Amazon SES
- **AWS** manages the underlying service components or the operating system on which they reside

# What is IAM?

- A **web service** that allows you to securely control individual and group access to your AWS resources.
- Create and manage user identities ("**IAM users**") and grant permissions.
- Features:
  - **Shared access** to your AWS account
  - **Granular** permissions
  - Secure access to AWS resources for applications that run on **Amazon EC2**
  - **Identity federation** to grant permissions for users outside of AWS
  - Payment Card Industry (**PCI**) Data Security Standard (**DSS**) Compliance
  - Access log auditing using **CloudTrail**
  - **Eventually** Consistent
  - **Free** to use




aws certified
Cloud Practitioner
IAM, Organisations, & CloudTrail
1
Shared Responsibility Model
2
Users, Groups & Roles
3
AWS Organisations
4
IAM Policies
5
Identity Federation
6
AWS CloudTrail
AWS Certification Preparation
© BackSpace Technology LLC
BackSpace

# Users

- Represent the person or service accessing your account
- Consists of a **name** and **credentials**
- Users are identified by:
  - A "**friendly name**“ eg “Bill”
  - Amazon Resource Name (**ARN**)
    - arn:aws:iam::account-ID-without-hyphens:user/Bill
  - **Unique identifier** which is returned only when you use the API, SDKs, Tools for Windows PowerShell, or AWS CLI to create the user.
- Credentials can be associated to a user:
  - **Console password**. User will have a url link to login to the console.
  - **Access keys** (access key ID and a secret access key), max 2.
- **Never use root user** to access resources unless absolutely essential . Create admin users with required permissions. Always enable multi-factor authentication of the root user.



# Users

- Represent the person or service accessing your account
- Consists of a **name** and **credentials**
- Users are identified by:
  - A "**friendly name**“ eg “Bill”
  - Amazon Resource Name (**ARN**)
    - arn:aws:iam::account-ID-without-hyphens:user/Bill
  - **Unique identifier** which is returned only when you use the API, SDKs, Tools for Windows PowerShell, or AWS CLI to create the user.
- Credentials can be associated to a user:
  - **Console password**. User will have a url link to login to the console.
  - **Access keys** (access key ID and a secret access key), max 2.
- **Never use root user** to access resources unless absolutely essential . Create admin users with required permissions. Always enable multi-factor authentication of the root user.



# User Password Policies

You can use a password policy to do these things:

- Set a minimum password length.
- Require specific character types.
- Allow all IAM users to change their own passwords.
- Password expiration.
- Prevent users from reusing previous passwords.
- Force users to contact an account administrator when the password has expired.



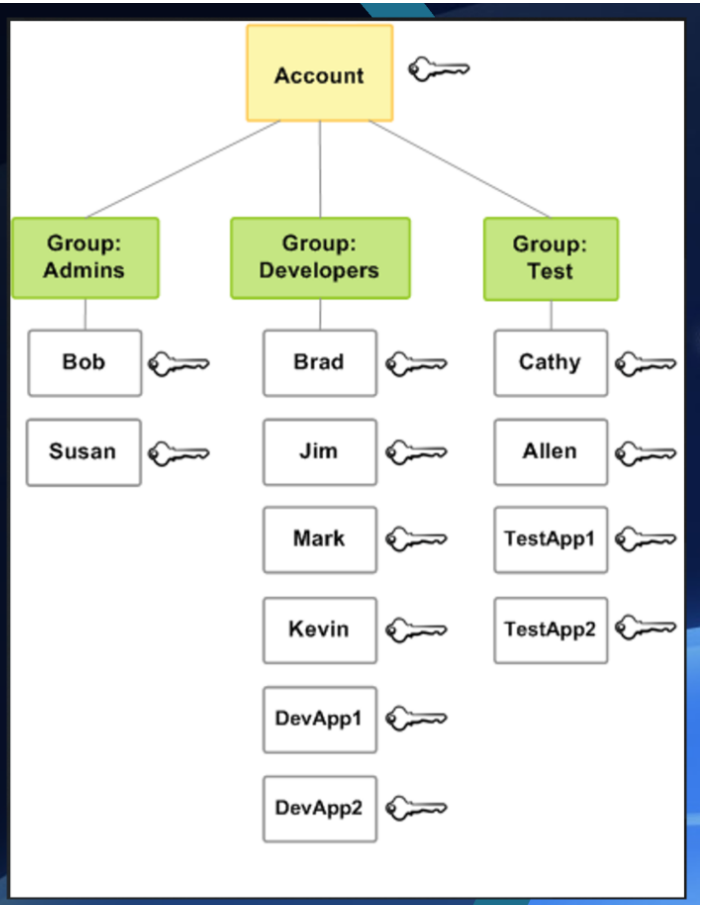
# Sign In URL

- Your sign-in page URL has the following format, by default.
  - https://**Your_AWS_Account_ID**.signin.aws.amazon.com/console/
- If you want the URL for your sign-in page to contain your company name (or other friendly identifier) instead of your AWS account ID, you can create an alias for your AWS account ID:
  - https://**Your_Alias**.signin.aws.amazon.com/console/



# Groups

- **Collection** of IAM users.
- Users **assume** the permissions of the group.
- Users can belong to **multiple groups**.
- Groups can only contain users, **cannot be nested**.



# Roles

- Defined permissions that can be assumed by **users or resources**.
- Allow **EC2 instances** to access other AWS resources.
- Grant access to your resources to users in **another AWS account**
- Can be used to allow users to temporarily assume a role with least privilege access to critical resources. **Identity federation** using:
  - AWS Cognito
  - OAUTH (Facebook, Google etc)
  - Enterprise Single Sign On with LDAP or Active Directory




aws certified
Cloud Practitioner
IAM, Organisations, & CloudTrail
AWS Organisations
IAM Policies
Users, Groups & Roles
Identity Federation
Shared Responsibility Model
AWS CloudTrail
1
2
3
4
5
6
AWS Certification Preparation
© BackSpace Technology LLC
BackSpace

# AWS Organisations

- Allows multiple AWS accounts used by an organisation to be part of an **Organisational Unit** (OU)
- **Service Control Policies** (SCPs) allow the whitelisting or blacklisting of services within an Organisational Unit.
- A **blacklisted** service will not be available even if the IAM user or group policy allows it.
- Benefits:
  - **Centrally manage** policies across multiple AWS accounts
  - **Control access** to AWS services
  - **Automate** AWS account creation and management programmatically with APIs
  - **Consolidate billing** across multiple AWS accounts

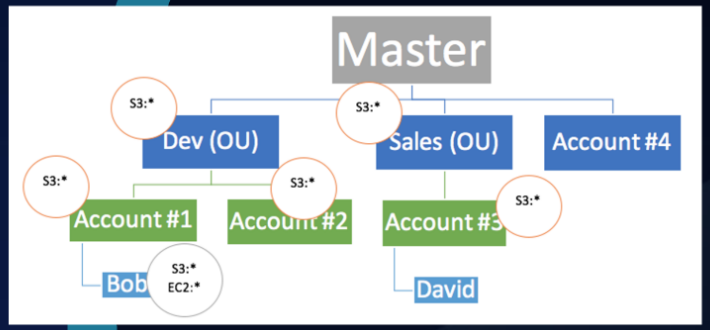


# AWS Organisations

- Allows multiple AWS accounts used by an organisation to be part of an **Organisational Unit** (OU)
- **Service Control Policies** (SCPs) allow the whitelisting or blacklisting of services within an Organisational Unit.
- A **blacklisted** service will not be available even if the IAM user or group policy allows it.
- Benefits:
  - **Centrally manage** policies across multiple AWS accounts
  - **Control access** to AWS services
  - **Automate** AWS account creation and management programmatically with APIs
  - **Consolidate billing** across multiple AWS accounts

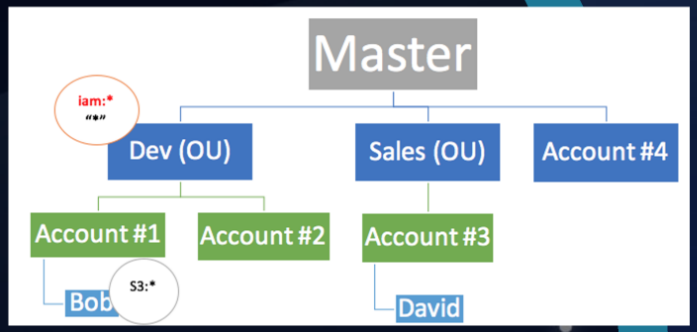


# AWS Organisations




- S3 Whitelisted
- IAM Policy access for S3 & EC2

- -> Bob can access S3 but not EC2




- IAM Blacklisted
- "*" Whitelisted
- IAM Policy access for S3

- -> Bob can access S3 but not IAM


aws certified
Cloud Practitioner
IAM, Organisations, & CloudTrail
AWS Organisations
IAM Policies
Users, Groups & Roles
Identity Federation
Shared Responsibility Model
AWS CloudTrail
AWS Certification Preparation
© BackSpace Technology LLC
BackSpace

# IAM Policies

- By default, users can't access anything in your account.
- Grant permissions through **policies** that define the effect, actions, resources, and optional conditions.

```
{
 "Version": "2012-10-17",
 "Statement": {
  "Effect": "Allow",
  "Action": "dynamodb:*",
  "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
 }
}
```



# IAM Policies

- By default, users can't access anything in your account.
- Grant permissions through **policies** that define the effect, actions, resources, and optional conditions.

```
{
 "Version": "2012-10-17",
 "Statement": {
  "Effect": "Allow",
  "Action": "dynamodb:*",
  "Resource": "arn:aws:dynamodb:us-west-2:123456789012:table/Books"
 }
}
```



# Amazon Resource Names (ARNs)

The access policy language requires you to specify the resource or resources using the following Amazon Resource Name (ARN) format:

**arn:aws:iam::account::resource** (note region missing)

**Examples:**

An IAM user in the account: **arn:aws:iam::123456789012:user/Paul**

An IAM user group: **arn:aws:iam::123456789012:group/Developers**

An IAM role: **arn:aws:iam::123456789012:role/S3Access**

A federated user identified in IAM as "Paul":

**arn:aws:sts::123456789012:federated-user/Paul**



# User- Based v Resource Based Policies

- **IAM policies** are attached to a user group, or role and specify the actions that are permitted and the resource (EC2 instance, RDS database etc.) that can be accessed.

- **Resource-based policies** (as opposed to IAM policies) are attached to a resource and only available for:
  - Amazon S3 buckets (bucket policies and ACL's),
  - Amazon Glacier vaults (vault access policies) ,
  - Amazon SNS topics ,
  - Amazon SQS queues, and
  - AWS Key Management Service encryption keys.




aws certified
Cloud Practitioner
IAM, Organisations, & CloudTrail
AWS Organisations
IAM Policies
Users, Groups & Roles
Identity Federation
Shared Responsibility Model
AWS CloudTrail
1
2
3
4
5
6
AWS Certification Preparation
© BackSpace Technology LLC
BackSpace

# Identity Federation

- An IAM role can be used to specify permissions for externally identified (federated) users.
- Max 5000 IAM users per account. Identity Federation enables unlimited temporary credentials.
- Identified by your organisation or a third-party identity provider .
- Methods of federating users:
  - Amazon **Cognito** developer authenticated identities, guest access or public identity service provider.
  - Public identity service providers or open ID connect (Facebook, Google, Amazon etc).
  - Identity provider software package that supports **SAML 2.0** (Security Assertion Markup Language)
  - Creating a custom identity broker application that authenticates users (e.g. with the enterprise's LDAP or active directory service. The application then assumes temporary credentials for the user.
  - AWS Directory Service for Active Directory and use this for enterprise and AWS access.



# Identity Federation

- An IAM role can be used to specify permissions for externally identified (federated) users.
- Max 5000 IAM users per account. Identity Federation enables unlimited temporary credentials.
- Identified by your organisation or a third-party identity provider .
- Methods of federating users:
  - Amazon **Cognito** developer authenticated identities, guest access or public identity service provider.
  - Public identity service providers or open ID connect (Facebook, Google, Amazon etc).
  - Identity provider software package that supports **SAML 2.0** (Security Assertion Markup Language)
  - Creating a custom identity broker application that authenticates users (e.g. with the enterprise's LDAP or active directory service. The application then assumes temporary credentials for the user.
  - AWS Directory Service for Active Directory and use this for enterprise and AWS access.