training and
certification

AWS Certified SysOps Administrator – Associate (SOA-C02) Exam Guide

Introduction

The AWS Certified SysOps Administrator – Associate (SOA-C02) exam is intended for system administrators in a cloud operations role. The exam validates a candidate's ability to deploy, manage, and operate workloads on AWS.

The exam also validates a candidate's ability to complete the following tasks:

- Support and maintain AWS workloads according to the AWS Well-Architected Framework
- Perform operations by using the AWS Management Console and the AWS CLI
- Implement security controls to meet compliance requirements
- Monitor, log, and troubleshoot systems
- Apply networking concepts (for example, DNS, TCP/IP, firewalls)
- Implement architectural requirements (for example, high availability, performance, capacity)
- Perform business continuity and disaster recovery procedures
- Identify, classify, and remediate incidents

Target candidate description

The target candidate should have 1 year of experience with deployment, management, networking, and security on AWS.

Recommended general IT knowledge

The target candidate should have the following knowledge:

- 1–2 years of experience as a systems administrator in an operations role
- Experience in monitoring, logging, and troubleshooting
- Knowledge of networking concepts (for example, DNS, TCP/IP, firewalls)
- Ability to implement architectural requirements (for example, high availability, performance, capacity)

Recommended AWS knowledge

The target candidate should have the following knowledge:

- Minimum of 1 year of hands-on experience with AWS technology
- Experience in deploying, managing, and operating workloads on AWS
- Understanding of the AWS Well-Architected Framework
- Hands-on experience with the AWS Management Console and the AWS CLI
- Understanding of AWS networking and security services
- Hands-on experience in implementing security controls and compliance requirements

What is considered out of scope for the target candidate?

The following is a non-exhaustive list of related job tasks that the target candidate is not expected to be able to perform. These items are considered out of scope for the exam:

- Design distributed architectures
- Design continuous integration and continuous delivery (CI/CD) pipelines
- Design hybrid and multi-VPC networking
- Develop software
- Define security, compliance, and governance requirements

For a detailed list of specific tools and technologies that might be covered on the exam, as well as lists of in-scope and out-of-scope AWS services, refer to the Appendix.

Exam content

Response types

There are three types of questions on the exam:

- **Multiple choice:** Has one correct response and three incorrect responses
- **Multiple response:** Has two or more correct responses out of five or more response options
- **Exam lab:** Has a scenario that is composed of a set of tasks to perform in the AWS Management Console or AWS CLI

Multiple choice and multiple response: Select one or more responses that best complete the statement or answer the question. Distractors, or incorrect answers, are response options that a candidate with incomplete knowledge or skill might choose. Distractors are generally plausible responses that match the content area.

All multiple-choice and multiple-response questions will appear at the start of the exam in one section. The end of this section will include a review screen, where you can return to any of the multiple-choice and multiple-response questions. This will be the last opportunity to answer the questions or change any answer selections. If your exam contains exam labs, that section will appear after the multiple-choice and multiple-response section. You will NOT be able to go back to the first section after you start the second section.

Exam labs: Complete the required tasks for a given scenario in the AWS Management Console or AWS CLI in the provided AWS account.

When you begin your exam, you will receive notification about the number of questions in the multiple-choice and multiple-response section, and the number of exam labs in the exam lab section. You will also learn the percentage of your score that will be determined by your work in the exam labs. Plan to leave 20 minutes to complete each exam lab.

Finish all work on an exam lab before you move to the next exam lab. You will NOT be able to return to a prior exam lab. You are welcome to use the virtual machine notepad or AWS CLI while working on your exam labs.

There might be more than one way to perform an exam lab. In those cases, you will receive full credit if you achieve the correct end state to the scenario. You will receive partial credit for partial completion of exam labs. However, exam content and the associated scoring are confidential, so you will receive no further information regarding partial credit that is awarded for an exam lab.

> Tip: If you take your exam through online proctoring, you can use an external monitor as your ONLY display. Set your screen resolution to 1280 pixels x 1024 pixels or greater for a PC, and 1440 pixels x 900 pixels or greater for a Mac. Set the scaling to 100%. Other settings might result in a need to scroll within the console.

On the exam, unanswered questions are scored as incorrect; there is no penalty for guessing. The exam includes 50 questions that affect your score. These questions include multiple-choice questions, multiple-response questions, and exam labs. Each scored multiple-choice question and each scored multiple-response question counts as a single scored opportunity. A scored exam lab includes multiple scored opportunities.

For a sample of the multiple-choice and multiple-response questions and exam labs, see AWS Certified SysOps Administrator – Associate (SOA-C02) Sample Exam Questions.

Unscored content

The exam includes 15 unscored questions that do not affect your score. AWS collects information about candidate performance on these unscored questions to evaluate these questions for future use as scored questions. These unscored questions are not identified on the exam.

Exam results

The AWS Certified SysOps Administrator – Associate (SOA-C02) exam is a pass or fail exam. The exam is scored against a minimum standard established by AWS professionals who follow certification industry best practices and guidelines.

Your results for the exam are reported as a scaled score of 100–1,000. The minimum passing score is 720. Your score shows how you performed on the exam as a whole and whether or not you passed. Scaled scoring models help equate scores across multiple exam forms that might have slightly different difficulty levels.

Your score report may contain a table of classifications of your performance at each section level. This information is intended to provide general feedback about your exam performance. The exam uses a compensatory scoring model, which means that you do not need to achieve a passing score in each section. You need to pass only the overall exam.

Each section of the exam has a specific weighting, so some sections have more questions than other sections have. The table contains general information that highlights your strengths and weaknesses. Use caution when interpreting section-level feedback.

Content outline

This exam guide includes weightings, test domains, and objectives for the exam. It is not a comprehensive listing of the content on the exam. However, additional context for each of the objectives is available to help guide your preparation for the exam. The following table lists the main content domains and their weightings. The table precedes the complete exam content outline, which includes the additional context. The percentage in each domain represents only scored content.

Domain	% of Exam
Domain 1: Monitoring, Logging, and Remediation	20%
Domain 2: Reliability and Business Continuity	16%
Domain 3: Deployment, Provisioning, and Automation	18%
Domain 4: Security and Compliance	16%
Domain 5: Networking and Content Delivery	18%
Domain 6: Cost and Performance Optimization	12%
TOTAL	100%

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)

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:

- Analytics
- Application Integration
- AWS Cost Management
- Compute
- Containers
- Database
- Management, Monitoring, and Governance
- Migration and Transfer
- Networking and Content Delivery
- Security, Identity, and Compliance
- Storage

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
- 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)

- 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

AWS Certified SysOps Administrator – Associate (SOA-C02)
Sample Exam Questions

1) **A company hosts a web application on an Amazon EC2 instance. Users report that the web application is occasionally unresponsive. Amazon CloudWatch metrics indicate that the CPU utilization is 100% during these times. A SysOps administrator must implement a solution to monitor for this issue.**

   Which solution will meet this requirement?

   A. Create a CloudWatch alarm that monitors AWS CloudTrail events for the EC2 instance.
   B. Create a CloudWatch alarm that monitors CloudWatch metrics for EC2 instance CPU utilization.
   C. Create an Amazon Simple Notification Service (Amazon SNS) topic to monitor CloudWatch metrics for EC2 instance CPU utilization.
   D. Create a recurring assessment check on the EC2 instance by using Amazon Inspector to detect deviations in CPU utilization.

2) **A company has an application that uses Amazon ElastiCache for Memcached to cache query responses to improve latency. However, the application's users are reporting slow response times. A SysOps administrator notices that the Amazon CloudWatch metrics for Memcached evictions are high.**

   Which actions should the SysOps administrator take to fix this issue? (Select TWO.)

   A. Flush the contents of ElastiCache for Memcached.
   B. Increase the ConnectionOverhead parameter value.
   C. Increase the number of nodes in the cluster.
   D. Increase the size of the nodes in the cluster.
   E. Decrease the number of nodes in the cluster.

3) **A company needs to ensure that an AWS Lambda function can access resources in a VPC in the company's account. The Lambda function requires access to third-party APIs that can be accessed only over the internet.**

   Which action should a SysOps administrator take to meet these requirements?

   A. Attach an Elastic IP address to the Lambda function and configure a route to the internet gateway of the VPC.
   B. Connect the Lambda function to a private subnet that has a route to the virtual private gateway of the VPC.
   C. Connect the Lambda function to a public subnet that has a route to the internet gateway of the VPC.
   D. Connect the Lambda function to a private subnet that has a route to a NAT gateway deployed in a public subnet of the VPC.

4) A company runs an application on a large fleet of Amazon EC2 instances to process financial transactions. The EC2 instances share data by using an Amazon Elastic File System (Amazon EFS) file system.

The company wants to deploy the application to a new Availability Zone and has created new subnets and a mount target in the new Availability Zone. When a SysOps administrator launches new EC2 instances in the new subnets, the EC2 instances are unable to mount the file system.

Which of the following is a possible reason for this issue?

A. The EFS mount target has been created in a private subnet.
B. The IAM role that is associated with the EC2 instances does not allow the efs:MountFileSystem action.
C. The route tables have not been configured to route traffic to a VPC endpoint for Amazon EFS in the new Availability Zone.
D. The security group for the mount target does not allow inbound NFS connections from the security group used by the EC2 instances.

5) A company uses AWS Organizations to create and manage many AWS accounts. The company wants to deploy new IAM roles in each account.

How could a SysOps administrator deploy the new roles in each of the organization's accounts?

A. Create a service control policy (SCP) in the organization to add the new IAM roles to each account.
B. Deploy an AWS CloudFormation change set to the organization with a template to create the new IAM roles.
C. Use AWS CloudFormation StackSets to deploy a template to each account to create the new IAM roles.
D. Use AWS Config to create an organization rule to add the new IAM roles to each account.

6) **A company runs several production workloads on Amazon EC2 instances. A SysOps administrator discovered that a production EC2 instance failed a system health check. The SysOps administrator recovered the instance manually.**

The SysOps administrator wants to automate the recovery task of EC2 instances and receive notifications whenever a system health check fails. Detailed monitoring is activated for all of the company's production EC2 instances.

Which of the following is the MOST operationally efficient solution that meets these requirements?

A. For each production EC2 instance, create an Amazon CloudWatch alarm for Status Check Failed: System. Set the alarm action to recover the EC2 instance. Configure the alarm notification to be published to an Amazon Simple Notification Service (Amazon SNS) topic.
B. On each production EC2 instance, create a script that monitors the system health by sending a heartbeat notification every minute to a central monitoring server. If an EC2 instance fails to send a heartbeat, run a script on the monitoring server to stop and start the EC2 instance and to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic.
C. On each production EC2 instance, create a script that sends network pings to a highly available endpoint by way of a cron job. If the script detects a network response timeout, invoke a command to reboot the EC2 instance.
D. On each production EC2 instance, configure an Amazon CloudWatch agent to collect and send logs to a log group in Amazon CloudWatch Logs. Create a CloudWatch alarm that is based on a metric filter that tracks errors. Configure the alarm to invoke an AWS Lambda function to reboot the EC2 instance and send a notification email.

7) **The company uses AWS Organizations to manage its accounts. For the production account, a SysOps administrator must ensure that all data is backed up daily for all current and future Amazon EC2 instances and Amazon Elastic File System (Amazon EFS) file systems. Backups must be retained for 30 days.**

Which solution will meet these requirements with the LEAST amount of effort?

A. Create a backup plan in AWS Backup. Assign resources by resource ID, selecting all existing EC2 and EFS resources that are running in the account. Edit the backup plan daily to include any new resources. Schedule the backup plan to run every day with a lifecycle policy to expire backups after 30 days.
B. Create a backup plan in AWS Backup. Assign resources by tags. Ensure that all existing EC2 and EFS resources are tagged correctly. Apply a service control policy (SCP) for the production account OU that prevents instance and file system creation unless the correct tags are applied. Schedule the backup plan to run every day with a lifecycle policy to expire backups after 30 days.
C. Create a lifecycle policy in Amazon Data Lifecycle Manager (Amazon DLM). Assign all resources by resource ID, selecting all existing EC2 and EFS resources that are running in the account. Edit the lifecycle policy daily to include any new resources. Schedule the lifecycle policy to create snapshots every day with a retention period of 30 days.
D. Create a lifecycle policy in Amazon Data Lifecycle Manager (Amazon DLM). Assign all resources by tags. Ensure that all existing EC2 and EFS resources are tagged correctly. Apply a service control policy (SCP) that prevents resource creation unless the correct tags are applied. Schedule the lifecycle policy to create snapshots every day with a retention period of 30 days.

8) **A company is using AWS CloudTrail and wants to ensure that SysOps administrators can easily verify that the log files have not been deleted or changed.**

Which action should a SysOps administrator take to meet this requirement?

A. Grant administrators access to the AWS Key Management Service (AWS KMS) key used to encrypt the log files.
B. Enable CloudTrail log file integrity validation when the trail is created or updated.
C. Turn on Amazon S3 server access logging for the bucket storing the log files.
D. Configure the S3 bucket to replicate the log files to another bucket.

9) **A company is running a custom database on an Amazon EC2 instance. The database stores its data on an Amazon Elastic Block Store (Amazon EBS) volume. A SysOps administrator must set up a backup strategy for the EBS volume.**

What should the SysOps administrator do to meet this requirement?

A. Create an Amazon CloudWatch alarm for the VolumeIdleTime metric with an action to take a snapshot of the EBS volume.
B. Create a pipeline in AWS Data Pipeline to take a snapshot of the EBS volume on a recurring schedule.
C. Create an Amazon Data Lifecycle Manager (Amazon DLM) policy to take a snapshot of the EBS volume on a recurring schedule.
D. Create an AWS DataSync task to take a snapshot of the EBS volume on a recurring schedule.

10) **A company runs a large number of Amazon EC2 instances for internal departments. The company needs to track the costs of its existing AWS resources by department.**

What should a SysOps administrator do to meet this requirement?

A. Activate all of the AWS generated cost allocation tags for the account.
B. Apply user-defined tags to the instances through Tag Editor. Activate these tags for cost allocation.
C. Schedule an AWS Lambda function to run the AWS Pricing Calculator for EC2 usage on a recurring schedule.
D. Use the AWS Trusted Advisor dashboard to export EC2 cost reports.

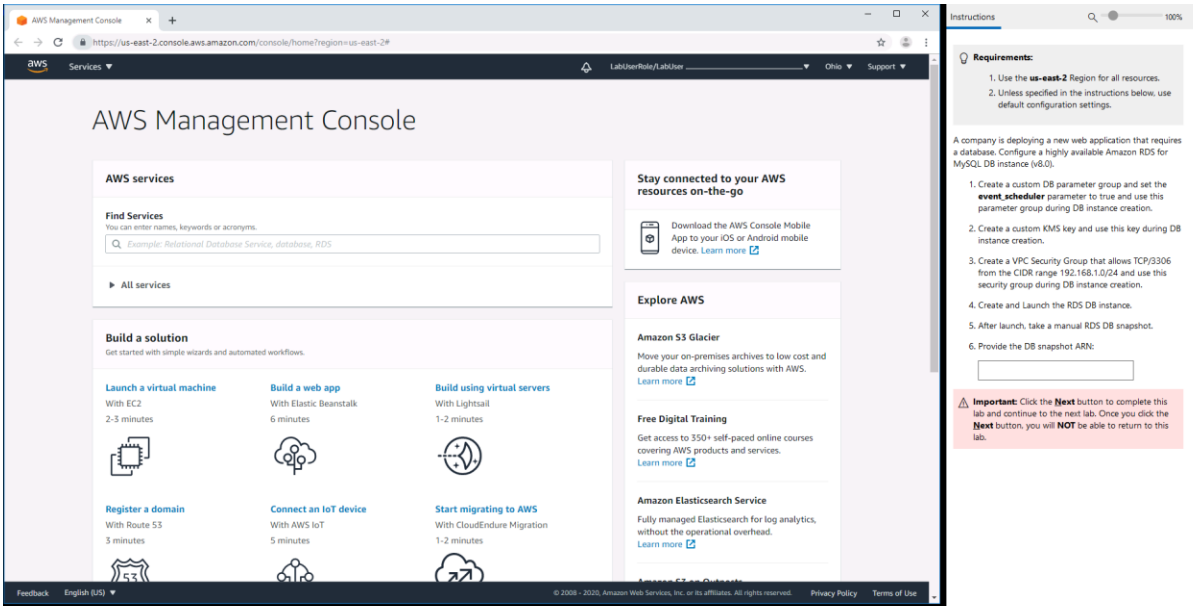
11) Sample Exam Lab

A company is deploying a new web application. Configure a highly available MySQL 8.0 database with the following:

1. Create a custom DB parameter group and set the **event_scheduler** parameter to true and use this parameter during DB instance creation.
2. Create a custom AWS Key Management Service (AWS KMS) key and use this key during DB instance creation.
3. Create a VPC security group that allows TCP port 3306 from the CIDR block 192.168.1.0/24. Use this security group during DB instance creation.
4. Launch the Amazon RDS DB instance.
5. After launch, take a manual RDS DB snapshot.

Provide the snapshot Amazon Resource Name (ARN): ________________

Note: Below is a screenshot of how this sample exam lab would appear during the exam.



AWS Management Console

AWS services

Find Services
You can enter names, keywords or acronyms.
Example: Relational Database Service, database, RDS

▶ All services

Build a solution
Get started with simple wizards and automated workflows.

Launch a virtual machine
With EC2
2-3 minutes

Build a web app
With Elastic Beanstalk
6 minutes

Build using virtual servers
With Lightsail
1-2 minutes

Register a domain
With Route 53
3 minutes

Connect an IoT device
With AWS IoT
5 minutes

Start migrating to AWS
With CloudEndure Migration
1-2 minutes

Stay connected to your AWS resources on-the-go

Download the AWS Console Mobile App to your iOS or Android mobile device. Learn more

Explore AWS

Amazon S3 Glacier
Move your on-premises archives to low cost and durable data archiving solutions with AWS.
Learn more

Free Digital Training
Get access to 350+ self-paced online courses covering AWS products and services.
Learn more

Amazon Elasticsearch Service
Fully managed Elasticsearch for log analytics, without the operational overhead.
Learn more

Feedback English (US) ▼ © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Requirements:

1. Use the **us-east-2** Region for all resources.
2. Unless specified in the instructions below, use default configuration settings.

A company is deploying a new web application that requires a database. Configure a highly available Amazon RDS for MySQL DB instance (v8.0).

1. Create a custom DB parameter group and set the **event_scheduler** parameter to true and use this parameter group during DB instance creation.
2. Create a custom KMS key and use this key during DB instance creation.
3. Create a VPC Security Group that allows TCP/3306 from the CIDR range 192.168.1.0/24 and use this security group during DB instance creation.
4. Create and Launch the RDS DB instance.
5. After launch, take a manual RDS DB snapshot.
6. Provide the DB snapshot ARN:

⚠ **Important:** Click the **Next** button to complete this lab and continue to the next lab. Once you click the **Next** button, you will **NOT** be able to return to this lab.

Answers

1) B — Amazon CloudWatch provides you with data and actionable insights to monitor your applications. Amazon EC2 sends metrics to CloudWatch. The CPUUtilization metric represents the percentage of allocated EC2 compute units that are currently in use on an instance. You can create a CloudWatch alarm that monitors CPUUtilization for one of your instances. For example, you might want to receive an email notification when the average CPUUtilization over a 5-minute period is greater than 75%.

2) C, D — The Evictions metric for Amazon ElastiCache for Memcached represents the number of non-expired items that the cache evicted to provide space for new items. If you are experiencing evictions with your cluster, it is usually a sign that you need to scale up (use a node that has a larger memory footprint) or scale out (add additional nodes to the cluster) to accommodate the additional data.

3) D — By default, AWS Lambda runs your functions in a secure VPC with access to AWS services and the internet. Lambda owns this VPC, which is not connected to your account's default VPC. When you connect a Lambda function to a VPC in your account to access private resources, the function cannot access the internet unless your VPC provides access. Internet access from a private subnet requires network address translation (NAT). To give your function access to the internet, route outbound traffic to a NAT gateway in a public subnet.

4) D — The security groups that you associate with a mount target must allow inbound access for the TCP protocol on the NFS port from the security group used by the instances.

5) C — With AWS CloudFormation StackSets, you can create, update, or delete stacks across multiple accounts and AWS Regions with a single operation. A user in the AWS Organizations management account can create a stack set with service-managed permissions that deploys stack instances to accounts in the organization or in specific organizational units (OUs). For example, you can use AWS CloudFormation StackSets to deploy your centralized IAM roles to all accounts in your organization.

6) A — You can use Amazon CloudWatch alarm actions to create alarms that automatically stop, terminate, reboot, or recover your Amazon EC2 instances. For example, if an instance becomes impaired due to hardware or software issues on the physical host, loss of network connectivity, or loss of system power, you can automatically initiate a recovery action to migrate the instance to new hardware. You also can configure a message to be published to an Amazon Simple Notification Service (Amazon SNS) topic to receive a notification of the recovery action.

7) B — AWS Backup is a fully managed backup service that makes it easy to centralize and automate the backup of data across AWS services. The use of tags to assign resources is a simple and scalable way to back up multiple resources. Any resources with the tags that you specify are assigned to the backup plan. A tag policy is a type of service control policy (SCP) in AWS Organizations that can help you standardize and enforce tags across resources in your organization's accounts.

8) B — You can validate the integrity of AWS CloudTrail log files and detect whether the log files were unchanged, modified, or deleted since CloudTrail delivered them to your Amazon S3 bucket. With a validated log file, you can assert positively that the log file itself has not changed, or that particular user credentials performed specific API activity. The CloudTrail log file integrity validation process also informs

you if a log file has been deleted or changed. You gain the insight to assert positively that log files either were delivered or were not delivered to your account during a given period of time. You can activate log file integrity validation with the CloudTrail console when you create or update a trail.

9) C — You can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation, retention, and deletion of Amazon Elastic Block Store (Amazon EBS) snapshots. You can create a lifecycle policy that includes specific tags to back up EBS volumes on a specified schedule and for a specified retention period. For example, you can take a snapshot of an EBS volume every day and keep the snapshots for 30 days.

10) B — User-defined tags are tags that you define, create, and apply to resources manually. You can use Tag Editor to search for all resources and apply tags to them. Use cost allocation tags to track your AWS costs on a detailed level. After you activate cost allocation tags, AWS uses the tags to organize your resource costs to make it easier for you to categorize and track your AWS costs. For example, to track costs by department, you can use a tag that is named "Department" with the value equal to the department name.

11) Lab solution:

Create a custom DB parameter group and set the event_scheduler parameter to true and use this parameter during DB instance creation.

i. Open the Amazon RDS console from https://console.amazonaws.com/rds/.
ii. In the **Resources** section, choose **Parameter groups**.
iii. Choose **Create parameter group**.
iv. In the **Parameter group family** list, select **mysql8.0**
v. In the **Group name** box, enter the new DB cluster parameter group name of **mysql80witheventscheduler**.
vi. In the **Description** box, enter a description for the new DB cluster parameter group.
vii. Choose **Create**.
viii. In the list of parameter groups, check the box next to the parameter group that you want to modify, which is **mysql80witheventscheduler**.
ix. Choose **Parameter group actions** and choose **Edit**.
x. In the **Filter parameters** box, enter **event_s**. This should filter just the **event_scheduler** parameter.
xi. Choose the box for the **event_scheduler** parameter. Under **Values**, change the setting to **ON**.
xii. Choose **Save changes**.

Create a custom AWS Key Management Service (AWS KMS) key and use this key during DB instance creation.

Open the AWS KMS console from https://console.aws.amazon.com/kms.

i. In the navigation pane, choose **Customer managed keys**.
ii. Choose **Create key**.
iii. To create a symmetric CMK, for **Key type,** choose **Symmetric**.
iv. Choose **Next**.
v. Type the alias or display name for the CMK. For this walkthrough, use the value **mysqlDbKey**
vi. (Optional) Type a description for the CMK.
vii. Choose **Next**.
viii. (Optional) To add a tag, click **Add tag**. Type a tag key and an optional tag value. To add more than one tag to the CMK, choose **Add tag**.

ix. Once completed, choose **Next**.
x. Select the IAM users and roles that can administer the CMK. For this walkthrough, use your IAM user.
xi. Choose **Next**.
xii. Select the IAM users and roles that can use the CMK for cryptographic operations. For this walkthrough, none are needed.
xiii. Choose **Next**.
xiv. Review the key policy document that was created from your choices. Note that it can also be edited.
xv. Choose **Finish** to create the CMK.

Create a VPC security group that allows TCP port 3306 from the CIDR block 192.168.1.0/24 and use this security group during DB instance creation.

i. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/home.
ii. In the navigation pane, choose **Security Groups**.
iii. Choose **Create security group**.
iv. Enter a name for the security group (for example, **mysqlAccessGroup**) and then provide a description.
v. From **VPC**, select the ID of your VPC.
vi. Under **Inbound rules**, choose **Add rule**.
vii. Set **Type** to **MYSQL/Aurora.**
viii. Set **Source** to **My IP.**
ix. Scroll down and choose **Create security group**.

Launch the Amazon RDS DB instance.

i. Open the Amazon RDS console from https://console.aws.amazon.com/rds/.
ii. In the navigation pane, choose **Databases**.
iii. Choose **Create database**.
iv. On the **Create database** page, verify that the **Standard create** option is chosen. Then choose **MySQL**.
v. In the **Templates** section, choose **Production.**
vi. In the **DB instance identifier** section, type the name **mysqldemo**
vii. In the **Settings** section, set these values:
    i. **Master password**
    ii. **Confirm password** – Retype the password.
viii. In the **DB instance size** section, set these values:
    iii. **Burstable classes (includes t classes)**
    iv. **db.t3.micro**
ix. In the **Connectivity** section, for **Virtual private cloud (VPC)**, choose an existing VPC.
x. Expand the **Additional connectivity configuration** menu and set these values:
    v. For **Subnet group** select the DB subnet group.
    vi. For **Public access**, select **No**.
    vii. For **Existing VPC security groups** choose **mysqlAccessGroup**.
xi. Remove the other existing security groups, such as the default security group, by choosing the **X** associated with each.
xii. Expand the **Additional configuration** section.
xiii. For the **DB parameter group**, select **mysql80witheventscheduler**
xiv. For **Master key,** select **mysqlDbKey**
xv. Choose **Create database** to create your RDS MySQL DB instance.

After launch, take a manual RDS DB snapshot.

i. Open the Amazon RDS console from https://console.aws.amazon.com/rds/.
ii. In the navigation pane, choose **Databases**.
iii. In the list of DB instances, choose the DB instance for which you want to take a snapshot.

iv. Choose **Actions** and choose **Take snapshot**.
v. The **Take DB snapshot** window appears.
vi. In the **Snapshot name** box, type the name of the snapshot. For this walkthrough, use **mysqlsnapshot**.
vii. Choose **Take snapshot**.
viii. From the RDS console, in the navigation pane, choose **Snapshots**.
ix. Choose the snapshot name **mysqlsnapshot**
x. In the **Details** section, note the ARN field and the ARN.

Provide the DB snapshot ARN: ____________