



**Amazon**

## **Exam Questions AWS-SysOps**

Amazon AWS Certified SysOps Administrator - Associate

### NEW QUESTION 1

- (Exam Topic 1)

A company hosts an application on an Amazon EC2 instance in a single AWS Region. The application requires support for non-HTTP TCP traffic and HTTP traffic. The company wants to deliver content with low latency by leveraging the AWS network. The company also wants to implement an Auto Scaling group with an Elastic Load Balancer.

How should a SysOps administrator meet these requirements?

- A. Create an Auto Scaling group with an Application Load Balancer (ALB). Add an Amazon CloudFront distribution with the ALB as the origin.
- B. Create an Auto Scaling group with an Application Load Balancer (ALB). Add an accelerator with AWS Global Accelerator with the ALB as an endpoint.
- C. Create an Auto Scaling group with a Network Load Balancer (NLB). Add an Amazon CloudFront distribution with the NLB as the origin.
- D. Create an Auto Scaling group with a Network Load Balancer (NLB). Add an accelerator with AWS Global Accelerator with the NLB as an endpoint.

**Answer:** D

#### Explanation:

AWS Global Accelerator and Amazon CloudFront are separate services that use the AWS global network and its edge locations around the world. CloudFront improves performance for both cacheable content (such as images and videos) and dynamic content (such as API acceleration and dynamic site delivery). Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover. Both services integrate with AWS Shield for DDoS protection.

<https://medium.com/awesome-cloud/aws-difference-between-application-load-balancer-and-network-load-balan> [https://aws.amazon.com/global-accelerator/faqs/?nc1=h\\_ls](https://aws.amazon.com/global-accelerator/faqs/?nc1=h_ls)

### NEW QUESTION 2

- (Exam Topic 1)

A company runs workloads on 90 Amazon EC2 instances in the eu-west-1 Region in an AWS account. In 2 months, the company will migrate the workloads from eu-west-1 to the eu-west-3 Region.

The company needs to reduce the cost of the EC2 instances. The company is willing to make a 1-year commitment that will begin next week. The company must choose an EC2 Instance purchasing option that will provide discounts for the 90 EC2 Instances regardless of Region during the 1-year period. Which solution will meet these requirements?

- A. Purchase EC2 Standard Reserved Instances.
- B. Purchase an EC2 Instance Savings Plan.
- C. Purchase EC2 Convertible Reserved Instances.
- D. Purchase a Compute Savings Plan.

**Answer:** B

### NEW QUESTION 3

- (Exam Topic 1)

A SysOps administrator needs to give users the ability to upload objects to an Amazon S3 bucket. The SysOps administrator creates a presigned URL and provides the URL to a user, but the user cannot upload an object to the S3 bucket. The presigned URL has not expired, and no bucket policy is applied to the S3 bucket.

Which of the following could be the cause of this problem?

- A. The user has not properly configured the AWS CLI with their access key and secret access key.
- B. The SysOps administrator does not have the necessary permissions to upload the object to the S3 bucket.
- C. The SysOps administrator must apply a bucket policy to the S3 bucket to allow the user to upload the object.
- D. The object already has been uploaded through the use of the presigned URL, so the presigned URL is no longer valid.

**Answer:** B

### NEW QUESTION 4

- (Exam Topic 1)

A company is deploying a third-party unit testing solution that is delivered as an Amazon EC2 Amazon Machine Image (AMI). All system configuration data is stored in Amazon DynamoDB. The testing results are stored in Amazon S3.

A minimum of three EC2 instances are required to operate the product. The company's testing team wants to use an additional three EC2 Instances when the Spot Instance prices are at a certain threshold. A SysOps administrator must Implement a highly available solution that provides this functionality.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Define an Amazon EC2 Auto Scaling group by using a launch configuratio
- B. Use the provided AMI In the launch configuratio
- C. Configure three On-Demand Instances and three Spot Instance
- D. Configure a maximum Spot Instance price In the launch configuration.
- E. Define an Amazon EC2 Auto Scaling group by using a launch templat
- F. Use the provided AMI in the launch templat
- G. Configure three On-Demand Instances and three Spot Instance
- H. Configure a maximum Spot Instance price In the launch template.
- I. Define two Amazon EC2 Auto Scaling groups by using launch configuration
- J. Use the provided AMI in the launch configuration
- K. Configure three On-Demand Instances for one Auto Scaling grou
- L. Configure three Spot Instances for the other Auto Scaling grou
- M. Configure a maximum Spot Instance price in the launch configuration for the Auto Scaling group that has Spot Instances.
- N. Define two Amazon EC2 Auto Scaling groups by using launch template
- O. Use the provided AMI in the launch template
- P. Configure three On-DemandInstances for one Auto Scaling grou
- Q. Configure three Spot Instances for the other Auto Scaling grou
- R. Configure a maximum Spot Instance price in the launch template for the Auto Scaling group that has Spot Instances.

**Answer:** A

**Explanation:**

- <https://docs.aws.amazon.com/autoscaling/ec2/userguide/LaunchTemplates.html>
- <https://docs.aws.amazon.com/autoscaling/ec2/userguide/LaunchConfiguration.html>

**NEW QUESTION 5**

- (Exam Topic 1)

A SysOps administrator creates an AWS CloudFormation template to define an application stack that can be deployed in multiple AWS Regions.

The SysOps administrator also creates an Amazon CloudWatch dashboard by using the AWS Management Console. Each deployment of the application requires its own CloudWatch dashboard.

How can the SysOps administrator automate the creation of the CloudWatch dashboard each time the application is deployed?

- A. Create a script by using the AWS CLI to run the `aws cloudformation put-dashboard` command with the name of the dashboard
- B. Run the command each time a new CloudFormation stack is created.
- C. Export the existing CloudWatch dashboard as JSON
- D. Update the CloudFormation template to define an `AWS::CloudWatch::Dashboard` resource
- E. Include the exported JSON in the resource's `DashboardBody` property.
- F. Update the CloudFormation template to define a resource
- G. Use the `intrinsic Ref` function to reference the ID of the existing CloudWatch dashboard.
- H. Update the CloudFormation template to define an `AWS::CloudWatch::Dashboard` resource
- I. Specify the name of the existing dashboard in the `DashboardName` property.

**Answer:** B

**Explanation:**

You can only use the `Intrinsic Ref` function to reference a resource that is being created at the same time as the current CloudFormation template. The question states that the CloudWatch dashboard was previously created using the AWS Management Console, so there is no ID to reference the existing CloudWatch dashboard in the CloudFormation template. You would need to export the existing CloudWatch dashboard as JSON, then use the `DashboardBody` property in the CloudFormation template to replicate it upon each deployment

(<https://docs.aws.amazon.com/AmazonCloudWatch/latest/APIReference/CloudWatch-Dashboard-Body-Structu>)

**NEW QUESTION 6**

- (Exam Topic 1)

A company needs to view a list of security groups that are open to the internet on port 3389. What should a SysOps administrator do to meet this requirement?

- A. Configure Amazon GuardDuty to scan security groups and report unrestricted access on port 3389.
- B. Configure a service control policy (SCP) to identify security groups that allow unrestricted access on port 3389
- C. Use AWS Identity and Access Management Access Analyzer to find any instances that have unrestricted access on port 3389.
- D. Use AWS Trusted Advisor to find security groups that allow unrestricted access on port 3389.

**Answer:** D

**NEW QUESTION 7**

- (Exam Topic 1)

A SysOps administrator developed a Python script that uses the AWS SDK to conduct several maintenance tasks. The script needs to run automatically every night.

What is the MOST operationally efficient solution that meets this requirement?

- A. Convert the Python script to an AWS Lambda function
- B. Use an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke the function every night.
- C. Convert the Python script to an AWS Lambda function
- D. Use AWS CloudTrail to invoke the function every night.
- E. Deploy the Python script to an Amazon EC2 instance
- F. Use Amazon EventBridge (Amazon CloudWatch Events) to schedule the instance to start and stop every night.
- G. Deploy the Python script to an Amazon EC2 instance
- H. Use AWS Systems Manager to schedule the instance to start and stop every night.

**Answer:** A

**NEW QUESTION 8**

- (Exam Topic 1)

A company migrated an I/O intensive application to an Amazon EC2 general purpose instance. The EC2 instance has a single General Purpose SSD Amazon Elastic Block Store (Amazon EBS) volume attached.

Application users report that certain actions that require intensive reading and writing to the disk are taking much longer than normal or are failing completely. After reviewing the performance metrics of the EBS volume, a SysOps administrator notices that the `VolumeQueueLength` metric is consistently high during the same times in which the users are reporting issues. The SysOps administrator needs to resolve this problem to restore full performance to the application.

Which action will meet these requirements?

- A. Modify the instance type to be storage optimized.
- B. Modify the volume properties by deselecting `Auto-Enable Volume 10`.
- C. Modify the volume properties to increase the IOPS.
- D. Modify the instance to enable enhanced networking.

**Answer:** C

**NEW QUESTION 9**

- (Exam Topic 1)

A SysOps administrator uses AWS Systems Manager Session Manager to connect to instances. After the SysOps administrator launches a new Amazon EC2 instance, the EC2 instance does not appear in the Session Manager list of systems that are available for connection. The SysOps administrator verifies that Systems Manager Agent is installed, updated, and running on the EC2 instance. What is the reason for this issue?

- A. The SysOps administrator does not have access to the key pair that is required for connection.
- B. The SysOps administrator has not attached a security group to the EC2 instance to allow SSH on port 22.
- C. The EC2 instance does not have an attached IAM role that allows Session Manager to connect to the EC2 instance.
- D. The EC2 instance ID has not been entered into the Session Manager configuration.

**Answer: C**

#### NEW QUESTION 10

- (Exam Topic 1)

A company is managing many accounts by using a single organization in AWS Organizations. The organization has all features enabled. The company wants to turn on AWS Config in all the accounts of the organization and in all AWS Regions. What should a SysOps administrator do to meet these requirements in the MOST operationally efficient way?

- A. Use AWS CloudFormation StackSets to deploy stack instances that turn on AWS Config in all accounts and in all Regions.
- B. Use AWS CloudFormation StackSets to deploy stack policies that turn on AWS Config in all accounts and in all Regions.
- C. Use service control policies (SCPs) to configure AWS Config in all accounts and in all Regions.
- D. Create a script that uses the AWS CLI to turn on AWS Config in all accounts in the organization.
- E. Run the script from the organization's management account.

**Answer: C**

#### NEW QUESTION 10

- (Exam Topic 1)

A company is testing Amazon Elasticsearch Service (Amazon ES) as a solution for analyzing system logs from a fleet of Amazon EC2 instances. During the test phase, the domain operates on a single-node cluster. A SysOps administrator needs to transition the test domain into a highly available production-grade deployment.

Which Amazon ES configuration should the SysOps administrator use to meet this requirement?

- A. Use a cluster of four data nodes across two AWS Regions.
- B. Deploy four dedicated master nodes in each Region.
- C. Use a cluster of six data nodes across three Availability Zones.
- D. Use three dedicated master nodes.
- E. Use a cluster of six data nodes across three Availability Zones.
- F. Use six dedicated master nodes.
- G. Use a cluster of eight data nodes across two Availability Zones.
- H. Deploy four master nodes in a failover AWS Region.

**Answer: B**

#### NEW QUESTION 11

- (Exam Topic 1)

A company runs an application on an Amazon EC2 instance. A SysOps administrator creates an Auto Scaling group and an Application Load Balancer (ALB) to handle an increase in demand. However, the EC2 instances are failing the health check.

What should the SysOps administrator do to troubleshoot this issue?

- A. Verify that the Auto Scaling group is configured to use all AWS Regions.
- B. Verify that the application is running on the protocol and the port that the listener is expecting.
- C. Verify the listener priority in the ALB. Change the priority if necessary.
- D. Verify the maximum number of instances in the Auto Scaling group. Change the number if necessary.

**Answer: B**

#### NEW QUESTION 14

- (Exam Topic 1)

A SysOps administrator is optimizing the cost of a workload. The workload is running in multiple AWS Regions and is using AWS Lambda with Amazon EC2 On-Demand Instances for the compute. The overall usage is predictable. The amount of compute that is consumed in each Region varies, depending on the users' locations.

Which approach should the SysOps administrator use to optimize this workload?

- A. Purchase Compute Savings Plans based on the usage during the past 30 days.
- B. Purchase Convertible Reserved Instances by calculating the usage baseline.
- C. Purchase EC2 Instance Savings Plan based on the usage during the past 30 days.
- D. Purchase Standard Reserved Instances by calculating the usage baseline.

**Answer: C**

#### NEW QUESTION 18

- (Exam Topic 1)

A software development company has multiple developers who work on the same product. Each developer must have their own development environment, and these development environments must be identical. Each development environment consists of Amazon EC2 instances and an Amazon RDS DB instance. The development environments should be created only when necessary, and they must be terminated each night to minimize costs.

What is the MOST operationally efficient solution that meets these requirements?



- A. Provide developers with access to the same AWS CloudFormation template so that they can provision their development environment when necessary
- B. Schedule a nightly cron job on each development instance to stop all running processes to reduce CPU utilization to nearly zero.
- C. Provide developers with access to the same AWS CloudFormation template so that they can provision their development environment when necessary
- D. Schedule a nightly Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function to delete the AWS CloudFormation stacks.
- E. Provide developers with CLI commands so that they can provision their own development environment when necessary
- F. Schedule a nightly Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function to terminate all EC2 instances and the DB instance.
- G. Provide developers with CLI commands so that they can provision their own development environment when necessary
- H. Schedule a nightly Amazon EventBridge (Amazon CloudWatch Events) rule to cause AWS CloudFormation to delete all of the development environment resources.

**Answer: B**

#### NEW QUESTION 22

- (Exam Topic 1)

A company has a new requirement stating that all resources in AWS must be tagged according to a set policy. Which AWS service should be used to enforce and continually identify all resources that are not in compliance with the policy?

- A. AWS CloudTrail
- B. Amazon Inspector
- C. AWSConfig
- D. AWS Systems Manager

**Answer: C**

#### NEW QUESTION 27

- (Exam Topic 1)

A company needs to view a list of security groups that are open to the internet on port 3389. What should a SysOps administrator do to meet this requirement?

- A. Configure Amazon GuardDuty to scan security groups and report unrestricted access on port 3389.
- B. Configure a service control policy (SCP) to identify security groups that allow unrestricted access on port 3389.
- C. Use AWS Identity and Access Management Access Analyzer to find any instances that have unrestricted access on port 3389.
- D. Use AWS Trusted Advisor to find security groups that allow unrestricted access on port 3389

**Answer: D**

#### NEW QUESTION 29

- (Exam Topic 1)

A new application runs on Amazon EC2 instances and accesses data in an Amazon RDS database instance. When fully deployed in production, the application fails. The database can be queried from a console on a bastion host. When looking at the web server logs, the following error is repeated multiple times:

\*\*\* Error Establishing a Database Connection

Which of the following may be causes of the connectivity problems? (Select TWO.)

- A. The security group for the database does not have the appropriate egress rule from the database to the web server.
- B. The certificate used by the web server is not trusted by the RDS instance.
- C. The security group for the database does not have the appropriate ingress rule from the web server to the database.
- D. The port used by the application developer does not match the port specified in the RDS configuration.
- E. The database is still being created and is not available for connectivity.

**Answer: CD**

#### NEW QUESTION 33

- (Exam Topic 1)

A company's SysOps administrator deploys a public Network Load Balancer (NLB) in front of the company's web application. The web application does not use any Elastic IP addresses. Users must access the web application by using the company's domain name. The SysOps administrator needs to configure Amazon Route 53 to route traffic to the NLB.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a Route 53 AAAA record for the NLB.
- B. Create a Route 53 alias record for the NLB.
- C. Create a Route 53 CAA record for the NLB.
- D. Create a Route 53 CNAME record for the NLB.

**Answer: B**

#### NEW QUESTION 36

- (Exam Topic 1)

A company is running a serverless application on AWS Lambda. The application stores data in an Amazon RDS for MySQL DB instance. Usage has steadily increased and recently there have been numerous "too many connections" errors when the Lambda function attempts to connect to the database. The company already has configured the database to use the maximum max\_connections value that is possible.

What should a SysOps administrator do to resolve these errors?

- A. Create a read replica of the database. Use Amazon Route 53 to create a weighted DNS record that contains both databases.
- B. Use Amazon RDS Proxy to create a proxy. Update the connection string in the Lambda function.
- C. Increase the value in the max\_connect\_errors parameter in the parameter group that the database uses.
- D. Update the Lambda function's reserved concurrency to a higher value.

**Answer: B**

**Explanation:**

<https://aws.amazon.com/blogs/compute/using-amazon-rds-proxy-with-aws-lambda/>

RDS Proxy acts as an intermediary between your application and an RDS database. RDS Proxy establishes and manages the necessary connection pools to your database so that your application creates fewer database connections. Your Lambda functions interact with RDS Proxy instead of your database instance. It handles the connection pooling necessary for scaling many simultaneous connections created by concurrent Lambda functions. This allows your Lambda applications to reuse existing connections, rather than creating new connections for every function invocation.

Check "Database proxy for Amazon RDS" section in the link to see how RDS proxy help Lambda handle huge connections to RDS MySQL

<https://aws.amazon.com/blogs/compute/using-amazon-rds-proxy-with-aws-lambda/>

**NEW QUESTION 38**

- (Exam Topic 1)

An AWS Lambda function is intermittently failing several times a day A SysOps administrator must find out how often this error has occurred in the last 7 days Which action will meet this requirement in the MOST operationally efficient manner?

- A. Use Amazon Athena to query the Amazon CloudWatch logs that are associated with the Lambda function
- B. Use Amazon Athena to query the AWS CloudTrail logs that are associated with the Lambda function
- C. Use Amazon CloudWatch Logs Insights to query the associated Lambda function logs
- D. Use Amazon Elasticsearch Service (Amazon ES) to stream the Amazon CloudWatch logs for the Lambda function

**Answer: C**

**NEW QUESTION 39**

- (Exam Topic 1)

A SysOps administrator is responsible for a company's security groups. The company wants to maintain a documented trail of any changes that are made to the security groups. The SysOps administrator must receive notification whenever the security groups change.

Which solution will meet these requirements?

- A. Set up Amazon Detective to record security group change
- B. Specify an Amazon CloudWatch Logs log group to store configuration history log
- C. Create an Amazon Simple Queue Service (Amazon SQS) queue for notifications about configuration change
- D. Subscribe the SysOps administrator's email address to the SQS queue.
- E. Set up AWS Systems Manager Change Manager to record security group change
- F. Specify an Amazon CloudWatch Logs log group to store configuration history log
- G. Create an Amazon Simple Notification Service (Amazon SNS) topic for notifications about configuration change
- H. Subscribe the SysOps administrator's email address to the SNS topic.
- I. Set up AWS Config to record security group change
- J. Specify an Amazon S3 bucket as the location for configuration snapshots and history file
- K. Create an Amazon Simple Notification Service (Amazon SNS) topic for notifications about configuration change
- L. Subscribe the SysOps administrator's email address to the SNS topic.
- M. Set up Amazon Detective to record security group change
- N. Specify an Amazon S3 bucket as the location for configuration snapshots and history file
- O. Create an Amazon Simple Notification Service (Amazon SNS) topic for notifications about configuration change
- P. Subscribe the SysOps administrator's email address to the SNS topic.

**Answer: D**

**NEW QUESTION 40**

- (Exam Topic 1)

A company using AWS Organizations requires that no Amazon S3 buckets in its production accounts should ever be deleted.

What is the SIMPLEST approach the SysOps administrator can take to ensure S3 buckets in those accounts can never be deleted?

- A. Set up MFA Delete on all the S3 buckets to prevent the buckets from being deleted.
- B. Use service control policies to deny the s3:DeleteBucket action on all buckets in production accounts.
- C. Create an IAM group that has an IAM policy to deny the s3:DeleteBucket action on all buckets in production accounts.
- D. Use AWS Shield to deny the s3:DeleteBucket action on the AWS account instead of all S3 buckets.

**Answer: B**

**Explanation:**

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html)

If you're using AWS Organizations, check the service control policies for any statements that explicitly deny Amazon S3 access. In particular, check the service control policies for statements denying the s3:PutBucketPolicy action.

<https://aws.amazon.com/tw/premiumsupport/knowledge-center/s3-access-denied-bucket-policy/>

**NEW QUESTION 43**

- (Exam Topic 1)

A company's VPC has connectivity to an on-premises data center through an AWS Site-to-Site VPN. The company needs Amazon EC2 instances in the VPC to send DNS queries for example.com to the DNS servers in the data center.

Which solution will meet these requirements?

- A. Create an Amazon Route 53 Resolver inbound endpoint Create a conditional forwarding rule on the on-premises DNS servers to forward DNS requests for example.com to the inbound endpoints.
- B. Create an Amazon Route 53 Resolver inbound endpoint Create a forwarding rule on the resolver that sends all queries for example.com to the on-premises DNS server
- C. Associate this rule with the VPC.
- D. Create an Amazon Route 53 Resolver outbound endpoint Create a conditional forwarding rule on the on-premises DNS servers to forward DNS requests for example.com to the outbound endpoints
- E. Create an Amazon Route 53 Resolver outbound endpoint
- F. Create a forwarding rule on the resolver that sends all queries for exarrrc4e.com to the on-premises DNS servers Associate this rule with the VPC.

**Answer:** C

#### NEW QUESTION 47

- (Exam Topic 1)

A company wants to be alerted through email when IAM CreateUser API calls are made within its AWS account. Which combination of actions should a SysOps administrator take to meet this requirement? (Choose two.)

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with AWS CloudTrail as the event source and IAM CreateUser as the specific API call for the event pattern.
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with Amazon CloudSearch as the event source and IAM CreateUser as the specific API call for the event pattern.
- C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with AWS IAM Access Analyzer as the event source and IAM CreateUser as the specific API call for the event pattern.
- D. Use an Amazon Simple Notification Service (Amazon SNS) topic as an event target with an email subscription.
- E. Use an Amazon Simple Email Service (Amazon SES) notification as an event target with an email subscription.

**Answer:** AD

#### Explanation:

<https://aws.amazon.com/blogs/security/how-to-receive-alerts-when-your-iam-configuration-changes/>

#### NEW QUESTION 51

- (Exam Topic 1)

A SysOps administrator creates two VPCs, VPC1 and VPC2, in a company's AWS account. The SysOps administrator deploys a Linux Amazon EC2 instance in VPC1 and deploys an Amazon RDS for MySQL DB instance in VPC2. The DB instance is deployed in a private subnet. An application that runs on the EC2 instance needs to connect to the database.

What should the SysOps administrator do to give the EC2 instance the ability to connect to the database?

- A. Enter the DB instance connection string into the VPC1 route table.
- B. Configure VPC peering between the two VPCs.
- C. Add the same IPv4 CIDR range for both VPCs.
- D. Connect to the DB instance by using the DB instance's public IP address.

**Answer:** B

#### Explanation:

VPC peering allows two VPCs to communicate with each other securely. By configuring VPC peering between the two VPCs, the SysOps administrator will be able to give the EC2 instance in VPC1 the ability to connect to the database in VPC2. Once the VPC peering is configured, the EC2 instance will be able to communicate with the database using the private IP address of the DB instance in the private subnet.

#### NEW QUESTION 52

- (Exam Topic 1)

A company maintains a large set of sensitive data in an Amazon S3 bucket. The company's security team asks a SysOps administrator to help verify that all current objects in the S3 bucket are encrypted.

What is the MOST operationally efficient solution that meets these requirements?

- A. Create a script that runs against the S3 bucket and outputs the status of each object.
- B. Create an S3 Inventory configuration on the S3 bucket. Include the appropriate status fields.
- C. Provide the security team with an IAM user that has read access to the S3 bucket.
- D. Use the AWS CLI to output a list of all objects in the S3 bucket.

**Answer:** D

#### NEW QUESTION 53

- (Exam Topic 1)

A team of On-call engineers frequently needs to connect to Amazon EC2 Instances in a private subnet to troubleshoot and run commands. The Instances use either the latest AWS-provided Windows Amazon Machine Images (AMIs) or Amazon Linux AMIs.

The team has an existing IAM role for authorization. A SysOps administrator must provide the team with access to the Instances by granting IAM permissions to this. Which solution will meet this requirement?

- A. Add a statement to the IAM role policy to allow the `ssm:StartSession` action on the instance.
- B. Instruct the team to use AWS Systems Manager Session Manager to connect to the Instances by using the assumed IAM role.
- C. Associate an Elastic IP address and a security group with each instance.
- D. Add the engineers' IP addresses to the security group inbound rule.
- E. Add a statement to the IAM role policy to allow the `ec2:AuthorizeSecurityGroupIngress` action so that the team can connect to the Instances.
- F. Create a bastion host with an EC2 Instance, and associate the bastion host with the VPC.
- G. Add a statement to the IAM role policy to allow the `ec2:CreateVpnConnection` action on the bastion host.
- H. Instruct the team to use the bastion host endpoint to connect to the instances.
- I. Use two listeners.
- J. Forward port 22 to a target group of Linux instance.
- K. Forward port 3389 to a target group of Windows Instance.
- L. Add a statement to the IAM role policy to allow the `ec2:CreateRoute` action so that the team can connect to the Instances.

**Answer:** A

#### NEW QUESTION 57

- (Exam Topic 1)

A SysOps administrator is required to monitor free space on Amazon EBS volumes attached to Microsoft Windows-based Amazon EC2 instances within a



company's account. The administrator must be alerted to potential issues.

What should the administrator do to receive email alerts before low storage space affects EC2 instance performance?

- A. Use built-in Amazon CloudWatch metrics, and configure CloudWatch alarms and an Amazon SNS topic for email notifications
- B. Use AWS CloudTrail logs and configure the trail to send notifications to an Amazon SNS topic.
- C. Use the Amazon CloudWatch agent to send disk space metrics, then set up CloudWatch alarms using an Amazon SNS topic.
- D. Use AWS Trusted Advisor and enable email notification alerts for EC2 disk space

**Answer:** C

#### NEW QUESTION 58

- (Exam Topic 1)

A compliance team requires all administrator passwords for Amazon RDS DB instances to be changed at least annually

Which solution meets this requirement in the MOST operationally efficient manner?

- A. Store the database credentials in AWS Secrets Manager. Configure automatic rotation for the secret every 365 days.
- B. Store the database credentials as a parameter in the RDS parameter group. Create a database trigger to rotate the password every 365 days.
- C. Store the database credentials in a private Amazon S3 bucket. Schedule an AWS Lambda function to generate a new set of credentials every 365 days.
- D. Store the database credentials in AWS Systems Manager Parameter Store as a secure string parameter. Configure automatic rotation for the parameter every 365 days.

**Answer:** A

#### NEW QUESTION 61

- (Exam Topic 1)

A company is expanding its use of AWS services across its portfolios. The company wants to provision AWS accounts for each team to ensure a separation of business processes for security compliance and billing. Account creation and bootstrapping should be completed in a scalable and efficient way so new accounts are created with a defined baseline and governance guardrails in place. A SysOps administrator needs to design a provisioning process that saves time and resources.

Which action should be taken to meet these requirements?

- A. Automate using AWS Elastic Beanstalk to provision the AWS accounts, set up infrastructure, and integrate with AWS Organizations.
- B. Create bootstrapping scripts in AWS OpsWorks and combine them with AWS CloudFormation templates to provision accounts and infrastructure.
- C. Use AWS Config to provision accounts and deploy instances using AWS Service Catalog.
- D. Use AWS Control Tower to create a template in Account Factory and use the template to provision new accounts.

**Answer:** D

#### NEW QUESTION 63

- (Exam Topic 1)

An existing, deployed solution uses Amazon EC2 instances with Amazon EBS General Purpose SSD volumes, an Amazon RDS PostgreSQL database, an Amazon EFS file system, and static objects stored in an Amazon S3 bucket. The Security team now mandates that at-rest encryption be turned on immediately for all aspects of the application, without creating new resources and without any downtime.

To satisfy the requirements, which one of these services can the SysOps administrator enable at-rest encryption on?

- A. EBS General Purpose SSD volumes
- B. RDS PostgreSQL database
- C. Amazon EFS file systems
- D. S3 objects within a bucket

**Answer:** D

#### Explanation:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingEncryption.html>

#### NEW QUESTION 66

- (Exam Topic 1)

A company needs to automatically monitor an AWS account for potential unauthorized AWS Management Console logins from multiple geographic locations.

Which solution will meet this requirement?

- A. Configure Amazon Cognito to detect any compromised IAM credentials.
- B. Set up Amazon Inspector.
- C. Scan and monitor resources for unauthorized logins.
- D. Set up AWS Config.
- E. Add the iam-policy-blacklisted-check managed rule to the account.
- F. Configure Amazon GuardDuty to monitor the UnauthorizedAccess:IAMUser/ConsoleLoginSuccess finding.

**Answer:** D

#### NEW QUESTION 70

- (Exam Topic 1)

A company must migrate its applications to AWS. The company is using Chef recipes for configuration management. The company wants to continue to use the existing Chef recipes after the applications are migrated to AWS.

What is the MOST operationally efficient solution that meets these requirements?

- A. Use AWS CloudFormation to create an Amazon EC2 instance, install a Chef server, and add Chef recipes.
- B. Use AWS CloudFormation to create a stack and add layers for Chef recipes.
- C. Use AWS Elastic Beanstalk with the Docker platform to upload Chef recipes.



D. Use AWS OpsWorks to create a stack and add layers with Chef recipes.

**Answer:** D

#### NEW QUESTION 72

- (Exam Topic 1)

A Sysops administrator creates an Amazon Elastic Kubernetes Service (Amazon EKS) cluster that uses AWS Fargate. The cluster is deployed successfully. The Sysops administrator needs to manage the cluster by using the kubectl command line tool.

Which of the following must be configured on the Sysops administrator's machine so that kubectl can communicate with the cluster API server?

- A. The kubeconfig file
- B. The kube-proxy Amazon EKS add-on
- C. The Fargate profile
- D. The eks-connector.yaml file

**Answer:** A

#### Explanation:

The kubeconfig file is a configuration file used to store cluster authentication information, which is required to make requests to the Amazon EKS cluster API server. The kubeconfig file will need to be configured on the SysOps administrator's machine in order for kubectl to be able to communicate with the cluster API server.

<https://aws.amazon.com/blogs/developer/running-a-kubernetes-job-in-amazon-eks-on-aws-fargate-using-aws-ste>

#### NEW QUESTION 75

- (Exam Topic 1)

A company is expanding globally and needs to back up data on Amazon Elastic Block Store (Amazon EBS) volumes to a different AWS Region. Most of the EBS volumes that store the data are encrypted, but some of the EBS volumes are unencrypted. The company needs the backup data from all the EBS volumes to be encrypted.

Which solution will meet these requirements with the LEAST management overhead?

- A. Configure a lifecycle policy in Amazon Data Lifecycle Manager (Amazon DLM) to create the EBS volume snapshots with cross-Region backups enable
- B. Encrypt the snapshot copies by using AWS Key Management Service (AWS KMS).
- C. Create a point-in-time snapshot of the EBS volume
- D. When the snapshot status is COMPLETED, copy the snapshots to another Region and set the Encrypted parameter to False.
- E. Create a point-in-time snapshot of the EBS volume
- F. Copy the snapshots to an Amazon S3 bucket that uses server-side encryption
- G. Turn on S3 Cross-Region Replication on the S3 bucket.
- H. Schedule an AWS Lambda function with the Python runtime
- I. Configure the Lambda function to create the EBS volume snapshots, encrypt the unencrypted snapshots, and copy the snapshots to another Region.

**Answer:** A

#### Explanation:

Encrypt the snapshot copies by using AWS Key Management Service (AWS KMS). This solution will allow the company to automatically create encrypted snapshots of the EBS volumes and copy them to different AWS Regions with minimal effort.

#### NEW QUESTION 77

- (Exam Topic 1)

A SysOps administrator has Nocked public access to all company Amazon S3 buckets. The SysOps administrator wants to be notified when an S3 bucket becomes publicly readable in the future.

What is the MOST operationally efficient way to meet this requirement?

- A. Create an AWS Lambda function that periodically checks the public access settings for each S3 bucket.Set up Amazon Simple Notification Service (Amazon SNS) to send notifications.
- B. Create a cron script that uses the S3 API to check the public access settings for each S3 bucke
- C. Set up Amazon Simple Notification Service (Amazon SNS) to send notifications
- D. Enable S3 Event notified tons for each S3 bucke
- E. Subscribe S3 Event Notifications to an Amazon Simple Notification Service (Amazon SNS) topic.
- F. Enable the s3-bucket-public-read-prohibited managed rule in AWS Confi
- G. Subscribe the AWS Config rule to an Amazon Simple Notification Service (Amazon SNS) topic.

**Answer:** D

#### NEW QUESTION 80

- (Exam Topic 1)

A SysOps administrator is trying to set up an Amazon Route 53 domain name to route traffic to a website hosted on Amazon S3. The domain name of the website is www.anycompany.com and the S3 bucket name is anycompany-static. After the record set is set up in Route 53, the domain name www.anycompany.com does not seem to work, and the static website is not displayed in the browser.

Which of the following is a cause of this?

- A. The S3 bucket must be configured with Amazon CloudFront first.
- B. The Route 53 record set must have an IAM role that allows access to the S3 bucket.
- C. The Route 53 record set must be in the same region as the S3 bucket.
- D. The S3 bucket name must match the record set name in Route 53.

**Answer:** D

#### NEW QUESTION 81

- (Exam Topic 1)

A SysOps administrator is configuring an application on Amazon EC2 instances for a company Teams in other countries will use the application over the internet. The company requires the application endpoint to have a static public IP address. How should the SysOps administrator deploy the application to meet this requirement?

- A. Behind an Amazon API Gateway API
- B. Behind an Application Load Balancer
- C. Behind an internet-facing Network Load Balancer
- D. In an Amazon CloudFront distribution

**Answer: C**

#### NEW QUESTION 85

- (Exam Topic 1)

A company uses an Amazon CloudFront distribution to deliver its website. Traffic logs for the website must be centrally stored, and all data must be encrypted at rest.

Which solution will meet these requirements?

- A. Create an Amazon OpenSearch Service (Amazon Elasticsearch Service) domain with internet access and server-side encryption that uses the default AWS managed key
- B. Configure CloudFront to use the Amazon OpenSearch Service (Amazon Elasticsearch Service) domain as a log destination.
- C. Create an Amazon OpenSearch Service (Amazon Elasticsearch Service) domain with VPC access and server-side encryption that uses AES-256. Configure CloudFront to use the Amazon OpenSearch Service (Amazon Elasticsearch Service) domain as a log destination.
- D. Create an Amazon S3 bucket that is configured with default server-side encryption that uses AES-256. Configure CloudFront to use the S3 bucket as a log destination.
- E. Create an Amazon S3 bucket that is configured with no default encryption
- F. Enable encryption in the CloudFront distribution, and use the S3 bucket as a log destination.

**Answer: C**

#### NEW QUESTION 86

- (Exam Topic 1)

A large company is using AWS Organizations to manage hundreds of AWS accounts across multiple AWS Regions. The company has turned on AWS Config throughout the organization.

The company requires all Amazon S3 buckets to block public read access. A SysOps administrator must generate a monthly report that shows all the S3 buckets and whether they comply with this requirement.

Which combination of steps should the SysOps administrator take to collect this data? (Select TWO).

- A. Create an AWS Config aggregator in an aggregator account
- B. Use the organization as the source. Retrieve the compliance data from the aggregator.
- C. Create an AWS Config aggregator in each account
- D. Use an S3 bucket in an aggregator account as the destination
- E. Retrieve the compliance data from the S3 bucket
- F. Edit the AWS Config policy in AWS Organization
- G. Use the organization's management account to turn on the s3-bucket-public-read-prohibited rule for the entire organization.
- H. Use the AWS Config compliance report from the organization's management account
- I. Filter the results by resource, and select Amazon S3.
- J. Use the AWS Config API to apply the s3-bucket-public-read-prohibited rule in all accounts for all available Regions.

**Answer: CD**

#### NEW QUESTION 89

- (Exam Topic 1)

A company is releasing a new static website hosted on Amazon S3. The static website hosting feature was enabled on the bucket and content was uploaded: however, upon navigating to the site, the following error message is received:

403 Forbidden - Access Denied

What change should be made to fix this error?

- A. Add a bucket policy that grants everyone read access to the bucket.
- B. Add a bucket policy that grants everyone read access to the bucket objects.
- C. Remove the default bucket policy that denies read access to the bucket.
- D. Configure cross-origin resource sharing (CORS) on the bucket.

**Answer: B**

#### NEW QUESTION 92

- (Exam Topic 1)

Application A runs on Amazon EC2 instances behind a Network Load Balancer (NLB). The EC2 instances are in an Auto Scaling group and are in the same subnet that is associated with the NLB. Other applications from an on-premises environment cannot communicate with Application A on port 8080.

To troubleshoot the issue, a SysOps administrator analyzes the flow logs. The flow logs include the following records:

```
2 123456789010 eni-1235b8ca123456789 192.168.0.13 172.31.16.139 59003 8080 1 4 336 1432917027 1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca123456789 172.31.16.139 192.168.0.13 8080 59003 1 4 336 1432917094 1432917142 REJECT OK
```

What is the reason for the rejected traffic?

- A. The security group of the EC2 instances has no Allow rule for the traffic from the NLB.
- B. The security group of the NLB has no Allow rule for the traffic from the on-premises environment.
- C. The ACL of the on-premises environment does not allow traffic to the AWS environment.

D. The network ACL that is associated with the subnet does not allow outbound traffic for the ephemeral port range.

**Answer:** A

#### NEW QUESTION 97

- (Exam Topic 1)

A company requires that all IAM user accounts that have not been used for 90 days or more must have their access keys and passwords immediately disabled. A SysOps administrator must automate the process of disabling unused keys using the MOST operationally efficient method. How should the SysOps administrator implement this solution?

- A. Create an AWS Step Functions workflow to identify IAM users that have not been active for 90 days. Run an AWS Lambda function when a scheduled Amazon EventBridge (Amazon CloudWatch Events) rule is invoked to automatically remove the AWS access keys and passwords for these IAM users.
- B. Configure an AWS Config rule to identify IAM users that have not been active for 90 days. Set up an automatic weekly batch process on an Amazon EC2 instance to disable the AWS access keys and passwords for these IAM users.
- C. Develop and run a Python script on an Amazon EC2 instance to programmatically identify IAM users that have not been active for 90 days. Automatically delete these IAM users.
- D. Set up an AWS Config managed rule to identify IAM users that have not been active for 90 days. Set up an AWS Systems Manager automation runbook to disable the AWS access keys for these IAM users.

**Answer:** D

#### NEW QUESTION 98

- (Exam Topic 1)

A global company handles a large amount of personally identifiable information (PII) through an internal web portal. The company's application runs in a corporate data center that is connected to AWS through an AWS Direct Connect connection. The application stores the PII in Amazon S3. According to a compliance requirement, traffic from the web portal to Amazon S3 must not travel across the internet. What should a SysOps administrator do to meet the compliance requirement?

- A. Provision an interface VPC endpoint for Amazon S3. Modify the application to use the interface endpoint.
- B. Configure AWS Network Firewall to redirect traffic to the internal S3 address.
- C. Modify the application to use the S3 path-style endpoint.
- D. Set up a range of VPC network ACLs to redirect traffic to the Internal S3 address.

**Answer:** B

#### NEW QUESTION 99

- (Exam Topic 1)

A company has a stateless application that runs on four Amazon EC2 instances. The application requires four instances at all times to support all traffic. A SysOps administrator must design a highly available, fault-tolerant architecture that continually supports all traffic if one Availability Zone becomes unavailable. Which configuration meets these requirements?

- A. Deploy two Auto Scaling groups in two Availability Zones with a minimum capacity of two instances in each group.
- B. Deploy an Auto Scaling group across two Availability Zones with a minimum capacity of four instances.
- C. Deploy an Auto Scaling group across three Availability Zones with a minimum capacity of four instances.
- D. Deploy an Auto Scaling group across three Availability Zones with a minimum capacity of six instances.

**Answer:** C

#### NEW QUESTION 101

- (Exam Topic 1)

A company has a web application with a database tier that consists of an Amazon EC2 instance that runs MySQL. A SysOps administrator needs to minimize potential data loss and the time that is required to recover in the event of a database failure. What is the MOST operationally efficient solution that meets these requirements?

- A. Create an Amazon CloudWatch alarm for the StatusCheckFailed\_System metric to invoke an AWS Lambda function that stops and starts the EC2 instance.
- B. Create an Amazon RDS for MySQL Multi-AZ DB instance.
- C. Use a MySQL native backup that is stored in Amazon S3 to restore the data to the new database.
- D. Update the connection string in the web application.
- E. Create an Amazon RDS for MySQL Single-AZ DB instance with a read replica.
- F. Use a MySQL native backup that is stored in Amazon S3 to restore the data to the new database.
- G. Update the connection string in the web application.
- H. Use Amazon Data Lifecycle Manager (Amazon DLM) to take a snapshot of the Amazon Elastic Block Store (Amazon EBS) volume every hour.
- I. In the event of an EC2 instance failure, restore the EBS volume from a snapshot.

**Answer:** D

#### NEW QUESTION 102

- (Exam Topic 1)

A company is using Amazon CloudFront to serve static content for its web application to its users. The CloudFront distribution uses an existing on-premises website as a custom origin.

The company requires the use of TLS between CloudFront and the origin server. This configuration has worked as expected for several months. However, users are now experiencing HTTP 502 (Bad Gateway) errors when they view webpages that include content from the CloudFront distribution.

What should a SysOps administrator do to resolve this problem?

- A. Examine the expiration date on the certificate on the origin site.
- B. Validate that the certificate has not expired.
- C. Replace the certificate if necessary.

- D. Examine the hostname on the certificate on the origin sit
- E. Validate that the hostname matches one of the hostnames on the CloudFront distributio
- F. Replace the certificate if necessary.
- G. Examine the firewall rules that are associated with the origin serve
- H. Validate that port 443 is open for inbound traffic from the interne
- I. Create an inbound rule if necessary.
- J. Examine the network ACL rules that are associated with the CloudFront distributio
- K. Validate that port 443 is open for outbound traffic to the origin serve
- L. Create an outbound rule if necessary.

**Answer:** A

**Explanation:**

HTTP 502 errors from CloudFront can occur because of the following reasons:

There's an SSL negotiation failure because the origin is using SSL/TLS protocols and ciphers that aren't supported by CloudFront.

There's an SSL negotiation failure because the SSL certificate on the origin is expired or invalid, or because the certificate chain is invalid.

There's a host header mismatch in the SSL negotiation between your CloudFront distribution and the custom origin.

The custom origin isn't responding on the ports specified in the origin settings of the CloudFront distribution. The custom origin is ending the connection to CloudFront too quickly.

<https://aws.amazon.com/premiumsupport/knowledge-center/resolve-cloudfront-connection-error/>

**NEW QUESTION 103**

- (Exam Topic 1)

A company is using Amazon Elastic Container Sen/ice (Amazon ECS) to run a containerized application on Amazon EC2 instances. A SysOps administrator needs to monitor only traffic flows between the ECS tasks.

Which combination of steps should the SysOps administrator take to meet this requirement? (Select TWO.)

- A. Configure Amazon CloudWatch Logs on the elastic network interface of each task.
- B. Configure VPC Flow Logs on the elastic network interface of each task.
- C. Specify the awsvpc network mode in the task definition.
- D. Specify the bridge network mode in the task definition.
- E. Specify the host network mode in the task definition.

**Answer:** AE

**NEW QUESTION 106**

- (Exam Topic 1)

A SysOps administrator is investigating why a user has been unable to use RDP to connect over the internet from their home computer to a bastion server running on an Amazon EC2 Windows instance.

Which of the following are possible causes of this issue? (Choose two.)

- A. A network ACL associated with the bastion's subnet is blocking the network traffic.
- B. The instance does not have a private IP address.
- C. The route table associated with the bastion's subnet does not have a route to the internet gateway.
- D. The security group for the instance does not have an inbound rule on port 22.
- E. The security group for the instance does not have an outbound rule on port 3389.

**Answer:** AC

**NEW QUESTION 111**

- (Exam Topic 1)

A large multinational company has a core application that runs 24 hours a day, 7 days a week on Amazon EC2 and AWS Lambda. The company uses a combination of operating systems across different AWS Regions. The company wants to achieve cost savings and wants to use a pricing model that provides the most flexibility.

What should the company do to MAXIMIZE cost savings while meeting these requirements?

- A. Establish the compute expense by the hou
- B. Purchase a Compute Savings Plan.
- C. Establish the compute expense by the hou
- D. Purchase an EC2 Instance Savings Plan.
- E. Purchase a Reserved Instance for the instance types, operating systems, Region, and tenancy.
- F. Use EC2 Spot Instances to match the instances that run in each Region.

**Answer:** D

**NEW QUESTION 115**

- (Exam Topic 1)

A recent audit found that most resources belonging to the development team were in violation of patch compliance standards The resources were properly tagged

Which service should be used to quickly remediate the issue and bring the resources back into compliance?

- A. AWS Config
- B. Amazon Inspector
- C. AWS Trusted Advisor
- D. AWS Systems Manager

**Answer:** D

**NEW QUESTION 116**



- (Exam Topic 1)

A company runs hundreds of Amazon EC2 instances in a single AWS Region. Each EC2 instance has two attached 1 GiB General Purpose SSD (gp2) Amazon Elastic Block Store (Amazon EBS) volumes. A critical workload is using all the available IOPS capacity on the EBS volumes.

According to company policy, the company cannot change instance types or EBS volume types without completing lengthy acceptance tests to validate that the company's applications will function properly. A SysOps administrator needs to increase the I/O performance of the EBS volumes as quickly as possible.

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

- A. Increase the size of the 1 GiB EBS volumes.
- B. Add two additional elastic network interfaces on each EC2 instance.
- C. Turn on Transfer Acceleration on the EBS volumes in the Region.
- D. Add all the EC2 instances to a cluster placement group.

**Answer:** A

**Explanation:**

Increasing the size of the 1 GiB EBS volumes will increase the IOPS capacity of the volumes, which will improve the I/O performance of the EBS volumes. This option does not require any changes to the instance types or EBS volume types, so it can be done quickly without the need for lengthy acceptance tests to validate that the company's applications will function properly.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/requesting-ebs-volume-modifications.html>

**NEW QUESTION 121**

- (Exam Topic 1)

A company is creating a new multi-account architecture. A Sysops administrator must implement a login solution to centrally manage user access and permissions across all AWS accounts. The solution must be integrated with AWS Organizations and must be connected to a third-party Security Assertion Markup Language (SAML) 2.0 identity provider (IdP).

What should the SysOps administrator do to meet these requirements?

- A. Configure an Amazon Cognito user pool
- B. Integrate the user pool with the third-party IdP.
- C. Enable and configure AWS Single Sign-On with the third-party IdP.
- D. Federate the third-party IdP with AWS Identity and Access Management (IAM) for each AWS account in the organization.
- E. Integrate the third-party IdP directly with AWS Organizations.

**Answer:** A

**NEW QUESTION 124**

- (Exam Topic 1)

A SysOps administrator is designing a solution for an Amazon RDS for PostgreSQL DB instance. Database credentials must be stored and rotated monthly. The applications that connect to the DB instance send

write-intensive traffic with variable client connections that sometimes increase significantly in a short period of time.

Which solution should a SysOps administrator choose to meet these requirements?

- A. Configure AWS Key Management Service (AWS KMS) to automatically rotate the keys for the DB instance
- B. Use RDS Proxy to handle the increases in database connections.
- C. Configure AWS Key Management Service (AWS KMS) to automatically rotate the keys for the DB instance
- D. Use RDS read replicas to handle the increases in database connections.
- E. Configure AWS Secrets Manager to automatically rotate the credentials for the DB instance
- F. Use RDS Proxy to handle the increases in database connections.
- G. Configure AWS Secrets Manager to automatically rotate the credentials for the DB instance
- H. Use RDS read replicas to handle the increases in database connections.

**Answer:** A

**NEW QUESTION 127**

- (Exam Topic 1)

A company's SysOps administrator regularly checks the AWS Personal Health Dashboard in each of the company's accounts. The accounts are part of an organization in AWS Organizations. The company recently added 10 more accounts to the organization. The SysOps administrator must consolidate the alerts from each account's Personal Health Dashboard.

Which solution will meet this requirement with the LEAST amount of effort?

- A. Enable organizational view in AWS Health.
- B. Configure the Personal Health Dashboard in each account to forward events to a central AWS CloudTrail log.
- C. Create an AWS Lambda function to query the AWS Health API and to write all events to an Amazon DynamoDB table.
- D. Use the AWS Health API to write events to an Amazon DynamoDB table.

**Answer:** A

**Explanation:**

Enabling the organizational view in AWS Health will allow the SysOps administrator to consolidate the alerts from each account's Personal Health Dashboard. It will also provide the administrator with a single view of all the accounts in the organization, allowing them to easily monitor the health of all the accounts in the organization.

Reference:

[1] <https://aws.amazon.com/premiumsupport/knowledge-center/organizational-view-health-dashboard/>

**NEW QUESTION 130**

- (Exam Topic 1)

A SysOps administrator needs to configure a solution that will deliver digital content to a set of authorized

users through Amazon CloudFront. Unauthorized users must be restricted from access. Which solution will meet these requirements?

- A. Store the digital content in an Amazon S3 bucket that does not have public access blocked
- B. Use signed URLs to access the S3 bucket through CloudFront.
- C. Store the digital content in an Amazon S3 bucket that has public access blocked
- D. Use an origin access identity (OAI) to deliver the content through CloudFront
- E. Restrict S3 bucket access with signed URLs in CloudFront.
- F. Store the digital content in an Amazon S3 bucket that has public access blocked
- G. Use an origin access identity (OAI) to deliver the content through CloudFront
- H. Enable field-level encryption.
- I. Store the digital content in an Amazon S3 bucket that does not have public access blocked
- J. Use signed cookies for restricted delivery of the content through CloudFront.

**Answer: B**

#### NEW QUESTION 134

- (Exam Topic 1)

A company's public website is hosted in an Amazon S3 bucket in the us-east-1 Region behind an Amazon CloudFront distribution. The company wants to ensure that the website is protected from DDoS attacks. A SysOps administrator needs to deploy a solution that gives the company the ability to maintain control over the rate limit at which DDoS protections are applied. Which solution will meet these requirements?

- A. Deploy a global-scoped AWS WAF web ACL with an allow default action
- B. Configure an AWS WAF rate-based rule to block matching traffic
- C. Associate the web ACL with the CloudFront distribution.
- D. Deploy an AWS WAF web ACL with an allow default action in us-east-1. Configure an AWS WAF rate-based rule to block matching traffic
- E. Associate the web ACL with the S3 bucket.
- F. Deploy a global-scoped AWS WAF web ACL with a block default action
- G. Configure an AWS WAF rate-based rule to allow matching traffic
- H. Associate the web ACL with the CloudFront distribution.
- I. Deploy an AWS WAF web ACL with a block default action in us-east-1. Configure an AWS WAF rate-based rule to allow matching traffic
- J. Associate the web ACL with the S3 bucket.

**Answer: B**

#### NEW QUESTION 139

- (Exam Topic 1)

A company has launched a social media website that gives users the ability to upload images directly to a centralized Amazon S3 bucket. The website is popular in areas that are geographically distant from the AWS Region where the S3 bucket is located. Users are reporting that uploads are slow. A SysOps administrator must improve the upload speed.

What should the SysOps administrator do to meet these requirements?

- A. Create S3 access points in Regions that are closer to the users.
- B. Create an accelerator in AWS Global Accelerator for the S3 bucket.
- C. Enable S3 Transfer Acceleration on the S3 bucket.
- D. Enable cross-origin resource sharing (CORS) on the S3 bucket.

**Answer: C**

#### Explanation:

You might want to use Transfer Acceleration on a bucket for various reasons: ->Your customers upload to a centralized bucket from all over the world. ->You transfer gigabytes to terabytes of data on a regular basis across continents. ->You can't use all of your available bandwidth over the internet when uploading to Amazon S3." <https://docs.aws.amazon.com/AmazonS3/latest/userguide/transfer-acceleration.html>

#### NEW QUESTION 140

- (Exam Topic 1)

An application runs on multiple Amazon EC2 instances in an Auto Scaling group. The Auto Scaling group is configured to use the latest version of a launch template. A SysOps administrator must devise a solution that centrally manages the application logs and retains the logs for no more than 90 days.

Which solution will meet these requirements?

- A. Launch an Amazon Machine Image (AMI) that is preconfigured with the Amazon CloudWatch Logs agent to send logs to an Amazon S3 bucket. Apply a 90-day S3 Lifecycle policy on the S3 bucket to expire the application logs.
- B. Launch an Amazon Machine Image (AMI) that is preconfigured with the Amazon CloudWatch Logs agent to send logs to a log group. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled rule to perform an instance refresh every 90 days.
- C. Update the launch template user data to install and configure the Amazon CloudWatch Logs agent to send logs to a log group. Configure the retention period on the log group to be 90 days.
- D. Update the launch template user data to install and configure the Amazon CloudWatch Logs agent to send logs to a log group. Set the log rotation configuration of the EC2 instances to 90 days.

**Answer: C**

#### NEW QUESTION 141

- (Exam Topic 1)

A company asks a SysOps administrator to ensure that AWS CloudTrail files are not tampered with after they are created. Currently, the company uses AWS Identity and Access Management (IAM) to restrict access to specific trails. The company's security team needs the ability to trace the integrity of each file. What is the MOST operationally efficient solution that meets these requirements?

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function when a new file is delivered.
- B. Configure the Lambda function to compute an MD5 hash check on the file and store the result in an Amazon DynamoDB table.
- C. The security team can use the values that are stored in DynamoDB to verify the integrity of the delivered files.

- D. Create an AWS Lambda function that is invoked each time a new file is delivered to the CloudTrail bucket
- E. Configure the Lambda function to compute an MD5 hash check on the file and store the result as a tag in an Amazon S3 object
- F. The security team can use the information in the tag to verify the integrity of the delivered files.
- G. Enable the CloudTrail file integrity feature on an Amazon S3 bucket
- H. Create an IAM policy that grants the security team access to the file integrity logs that are stored in the S3 bucket.
- I. Enable the CloudTrail file integrity feature on the trail
- J. The security team can use the digest file that is created by CloudTrail to verify the integrity of the delivered files.

**Answer:** D

**Explanation:**

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html> "When you enable log file integrity validation, CloudTrail creates a hash for every log file that it delivers.

Every hour, CloudTrail also creates and delivers a file that references the log files for the last hour and contains a hash of each. This file is called a digest file. Validated log files are invaluable in security and forensic investigations"

**NEW QUESTION 143**

- (Exam Topic 1)

A company must ensure that any objects uploaded to an S3 bucket are encrypted. Which of the following actions will meet this requirement? (Choose two.)

- A. Implement AWS Shield to protect against unencrypted objects stored in S3 buckets.
- B. Implement Object access control list (ACL) to deny unencrypted objects from being uploaded to the S3 bucket.
- C. Implement Amazon S3 default encryption to make sure that any object being uploaded is encrypted before it is stored.
- D. Implement Amazon Inspector to inspect objects uploaded to the S3 bucket to make sure that they are encrypted.
- E. Implement S3 bucket policies to deny unencrypted objects from being uploaded to the buckets.

**Answer:** CE

**Explanation:**

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/default-bucket-encryption.html>

You can set the default encryption behavior on an Amazon S3 bucket so that all objects are encrypted when they are stored in the bucket. The objects are encrypted using server-side encryption with either Amazon S3-managed keys (SSE-S3) or AWS Key Management Service (AWS KMS) customer master keys (CMKs).

<https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/> How to Prevent Uploads of Unencrypted Objects to Amazon S3#

By using an S3 bucket policy, you can enforce the encryption requirement when users upload objects, instead of assigning a restrictive IAM policy to all users.

**NEW QUESTION 148**

- (Exam Topic 1)

A SysOps administrator is responsible for a legacy, CPU-heavy application. The application can only be scaled vertically. Currently, the application is deployed on a single t2 large Amazon EC2 instance. The system is showing 90% CPU usage and significant performance latency after a few minutes.

What change should be made to alleviate the performance problem?

- A. Change the Amazon EBS volume to Provisioned IOPS
- B. Upgrade to a compute-optimized instance
- C. Add additional 12 large instances to the application
- D. Purchase Reserved Instances

**Answer:** B

**NEW QUESTION 149**

- (Exam Topic 1)

A SysOps administrator is testing an application that is hosted on five Amazon EC2 instances. The instances run in an Auto Scaling group behind an Application Load Balancer (ALB). High CPU utilization during load testing is causing the Auto Scaling group to scale out. The SysOps administrator must troubleshoot to find the root cause of the high CPU utilization before the Auto Scaling group scales out.

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

- A. Enable instance scale-in protection.
- B. Place the instance into the Standby state.
- C. Remove the listener from the ALB
- D. Suspend the Launch and Terminate process types.

**Answer:** A

**NEW QUESTION 151**

- (Exam Topic 1)

A company uses an AWS CloudFormation template to provision an Amazon EC2 instance and an Amazon RDS DB instance. A SysOps administrator must update the template to ensure that the DB instance is created before the EC2 instance is launched.

What should the SysOps administrator do to meet this requirement?

- A. Add a wait condition to the template. Update the EC2 instance user data script to send a signal after the EC2 instance is started.
- B. Add the DependsOn attribute to the EC2 instance resource, and provide the logical name of the RDS resource.
- C. Change the order of the resources in the template so that the RDS resource is listed before the EC2 instance resource.
- D. Create multiple templates. Use AWS CloudFormation StackSets to wait for one stack to complete before the second stack is created.

**Answer:** B

**Explanation:**

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-dependson.html> Syntax The DependsOn attribute can take a single string or list



of strings. "DependsOn" : [ String, ... ]

Example The following template contains an AWS::EC2::Instance resource with a DependsOn attribute that specifies myDB, an AWS::RDS::DBInstance. When CloudFormation creates this stack, it first creates myDB, then creates Ec2Instance.

#### NEW QUESTION 156

- (Exam Topic 1)

A SysOps administrator created an Amazon VPC with an IPv6 CIDR block, which requires access to the internet. However, access from the internet towards the VPC is prohibited. After adding and configuring the required components to the VPC. the administrator is unable to connect to any of the domains that reside on the internet.

What additional route destination rule should the administrator add to the route tables?

- A. Route ::/0 traffic to a NAT gateway
- B. Route ::/0 traffic to an internet gateway
- C. Route 0.0.0.0/0 traffic to an egress-only internet gateway
- D. Route ::/0 traffic to an egress-only internet gateway

**Answer: D**

#### Explanation:

<https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html>

#### NEW QUESTION 161

- (Exam Topic 1)

A company runs a web application on three Amazon EC2 instances behind an Application Load Balancer (ALB). The company notices that random periods of increased traffic cause a degradation in the application's performance. A SysOps administrator must scale the application to meet the increased traffic.

Which solution meets these requirements?

- A. Create an Amazon CloudWatch alarm to monitor application latency and increase the size of each EC2 instance If the desired threshold is reached.
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to monitor application latency and add an EC2 instance to the ALB if the desired threshold is reached.
- C. Deploy the application to an Auto Scaling group of EC2 instances with a target tracking scaling policy. Attach the ALB to the Auto Scaling group.
- D. Deploy the application to an Auto Scaling group of EC2 instances with a scheduled scaling policy. Attach the ALB to the Auto Scaling group.

**Answer: C**

#### Explanation:

[docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html](https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html)

#### NEW QUESTION 165

- (Exam Topic 1)

A SysOps administrator wants to upload a file that is 1 TB in size from on-premises to an Amazon S3 bucket using multipart uploads. What should the SysOps administrator do to meet this requirement?

- A. Upload the file using the S3 console.
- B. Use the s3api copy-object command.
- C. Use the s3api put-object command.
- D. Use the s3 cp command.

**Answer: D**

#### Explanation:

It's a best practice to use aws s3 commands (such as aws s3 cp) for multipart uploads and downloads, because these aws s3 commands automatically perform multipart uploading and downloading based on the file size. By comparison, aws s3api commands, such as aws s3api create-multipart-upload, should be used only when aws s3 commands don't support a specific upload need, such as when the multipart upload involves multiple servers, a multipart upload is manually stopped and resumed later, or when the aws s3 command doesn't support a required request parameter.

<https://aws.amazon.com/premiumsupport/knowledge-center/s3-multipart-upload-cli/>

#### NEW QUESTION 168

- (Exam Topic 1)

A SysOps administrator is troubleshooting connection timeouts to an Amazon EC2 instance that has a public IP address. The instance has a private IP address of 172.31.16.139. When the SysOps administrator tries to ping the instance's public IP address from the remote IP address 203.0.113.12, the response is "request timed out." The flow logs contain the following information:

```
2 123456789010 eni-1235b8ca123456789 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca123456789 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK
```

What is one cause of the problem?

- A. Inbound security group deny rule
- B. Outbound security group deny rule
- C. Network ACL inbound rules
- D. Network ACL outbound rules

**Answer: D**

#### NEW QUESTION 171

- (Exam Topic 1)



A company has an internal web application that runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group in a single Availability Zone. A SysOps administrator must make the application highly available.

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

- A. Increase the maximum number of instances in the Auto Scaling group to meet the capacity that is required at peak usage.
- B. Increase the minimum number of instances in the Auto Scaling group to meet the capacity that is required at peak usage.
- C. Update the Auto Scaling group to launch new instances in a second Availability Zone in the same AWS Region.
- D. Update the Auto Scaling group to launch new instances in an Availability Zone in a second AWS Region.

**Answer:** C

#### NEW QUESTION 173

- (Exam Topic 1)

A company uses AWS Organizations to manage its AWS accounts. A SysOps administrator must create a backup strategy for all Amazon EC2 instances across all the company's AWS accounts.

Which solution will meet these requirements In the MOST operationally efficient way?

- A. Deploy an AWS Lambda function to each account to run EC2 instance snapshots on a scheduled basis.
- B. Create an AWS CloudFormation stack set in the management account to add an AutoBackup=True tag to every EC2 instance
- C. Use AWS Backup In the management account to deploy policies for all accounts and resources.
- D. Use a service control policy (SCP) to run EC2 instance snapshots on a scheduled basis in each account.

**Answer:** B

#### NEW QUESTION 177

- (Exam Topic 1)

A SysOps administrator has created a VPC that contains a public subnet and a private subnet. Amazon EC2 instances that were launched in the private subnet cannot access the internet. The default network ACL is active on all subnets in the VPC, and all security groups allow all outbound traffic:

Which solution will provide the EC2 instances in the private subnet with access to the internet?

- A. Create a NAT gateway in the public subne
- B. Create a route from the private subnet to the NAT gateway.
- C. Create a NAT gateway in the public subne
- D. Create a route from the public subnet to the NAT gateway.
- E. Create a NAT gateway in the private subne
- F. Create a route from the public subnet to the NAT gateway.
- G. Create a NAT gateway in the private subne
- H. Create a route from the private subnet to the NAT gateway.

**Answer:** A

#### Explanation:

NAT Gateway resides in public subnet, and traffic should be routed from private subnet to NAT Gateway: <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>

#### NEW QUESTION 179

- (Exam Topic 1)

A SysOps administrator wants to manage a web server application with AWS Elastic Beanstalk. The Elastic Beanstalk service must maintain full capacity for new deployments at all times.

Which deployment policies satisfy this requirement? (Select TWO.)

- A. All at once
- B. Immutable
- C. Rebuild
- D. Rolling
- E. Rolling with additional batch

**Answer:** BE

#### Explanation:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.rolling-version-deploy.html>

#### NEW QUESTION 181

- (Exam Topic 1)

A company is partnering with an external vendor to provide data processing services. For this integration, the vendor must host the company's data in an Amazon S3 bucket in the vendor's AWS account. The vendor is allowing the company to provide an AWS Key Management Service (AWS KMS) key to encrypt the company's data. The vendor has provided an IAM role Amazon Resource Name (ARN) to the company for this integration.

What should a SysOps administrator do to configure this integration?

- A. Create a new KMS ke
- B. Add the vendor's IAM role ARN to the KMS key polic
- C. Provide the new KMS key ARN to the vendor.
- D. Create a new KMS ke
- E. Create a new IAM use
- F. Add the vendor's IAM role ARN to an inline policy that is attached to the IAM use
- G. Provide the new IAM user ARN to the vendor.
- H. Configure encryption using the KMS managed S3 ke
- I. Add the vendor's IAM role ARN to the KMS managed S3 key polic

- J. Provide the KMS managed S3 key ARN to the vendor.
- K. Configure encryption using the KMS managed S3 ke
- L. Create an S3 bucke
- M. Add the vendor's IAM role ARN to the S3 bucket polic
- N. Provide the S3 bucket ARN to the vendor.

**Answer:** C

#### NEW QUESTION 184

- (Exam Topic 1)

A database is running on an Amazon RDS Multi-AZ DB instance. A recent security audit found the database to be out of compliance because it was not encrypted. Which approach will resolve the encryption requirement?

- A. Log in to the RDS console and select the encryption box to encrypt the database
- B. Create a new encrypted Amazon EBS volume and attach it to the instance
- C. Encrypt the standby replica in the secondary Availability Zone and promote it to the primary instance.
- D. Take a snapshot of the RDS instance, copy and encrypt the snapshot and then restore to the new RDS instance

**Answer:** D

#### NEW QUESTION 188

- (Exam Topic 1)

A company is running a website on Amazon EC2 instances behind an Application Load Balancer (ALB). The company configured an Amazon CloudFront distribution and set the ALB as the origin. The company created an Amazon Route 53 CNAME record to send all traffic through the CloudFront distribution. As an unintended side effect, mobile users are now being served the desktop version of the website.

Which action should a SysOps administrator take to resolve this issue?

- A. Configure the CloudFront distribution behavior to forward the User-Agent header.
- B. Configure the CloudFront distribution origin setting
- C. Add a User-Agent header to the list of origin custom headers.
- D. Enable IPv6 on the AL
- E. Update the CloudFront distribution origin settings to use the dualstack endpoint.
- F. Enable IPv6 on the CloudFront distributio
- G. Update the Route 53 record to use the dualstack endpoint.

**Answer:** A

#### Explanation:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/header-caching.html#header-caching->

#### NEW QUESTION 193

- (Exam Topic 1)

An application team uses an Amazon Aurora MySQL DB cluster with one Aurora Replica. The application team notices that the application read performance degrades when user connections exceed 200. The number of user connections is typically consistent around 180. with occasional sudden increases above 200 connections. The application team wants the application to automatically scale as user demand increases or decreases.

Which solution will meet these requirements?

- A. Migrate to a new Aurora multi-master DB cluste
- B. Modify the application database connection string.
- C. Modify the DB cluster by changing to serverless mode whenever user connections exceed 200.
- D. Create an auto scaling policy with a target metric of 195 DatabaseConnections
- E. Modify the DB cluster by increasing the Aurora Replica instance size.

**Answer:** C

#### NEW QUESTION 197

- (Exam Topic 1)

A SysOps administrator must set up notifications for whenever combined billing exceeds a certain threshold for all AWS accounts within a company. The administrator has set up AWS Organizations and enabled Consolidated Billing.

Which additional steps must the administrator perform to set up the billing alerts?

- A. In the payer account: Enable billing alerts in the Billing and Cost Management console; publish an Amazon SNS message when the billing alert triggers.
- B. In each account: Enable billing alerts in the Billing and Cost Management console; set up a billing alarm in Amazon CloudWatch; publish an SNS message when the alarm triggers.
- C. In the payer account: Enable billing alerts in the Billing and Cost Management console; set up a billing alarm in the Billing and Cost Management console to publish an SNS message when the alarm triggers.
- D. In the payer account: Enable billing alerts in the Billing and Cost Management console; set up a billing alarm in Amazon CloudWatch; publish an SNS message when the alarm triggers.

**Answer:** D

#### NEW QUESTION 202

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### AWS-SysOps Practice Exam Features:

- \* AWS-SysOps Questions and Answers Updated Frequently
- \* AWS-SysOps Practice Questions Verified by Expert Senior Certified Staff
- \* AWS-SysOps Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* AWS-SysOps Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The AWS-SysOps Practice Test Here](#)**