



IAM, Organisations, & CloudTrail

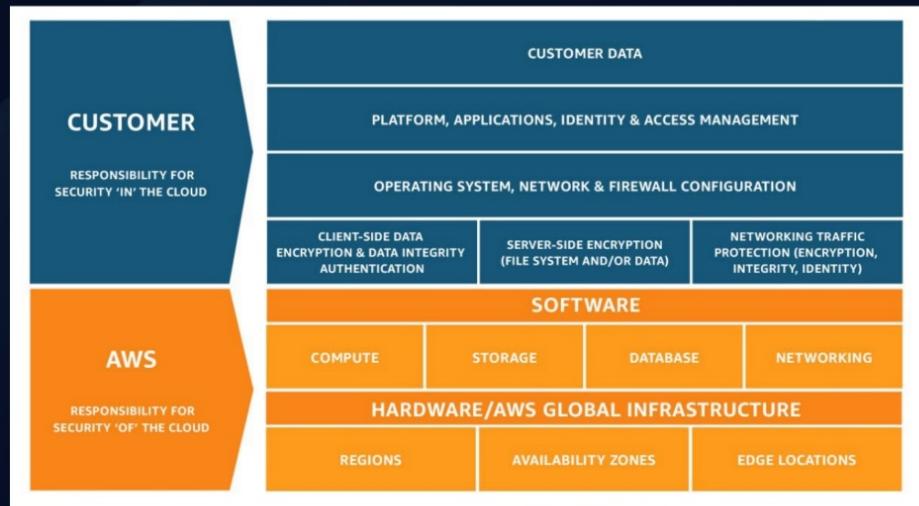
AWS Certification Preparation



© BackSpace Technology LLC

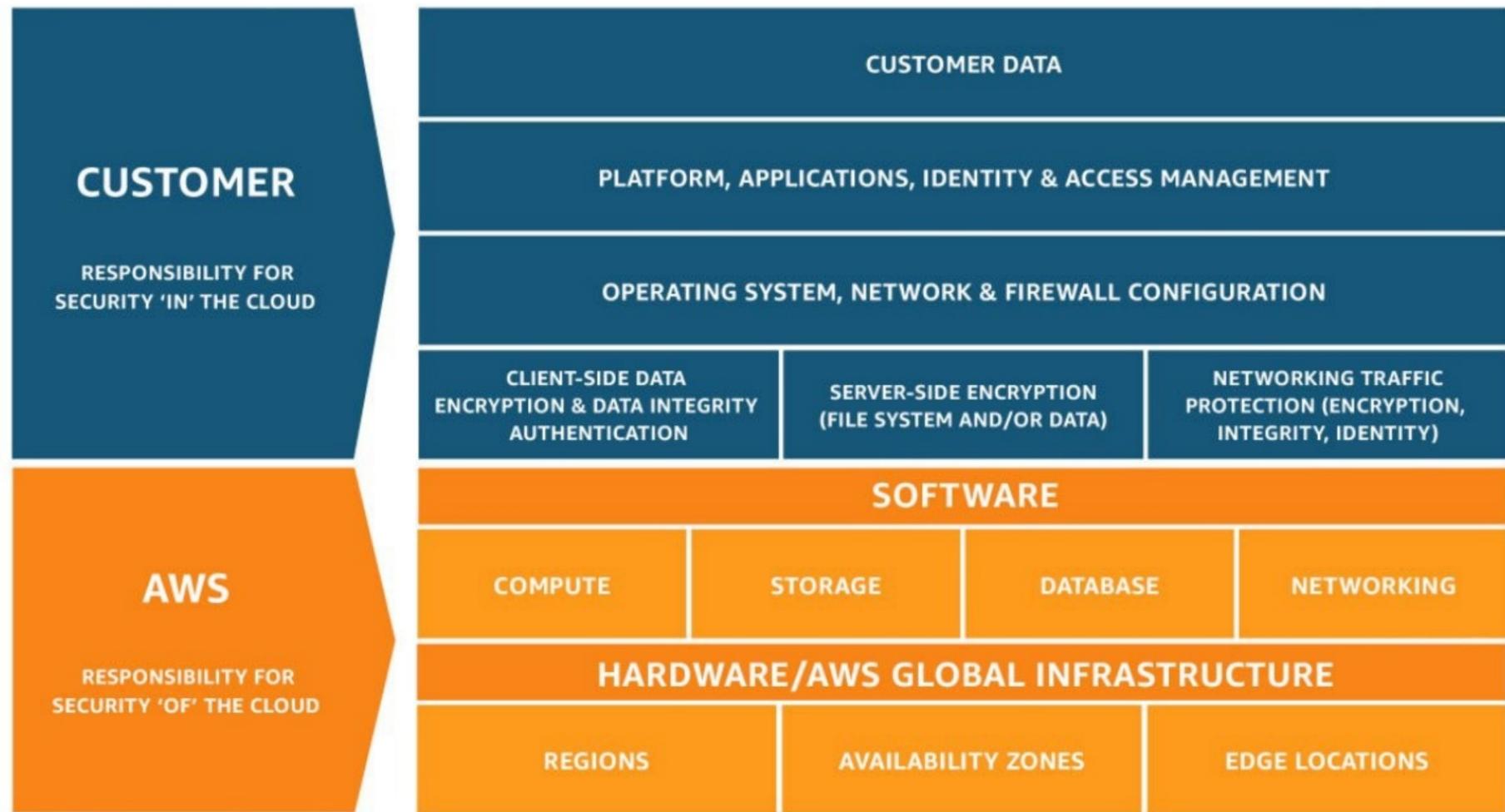


AWS Shared Responsibility Model

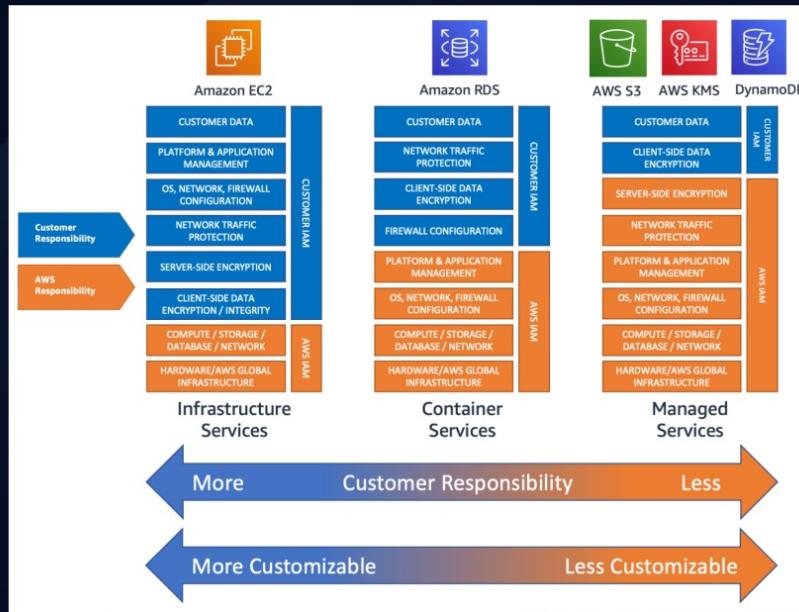


© BackSpace Technology LLC



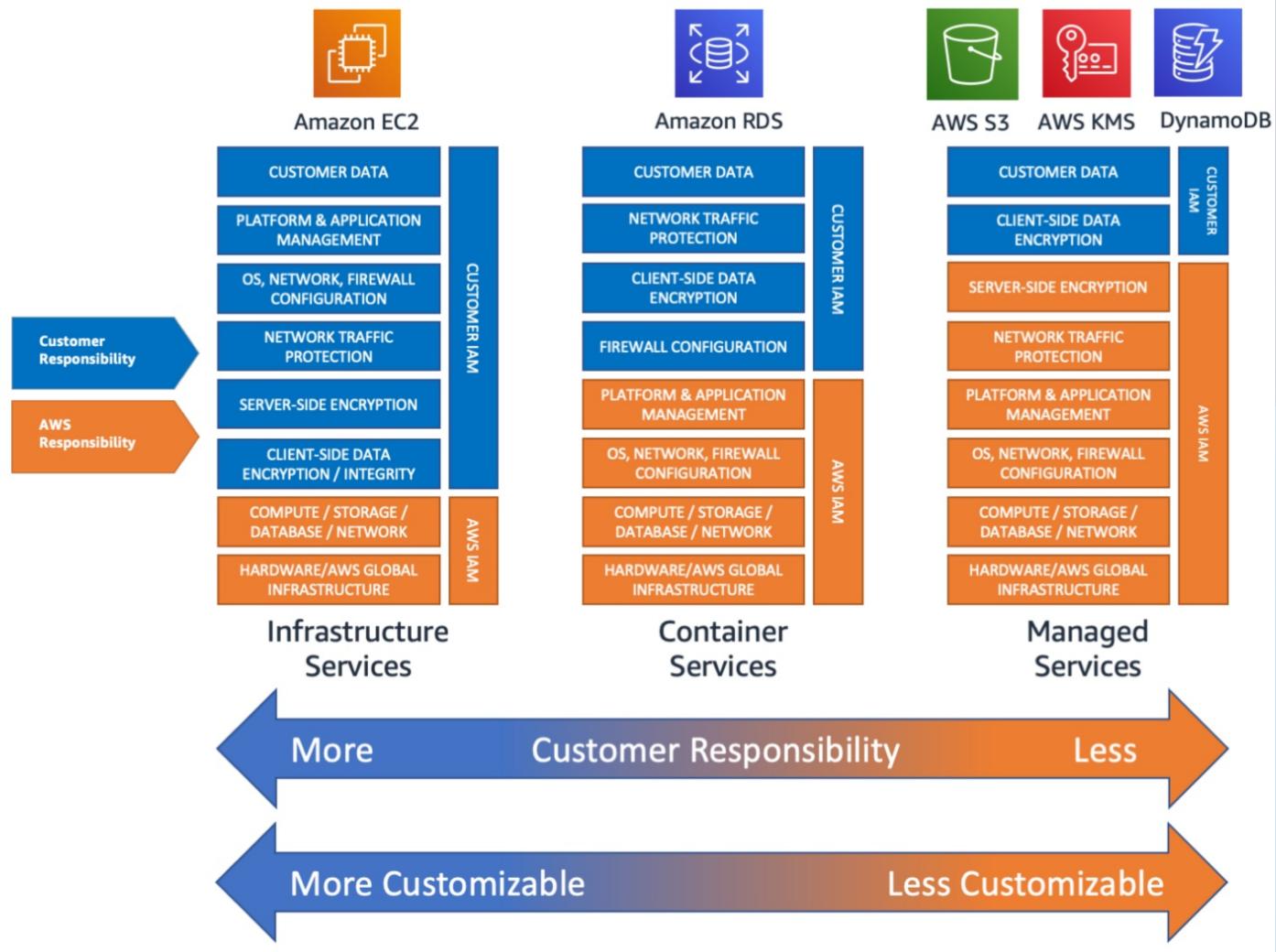


AWS Shared Responsibility Model

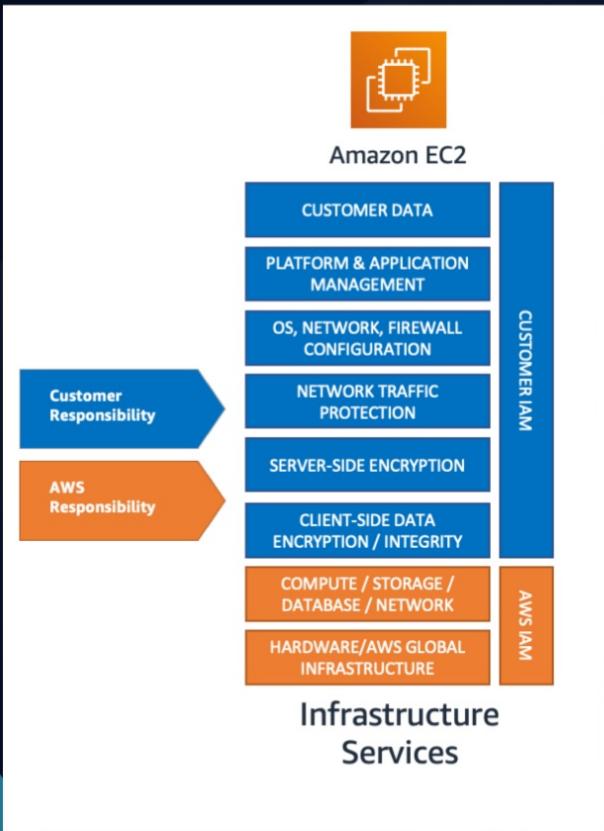


© BackSpace Technology LLC





Infrastructure Services



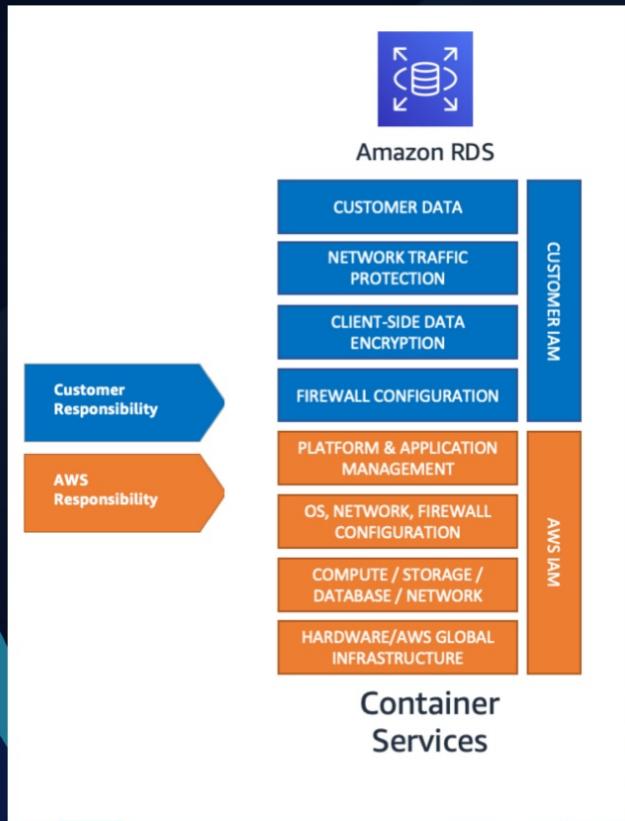
Infrastructure Services e.g.

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

© BackSpace Technology LLC



Container Services

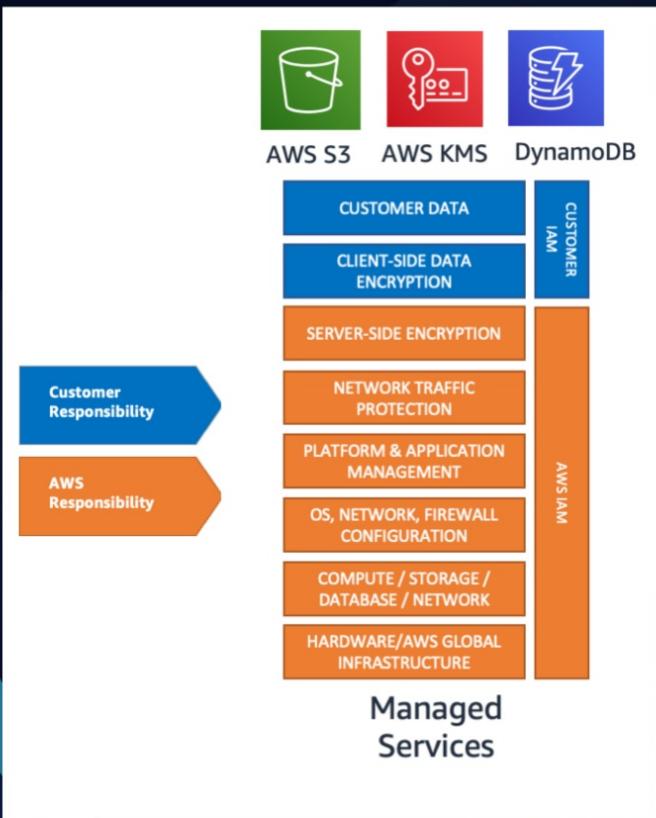


- Container Services e.g.
 - Amazon RDS
 - Amazon EMR,
 - AWS Elastic Beanstalk
- AWS provides a managed service
- **You** are responsible for:
 - network controls eg firewall rules
 - platform-level security separate from IAM

© BackSpace Technology LLC



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

© BackSpace Technology LLC



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

© BackSpace Technology LLC





IAM, Organisations, & CloudTrail

AWS Certification Preparation



© BackSpace Technology LLC



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.

© BackSpace Technology LLC



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.

© BackSpace Technology LLC



Sign In URL

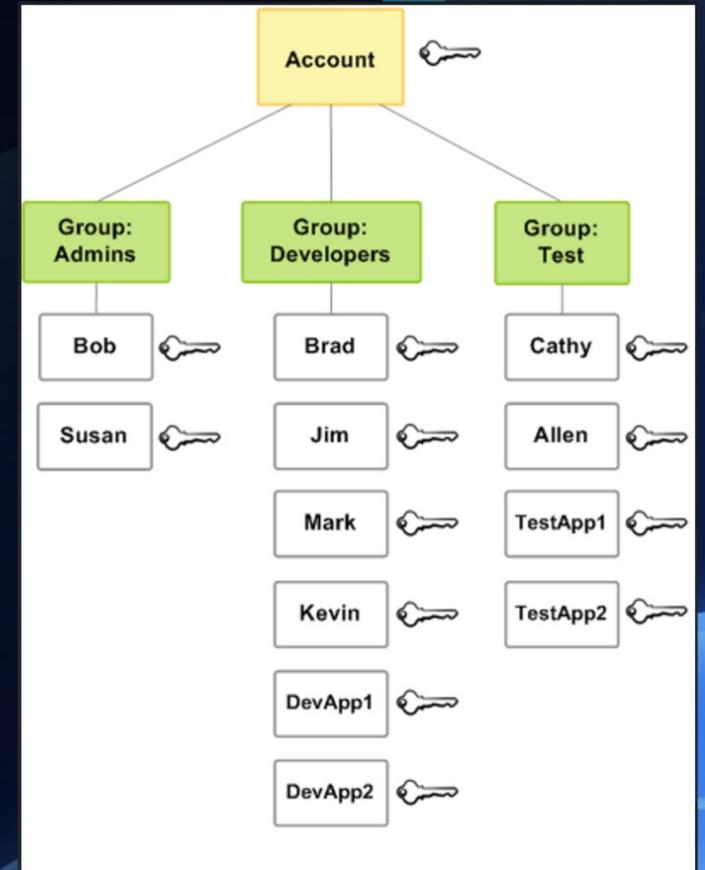
- Your sign-in page URL has the following format, by default.
 - https://Your_AWS_Account_ID.signin.aws.amazon.com/console/
- If you want the URL for your sign-in page to contain your company name (or other friendly identifier) instead of your AWS account ID, you can create an alias for your AWS account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

© BackSpace Technology LLC



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**.



© BackSpace Technology LLC



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

© BackSpace Technology LLC





IAM, Organisations, & CloudTrail

AWS Certification Preparation



© BackSpace Technology LLC



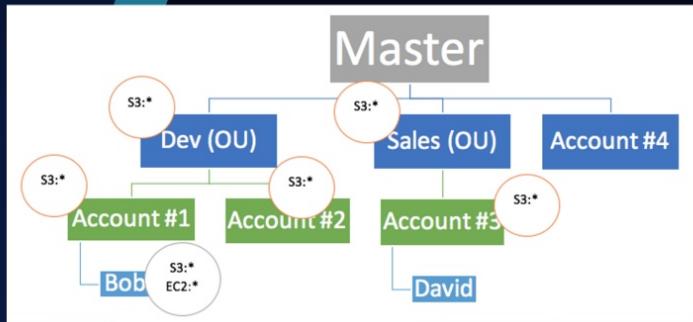
AWS Organisations

- 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

© BackSpace Technology LLC



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



IAM, Organisations, & CloudTrail

AWS Certification Preparation



© BackSpace Technology LLC



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

© BackSpace Technology LLC



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:
 - Amazon S3 buckets (bucket policies and ACL's) & Glacier vaults (access policies),
 - Amazon SNS topics & SQS queues, and
 - AWS Key Management Service encryption keys.
 - Full list at: docs.aws.amazon.com/IAM/latest/UserGuide/reference_aws-services-that-work-with-iam.html



IAM, Organisations, & CloudTrail

AWS Certification Preparation



© BackSpace Technology LLC



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.

© BackSpace Technology LLC





IAM, Organisations, & CloudTrail

AWS Certification Preparation

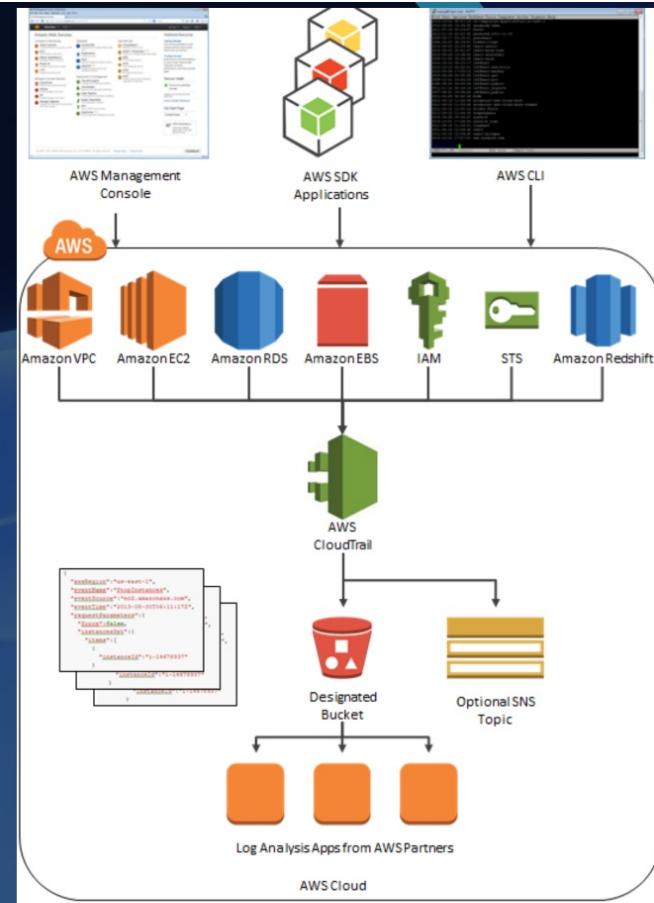


© BackSpace Technology LLC



AWS CloudTrail

- AWS Management Console, SDK and CLI all use the **AWS API** to communicate to AWS services.
- CloudTrail can **log calls** to AWS services from the AWS API.
- Logs are stored in a **bucket** and can be analysed (Amazon Athena, EMR etc).
- **SNS topic** can alert security issues.



© BackSpace Technology LLC



IAM Best Practices

- Lock Away Your AWS Account [Root User Access Keys](#)
- Create Individual [IAM Users](#)
- Use [Groups](#) to Assign Permissions to IAM Users
- Use [AWS Defined Policies](#) to Assign Permissions Whenever Possible
- Grant [Least Privilege](#)
- Use [Access Levels](#) to Review IAM Permissions (List, Read, Write, or Permissions management)
- Configure a Strong [Password Policy](#) for Your Users
- Enable [Multi-Factor Authentication \(MFA\)](#) for Privileged Users
- Delegate by Using [Roles](#) Instead of by Sharing Credentials
- Use [Roles for Applications](#) That Run on Amazon EC2 Instances
- [Rotate Credentials](#) Regularly
- Remove [Unnecessary Credentials](#)
- Use [Policy Conditions](#) for Extra Security (eg MFA login)
- [Monitor](#) Activity in Your AWS Account (eg CloudTrail)

© BackSpace Technology LLC



- Lock Away Your AWS Account **Root User Access Keys**
- Create Individual **IAM Users**
- Use **Groups** to Assign Permissions to IAM Users
- Use **AWS Defined Policies** to Assign Permissions Whenever Possible
- Grant **Least Privilege**
- Use **Access Levels** to Review IAM Permissions (List, Read, Write, or Permissions management)
- Configure a Strong **Password Policy** for Your Users
- Enable **Multi-Factor Authentication (MFA)** for Privileged Users
- Delegate by Using **Roles** Instead of by Sharing Credentials
- Use **Roles for Applications** That Run on Amazon EC2 Instances
- **Rotate Credentials** Regularly
- Remove **Unnecessary Credentials**
- Use **Policy Conditions** for Extra Security (eg MFA login)
- **Monitor** Activity in Your AWS Account (eg CloudTrail)



IAM, Organisations, & CloudTrail

AWS Certification Preparation



© BackSpace Technology LLC

