**AWS Basics Tutorial**

**Chapter 1: Getting Started with AWS**

**1. AWS Account Setup**

**Concept**

Amazon Web Services (AWS) is a cloud computing platform that provides a wide array of services. To use AWS, you need to create an account.

**Steps**

1. Go to <https://aws.amazon.com/>
2. Click on "Create an AWS Account"
3. Fill in your email address and a password
4. Choose an AWS account name (usually your company name or your name for personal use)
5. Fill in your contact information
6. Provide a valid credit card (you won't be charged unless you use services beyond the free tier)
7. Verify your identity via phone
8. Choose a support plan (select the basic plan for now, it's free)

**Hands-on Task**

Create your AWS account following the steps above. Once completed, you should be able to log into the AWS Management Console.

**2. Setting up Multi-Factor Authentication (MFA)**

**Concept**

MFA adds an extra layer of security to your account by requiring a second form of authentication besides your password.

**Steps**

1. Log into the AWS Management Console
2. Click on your account name in the top right corner, then "My Security Credentials"
3. Expand the "Multi-factor authentication (MFA)" section
4. Click "Activate MFA"
5. Choose "Virtual MFA device"
6. Install an MFA app on your phone (like Google Authenticator or Authy)
7. Scan the QR code with your MFA app
8. Enter two consecutive MFA codes from your app
9. Click "Assign MFA"

**Hands-on Task**

Set up MFA for your root account following the steps above. After this, you'll need to provide an MFA code when logging in.

**3. Identity and Access Management (IAM)**

**Concept**

IAM allows you to manage access to AWS services and resources securely. You can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

**Steps to Create an IAM User**

1. In the AWS Management Console, navigate to the IAM dashboard
2. Click "Users" in the left sidebar, then "Add user"
3. Set a username (e.g., "AdminUser")
4. Select "Programmatic access" and "AWS Management Console access"
5. Set a custom password or let AWS generate one
6. Click "Next: Permissions"
7. Choose "Attach existing policies directly"
8. Search for and select "AdministratorAccess"
9. Click through the next steps and create the user

**Hands-on Task**

Create an IAM user with administrative access. Note down the Access key ID and Secret access key provided at the end of the user creation process. You'll need these for programmatic access to AWS services.

**4. Launching EC2 Instances**

**Concept**

Amazon Elastic Compute Cloud (EC2) provides resizable compute capacity in the cloud. It's essentially a virtual server in the AWS ecosystem.

**Steps**

1. In the AWS Management Console, navigate to EC2
2. Click "Launch Instance"
3. Choose an Amazon Machine Image (AMI) - select "Amazon Linux 2 AMI"
4. Choose an instance type - select "t2.micro" (free tier eligible)
5. Configure instance details - use default settings
6. Add storage - use default settings
7. Add tags - add a tag with key "Name" and value "MyFirstEC2Instance"
8. Configure security group - create a new security group, allow SSH (port 22) from your IP
9. Review and launch
10. Create a new key pair, download it, and launch the instance

**Hands-on Task**

Launch an EC2 instance following the steps above. Once the instance is running, try to connect to it using SSH:

bash

Copy

chmod 400 your-key-pair.pem

ssh -i "your-key-pair.pem" ec2-user@your-instance-public-dns

Replace your-key-pair.pem with the path to your downloaded key pair, and your-instance-public-dns with your instance's public DNS (found in the EC2 dashboard).

**5. S3 Basics**

**Concept**

Amazon Simple Storage Service (S3) is an object storage service offering industry-leading scalability, data availability, security, and performance.

**Steps to Create a Bucket**

1. In the AWS Management Console, navigate to S3
2. Click "Create bucket"
3. Choose a globally unique bucket name (e.g., "my-first-s3-bucket-12345")
4. Choose a region
5. Leave other settings as default
6. Click "Create bucket"

**Steps to Upload an Object**

1. Click on your newly created bucket
2. Click "Upload"
3. Click "Add files" and select a file from your computer
4. Click "Upload"

**Hands-on Task**

Create an S3 bucket and upload a file to it. You can use this sample text file:

1. Create a file named sample.txt on your local machine with the following content:

Copy

Hello, AWS! This is my first S3 upload.

1. Upload this file to your S3 bucket following the steps above.
2. After uploading, try to download the file from the S3 console to verify it was uploaded correctly.

**6. Networking Basics**

**Concept**

Amazon Virtual Private Cloud (VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define.

**Steps to Create a VPC**

1. In the AWS Management Console, navigate to VPC
2. Click "Create VPC"
3. Choose "VPC and more"
4. Set a name tag (e.g., "MyFirstVPC")
5. Leave IPv4 CIDR block as default
6. Number of Availability Zones: 2
7. Number of public subnets: 2
8. Number of private subnets: 2
9. Leave other settings as default
10. Click "Create VPC"

**Hands-on Task**

Create a VPC following the steps above. After creation, explore the VPC dashboard to see the subnets, route tables, and internet gateway that were created.

**Conclusion**

Congratulations! You've now completed the basics of AWS. You've:

1. Set up an AWS account and secured it with MFA
2. Created an IAM user
3. Launched an EC2 instance
4. Created an S3 bucket and uploaded a file
5. Set up a VPC

These fundamental services form the backbone of many AWS-based applications and solutions. In the next chapters, we'll build on these basics to explore more advanced AWS services and concepts.

Remember to always be aware of the AWS services you're using to avoid unexpected charges. When you're done experimenting, make sure to terminate any running EC2 instances and delete any resources you no longer need.