Study Guide

AWS Certified SysOps Administrator – Associate (SOA-C02)

Here is the Exam Guide provided by AWS. This will cover exam prerequisites, candidate expectations, response types, content outline, and domain weightings.

Below are what we consider *Exam Essentials* that may not be specifically called out in the vendor exam guide or we want to reiterate the importance. These are the things you'll want to make sure you know in addition to the exam objectives.

Exam Essentials: What you need to know

Domain 1: Monitoring, Logging, and Remediation

- CloudWatch Logs can manage the logs from all systems, applications, and AWS services that you use.
- CloudWatch Log agents can be installed on EC2 Instances or on on-premise servers.
- CloudTrail Logs help monitor account activity related to actions performed via the AWS Management Console, AWS SDKs, command line tools, and other AWS services.
- EventBridge Rules execute custom actions in response to CloudWatch Alarms.
- Amazon Simple Notification Service can send e-mail notifications in response to CloudWatch alarms.

Exam Essentials: What you need to know

Domain 2: Reliability and Business Continuity

- Route 53 provides DNS, domain registration, and health-checking web services.
- The different Route 53 DNS Routing policies are: Simple, Failover, Geolocation, Geoproximity, Latency, Multivalue answer, Weighted.
- Load Balancers help distribute traffic across a number of services. They can point to Auto Scaling Groups and be the target of an alias record in Route 53.
- Setup automated database snapshots in order to comply with RTO and PTO.
- S3 Object Versioning allows retrieving previous versions of an object.

Domain 3: Deployment, Provisioning, and Automation

- EC2 instances can be Spot Instances (lower cost) or On Demand (always readily available).
- Auto Scaling Groups manage the appropriate number of EC2 instances according to scaling policies.
- CloudFormation templates offer a declarative way to automate the provisioning and management of resources, and can be written in JSON or YAML
- AWS Beanstalk is a service that offers a low-barrier strategy to migrate existing applications to the AWS cloud.
- AWS OpsWork allows using Chef to manage infrastructure and deployment.

Exam Essentials: What you need to know

- CodeDeploy provides two deployment type options: in-place deployments and blue/green deployments.
    - In Place: Re-deploys to existing instances. The application on each instance is stopped, the latest application revision is installed, and the new version of the application is started and validated.
    - Blue/green deployment: Instances in a deployment group (the original environment) are replaced by a different set of instances (the replacement environment) running the new version of the application.

Domain 4: Security and Compliance

- Use AWS System Manager Parameter Store to store configuration data and passwords for other AWS services.
- Avoid using the root user to manage infrastructure and add MFA as an extra layer of protection.
- Avoid storing AWS Access Keys in EC2 instances. Instead, use IAM Service Roles to manage access to resources.
- Use AWS Secrets Manager to store and manage database credentials.
- Use AWS Config to assess, audit, and evaluate configuration changes to your AWS resources.
- S3 supports server-side encryption with either Amazon S3-managed keys (SSE-S3) or AWS KMS keys stored in AWS Key Management Service (AWS KMS) (SSE-KMS).

Exam Essentials: What you need to know

Domain 5: Networking and Content Delivery

- VPCs can have private and public subnets
    - Public subnets are associated with a Route Table that has a route to an Internet Gateway. They can be accessed by the internet.
    - Private subnets are associated with a Route Table that does NOT have a route to an Internet Gateway. They cannot be accessed by the internet but can send requests out to the internet through a NAT Gateway.
- VPC Flow Logs:
    - Capture information about the IP traffic going to and from network interfaces in a VPC.
    - Can be published to Amazon CloudWatch Logs or Amazon S3.
- CloudFront is a CDN and works with any AWS origin, such as Amazon S3, Amazon EC2, Elastic Load Balancing, or with any custom HTTP origin.

Exam Essentials: What you need to know

Domain 6: Cost and Performance Optimization

- Trusted Advisors checks assist identifying improvement opportunities for security, performance, and costs, and also helps monitor service quotas.
- Use read replicas to scale out read-heavy database workloads.
- Implement a caching strategy to reduce database costs and improve overall application performance.
- S3 Storage Classes and Lifecycle Rules help optimize for cost.

Self-Assessment Questions: Test your Understanding

Below is a series of practice questions meant to mimic the style and difficulty of the exam. If a question has more than one correct answer, you will be asked to *Choose Two*. You can find the correct answers at the end of this document.

Domain 1: Monitoring, Logging, and Remediation

1. A company hosts a web application on Amazon EC2 instances. A new version of the application is deployed, including a new CPU-intensive feature. A SysOps administrator must implement a solution to monitor the instances' CPU utilization and alert the operations team when the average CPU utilization is higher than a specific threshold. Which solution will meet this requirement?

    a. Create a CloudWatch alarm that monitors the CPU Utilization metric from EC2 instances and publishes alarm notifications to an Amazon Simple Notification Service (Amazon SNS) topic.
    b. Create a CloudTrail alarm that monitors the resource usage trail from EC2 instances and publishes alarm notifications to an Amazon Simple Notification Service (Amazon SNS) topic.
    c. Create an Amazon Simple Notification Service (Amazon SNS) topic that continually polls CPU utilization information from EC2 instances, then create a subscription and subscription filter for the operations team.
    d. Configure AWS Trusted Advisor to send an alarm notification to the operations team when compute resources are being overutilized.

2. A company runs several production workloads on Amazon EC2 instances. As a security guideline, the company decides that instances should not have a public IP address. A SysOps administrator must implement a solution that audits the configuration of EC2 instances and automatically publishes an Amazon Simple Notification Service (Amazon SNS) notification when an Elastic IP Address is associated with an EC2 instance. Which solution will meet this requirement?

a. Create an AWS Config rule that checks whether Amazon EC2 instances have a public IP address association. Configure an AWS Config alarm for when the rule's status equals NON_COMPLIANT that publishes a notification on an Amazon SNS topic.
b. Create an automation script that runs locally on each instance and checks for a network interface with a public IP address. Use AWS OpsWorks Stacks to periodically run the script across all EC2 instances and publish an Amazon SNS notification if a public IP address is detected.
c. On each EC2 instance, run a script that periodically tries to make a connection to a public website. Make an API call to Amazon SNS to publish a notification if the connection succeeds.
d. Create an AWS Config rule that checks whether Amazon EC2 instances have a public IP address association. Select the Automatic remediation option and an AWS Systems Manager Automation document that publishes an Amazon SNS notification.

3. A company runs Apache web servers on a fleet of EC2 instances. The Apache server logs are collected in a CloudWatch log group. The company wants to understand how often site visitors are unable to find the resource they need by monitoring how many times the Apache servers return an HTTP 404 response. Which action should a SysOps administrator take to implement this solution?

a. In Cloud Watch, create a custom metric that uses a REGEX matching pattern to detect the HTTP 404 responses in the Apache server logs. Retrieve the metric to determine the count of HTTP 404 responses.
b. In the log group, create a metric filter that specifies an HTTP status code equal to 404. Retrieve the corresponding metric in CloudWatch to determine the count of HTTP 404 responses.
c. Use Amazon Inspector to inspect the log group for anomalies. Retrieve the "Page Not Found" anomaly event history to determine the count of HTTP 404 responses.
d. On each web server, run a script that parses the web server logs and counts HTTP 404 events. Use AWS Systems Manager to aggregate the numbers from all web servers to determine the count of HTTP 404 responses.

4. A SysOps administrator is implementing a solution that logs all management operations performed on resources in a company's AWS account and can easily verify whether log files have been deleted or changed. Which actions should the SysOps administrator take to meet this requirement? (Select TWO.)
    a. Create an AWS Config audit rule.
    b. Enable CloudTrail log file integrity validation.
    c. Turn on Amazon S3 server access logging for the bucket storing the logs.
    d. Create a CloudTrail trail for management events.

5. A company has a development AWS account where users can create EC2 instances for testing new application developments. The company wants to log the launch of any new EC2 instance for tracking purposes.
Which actions should a SysOps administrator take to meet this requirement? (Select TWO.)

    a. Create a CloudWatch alarm for the condition instanceState:pending.
    b. Create a CloudWatch Events rule to trigger a lambda function when an EC2 instance's state changes to running.
    c. Create a lambda function that writes a log record of the event.
    d. Configure a CloudWatch log group.

Domain 2: Reliability and Business Continuity

1. A company runs several production workloads on Amazon EC2 instances. A SysOps administrator must ensure that all data is backed up twice daily for all EC2 instances. Backups must be retained for 30 days. Which of the following is the MOST operationally efficient solution that meets these requirements?

    a. Create a backup plan in AWS Backup. Assign EC2 instance resources by their resource ID, editing the backup plan twice daily to include any new EC2 resources. Schedule the backup plan to run every day and expire backups after 30 days.

b. Apply a service control policy (SCP) for the production account that prevents instance creation unless a backup is enabled. Configure the instance's backup scheduler to run twice daily and remove backups after 30 days.
c. Ensure all EC2 instances are tagged correctly and create a lifecycle policy in Amazon Data Lifecycle Manager (Amazon DLM). Assign all resources by tags, and schedule the lifecycle policy to create snapshots every 12 hours with a retention period of 30 days.
d. Use AWS Config to create and export an inventory of all running EC2 instances daily. Create a lifecycle policy in Amazon Data Lifecycle Manager (Amazon DLM), assigning EC2 resources by resource IDs from the inventory. Schedule the lifecycle policy to create snapshots every 12 hours with a retention period of 30 days.

2. A company wants to deploy a 3-tier ecommerce web application on AWS using Amazon EC2 and Amazon Relational Database Service (Amazon RDS). The solution must be resilient against any failure that affects an AWS datacenter.
Which solution will meet this requirement with the LEAST amount of downtime and data loss during failure events?

a. Deploy EC2 instances on different Availability Zones. Deploy an Elastic Load Balancer to distribute load across instances. Provision a Multi-AZ Relational Database Service (RDS) database instance.
b. Deploy EC2 instances on different Availability Zones. Deploy an Elastic Load Balancer to distribute load across instances. Provision a Single-AZ Relational Database Service (RDS) database instance. Create an AWS Backup plan and configure hourly database snapshots. Create an AWS Systems Manager Automation document to automatically provision a new database from a snapshot.
c. Deploy EC2 instances with public IP addresses in primary and secondary regions. Configure a DNS failover policy in Amazon Route 53. Provision an

Amazon Relational Database Service (RDS) database instance in the primary region and create a read replica in the secondary region.

d. Deploy EC2 instances and the Amazon Relational Database Service (RDS) database on a single Availability Zone using a CloudFormation template. Create an AWS Backup plan and configure hourly database snapshots. Create a script that automatically deploys the CloudFormation template to a separate region in the event of failure.

3. A company hosts a production MySQL database on Amazon Relational Database Service (Amazon RDS). During the latest performance test, the developers find that the current database capacity will not be able to support the increase in the database read load expected over the next months. Which is the MOST cost-effective and operationally efficient solution a SysOps administrator can implement to meet the capacity growth requirement?

   a. Increase the database instance class to a size that can handle the largest expected number of concurrent users.
   b. Configure a CloudWatch alarm for when the database instance's CPU utilization metric is near 100%. Configure the alarm to trigger a Lambda function that updates the database's instance class to one that doubles the number of virtual CPUs.
   c. Create a read replica for the existing database. Have the development team update the application to direct some of the read requests to the replica.
   d. Create a snapshot of the existing database. Create a new database from the snapshot and configure it as a read replica of the main database. Ensure the development team updates the application to direct some of the read requests to the replica.

4. A company has an Elastic Beanstalk development environment for its web application. The instances connect to a MySQL-compatible Amazon Aurora database with a configured backup retention period of 7 days. A developer accidentally corrupts

a large number of database rows while working alone on Saturday. A SysOps administrator is notified on Monday. The database is used only for development purposes and there has been no other activity since the incident. Which action should the SysOps administrator take to fix the issue?

a. Use the point-in-time restore feature and choose a custom restore time between the last valid update and the incident. Ask the development team to point the application to the new database connection endpoint.
b. Use the point-in-time restore feature and choose the latest restorable time. Tell the development team to continue using the same database connection endpoint.
c. Use the Elastic Beanstalk deployment rollback feature to undo the latest application changes that corrupted the database data. Tell the development team to continue using the same database connection endpoint.
d. Enable the backtrack feature in Amazon Aurora with a target backtrack window of 72 hours. Backtrack the database cluster to a point in time between the last valid update and the incident. Tell the development team to continue using the same database connection endpoint.

5. A company uses Amazon Simple Storage Service (Amazon S3) to host a static website in a single AWS region. A SysOps administrator must implement a business continuity solution that ensures the website is available in the event of a regional outage. Which actions should the SysOps administrator take to meet this requirement? (Choose TWO.)

a. Update the existing DNS record.
b. Create a CloudWatch alarm based on S3 request metrics.
c. Configure cross-region replication in the source S3 bucket.
d. Configure a Route 53 failover routing policy.

Domain 3: Deployment, Provisioning, and Automation

1. A company runs production workloads using a multi-account setup on AWS. In one of the accounts (account A), the company hosts objects on a non-public Amazon S3 bucket. A SysOps administrator must enable an AWS Lambda function hosted on a separate account (account B) to access these objects while preventing access from any individual. Which solution will meet this requirement?

    a. Make the S3 bucket public in account A. Configure a bucket policy that only allows access to the bucket from the IP address ranges used by the Lambda function in account B.
    b. Create an IAM role in account B with GET Object permission on the S3 bucket in account A. Assign the IAM role to the Lambda function in account B. Configure the bucket policy in account A to grant GET Object permission to the IAM role in account B.
    c. Create an IAM role and bucket policy in account A with GET Object permission on the S3 bucket. Share the IAM role definition with account B using AWS Resource Access Manager. Assign the IAM role to the Lambda function in account B.
    d. Place both AWS accounts under the same Organizational Unit (OU). Create an IAM user in account B. Create an IAM policy with GET Object permission on the S3 bucket in account A and assign it to the IAM user. Have the Lambda function use the IAM user's credentials.

2. A company uses Elastic Beanstalk to host a production web application on AWS. Lately, website users are reporting several UI bugs and complaining about long wait times for fixes. The operations team notices that while the application passes health checks, certain monitoring metrics often indicate negatively impacted user experience. A SysOps administrator must implement a solution that enables

developers to test new UI features on a small subset of users to minimize business impact. Developers should also be able to quickly revert changes if needed. Which solution will meet this requirement?

a. Configure a traffic-splitting deployment option in Elastic Beanstalk. Assign a small percentage of incoming client traffic to a new application version and specify an evaluation period. Cancel the deployment if monitoring metrics indicate negatively impacted user experience.
b. Configure a blue/green deployment scenario in Elastic Beanstalk. Deploy new application versions to a non-production environment and swap environment URLs to promote it to production. Swap URLs back if monitoring metrics indicate a negative user experience.
c. Configure a rolling deployment option in Elastic Beanstalk. Deploy new application versions to the environment. If monitoring metrics indicate poor user experience, perform a manual rollback.
d. Configure an immutable deployment option in Elastic Beanstalk. Deploy new application versions to the environment. If monitoring metrics indicate poor user experience, re-deploy the previous application version.

3. A global software company runs a pilot for a new production workload on an AWS account. All resources were deployed from the management account using a CloudFormation template. A SysOps administrator now needs to replicate the environment to 5 additional AWS accounts each located in a different region. All accounts belong to the same AWS Organization. Which actions should the SysOps admin take to meet this requirement with the LEAST amount of effort? (Choose TWO.)
    a. Create a CloudFormation StackSet in the management account.
    b. Import the CloudFormation template in each target account.
    c. Create a CloudFormation Stack in the management account.
    d. Configure the five additional accounts as deployment targets.
    e. Create one CloudFormation Stack for each target account.

4. A large enterprise organization has a large fleet of EC2 servers on AWS for various production workloads. A recent security incident has prompted the organization to look for ways to more quickly patch instances' operating systems (OSes) when upgrades are available. The EC2 fleet includes Amazon Linux 2, Read Hat Enterprise Linux (RHEL), and Windows Server instances. A SysOps administrator must implement a solution to patch all instances within 5 days of an OS patch release. The administrator must also be able to easily visualize the patch compliance status of all EC2 instances. Which of the following is the MOST operationally efficient solution that meets these requirements?

    a. Use AWS OpsWorks Stacks to create a patching stack for each OS. Write chef recipes for each OS that checks for and installs the latest patches. Configure a schedule to execute recipes daily. Use AWS Config to create a custom compliance rule that checks daily if EC2 instances are patched.
    b. Use AWS Systems Manager Automation to create automation runbooks for each OS. Customize each automation runbook to apply the required patches to the corresponding OS. Create an Amazon EventBridge event that is triggered on each patch release. Configure each event rule to run the patching automation runbook. Configure AWS Systems Manager Automation to generate runbook execution reports on a schedule.
    c. Use AWS Systems Manager Patch Manager to create a patch baseline. Include a notification rule to send an email notification for patch releases. Ensure patches are approved by a security administrator within 5 days of release. Add all EC2 instances to the patch group. Schedule patching to run as a Systems Manager maintenance window task. Configure Patch Manager to generate patch compliance reports on a schedule.
    d. Use AWS Systems Manager Patch Manager to create a patch baseline for each OS. Include an auto-approval rule to approve patches after 5 days of their release. Configure tag values for the patch group and ensure all EC2 instances are tagged correctly. Schedule patching to run as a Systems Manager

maintenance window task. Configure Patch Manager to generate patch compliance reports on a schedule.

5. A company wants to deploy a workload to a new AWS account using Amazon EC2 and Amazon S3. A SysOps administrator created a CloudFormation template to deploy the resources; however, after uploading a template and successfully creating a stack, CloudFormation fails to deploy the resources. The administrator checks that they have the required permissions to use AWS CloudFormation.
Which of the following is a possible reason for this issue?

    a. The CloudFormation template is in an unsupported format or contains an invalid character.
    b. The subnet size of the underlying VPC is not large enough to accommodate all EC2 instances and S3 buckets defined in the template.
    c. The SysOps administrator lacks permissions to create EC2 instances and/or Amazon S3 buckets on the new account.
    d. CloudFormation is not supported in the region(s) where resources are being deployed to.

Domain 4: Security and Compliance

1. A company is setting up a new AWS account for a pilot deployment of a cloud-native application. AWS IAM users are created for the developers involved in the pilot, and a SysOps administrator has access to the root user credentials. The company wants the root user to be secured with multi-factor authentication (MFA), and to enforce a minimum password length of 8 characters and a password expiration period of 90 days for all other users. Which actions should the SysOps administrator take to secure the root and user accounts according to these requirements?

    a. Use AWS Directory Service to create a managed Microsoft Active Directory (AD). Create AD users and map them to existing IAM users. In AWS Directory

Service, enable MFA for the root user and configure a password policy for all users.

b. Log in to the AWS console as the root user. Navigate to the AWS Marketplace and find a third-party MFA software vendor. Use AWS Systems Manager Automation to create a runbook to expire users' passwords every 90 days. Use AWS Config to enforce the minimum password length requirement.
c. Log in to the AWS console as the root user. Navigate to My Security Credentials and choose Activate MFA to configure MFA for the root user. In AWS IAM, set a password policy with a minimum length and expiration period.
d. Log in to the AWS console as the root user. In AWS IAM, select the root user and choose Activate MFA for the root user. For each remaining user, set a password policy with a minimum length and expiration period.

2. A company is running a development environment on AWS using Amazon Elastic Container Service (Amazon ECS) and Amazon DocumentDB. To prevent exposing the database connection strings and application secrets, a SysOps administrator must implement a solution that enables developers to easily generate and securely store secrets. This solution must also allow secrets to be rotated regularly without disruption to the applications. Which solution will meet this requirement?

a. Use AWS Systems Manager Parameter Store to generate and store secrets. Enable automatic rotation on all secrets. Have the applications use AWS SDK operations to retrieve the secrets.
b. Use AWS Secrets Manager to generate and store secrets. Enable automatic rotation on all secrets. Have the applications use AWS SDK operations to retrieve the secrets.
c. Have the applications use standard programming libraries to generate secrets. Use AWS Systems Manager parameter store to store secrets. Configure Amazon ECS scheduled tasks to regenerate passwords regularly. Have the applications retrieve secrets from the ParameterStore environment variable.

d. Use AWS Secrets Manager to generate and store secrets. Enable renewal notification on all secrets and publish notification events to an Amazon Simple Notification Service (Amazon SNS) topic. Write a Lambda function to regenerate the password using AWS SDK operations. Have the applications use AWS SDK operations to retrieve the secrets.

3. A company uses AWS Organizations to create and manage multiple AWS accounts. The company wants to improve its security posture and enforce the least privilege principle by prohibiting access to unused AWS services while avoiding any disruptions to their engineers and account users. A security admin creates a service control policy (SCP) that denies access to AWS services believed to be unused. What steps can a SysOps administrator take to validate and implement the SCP across all accounts while minimizing the impact of a potential disruption?

    a. In the Management Account, view the services' last accessed information for the AWS Organization to confirm which services are unused. Update the SCP as needed. Create an Organizational Unit (OU) and attach the SCP to it. Add accounts to the OU in small numbers while monitoring AWS usage to ensure users weren't inadvertently locked out of key services. Repeat until all accounts are added to the OU.
    b. In the Management Account, attach the SCP to the AWS Organization's root account. Review CloudTrail logs hourly to identify any denied API calls to AWS services. Update the SCP as needed.
    c. In the Management Account, upload and deploy a CloudFormation template that attaches the SCP to the root account of the AWS Organization. Monitor user complaints to identify whether users were locked out of key AWS services. Roll back the deployment and update the SCP as needed.
    d. Create a script that deploys the SCP in each account one at a time. Create an AWS CloudWatch Events rule for API access denied events. Have the event trigger a Lambda function that removes the SCP from the account and sends an email notification. Update the SCP and repeat as needed.

4. A company is migrating an ecommerce web application to EC2 instances on AWS. The instances only have private IP addresses and are behind an Application Load Balancer (ALB). A SysOps administrator must implement a solution to encrypt traffic in transit for communication over the public Internet. The company already owns a Secure Sockets Layer (SSL) certificate from a third-party issuer. Which actions should the SysOps administrator take to meet this requirement? (Choose TWO.)

    a. Install the existing certificate directly on the ALB.
    b. Import the existing certificate into AWS Certificate Manager.
    c. Leverage the Amazon S3 integration with Elastic Load Balancing to deploy the certificate on the ALB.
    d. Leverage the AWS Certificate Manager integration with Elastic Load Balancing to deploy the certificate on the ALB.
    e. Upload the existing certificate to Amazon S3.

5. A company uses Amazon GuardDuty and Amazon Inspector in an AWS account that hosts a production workload. Although these services have been previously set up, the company lacks visibility and cannot report findings in a timely manner. A new security process requires a SysOps administrator to identify and report any anomalous employee activity behavior on AWS, and generate a report of any vulnerabilities found in EC2 instances. What actions should the SysOps administrator regularly take to meet this requirement?

    a. Review Amazon GuardDuty findings and search for anomalous IAM user behavior. Review Amazon Inspector assessments for EC2 activities from malicious IP addresses. Select all relevant Inspector findings and export results to Amazon S3.

b. Review Amazon GuardDuty findings and search for anomalous IAM user behavior. Review Amazon Inspector assessments for common vulnerabilities and exposures (CVEs). Generate an assessment report.
c. Review Amazon Inspector assessments for anomalous Identity and Access Management (IAM) user behavior. Review Amazon GuardDuty findings and search for common vulnerabilities and exposures (CVEs). Generate a GuardDuty findings report.
d. Use AWS CloudWatch to review Amazon GuardDuty and Amazon Inspector metrics. Create CloudWatch alarms based on anomalous user activity count and EC2 vulnerabilities count metrics. Find and review the corresponding logs in AWS CloudTrail for more details and to generate a report of vulnerability findings.

Domain 5: Networking and Content Delivery

1. A company is migrating a 3-tier web application to AWS by using a lift-and-shift strategy. A SysOps administrator must configure a VPC to receive this workload. The VPC must contain a public demilitarized zone (DMZ) network segment, a private network for the backend application, and a separate private network for databases. Instances in private networks should not be publicly accessible, but they should be able to reach the Internet for downloading updates and dependencies. The company wants to distribute the workloads across at least two Availability Zones (AZs). Which solution will meet this requirement?

    a. Configure three subnets for each AZ. Have the DMZ subnet contain a route table with a default route to the VPC's Internet Gateway. Deploy a Network Address Translation (NAT) gateway on this subnet. Have the remaining subnets contain a route table with a default route to the NAT Gateway instance. Configure Network Access Control Lists (NACLs) to allow required network communications.

b. Configure three subnets for each AZ. Have all subnets contain a route table with a default route to the VPC's Internet Gateway. Configure a Network Access Control List (NACL) to allow all inbound traffic on the DMZ subnet. Configure NACLs to block all inbound traffic on the remaining subnets.
c. Deploy three multi-AZ subnets. Have the DMZ subnet contain a route table with a default route to the VPC's Internet Gateway. Deploy a Network Address Translation (NAT) gateway on this subnet. Have the remaining subnets contain a route table with a default route to the NAT Gateway instance. Configure security groups on each subnet to allow required network communications.
d. Deploy three subnets with the option "Availability Zone" set to "None". Have all subnets contain a route table with a default route to the VPC's Internet Gateway. Configure a Network Access Control List (NACL) to allow all inbound traffic on the DMZ subnet. On the remaining subnets, configure NACLs to block all inbound traffic, except traffic from the DMZ subnet and the backend application subnet.

2. A company deploys a fleet of EC2 instances for hosting an internal Linux-based application. A SysOps administrator must implement a solution to allow team members to connect privately to the EC2 instances via Secure Shell Protocol (SSH). Which solution will meet this requirement in the MOST secure and operationally efficient way?

a. Deploy an EC2 instance with a public IP address and configure it as a bastion host. Configure the instance's security group to only allow access from office IP address ranges. Configure existing security groups to allow SSH access from bastion hosts.
b. Deploy EC2 instances in an autoscaling group behind an Elastic Load Balancer (ELB) with a public IP address. Configure the instances as bastion hosts. Configure the ELB's security group to allow access only from office IP address ranges. Configure existing security groups to allow SSH access from bastion hosts.

c. Write a Lambda function that starts an interactive SSH session with an EC2 instance. Configure the function's resource policy to only allow access from team members. Have the team use the Lambda function as a bastion host.
d. Ensure the AWS Systems Manager (SSM) agent is installed on all EC2 instances. Ensure team members' IAM policy allows users to start SSM sessions on EC2 instances. Have the team members use Session Manager to connect to EC2 instances.

3. A software company is developing a static landing page for a new mobile application. The company chooses Amazon S3 to host the static website. A SysOps administrator must set up and configure an Amazon S3 bucket for hosting the website. Which actions should the SysOps administrator take?

a. Create a bucket and edit the public access settings to make it publicly accessible. Configure the name of the index and error documents.
b. Create a bucket and enable static website hosting. Edit the public access settings to make it publicly accessible. Ensure no bucket policy is attached. Configure the name of the index and error documents.
c. Create a bucket and enable static website hosting. Edit the public access settings to make it publicly accessible. Add a bucket policy that makes the content publicly available for reads only. Configure the name of the index and error documents.
d. Create a bucket and edit the public access settings to make it publicly accessible. Add a bucket policy that makes the content publicly available for reads. Enable cross-region replication to all AWS regions.

4. A company runs a web application on AWS and hosts all static website content on Amazon S3. To improve static content delivery performance, a SysOps administrator must configure an Amazon CloudFront distribution to serve S3 content. The company also wants to ensure that users can only access the content through CloudFront.

Which actions should the SysOps administrator take? (Choose TWO.)

a. Configure an origin access identity (OAI) for the CloudFront distribution.
b. Configure the S3 bucket policy to allow the OAI principal to access the files in the bucket.
c. Configure the S3 bucket policy to allow the CloudFront service role to access the files in the bucket.
d. Configure a security group to only allow access from CloudFront edge IP address ranges.
e. Associate the security group with the S3 bucket.

5. A company runs a production workload distributed across six different regions on AWS. The company decides to use Amazon Route 53 to manage DNS records. A SysOps administrator must implement a solution to route user traffic based on the shortest physical distance between the user and the resources.
Which solution meets this requirement?

a. Create a Route 53 traffic policy. Add a Geolocation rule with the corresponding endpoint location for each region.
b. Create a Route 53 traffic policy. Add a Geoproximity rule with the corresponding endpoint location for each region.
c. Create a Route 53 traffic policy with a Latency rule. Configure a latency test.
d. Create two Route 53 traffic policies. Configure one policy with a Latency rule and a second policy with a Failover rule. Configure a health check.

Domain 6: Cost and Performance Optimization

1. A company needs to reduce unnecessary cloud expenses on AWS to meet its budget goals. How can a SysOps administrator help to identify underutilized or unused resources in an AWS account?

a. Use AWS CloudWatch to look for CPU utilization metrics for all resources. Identify resources with an average low CPU utilization.
b. Use AWS Cost Explorer. Under Savings Plans, check the Utilization report to identify underutilized resources.
c. Use AWS Trusted Advisor. Under the Cost Optimization checks. Look for resources flagged with low resource utilization. Check the Trusted Advisor's recommended remediation actions.
d. Use AWS Trusted Advisor. Under the Performance checks, ensure all resources are flagged with high resource utilization. Compile a list of resources that failed the check.

2. A company's Chief Financial Officer (CFO) wants better control over their AWS consumption costs and wants to ensure they remain within an allocated budget. A SysOps administrator must implement a solution to automatically notify the CFO when monthly consumption costs for an AWS account reaches 80% of the allocated monthly budget for that account. The company wants to prevent service disruptions and does not prefer to automatically shut down resources. Which solution will meet this requirement?

a. Configure an AWS budget for the account. Configure a CloudWatch alarm for when the Total Estimated Charge metric reaches 80% of the allocated budget. Upon an alarm, notify the CFO and downsize resources immediately to prevent resource usage from being automatically capped by AWS.
b. Configure an AWS budget for the account. Configure a budget alert with a threshold of 80% of the budgeted amount. Specify the CFO's email address in the Email recipients list.
c. Configure a CloudWatch alarm for when the Current Charge metric reaches 80% of the allocated budget. Publish the alarm notification to an Amazon Simple Notification Service (Amazon SNS) topic. Configure an Amazon SNS subscription with the email address of the CFO.

d. Write a script that continually calls the AWS Budget API to obtain the total forecasted monthly charges. Have the script send an email to the CFO if the value is greater than 80% of the allocated budget.

3. A company runs a web application on AWS that allows users to upload their pictures during a live event. Pictures are uploaded to Amazon S3. A SysOps administrator must implement a solution to improve the user upload transfer speed. Which actions should a SysOps administrator take to meet this requirement? (Choose TWO.)

   a. Create a CloudFront distribution.
   b. Enable Amazon S3 Transfer Acceleration.
   c. Update the S3 bucket policy.
   d. Update the S3 endpoint used in the client application.
   e. Configure an origin access identity (OAI).

4. A company uses AWS Organizations to create and manage several AWS accounts. The company wants to enforce a cost allocation tag for new resources created in any of the accounts. The tag must contain information about the user principal who created the resource. Which solution can a SysOps administrator implement to meet this requirement in the MOST operationally efficient way?

   a. Log in to the management account. In AWS Billing, activate the AWS-generated cost allocation tag aws:createdBy.
   b. Log in to the management account. In AWS Billing, create a user-defined cost allocation tag with the key createdBy and a placeholder value. Instruct all users to set the tag's value to their account IDs when creating a resource.
   c. In each account, use AWS Billing to activate the AWS-generated cost allocation tag aws:createdBy. Create an AWS Config rule to search for tagged resources and report compliance. Configure an automated remediation for non-compliant resources to set the tag with the account ID of the principal who created the resource.

d. Create an AWS CLI script that appends the tag createdBy to a specified resource and sets its value to the account ID of the caller. Have the script run as a post-creation job in deployment pipelines. Instruct users to run the script after each manual deployment.

5. A company wants to optimize the performance and resource utilization efficiency of its fleet of Amazon EC2 instances. All EC2 instances are backed by Elastic Block Storage (EBS) volumes. Some instances are part of an EC2 Auto Scaling group. A SysOps administrator must recommend optimal resource configurations to improve performance without incurring unnecessary costs. Which actions will allow the SysOps administrator to recommend the MOST optimal resource configurations?

   a. Identify all relevant performance metrics for EC2 and EBS resources. Create a custom CloudWatch dashboard with metrics graphs for a time span of 24 hours. Visually identify which metrics indicate performance bottlenecks or resource underutilization and make configuration recommendations accordingly. Repeat this exercise regularly.
   b. Run a performance test on all running instances simulating the highest expected load in production. Analyze relevant CloudWatch metrics to assess whether the workloads were able to sustain the load. In case of performance degradation, reconfigure resources with higher specifications and repeat the test until no degradation is observed.
   c. Configure Auto Scaling groups for any EC2 instances not currently in a group. Specify a minimum instance count of one and use the smallest available EC2 instance type. Specify a scaling metric and configure upper and lower thresholds for scaling events. Run several performance tests to assess and fine-tune scaling behavior.
   d. Enable AWS Compute Optimizer in the account. Allow up to 12 hours for findings to be collected. Analyze findings and view recommendations for EC2 instances, EBS volumes, and Auto Scaling groups. Review recommendations regularly over time.

Answers to Self-Assessment Questions:

Domain 1: Monitoring, Logging, and Remediation

1. A
2. D
3. B
4. B & D
5. B & C

Domain 2: Reliability and Business Continuity

1. C
2. A
3. C
4. A
5. C & D

Domain 3: Deployment, Provisioning, and Automation

1. B
2. A
3. A & D
4. D
5. C

Domain 4: Security and Compliance

1. C
2. B
3. A
4. B & D
5. B

Answers to Self-Assessment Questions:

Domain 5: Networking and Content Delivery

1. A
2. D
3. C
4. A & B
5. B

Domain 6: Cost and Performance Optimization

1. C
2. B
3. B & D
4. A
5. D