	**Checkout:** Pravin Mishra's AWS University **Subscribe:** My AWS Youtube Channel (AWS with Pravin Mishra)

30 AWS Production Account: Best Practice that every **Cloud Engineer** should know

1. Establishing a Separate Production Account

What is it?

It's creating a separate AWS account specifically for production workloads.

Why use it?

It isolates production resources from development and test environments, reducing the risk of accidental changes or deletions.

How to use it?

Create a new AWS account and move all production resources into this account. Use AWS Organizations for centralized management.

Not using then be ready with?

You risk inadvertent changes affecting your production environment, which could cause downtime or loss of data.

2. Enforcing Strong Access Controls

What is it?

Implementing strict IAM policies and roles to limit who can access what in your AWS production account.

Why use it?

To ensure only authorized users can access and modify production resources.

How to use it?

Use IAM policies and roles to limit access. Consider using AWS Managed Policies for job functions for predefined roles.

Not using then be ready with?

Unwanted changes or potential security breaches due to overly broad permissions.

3. Implementing AWS CloudTrail

What is it?

AWS CloudTrail is a service that provides event history of your AWS account activity.

Why use it?

It helps with security analysis, resource change tracking, and compliance auditing.

How to use it?

Enable CloudTrail in your AWS production account to start logging activities.

Not using then be ready with?

Difficulty in tracking resource changes and challenges in identifying security issues or meeting compliance requirements.

4. Using Amazon GuardDuty

What is it?

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity.

Why use it?

To identify and alert on potential security threats and suspicious activities.

How to use it?

Enable GuardDuty in your AWS production account. It uses machine learning and anomaly detection to find threats.

Not using then be ready with?

Increased risk of undetected malicious activities or compromised resources.

5. Enabling AWS Config

What is it?

AWS Config is a service that provides a detailed inventory of your AWS resources and configuration.

Why use it?

It helps you analyze your resources, manage changes, and audit your environment for compliance.

How to use it?

Enable AWS Config in your AWS production account. Use Config Rules to automatically check for compliance.

Not using then be ready with?

Loss of visibility into resource configurations and changes, and challenges in demonstrating compliance.

	**Checkout:** Pravin Mishra's AWS University **Subscribe:** My AWS Youtube Channel (AWS with Pravin Mishra)

6. Applying Service Control Policies (SCPs)

What is it?

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

Why use it?

To centrally control AWS service use across multiple AWS accounts.

How to use it?

Create and apply SCPs from your AWS Organizations master account.

Not using then be ready with?

Difficulty managing cross-account permissions and potential for unauthorized use of AWS services.

7. Establishing a Backup and Recovery Plan

What is it?

A strategic plan to backup AWS resources and recover them in the event of a loss or failure.

Why use it?

To ensure business continuity and data protection.

How to use it?

Use AWS Backup to centrally manage backups, and create a recovery plan that fits your business needs.

Not using then be ready with?

Risk of data loss and prolonged downtime in the event of a disaster.

	**Checkout:** Pravin Mishra's AWS University **Subscribe:** My AWS Youtube Channel (AWS with Pravin Mishra)

8. Implementing AWS Shield

What is it?

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service.

Why use it?

To protect your applications running on AWS from DDoS attacks.

How to use it?

Enable AWS Shield on your production account and apply it to the resources you want to protect.

Not using then be ready with?

Increased risk of your application becoming unavailable during DDoS attacks.

9. Setting up AWS Systems Manager

What is it?

AWS Systems Manager offers a unified interface to manage AWS resources.

Why use it?

It simplifies resource and application management, shortens time to detect and resolve operational problems.

How to use it?

Use Systems Manager services like OpsCenter, Patch Manager, and Automation in your production account.

Not using then be ready with?

Increased operational overhead and potential delays in problem resolution.

	**Checkout:** Pravin Mishra's AWS University **Subscribe:** My AWS Youtube Channel (AWS with Pravin Mishra)

10. Implementing Amazon Macie

What is it?

Amazon Macie is a fully managed data privacy and security service that uses machine learning and pattern matching to discover and protect sensitive data.

Why use it?

To protect sensitive data in AWS.

How to use it?

Enable Amazon Macie in your production account and configure it to monitor your S3 buckets.

Not using then be ready with?

Increased risk of data breaches and non-compliance with data protection regulations.

11. Applying VPC Security Best Practices

What is it?

This refers to implementing security measures within your Virtual Private Cloud (VPC) such as using security groups and NACLs, and implementing subnet strategies.

Why use it?

To ensure your network is secure and to prevent unauthorized access to your AWS resources.

How to use it?

Follow AWS guidelines on setting up and securing your VPC. This includes minimal access permissions, isolating public and private subnets, and limiting open ports.

Not using then be ready with?

Increased risk of attacks due to exposed resources or lax security measures.

12. Setting up AWS Trusted Advisor

What is it?

AWS Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment.

Why use it?

To ensure your AWS environment adheres to best practices across four categories: cost optimization, performance, security, and fault tolerance.

How to use it?

Enable AWS Trusted Advisor in your production account and review its recommendations regularly.

Not using then be ready with?

Potential oversights in cost management, performance optimization, and security posture.

13. Implementing Amazon Inspector

What is it?

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

Why use it?

To identify vulnerabilities or deviations from best practices in your applications.

How to use it?

Set up an Amazon Inspector in your production account to start regular security assessments.

Not using then be ready with?

Increased risk of undiscovered vulnerabilities and compliance issues in your applications.

14. Using AWS Secrets Manager

What is it?

AWS Secrets Manager protects access to your applications, services, and IT resources.

Why use it?

To avoid the upfront investment and on-going maintenance costs of operating your own infrastructure for managing secrets.

How to use it?

Store and retrieve database credentials, on-demand tokens, or other secrets through AWS Secrets Manager.

Not using then be ready with?

Increased risk of secrets leakage which could lead to serious security breaches.

15. Setting up AWS CloudFormation StackSets

What is it?

AWS CloudFormation StackSets extends the functionality of stacks to create, update, or delete stacks across multiple accounts and regions with a single operation.

Why use it?

To ensure consistency across your production, development, and testing environments.

How to use it?

Configure AWS CloudFormation StackSets to manage resources across your AWS accounts and regions.

Not using then be ready with?

Increased complexity in managing and synchronizing resources across accounts and regions.

16. Using Amazon S3 Versioning and Lifecycle Policies

What is it?

These are features in Amazon S3 that allows you to preserve, retrieve, and restore every version of every object in your bucket and manage their lifecycle.

Why use it?

To provide an additional level of protection for your data and to manage the lifecycle of your objects so that they are automatically transferred to a lower-cost storage class or archived or deleted.

How to use it?

Enable versioning and set lifecycle policies for your S3 buckets in your AWS production account.

Not using then be ready with?

Increased risk of data loss and unnecessary storage costs for outdated or infrequently accessed data.

17. Implementing AWS WAF

What is it?

AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits.

Why use it?

To protect your web applications or APIs from common threats such as SQL injection and cross-site scripting (XSS).

How to use it?

Deploy AWS WAF on your Amazon CloudFront distributions or Application Load Balancers in your production account.

Not using then be ready with?

Increased risk of common web attacks leading to security breaches or service disruptions.

18. Setting up AWS CloudTrail

What is it?

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account.

Why use it?

To log, continuously monitor, and retain account activity related to actions across your AWS infrastructure.

How to use it?

Enable AWS CloudTrail in your production account and configure it to track user activity and API usage.

Not using then be ready with?

Lack of visibility into user and API activity, making it difficult to analyze past events or detect suspicious activity.

19. Using Amazon RDS Snapshots

What is it?

Amazon RDS Snapshots are backups of your RDS database.

Why use it?

To protect your database from accidental deletion, to restore to a point in time, or to migrate data across regions or accounts.

How to use it?

Regularly create snapshots of your RDS databases in your production account.

Not using then be ready with?

Risk of data loss and potential service disruptions in case of database issues.

20. Implementing AWS Auto Scaling

What is it?

AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost.

Why use it?

To ensure that your applications always have the right resources at the right time.

How to use it?

Set up Auto Scaling for your EC2 instances or other AWS resources in your production account.

Not using then be ready with?

Manual management of resource capacity, potential over-provisioning or under-provisioning of resources.

21. Implementing AWS IAM Best Practices

What is it?

It involves applying best practices to AWS Identity and Access Management (IAM) to enhance the security of your AWS production account.

Why use it?

To manage AWS resources securely and provide fine-grained access control to your AWS services and resources.

How to use it?

Regularly review and apply IAM best practices such as least privilege, password policies, and multi-factor authentication.

Not using then be ready with?

Increased risk of unauthorized access or privilege escalation.

22. Setting up AWS CloudWatch

What is it?

Amazon CloudWatch is a monitoring service for AWS resources and applications that you run on AWS.

Why use it?

To gain system-wide visibility into resource utilization, application performance, and operational health.

How to use it?

Configure CloudWatch to collect monitoring and operational data in the form of logs, metrics, and events.

Not using then be ready with?

Lack of visibility into application performance and resource utilization, leading to operational issues going unnoticed.

23. Implementing AWS Direct Connect

What is it?

AWS Direct Connect is a cloud service solution that provides a more stable and secure network connection between your network and your AWS production account.

Why use it?

To reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections.

How to use it?

Establish a dedicated network connection from your premises to AWS using AWS Direct Connect.

Not using then be ready with?

Potential network latency and security issues associated with public internet connections.

	**Checkout:** Pravin Mishra's AWS University **Subscribe:** My AWS Youtube Channel (AWS with Pravin Mishra)

24. Setting up AWS Backup

What is it?

AWS Backup is a fully managed backup service that makes it easy to centralize and automate the backup of data across AWS services.

Why use it?

To protect your AWS resources including EBS volumes, RDS databases, DynamoDB tables, EFS file systems, and more.

How to use it?

Configure AWS Backup to create, manage, and restore backups according to your operational and compliance needs.

Not using then be ready with?

Increased risk of data loss and potential non-compliance with data protection regulations.

25. Implementing AWS GuardDuty

What is it?

AWS GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads.

Why use it?

To protect your AWS environment from potential threats, breaches, or malicious actors.

How to use it?

Enable AWS GuardDuty in your production account to continuously monitor and protect your account.

Not using then be ready with?

Increased risk of undetected malicious activity in your AWS environment.

26. Using Amazon Macie

What is it?

Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS.

Why use it?

To understand where sensitive data is located and whether it's appropriately protected.

How to use it?

Enable Amazon Macie in your production account to automatically discover, classify, and protect sensitive data.

Not using then be ready with?

Increased risk of data breaches and non-compliance with data privacy regulations.

27. Setting up AWS Organizations

What is it?

AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns.

Why use it?

To centrally manage and govern your environment as you grow and scale your AWS resources.

How to use it?

Create an organization in AWS Organizations, invite existing accounts, or create new ones.

Not using then be ready with?

Difficulty in managing multiple AWS accounts, lack of centralized control and governance.

28. Implementing AWS Trusted Advisor

What is it?

AWS Trusted Advisor is a real-time guide to help you provision your resources following AWS best practices.

Why use it?

To optimize the AWS environment by reducing cost, improving system performance, and closing security gaps.

How to use it?

Regularly review and apply recommendations from AWS Trusted Advisor.

Not using then be ready with?

Missed opportunities to optimize your AWS environment for cost, performance, and security.

29. Using AWS Secrets Manager

What is it?

AWS Secrets Manager protects access to your applications, services, and IT resources, without the upfront investment and on-going maintenance costs of operating your own infrastructure.

Why use it?

To securely manage and rotate secrets such as database credentials, on-going APIs keys, and more.

How to use it?

Use AWS Secrets Manager to store, manage, and retrieve secrets in your production account.

Not using then be ready with?

Increased risk of unauthorized access and potential security breaches due to mishandled secrets.

30. Implementing AWS Systems Manager

What is it?

AWS Systems Manager gives you visibility and control of your infrastructure on AWS.

Why use it?

To manage operational tasks on AWS resources such as EC2 instances, S3 buckets, and more.

How to use it?

Use AWS Systems Manager for operational tasks like patch management, state management, and automation.

Not using then be ready with?

Checkout: Pravin Mishra's AWS University

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

Manual and potentially inconsistent operational management of AWS resources.