# 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)

### Collect metrics and logs using the CloudWatch agent

### 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)

### Troubleshoot and audit access issues by using AWS services (for example, CloudTrail, IAM

### Access Analyzer, IAM policy simulator)

### 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)

## 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)