Checkout: Pravin Mishra's AWS University

Subscribe: My AWS Youtube Channel (AWS with Pravin Mishra)

10 AWS Account-related Best Practices

1. Use AWS Organizations:

AWS Organizations allows you to centrally manage and enforce policies for multiple AWS accounts. This makes it easier to manage access, compliance, and security for all of your AWS resources.

What:

AWS Organizations is a service that allows you to manage and control multiple AWS accounts from a single parent account.

Why:

It simplifies billing across multiple accounts, allows for better resource and policy management, and enforces compliance across all accounts.

How:

Create an organization from the AWS Management Console, invite or create new member accounts, then apply service control policies (SCPs) to centrally control AWS services across multiple AWS accounts.

Not Using AWS Organizations:

Not leveraging AWS Organizations can lead to a decentralized and inefficient management of AWS accounts. This could result in difficulty in enforcing consistent policies and monitoring across accounts, potentially leading to security vulnerabilities or non-compliance issues.

2. Set up Multi-Factor Authentication (MFA)

It's always a good practice to have MFA enabled for all root and IAM users in your AWS account. This adds an extra layer of security that helps protect your AWS resources.

What:

MFA is a security feature that requires users to present two separate forms of identification before they can access an account.

Why:

It provides an additional layer of security by preventing unauthorized access even if a password is compromised.

How:

Go to the IAM console, select the user, then go to the Security Credentials tab and assign an MFA device.

Not Setting up Multi-Factor Authentication (MFA):

If MFA is not set up, your account becomes vulnerable to unauthorized access if your login credentials are compromised. An attacker may gain access to your AWS resources and could misuse them, leading to potential data breaches or financial loss.

3. Follow the Principle of Least Privilege:

Each IAM user should have the minimal amount of privileges necessary to perform their job. This minimizes the potential damage if an account is compromised.

What:

This principle implies giving an IAM user the minimal amount of permissions necessary to perform their job.

Why:

This minimizes the potential damage if an account is compromised.

How:

When creating IAM roles or policies, only allow necessary services and actions. Regularly review and reduce permissions where necessary.

Not Following the Principle of Least Privilege:

Providing unnecessary permissions can lead to misuse, either intentionally or accidentally. A compromised user with excessive permissions could lead to a much larger security incident, such as widespread data loss or unauthorized modifications.

4. **Regularly Rotate Security Credentials:**

Regularly change and rotate security credentials to mitigate the risk of credentials being misused.

What:

This means changing your access keys (both access key ID and secret access key) regularly.

Why:

Regular rotation reduces the risk of keys being misused if they are accidentally exposed.

How:

For IAM users, create a new access key, replace all instances of the old key with the new one, then deactivate and eventually delete the old key.

Not Regularly Rotating Security Credentials:

If access keys are not regularly rotated, a key that was unknowingly compromised could provide ongoing unauthorized access to your AWS resources. This could lead to misuse of your resources, data breaches, or unexpected charges.

5. **Enable AWS CloudTrail:**

AWS CloudTrail records AWS API calls for your account. These logs can provide valuable information for auditing and reviewing account activity.

What:

CloudTrail is a service that records AWS API calls for your account.

Why:

This information can help with auditing, compliance, operational troubleshooting, and investigating security incidents.

How:

Enable CloudTrail in the AWS Management Console, specify an S3 bucket for the logs, and enable logging across all regions.

Not Enabling AWS CloudTrail:

Without CloudTrail, you lose visibility into activity within your AWS environment. This could hinder your ability to investigate security incidents, troubleshoot operational issues, or maintain regulatory compliance.

6. Implement Billing Alerts:

Set up AWS Budgets to send you alerts when your usage exceeds predefined cost and usage thresholds. This can help avoid unexpected charges.

What:

AWS Budgets lets you set custom cost and usage budgets that alert you when your usage exceeds your budgeted amount.

Why:

This can help avoid unexpected charges on your AWS bill.

How:

From the AWS Budgets dashboard, create a new budget, set your budget parameters, and define alert thresholds.

Not Implementing Billing Alerts:

Without billing alerts, you might not notice cost overruns until after they've occurred. This could lead to unexpected charges that could have been prevented with early notification.

7. Securely Store Access Keys

Never embed access keys directly into your code or check them into your source code repositories. Use IAM roles and instance profiles for applications running on Amazon EC2.

What:

Access keys consist of an access key ID and a secret access key, used to programmatically access AWS services.

Why:

Insecure handling of access keys can lead to unauthorized access or misuse of your AWS resources.

How:

Do not hardcode keys into your applications. Instead, use AWS's built-in mechanisms for managing keys such as IAM roles, or use environment variables or configuration files.

Not Securely Storing Access Keys:

If access keys are embedded in code or not securely stored, they could be accidentally exposed or discovered by unauthorized individuals. This could provide unauthorized access to your AWS resources, potentially leading to misuse or data breaches.

8. Use Service Control Policies (SCPs)

SCPs allow you to define which AWS service APIs can and cannot be executed by AWS Identity and Access Management (IAM) entities (users and roles) in your account.

What:

SCPs are a type of policy that you can use to manage permissions in your organization.

Why:

They provide central control over the maximum available permissions for all accounts in your organization.

How:

From the AWS Organizations console, you can create SCPs and attach them to an organization, organizational unit (OU), or individual AWS account.

Not Using Service Control Policies (SCPs):

Without SCPs, you lack a centralized mechanism to enforce permission guardrails across your AWS accounts. This could lead to users or roles having broader access than necessary, which increases the risk of accidental or malicious misuse.

9. Implement Regular Audits:

Regularly review and audit your AWS resources and settings. This includes checking for unused resources, reviewing security groups and network access rules, and ensuring your IAM policies are up to date.

What:

Regular reviews and audits of your AWS resources and settings.

Why:

This can help ensure your resources are being used effectively, cost-efficiently, and securely.

How:

Use services like AWS Trusted Advisor and AWS Config to regularly check your AWS environment for any deviations from best practices.

Not Implementing Regular Audits:

Without regular audits, you may miss opportunities to optimize resource usage, reduce costs, or identify and fix security vulnerabilities. This could lead to inefficient resource use, unnecessary costs, or increased risk of security incidents.

10. Use Encryption:

Use AWS's encryption capabilities to protect your data at rest and in transit. This includes using AWS Key Management Service (KMS) for key management, and encrypting data in storage and databases, as well as data being transferred.

What:

Encryption is the process of converting plaintext data into ciphertext to prevent unauthorized access.

Why:

Encrypting data at rest and in transit can protect it from unauthorized access.

How:

Use AWS Key Management Service (KMS) to manage cryptographic keys used for encrypting data. When creating storage resources such as S3 buckets or EBS volumes, enable encryption options.

Not Using Encryption:

If data is not encrypted, it's more vulnerable to unauthorized access. If a storage device or transmission is intercepted, unencrypted data could be read and potentially misused, leading to data breaches and non-compliance with regulations.