****This study guide is based on the video lesson available on TrainerTests.com****

Creating and Managing an AWS Free Tier Account Study Guide

Introduction to AWS

Amazon Web Services (AWS) is one of the leading cloud platforms, offering a broad set of global computing, storage, database, analytics, application, and deployment services. AWS allows users to scale their infrastructure on-demand and pay only for the services they use, making it a popular choice for individuals, startups, and large organizations alike. However, the pay-per-use model means that careful management of resources is crucial, especially when utilizing the AWS Free Tier.

AWS Free Tier Overview

The AWS Free Tier allows new customers to explore and use AWS services at no cost, up to certain usage limits, for the first 12 months following the account creation. It offers free access to over 85 products and services, including popular offerings such as Amazon EC2 (compute instances), Amazon S3 (storage), and Amazon RDS (databases). While the Free Tier provides ample room to experiment and develop, exceeding the usage limits will result in charges, so it's important to monitor usage closely.

Signing Up for an AWS Account

Step-by-Step Process

1. **Access the AWS Free Tier Website**: Begin by navigating to AWS Free Tier and clicking on the "Create a Free Account" button. This will lead you to the AWS sign-up page.
2. **Enter Your Email Address and Root User Information**: AWS requires you to provide an email address for the root user. The root user has full access to all AWS services and account settings. Be aware that this is the most powerful account type, so you must protect it by using a strong, secure password. Once you've entered your email and account name, you'll receive a verification code sent to your email address. Enter the code to confirm ownership of the email.
3. **Set Up Your Password**: After verifying your email, you'll need to create a password for the root account. Make sure this password is strong, following AWS's security guidelines to protect your account.
4. **Choose Your Account Type**: AWS provides two account types: Personal and Business. While the account type you choose affects the billing format and support options, both personal and business accounts provide access to the same set of AWS services.

5. **Enter Personal Information**: Fill in your contact details, including your name, address, and phone number. This information is important for billing and account management.
6. **Provide Payment Information**: Although the AWS Free Tier is free within specified limits, you must provide a valid credit card during account creation. This ensures AWS can bill you if you exceed Free Tier usage limits. AWS will make a small temporary charge to your card (usually $1) to verify your payment method, but this charge will be refunded.
7. **Identity Verification**: AWS will ask you to verify your identity by either a text message or phone call. You'll need to enter your phone number and select how you want to receive a verification code. Once you get the code, enter it on the AWS sign-up page.
8. **Choose a Support Plan**: AWS offers various support plans, including:
    - **Basic** (free): Includes 24/7 access to customer service, AWS documentation, whitepapers, and support forums.
    - **Developer, Business, and Enterprise Support**: Paid options with faster response times and more advanced features.

    For most users starting out, the **Basic** support plan will be sufficient.

9. **Complete the Account Setup**: Once you've confirmed your support plan, click on "Complete Sign-Up." Congratulations, you've now created your AWS account!

Managing Your AWS Free Tier Account

Once your account is created, you can log in to the AWS Management Console using your root user credentials. Here, you can access all of AWS's services and begin provisioning resources such as virtual machines (EC2 instances), storage (S3), or databases (RDS). However, managing your Free Tier usage is critical to avoid incurring unexpected charges.

AWS Free Tier Usage and Billing

While AWS Free Tier provides free access to many services, each service has its own usage limits. For instance, the Free Tier includes:

- **750 hours/month of EC2 compute time** (enough to run one EC2 instance full-time for a month).
- **5 GB of S3 storage**.
- **750 hours/month of RDS usage**.

Exceeding these limits will result in charges based on AWS's standard pricing for the services. Therefore, it's important to monitor your usage regularly to stay within the Free Tier limits.

Setting Up Billing Alerts

To help manage your usage and costs, AWS provides tools for monitoring your Free Tier usage and setting up billing alerts.

1. **Access the Billing Dashboard**: Once logged in, you can type "Billing" into the AWS Management Console's search bar and navigate to the Billing Dashboard.
2. **Free Tier Usage Monitoring**: Within the Billing Dashboard, you'll find a section dedicated to Free Tier usage. Here, AWS provides a breakdown of your current service usage against Free Tier limits. This allows you to see how much of your Free Tier allocation you've used for each service, helping you avoid unintentional overuse.

3. **Set Up Billing Alerts**: Under Billing Preferences, you can enable billing alerts. These alerts allow AWS to notify you when your estimated usage approaches or exceeds the Free Tier limits or when your charges exceed a specified threshold. AWS will send an email to the root user when the alert conditions are met, providing you with an early warning about potential costs.
    - **Enable Free Tier Usage Alerts**: AWS can automatically send notifications when you're close to exceeding your Free Tier limits.
    - **Set Billing Threshold Alerts**: For more control, you can set a specific dollar amount, and AWS will notify you if your bill exceeds that amount. This can be particularly useful to ensure you don't incur large charges unexpectedly.

Root User vs. IAM Users

The **root user** is the account owner and has full access to all AWS services, including billing and management. While you can perform any task as the root user, it's a best practice to create separate user accounts for everyday activities. This is where **Identity and Access Management (IAM)** comes into play.

Why Avoid Using the Root User for Daily Operations?

Using the root user for routine tasks increases security risks since this account has unrestricted access to all services and resources. If the root user credentials were compromised, an attacker could potentially cause serious damage to your AWS infrastructure.

Creating IAM Users

IAM allows you to create separate users for different tasks or team members, each with specific permissions. For instance, you could create an IAM user who only has access to launch EC2 instances, or one that can only manage billing information.

1. **Access IAM in the AWS Console**: Type "IAM" into the search bar and navigate to the IAM Dashboard.
2. **Create a New User**: Click on "Users" and then "Add User." You'll be prompted to create a username and set access levels. You can choose between **Programmatic access** (for command-line tools, SDKs, or APIs) and **AWS Management Console access** (for the web-based console).
3. **Assign Permissions**: IAM offers a wide range of pre-configured policies to assign permissions to the user. You can grant administrative access or limit access to specific services like EC2, S3, or RDS.
4. **Create Access Keys for Programmatic Access**: If you need the user to interact with AWS services via the CLI or SDKs, create an access key and secret access key for the IAM user. These keys allow the user to authenticate without needing a password.
5. **Review and Complete**: After assigning permissions, review the user's configuration and click "Create User."

Security Best Practices

- **Enable Multi-Factor Authentication (MFA)** for both the root user and IAM users to add an extra layer of security.
- **Regularly rotate access keys** for programmatic users to prevent unauthorized access.
- **Audit your IAM policies and users** regularly to ensure that permissions are correctly set.

Conclusion

Creating an AWS account and understanding how to manage it is the first step toward leveraging AWS cloud services. The AWS Free Tier offers a valuable opportunity to experiment with a wide range of services at no cost, but it's important to monitor your usage closely to avoid unexpected charges. By using billing alerts, IAM for secure user management, and the root account only for essential tasks, you can maintain a secure and cost-effective AWS environment as you explore the cloud.