# Domain 1: Monitoring, Logging, and Remediation

## 1.1 Implement metrics, alarms, and filters by using AWS monitoring and logging services

### Identify, collect, analyze, and export logs (for example, Amazon CloudWatch Logs, CloudWatch Logs Insights, AWS CloudTrail logs)

* + CloudWatch Logs
    - Monitor and store logs to help better understand and operate your systems and applications
    - Real-Time Application and System Monitoring
      * Monitor using log data
      * Can track number of errors that occur in your application logs and send you a notification whenever the rate of errors exceeds a threshold
    - Long-term log retention
      * Store log data indefinaitely in highly durable and cost effective storage without worrying about hard drives running out of space
      * Quickly move rotated and non-rotated logs files off host
  + Cloudwatch Logs Insights
    - Interactive, pay as you go and integrated log analytics capability for cloudwatch logs
    - Search and visualize logs
    - Allows you to understand your applications and make improvements and find and fix problems quickly
  + AWS CloudTrail Logs

### Collect metrics and logs using the CloudWatch agent

* + Monitor AWS cloud resources and applications run on AWS
  + Metrics are provided automatically for a number of AWS products and Services
    - EC2 instances
    - EBS Volumes
    - Elastic Load Balancer (ELB)
    - Auto Scaling
    - EMR job flow
    - RDS DB instances
    - DynamoDB tables
    - ElastiCache Cluster
    - Redshift clusters
    - OpsWorks stacks
    - Route53 health checks
    - SNS topics
    - SQS Queues
    - SQF workflows
    - Storage gateways
  + Retention

### Create CloudWatch alarms

### Create metric filters

### Create CloudWatch dashboards

### Configure notifications (for example, Amazon Simple Notification Service [Amazon SNS], Service Quotas, CloudWatch alarms, AWS Health events)

## 1.2 Remediate issues based on monitoring and availability metrics

### Troubleshoot or take corrective actions based on notifications and alarms

### Configure Amazon EventBridge rules to trigger actions

### Use AWS Systems Manager Automation documents to take action based on AWS Config rules

# Domain 2: Reliability and Business Continuity

## 2.1 Implement scalability and elasticity

### Create and maintain AWS Auto Scaling plans

### Implement caching

### Implement Amazon RDS replicas and Amazon Aurora Replicas

### Implement loosely coupled architectures

### Differentiate between horizontal scaling and vertical scaling

## 2.2 Implement high availability and resilient environments

### Configure Elastic Load Balancer and Amazon Route 53 health checks

### Differentiate between the use of a single Availability Zone and Multi-AZ deployments (for

### example, Amazon EC2 Auto Scaling groups, Elastic Load Balancing, Amazon FSx, Amazon RDS)

### Implement fault-tolerant workloads (for example, Amazon Elastic File System [Amazon EFS],

### Elastic IP addresses)

### Implement Route 53 routing policies (for example, failover, weighted, latency based)

## 2.3 Implement backup and restore strategies

### Automate snapshots and backups based on use cases (for example, RDS snapshots, AWS

### Backup, RTO and RPO, Amazon Data Lifecycle Manager, retention policy)

### Restore databases (for example, point-in-time restore, promote read replica)

### Implement versioning and lifecycle rules

### Configure Amazon S3 Cross-Region Replication

### Execute disaster recovery procedures

# Domain 3: Deployment, Provisioning, and Automation

## 3.1 Provision and maintain cloud resources

### Create and manage AMIs (for example, EC2 Image Builder)

### Create, manage, and troubleshoot AWS CloudFormation

### Provision resources across multiple AWS Regions and accounts (for example, AWS Resource

### Access Manager, CloudFormation StackSets, IAM cross-account roles)

### Select deployment scenarios and services (for example, blue/green, rolling, canary)

### Identify and remediate deployment issues (for example, service quotas, subnet sizing, CloudFormation and AWS OpsWorks errors, permissions)

## 3.2 Automate manual or repeatable processes

### Use AWS services (for example, OpsWorks, Systems Manager, CloudFormation) to automate

### deployment processes

### Implement automated patch management

### Schedule automated tasks by using AWS services (for example, EventBridge, AWS Config)

# Domain 4: Security and Compliance

## 4.1 Implement and manage security and compliance policies

### Implement IAM features (for example, password policies, MFA, roles, SAML, federated identity,resource policies, policy conditions)

* + Controls Internal Team accounts. NOT USER ACCOUNTS
  + Policy document bound to IAM User
    - Entity in AWS defines permissions for identity or resource
    - Allow statements
    - Deny statements
    - Policy types
      * Identity-based policy (IAM Policy)
        + Attach managed and inline policies to IAM identities

Users

Groups

roles

* + - * Resource-based policies
        + Attach inline polices to resources
        + S3 bucket policies and IAM Role Trust policies most common
      * AWS Organizations Service Control Policies (SCP)
        + Define max permissions for account members of an organization or OU
      * Access control Lists (ACL)
        + Control which principals in other accounts can access a resource to which the ACL is attached.
        + Similar to resource based policies
        + Does not use JSON structure
    - Policy Elements (JSON)
      * Effect
        + Allow or Deny
        + Implicit Deny
        + Most restrictive wins (Deny)
      * Principal
        + Account, user, role or federated user to which you want to allow or deny access
        + Only used with Resource-based policy
      * Action
        + List of actions the policy allows or denys
      * Resource
        + List of resources to which the action apply
        + Required for IAM Policy
        + Optional for Resource-based Policy
      * Condition
        + Circumstances under which the policy grants permission.
  + Authentication
    - Sign in to AWS
    - Users
      * Username and password
    - Federated users
      * Single Sign On
      * External Identity store (AD, Azure AD, LDAP, etc)
      * Assume IAM Role
    - Applications
      * Permissions to access AWS Resources can be assigned
      * Access/secret keys
        + Api level credentials
    - IAM Role
      * Policy document bount to IAM Role
  + Authorization
    - What you can do
    - Policy document
      * Explicitly grants permissions
        + Users

Can belong to multiple groups

* + - * + Groups

Collection of IAM Users

Cannot be nested

Not a principal

IAM document policy

* + - Default = New users have not permissions
  + MFA
    - Second factor auth
  + Access keys rotate
    - AWS Config can be used to identify access keys past due for rotation
  + Remove unnecessary credentials
    - Last time user logged in ( over x days) should probably be removed.

### Troubleshoot and audit access issues by using AWS services (for example, CloudTrail, IAM Access Analyzer, IAM policy simulator)

* + IAM Policy Simulator
    - Test policies

### Validate service control policies and permissions boundaries

### Review AWS Trusted Advisor security checks

### Validate AWS Region and service selections based on compliance requirements

### Implement secure multi-account strategies (for example, AWS Control Tower, AWS

### Organizations)

## 4.2 Implement data and infrastructure protection strategies

### Enforce a data classification scheme

### Create, manage, and protect encryption keys

### Implement encryption at rest (for example, AWS Key Management Service [AWS KMS])

### Implement encryption in transit (for example, AWS Certificate Manager, VPN)

### Securely store secrets by using AWS services (for example, AWS Secrets Manager, Systems Manager Parameter Store)

### Review reports or findings (for example, AWS Security Hub, Amazon GuardDuty, AWS Config, Amazon Inspector)

# Domain 5: Networking and Content Delivery

## 5.1 Implement networking features and connectivity

### Configure a VPC (for example, subnets, route tables, network ACLs, security groups, NAT

### gateway, internet gateway)

### Configure private connectivity (for example, Systems Manager Session Manager, VPC

### endpoints, VPC peering, VPN)

### Configure AWS network protection services (for example, AWS WAF, AWS Shield)

## 5.2 Configure domains, DNS services, and content delivery

### Configure Route 53 hosted zones and records

### Implement Route 53 routing policies (for example, geolocation, geoproximity)

### Configure DNS (for example, Route 53 Resolver)

### Configure Amazon CloudFront and S3 origin access identity (OAI)

### Configure S3 static website hosting

## 5.3 Troubleshoot network connectivity issues

### Interpret VPC configurations (for example, subnets, route tables, network ACLs, security groups)

### Collect and interpret logs (for example, VPC Flow Logs, Elastic Load Balancer access logs, AWS WAF web ACL logs, CloudFront logs)

### Identify and remediate CloudFront caching issues

### Troubleshoot hybrid and private connectivity issues

# Domain 6: Cost and Performance Optimization

## 6.1 Implement cost optimization strategies

### Implement cost allocation tags

### Identify and remediate underutilized or unused resources by using AWS services and tools (for example, Trusted Advisor, AWS Compute Optimizer, Cost Explorer)

### Configure AWS Budgets and billing alarms

### Assess resource usage patterns to qualify workloads for EC2 Spot Instances

### Identify opportunities to use managed services (for example, Amazon RDS, AWS Fargate, EFS)

* + Fargate
    - Serverless EKS and ECS

## 6.2 Implement performance optimization strategies

### Recommend compute resources based on performance metrics

### Monitor Amazon EBS metrics and modify configuration to increase performance efficiency

### Implement S3 performance features (for example, S3 Transfer Acceleration, multipart uploads)

### Monitor RDS metrics and modify the configuration to increase performance efficiency (for

### example, Performance Insights, RDS Proxy)

### Enable enhanced EC2 capabilities (for example, enhanced network adapter, instance store, placement groups)

## Appendix

Which key tools, technologies, and concepts might be covered on the exam?

The following is a non-exhaustive list of the tools and technologies that could appear on the exam. This list

is subject to change and is provided to help you understand the general scope of services, features, or

technologies on the exam. The general tools and technologies in this list appear in no particular order.

AWS services are grouped according to their primary functions. While some of these technologies will likely

be covered more than others on the exam, the order and placement of them in this list is no indication of

relative weight or importance:

AWS services and features

### Analytics:

* Amazon Elasticsearch Service (Amazon ES)
* Application Integration:
* Amazon EventBridge (Amazon CloudWatch Events)
* Amazon Simple Notification Service (Amazon SNS)
* Amazon Simple Queue Service (Amazon SQS)

### AWS Cost Management:

* AWS Cost and Usage Report
* AWS Cost Explorer
* Savings Plans

### Compute:

* AWS Application Auto Scaling
* Amazon EC2
* Amazon EC2 Auto Scaling
* Amazon EC2 Image Builder
* AWS Lambda

### Database:

* Amazon Aurora
* Amazon ElastiCache
* Amazon RDS

Management, Monitoring, and Governance:

* AWS CloudFormation
* AWS CloudTrail
* Amazon CloudWatch
  + Monitoring service for AWS cloud resources and the applications you run on AWS
  + Collects and tracks metrics
  + Collect and monitor log files
  + Set alarms
* AWS Command Line Interface (AWS CLI)
* AWS Compute Optimizer
* AWS Config
* AWS Control Tower
* AWS License Manager
* AWS Management Console
* AWS OpsWorks
* AWS Organizations
* AWS Personal Health Dashboard
* AWS Secrets Manager
* AWS Service Catalog
* AWS Systems Manager
* AWS Systems Manager Parameter Store
* AWS tools and SDKs
* AWS Trusted Advisor

### Migration and Transfer:

* AWS DataSync
* AWS Transfer Family

Networking and Content Delivery:

* AWS Client VPN
* Amazon CloudFront
* Elastic Load Balancing
* AWS Firewall Manager
* AWS Global Accelerator
* Amazon Route 53
* Amazon Route 53 Resolver
* AWS Transit Gateway
* Amazon VPC
* Amazon VPC Traffic Mirroring

### Security, Identity, and Compliance:

* AWS Certificate Manager (ACM)
* Amazon Detective
* AWS Directory Service
* Amazon GuardDuty
* AWS IAM Access Analyzer
* AWS Identity and Access Management (IAM)
* Amazon Inspector
* AWS Key Management Service (AWS KMS)
* AWS License Manager
* AWS Secrets Manager
* AWS Security Hub
* AWS Shield
* AWS WAF

### Storage:

* Amazon Elastic Block Store (Amazon EBS)
* Amazon Elastic File System (Amazon EFS)
* Amazon FSx
* Amazon S3
* Amazon S3 Glacier
* AWS Backup
* AWS Storage Gateway

## Out-of-scope AWS services and features

The following is a non-exhaustive list of AWS services and features that are not covered on the exam.

These services and features do not represent every AWS offering that is excluded from the exam content.

Services or features that are entirely unrelated to the target job roles for the exam are excluded from this

list because they are assumed to be irrelevant.

Out-of-scope AWS services and features include the following:

* Amazon API Gateway
* Amazon AppStream 2.0
* AWS Batch
* Amazon Chime
* Amazon Cloud Directory
* Amazon CloudSearch
* AWS CodeBuild
* AWS CodeCommit
* AWS CodeDeploy
* AWS CodeStar
* Amazon Connect
* AWS Deep Learning AMIs (DLAMI)
* AWS Device Farm
* Amazon DynamoDB
* Amazon DynamoDB Accelerator (DAX)
* Amazon Elastic Container Registry (Amazon ECR)
* Amazon Elastic Container Service (Amazon ECS)
* Amazon Elastic Transcoder
* Amazon EMR
* Amazon GameLift
* AWS IoT Button
* AWS IoT Greengrass
* AWS IoT Platform
* Amazon Kinesis
* Amazon Lex
* Amazon Lightsail
* Amazon Lumberyard
* Amazon Machine Learning (Amazon ML)
* Version 2.1 SOA-C02 10 | PAGE
* AWS Managed Services
* AWS Mobile Hub
* AWS Mobile SDK
* Apache MXNet on AWS
* Amazon Pinpoint
* Amazon Polly
* Amazon Redshift
* Amazon Rekognition
* AWS Schema Conversion Tool
* Amazon Simple Email Service (Amazon SES)
* AWS Snowmobile
* Amazon WorkDocs
* Amazon WorkMail
* Amazon WorkSpaces
* AWS X-Ray