**Customer runbook/playbook to guide operational tasks**

This document/ready-reckoner acts as a guide for the routine operational tasks for the AWS Customers, as AWS continues to evolve its components and services these runbooks cover most of the routine operational tasks as a ready reference for everyone's benefit.

|  |  |  |
| --- | --- | --- |
| **Operational Tasks** | **Description** | **Steps** |
| **Create an EC2 Instance** | Provision a new EC2 instance for your application or workload. | 1. Open the EC2 console. <br> 2. Click "Launch Instance" to start the launch wizard. <br> 3. Select the desired Amazon Machine Image (AMI). <br> 4. Choose the instance type. <br> 5. Configure instance details, including network settings. <br> 6. Add storage and tags. <br> 7. Configure security groups. <br> 8. Review and launch the instance. |
| **Reference:** [**Launching an Instance**](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EC2_GetStarted.html) |  |  |
| **Create an S3 Bucket** | Create a new S3 bucket to store and manage objects. | 1. Open the S3 console. <br> 2. Click "Create bucket." <br> 3. Provide a unique bucket name and choose the region. <br> 4. Configure additional settings like versioning, logging, and encryption. <br> 5. Set permissions for the bucket. <br> 6. Review and create the bucket. |
| **Reference:** [**Creating a Bucket**](https://docs.aws.amazon.com/AmazonS3/latest/userguide/create-bucket-overview.html) |  |  |
| **Configure Auto Scaling** | Set up auto scaling to automatically adjust the number of EC2 instances based on demand. | 1. Open the EC2 Auto Scaling console. <br> 2. Click "Create Auto Scaling group." <br> 3. Configure the launch template or specify an existing instance. <br> 4. Configure scaling policies based on CPU utilization, network traffic, or other metrics. <br> 5. Set desired capacity and other scaling options. |
| **Reference:** [**Getting Started with Auto Scaling**](https://docs.aws.amazon.com/autoscaling/ec2/userguide/GettingStartedTutorial.html) |  |  |
| **Create an RDS Instance** | Provision a new RDS database instance for your application. | 1. Open the Amazon RDS console. <br> 2. Click "Create database." <br> 3. Choose the database engine and edition. <br> 4. Configure instance specifications and storage. <br> 5. Set up networking and security. <br> 6. Configure backup and maintenance settings. <br> 7. Review and create the database instance. |
| **Reference:** [**Creating an Amazon RDS DB Instance**](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_GettingStarted.html) |  |  |
| **Create an IAM User** | Create a new IAM user with appropriate permissions for access to AWS resources. | 1. Open the IAM console. <br> 2. Click "Users" in the navigation pane. <br> 3. Click "Add user." <br> 4. Enter the user details and select access type. <br> 5. Set permissions by attaching policies. <br> 6. Review and create the user. |
| **Reference:** [**Creating IAM Users**](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_create.html) |  |  |
| **Configure AWS CloudTrail** | Enable CloudTrail to log API activity and monitor changes to your AWS account. | 1. Open the AWS CloudTrail console. <br> 2. Click "Create trail." <br> 3. Specify trail details, including bucket and logging options. <br> 4. Configure advanced settings like data events and management events. <br> 5. Review and create the trail. |
| **Reference:** [**Creating a Trail with the Console**](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-a-trail-using-the-console-first-time.html) |  |  |
| **Create a VPC** | Create a new Virtual Private Cloud (VPC) to isolate and control your network resources. | 1. Open the Amazon VPC console. <br> 2. Click "Start VPC Wizard." <br> 3. Choose the VPC configuration (e.g., VPC with a single public subnet). <br> 4. Configure VPC details, including CIDR block and subnet IP ranges. <br> 5. Set up route tables, internet gateways, and security groups. |
| **Reference:** [**Getting Started with Amazon VPC**](https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html) |  |  |
| **Create an Application Load Balancer** | Set up an Application Load Balancer to distribute incoming traffic across multiple EC2 instances. | 1. Open the EC2 console. <br> 2. Click "Load Balancers" in the navigation pane. <br> 3. Click "Create Load Balancer." <br> 4. Select "Application Load Balancer." <br> 5. Configure the load balancer, including listeners, target groups, and security settings. <br> 6. Review and create the load balancer. |
| **Reference:** [**Getting Started with Application Load Balancers**](https://docs.aws.amazon.com/elasticloadbalancing/latest/application/application-load-balancer-getting-started.html) |  |  |
| **Enable AWS Config** | Enable AWS Config to assess, audit, and evaluate the configuration of your AWS resources. | 1. Open the AWS Config console. <br> 2. Click "Get started" to set up AWS Config. <br> 3. Choose the resources to be monitored. <br> 4. Configure the delivery channel for AWS Config rules. <br> 5. Review and enable AWS Config. |
| **Reference:** [**Getting Started with AWS Config**](https://docs.aws.amazon.com/config/latest/developerguide/getting-started.html) |  |  |
| **Configure Amazon S3 Lifecycle** | Set up lifecycle policies for automatic management of objects in your S3 bucket. | 1. Open the S3 console. <br> 2. Select the desired bucket. <br> 3. Click "Management" > "Lifecycle" in the bucket toolbar. <br> 4. Click "Add lifecycle rule." <br> 5. Define the rule with transition and expiration actions. <br> 6. Review and save the lifecycle rule. |
| **Reference:** [**How Do I Add an S3 Lifecycle Configuration?**](https://docs.aws.amazon.com/AmazonS3/latest/userguide/configure-lifecycle-examples.html) |  |  |
| **Create an Amazon CloudFront Distribution** | Set up a CloudFront distribution to deliver content globally with low latency. | 1. Open the CloudFront console. <br> 2. Click "Create Distribution." <br> 3. Choose the delivery method (web, RTMP, or custom). <br> 4. Configure origin settings and behaviors. <br> 5. Configure caching, security, and logging settings. <br> 6. Review and create the distribution. |
| **Reference:** [**Creating a Web Distribution**](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-creating-console.html) |  |  |
| **Set up AWS Lambda Function** | Create a Lambda function to run serverless code in response to events or on a schedule. | 1. Open the AWS Lambda console. <br> 2. Click "Create function." <br> 3. Choose the authoring method (code or blueprint). <br> 4. Configure function details, including runtime, permissions, and environment variables. <br> 5. Write or upload the function code. <br> 6. Review and create the function. |
| **Reference:** [**Create a Simple Lambda Function**](https://docs.aws.amazon.com/lambda/latest/dg/getting-started-create-function.html) |  |  |
| **Configure AWS CloudWatch Alarms** | Set up CloudWatch alarms to monitor metrics and receive notifications when thresholds are breached. | 1. Open the CloudWatch console. <br> 2. Click "Alarms" in the navigation pane. <br> 3. Click "Create alarm." <br> 4. Configure the alarm conditions, including metric, threshold, and actions. <br> 5. Set up notification preferences. <br> 6. Review and create the alarm. |
| **Reference:** [**Creating Amazon CloudWatch Alarms**](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html) |  |  |
| **Enable AWS Trusted Advisor** | Activate and use AWS Trusted Advisor to get real-time guidance on optimizing your AWS environment. | 1. Open the Trusted Advisor console. <br> 2. Click "Get started." <br> 3. Review the available checks and enable them. <br> 4. Monitor the Advisor Dashboard for recommendations. <br> 5. Take actions based on the recommendations provided. |
| **Reference:** [**AWS Trusted Advisor Documentation**](https://aws.amazon.com/premiumsupport/technology/trusted-advisor/) |  |  |
| **Enable AWS Shield** | Activate AWS Shield to protect your applications against DDoS attacks. | 1. Open the AWS WAF & Shield console. <br> 2. Click "Get started" for AWS Shield Standard or Advanced. <br> 3. Follow the setup wizard to enable DDoS protection for your resources. <br> 4. Monitor the protection status and take actions if attacks are detected. |
| **Reference:** [**Getting Started with AWS Shield**](https://docs.aws.amazon.com/waf/latest/developerguide/getting-started.html) |  |  |
| **Set up AWS CloudFormation Stack** | Use CloudFormation to create and manage AWS resources using infrastructure as code. | 1. Open the CloudFormation console. <br> 2. Click "Create stack." <br> 3. Select a template source (e.g., template file, AWS S3 URL). <br> 4. Configure stack options, including parameters and tags. <br> 5. Review and create the stack. |
| **Reference:** [**Getting Started with AWS CloudFormation**](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html) |  |  |
| **Configure AWS Simple Email Service (SES)** | Set up AWS SES to send and receive email using AWS services. | 1. Open the AWS SES console. <br> 2. Click "Email Addresses" or "SMTP Settings" to configure sending or receiving emails. <br> 3. Follow the prompts to verify domains or configure SMTP settings. <br> 4. Test email sending and receiving functionality. <br> 5. Monitor email metrics and troubleshoot issues. |
| **Reference:** [**Getting Started with AWS SES**](https://docs.aws.amazon.com/ses/latest/DeveloperGuide/Welcome.html) |  |  |
| **Create an AWS SNS Topic** | Set up an SNS topic to send notifications to subscribers via email, SMS, or other endpoints. | 1. Open the Amazon SNS console. <br> 2. Click "Topics" in the navigation pane. <br> 3. Click "Create topic." <br> 4. Enter a topic name and display name. <br> 5. Configure topic policies and access control. <br> 6. Review and create the topic. |
| **Reference:** [**Creating an Amazon SNS Topic**](https://docs.aws.amazon.com/sns/latest/dg/sns-getting-started.html) |  |  |
| **Configure AWS Secrets Manager** | Use Secrets Manager to securely store and manage sensitive information, such as database credentials. | 1. Open the Secrets Manager console. <br> 2. Click "Store a new secret." <br> 3. Select the secret type (e.g., database credentials). <br> 4. Enter the secret details and configuration. <br> 5. Set up rotation and access control. <br> 6. Review and create the secret. |
| **Reference:** [**Getting Started with AWS Secrets Manager**](https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html) |  |  |
| **Configure AWS Step Functions** | Set up Step Functions to build and run workflows for coordinating AWS services. | 1. Open the AWS Step Functions console. <br> 2. Click "Create state machine." <br> 3. Design the state machine using the visual workflow editor. <br> 4. Define states, transitions, and inputs/outputs. <br> 5. Configure logging, tracing, and IAM roles. <br> 6. Review and create the state machine. |
| **Reference:** [**Getting Started with AWS Step Functions**](https://docs.aws.amazon.com/step-functions/latest/dg/getting-started.html) |  |  |
| **Set up AWS CodePipeline** | Use CodePipeline to create continuous delivery pipelines for automating software release processes. | 1. Open the AWS CodePipeline console. <br> 2. Click "Create pipeline." <br> 3. Specify pipeline details, including source, build, and deployment stages. <br> 4. Configure pipeline settings and options. <br> 5. Review and create the pipeline. |
| **Reference:** [**Getting Started with AWS CodePipeline**](https://docs.aws.amazon.com/codepipeline/latest/userguide/welcome.html) |  |  |
| **Configure AWS Glue** | Set up AWS Glue to discover, catalog, and transform your data for analytics and data processing. | 1. Open the AWS Glue console. <br> 2. Click "Crawlers" or "Jobs" to create a crawler or ETL job, respectively. <br> 3. Configure the crawler or job settings, including data source, transformation logic, and output. <br> 4. Schedule or run the crawler or job. <br> 5. Monitor and troubleshoot job runs. |
| **Reference:** [**AWS Glue Developer Guide**](https://docs.aws.amazon.com/glue/latest/dg/welcome.html) |  |  |
| **Enable AWS CloudFormation StackSets** | Use CloudFormation StackSets to deploy and manage CloudFormation stacks across multiple accounts and regions. | 1. Open the CloudFormation console. <br> 2. Click "StackSets" in the navigation pane. <br> 3. Click "Create StackSet." <br> 4. Specify the stack template and configuration settings. <br> 5. Select target accounts and regions. <br> 6. Review and create the StackSet. |
| **Reference:** [**AWS CloudFormation StackSets User Guide**](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/what-is-cfnstacksets.html) |  |  |
| **Configure AWS Certificate Manager** | Set up ACM to provision, manage, and deploy SSL/TLS certificates for your applications. | 1. Open the ACM console. <br> 2. Click "Request a certificate." <br> 3. Choose the certificate type and domain validation method. <br> 4. Configure domain names and additional settings. <br> 5. Review and confirm the certificate request. <br> 6. Use the certificate in your application or with other AWS services. |
| **Reference:** [**Getting Started with AWS Certificate Manager**](https://docs.aws.amazon.com/acm/latest/userguide/welcome.html) |  |  |
| **Configure AWS Cloud9** | Set up Cloud9, an integrated development environment (IDE) in the cloud. | 1. Open the Cloud9 console. <br> 2. Click "Create environment." <br> 3. Specify environment details, including name, description, and settings. <br> 4. Choose the instance type and platform. <br> 5. Review and create the environment. <br> 6. Access and use the Cloud9 IDE for development. |
| **Reference:** [**AWS Cloud9 Documentation**](https://docs.aws.amazon.com/cloud9/latest/user-guide/welcome.html) |  |  |
| **Configure AWS Chatbot** | Set up AWS Chatbot to receive notifications and interact with AWS services using chat tools. | 1. Open the AWS Chatbot console. <br> 2. Click "Configure clients" to set up chat integrations (e.g., Slack, Microsoft Teams). <br> 3. Follow the instructions to configure the chat client. <br> 4. Enable notifications and manage subscriptions for AWS services. |
| **Reference:** [**Getting Started with AWS Chatbot**](https://docs.aws.amazon.com/chatbot/latest/adminguide/what-is.html) |  |  |
| **Enable AWS X-Ray** | Activate X-Ray to analyze and debug distributed applications, microservices, and serverless applications. | 1. Open the X-Ray console. <br> 2. Click "Get started" to enable X-Ray for your application. <br> 3. Instrument your application code to emit X-Ray traces. <br> 4. Analyze and visualize traces in the X-Ray console. |
| **Reference:** [**Getting Started with AWS X-Ray**](https://docs.aws.amazon.com/xray/latest/devguide/aws-xray.html) |  |  |

Note: The steps provided above are high-level and may require additional configuration based on your specific requirements. Please refer to the respective AWS documentation links for more detailed information on each task.