AWS Cloud Computing Guide

1. Cloud Computing

Configuring Linux and Windows Virtual Servers

AWS offers Amazon EC2 (Elastic Compute Cloud) for virtual servers.

Tutorial:

1. Sign in to the AWS Management Console
2. Navigate to EC2 service
3. Click "Launch Instance"
4. Choose an Amazon Machine Image (AMI) - either Linux or Windows
5. Select an instance type
6. Configure instance details
7. Add storage
8. Configure security group
9. Review and launch

Resources:

- Amazon EC2 User Guide
- Launch an Amazon EC2 Instance

Configuring Linux and Windows Virtual Desktops

AWS provides Amazon WorkSpaces for virtual desktops.

Tutorial:

1. Set up a directory in AWS Directory Service
2. Navigate to Amazon WorkSpaces console
3. Launch WorkSpaces
4. Choose the directory
5. Select a bundle
6. Add user information
7. Review and launch

Resources:

- Amazon WorkSpaces Administration Guide
- Getting Started with Amazon WorkSpaces

Configuring Basic Network Services

Basic network services in AWS include DNS, DHCP, and VPN.

Tutorial for Route 53 (DNS):

1. Open the Route 53 console
2. Create a hosted zone
3. Create record sets

Resources:

- Amazon Route 53 Developer Guide
- VPN Setup Guide

2. Virtual Networks and Cloud Security

Configuring VPC

Amazon Virtual Private Cloud (VPC) lets you provision a logically isolated section of the AWS Cloud.

Tutorial:

1. Open the Amazon VPC console
2. Choose "Create VPC"
3. Select VPC and more
4. Configure VPC settings
5. Review and create

Resources:

- Amazon VPC User Guide
- Creating a VPC

Configuring Subnets

Subnets are ranges of IP addresses in your VPC.

Tutorial:

1. Open the Amazon VPC console
2. Choose "Subnets" in the navigation pane
3. Choose "Create subnet"
4. Select the VPC
5. Configure subnet settings
6. Create subnet

Resources:

- VPC and Subnet Basics

Configuring NAT

Network Address Translation (NAT) allows instances in a private subnet to connect to the internet.

Tutorial:

1. Open the Amazon VPC console

2. Navigate to "NAT Gateways"
3. Choose "Create NAT Gateway"
4. Select the subnet
5. Allocate an Elastic IP address
6. Create NAT Gateway

Resources:

- NAT Gateways

Configuring Gateways

Internet Gateways allow communication between your VPC and the Internet.

Tutorial:

1. Open the Amazon VPC console
2. Choose "Internet Gateways"
3. Choose "Create internet gateway"
4. Attach to your VPC

Resources:

- Internet Gateways

Configuring Firewalls

AWS provides several firewall options, including Security Groups and Network ACLs.

Tutorial for Security Groups:

1. Open the Amazon EC2 console
2. Choose "Security Groups" in the navigation pane
3. Choose "Create Security Group"
4. Configure rules
5. Create Security Group

Resources:

- Security Groups
- Network ACLs

Configuring Security Rules and Policies

AWS Identity and Access Management (IAM) helps you manage access to AWS services and resources securely.

Tutorial:

1. Open the IAM console
2. Choose "Policies"
3. Choose "Create policy"

4. Choose a service
5. Specify actions and resources
6. Review and create

Resources:

- IAM User Guide
- Creating IAM Policies

3. Cloud Storage and Databases

Configuring Databases

AWS offers various database services like Amazon RDS, DynamoDB, and Aurora.

Tutorial for Amazon RDS:

1. Open the Amazon RDS console
2. Choose "Create database"
3. Choose a database creation method
4. Configure settings
5. Create database

Resources:

- Amazon RDS User Guide
- Amazon DynamoDB Developer Guide

Configuring Cloud Storage

Amazon S3 (Simple Storage Service) is object storage built to store and retrieve any amount of data.

Tutorial:

1. Open the Amazon S3 console
2. Choose "Create bucket"
3. Configure bucket settings
4. Review and create

Resources:

- Amazon S3 User Guide
- Getting Started with Amazon S3

Configuring Access Rules and Policies

S3 bucket policies and IAM policies can be used to manage access to S3 resources.

Tutorial for S3 Bucket Policy:

1. Open the Amazon S3 console
2. Choose your bucket

3. Choose "Permissions"
4. Edit bucket policy
5. Add policy and save changes

Resources:

- Using Bucket Policies and User Policies

4. Infrastructure as Code (IaC) using Terraform

Terraform is an open-source IaC tool that can be used to provision and manage AWS resources.

Tutorial:

1. Install Terraform
2. Set up AWS credentials
3. Write Terraform configuration files (.tf)
4. Initialize Terraform working directory
5. Plan and apply the configuration

Example Terraform configuration for EC2 instance:

```
provider "aws" {
  region = "us-west-2"
}

resource "aws_instance" "example" {
  ami           = "ami-0c55b159cbfafe1f0"
  instance_type = "t2.micro"
}
```

Resources:

- Terraform Documentation
- Terraform AWS Provider Documentation
- Getting Started with Terraform on AWS