



## Amazon

### Exam Questions AWS-SysOps

Amazon AWS Certified SysOps Administrator - Associate

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

- (Exam Topic 1)

An organization with a large IT department has decided to migrate to AWS. With different job functions in the IT department, it is not desirable to give all users access to all AWS resources. Currently, the organization handles access via LDAP group membership. What is the BEST method to allow access using current LDAP credentials?

- A. Create an AWS Directory Service Simple AD. Replicate the on-premises LDAP directory to Simple AD.
- B. Create a Lambda function to read LDAP groups and automate the creation of IAM users.
- C. Use AWS CloudFormation to create IAM roles. Deploy Direct Connect to allow access to the on-premises LDAP server.
- D. Federate the LDAP directory with IAM using SAML. Create different IAM roles to correspond to different LDAP groups to limit permissions.

**Answer:** D

### NEW QUESTION 2

- (Exam Topic 1)

A SysOps administrator has used AWS CloudFormation to deploy a serverless application into a production VPC. The application consists of an AWS Lambda function, an Amazon DynamoDB table, and an Amazon API Gateway API. The SysOps administrator must delete the AWS CloudFormation stack without deleting the DynamoDB table.

Which action should the SysOps administrator take before deleting the AWS CloudFormation stack?

- A. Add a Retain deletion policy to the DynamoDB resource in the AWS CloudFormation stack.
- B. Add a Snapshot deletion policy to the DynamoDB resource in the AWS CloudFormation stack.
- C. Enable termination protection on the AWS CloudFormation stack.
- D. Update the application's IAM policy with a Deny statement for the dynamodb:DeleteTable action.

**Answer:** A

### NEW QUESTION 3

- (Exam Topic 1)

A SysOps administrator needs to secure the credentials for an Amazon RDS database that is created by an AWS CloudFormation template. The solution must encrypt the credentials and must support automatic rotation.

Which solution will meet these requirements?

- A. Create an AWS::SecretsManager::Secret resource in the CloudFormation template.
- B. Reference the credentials in the AWS::RDS::DBInstance resource by using the resolve:secretsmanager dynamic reference.
- C. Create an AWS::SecretsManager::Secret resource in the CloudFormation template.
- D. Reference the credentials in the AWS::RDS::DBInstance resource by using the resolve:ssm-secure dynamic reference.
- E. Create an AWS::SSM::Parameter resource in the CloudFormation template.
- F. Reference the credentials in the AWS::RDS::DBInstance resource by using the resolve:ssm dynamic reference.
- G. Create parameters for the database credentials in the CloudFormation template.
- H. Use the Ref intrinsic function to provide the credentials to the AWS::RDS::DBInstance resource.

**Answer:** A

### NEW QUESTION 4

- (Exam Topic 1)

A company creates a new member account by using AWS Organizations. A SysOps administrator needs to add AWS Business Support to the new account. Which combination of steps must the SysOps administrator take to meet this requirement? (Select TWO.)

- A. Sign in to the new account by using IAM credentials.
- B. Change the support plan.
- C. Sign in to the new account by using root user credentials.
- D. Change the support plan.
- E. Use the AWS Support API to change the support plan.
- F. Reset the password of the account root user.
- G. Create an IAM user that has administrator privileges in the new account.

**Answer:** BE

#### Explanation:

The best combination of steps to meet this requirement is to sign in to the new account by using root user credentials and change the support plan, and to create an IAM user that has administrator privileges in the new account.

Signing in to the new account by using root user credentials will allow the SysOps administrator to access the account and change the support plan to AWS Business Support. Additionally, creating an IAM user that has administrator privileges in the new account will ensure that the SysOps administrator has the necessary access to manage the account and make changes to the support plan if necessary.

Reference:

[1] [https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_accounts\\_access.html#orgs\\_ma](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html#orgs_ma)

### NEW QUESTION 5

- (Exam Topic 1)

A company applies user-defined tags to resources that are associated with the company's AWS workloads. Twenty days after applying the tags, the company notices that it cannot use the tags to filter views in the AWS Cost Explorer console.

What is the reason for this issue?

- A. It takes at least 30 days to be able to use tags to filter views in Cost Explorer.
- B. The company has not activated the user-defined tags for cost allocation.
- C. The company has not created an AWS Cost and Usage Report.

D. The company has not created a usage budget in AWS Budgets

**Answer: B**

#### NEW QUESTION 6

- (Exam Topic 1)

A company runs a website from Sydney, Australia. Users in the United States (US) and Europe are reporting that images and videos are taking a long time to load. However, local testing in Australia indicates no performance issues. The website has a large amount of static content in the form of images and videos that are stored in Amazon S3.

Which solution will result in the MOST improvement in the user experience for users in the US and Europe?

- A. Configure AWS PrivateLink for Amazon S3.
- B. Configure S3 Transfer Acceleration.
- C. Create an Amazon CloudFront distribution.
- D. Distribute the static content to the CloudFront edge locations.
- E. Create an Amazon API Gateway API in each AWS Region.
- F. Cache the content locally.

**Answer: D**

#### NEW QUESTION 7

- (Exam Topic 1)

A SysOps administrator is provisioning an Amazon Elastic File System (Amazon EFS) file system to provide shared storage across multiple Amazon EC2 instances. The instances all exist in the same VPC across multiple Availability Zones. There are two instances in each Availability Zone. The SysOps administrator must make the file system accessible to each instance with the lowest possible latency.

Which solution will meet these requirements?

- A. Create a mount target for the EFS file system in the VPC.
- B. Use the mount target to mount the file system on each of the instances.
- C. Create a mount target for the EFS file system in one Availability Zone of the VPC.
- D. Use the mount target to mount the file system on the instances in that Availability Zone.
- E. Share the directory with the other instances.
- F. Create a mount target for each instance.
- G. Use each mount target to mount the EFS file system on each respective instance.
- H. Create a mount target in each Availability Zone of the VPC. Use the mount target to mount the EFS file system on the instances in the respective Availability Zone.

**Answer: D**

#### Explanation:

A mount target provides an IP address for an NFSv4 endpoint at which you can mount an Amazon EFS file system. You mount your file system using its Domain Name Service (DNS) name, which resolves to the IP address of the EFS mount target in the same Availability Zone as your EC2 instance. You can create one mount target in each Availability Zone in an AWS Region. If there are multiple subnets in an Availability Zone in your VPC, you create a mount target in one of the subnets. Then all EC2 instances in that Availability Zone share that mount target. <https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html>

#### NEW QUESTION 8

- (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 cluster.
- 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 9

- (Exam Topic 1)

A company has created a NAT gateway in a public subnet in a VPC. The VPC also contains a private subnet that includes Amazon EC2 instances. The EC2 instances use the NAT gateway to access the internet to download patches and updates. The company has configured a VPC flow log for the elastic network interface of the NAT gateway. The company is publishing the output to Amazon CloudWatch Logs.

A SysOps administrator must identify the top five internet destinations that the EC2 instances in the private subnet communicate with for downloads.

What should the SysOps administrator do to meet this requirement in the MOST operationally efficient way?

- A. Use AWS CloudTrail Insights events to identify the top five internet destinations.
- B. Use Amazon CloudFront standard logs (access logs) to identify the top five internet destinations.
- C. Use CloudWatch Logs Insights to identify the top five internet destinations.
- D. Change the flow log to publish logs to Amazon S3. Use Amazon Athena to query the log files in Amazon S3.

**Answer: C**

#### NEW QUESTION 10

- (Exam Topic 1)

A company needs to archive all audit logs for 10 years. The company must protect the logs from any future edits.

Which solution will meet these requirements?

- A. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume
- B. Configure AWS Key Management Service (AWS KMS) encryption.
- C. Store the data in an Amazon S3 Glacier vault
- D. Configure a vault lock policy for write-once, read-many (WORM) access.
- E. Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Configure server-side encryption.
- F. Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Configure multi-factor authentication (MFA).

**Answer: B**

**Explanation:**

To meet the requirements of the workload, a company should store the data in an Amazon S3 Glacier vault and configure a vault lock policy for write-once, read-many (WORM) access. This will ensure that the data is stored securely and cannot be edited in the future. The other solutions (storing the data in an Amazon Elastic Block Store (Amazon EBS) volume and configuring AWS Key Management Service (AWS KMS) encryption, storing the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA) and configuring server-side encryption, or storing the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA) and configuring multi-factor authentication (MFA)) will not meet the requirements, as they do not provide a way to protect the audit logs from future edits.  
[https://docs.aws.amazon.com/zh\\_tw/AmazonS3/latest/userguide/object-lock.html](https://docs.aws.amazon.com/zh_tw/AmazonS3/latest/userguide/object-lock.html)

**NEW QUESTION 10**

- (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 11**

- (Exam Topic 1)

A company stores its data in an Amazon S3 bucket. The company is required to classify the data and find any sensitive personal information in its S3 files. Which solution will meet these requirements?

- A. Create an AWS Config rule to discover sensitive personal information in the S3 files and mark them as noncompliant.
- B. Create an S3 event-driven artificial intelligence/machine learning (AI/ML) pipeline to classify sensitive personal information by using Amazon Recognition.
- C. Enable Amazon GuardDut
- D. Configure S3 protection to monitor all data inside Amazon S3.
- E. Enable Amazon Maci
- F. Create a discovery job that uses the managed data identifier.

**Answer: D**

**Explanation:**

Amazon Macie is a security service designed to help organizations find, classify, and protect sensitive data stored in Amazon S3. Amazon Macie uses machine learning to automatically discover, classify, and protect sensitive data in Amazon S3. Creating a discovery job with the managed data identifier will allow Macie to identify sensitive personal information in the S3 files and classify it accordingly. Enabling AWS Config and Amazon GuardDuty will not help with this requirement as they are not designed to automatically classify and protect data.

**NEW QUESTION 16**

- (Exam Topic 1)

A company has multiple AWS Site-to-Site VPN connections between a VPC and its branch offices. The company manages an Amazon Elasticsearch Service (Amazon ES) domain that is configured with public access. The Amazon ES domain has an open domain access policy. A SysOps administrator needs to ensure that Amazon ES can be accessed only from the branch offices while preserving existing data.

Which solution will meet these requirements?

- A. Configure an identity-based access policy on Amazon E
- B. Add an allow statement to the policy that includes the Amazon Resource Name (ARN) for each branch office VPN connection.
- C. Configure an IP-based domain access policy on Amazon E
- D. Add an allow statement to the policy that includes the private IP CIDR blocks from each branch office network.
- E. Deploy a new Amazon ES domain in private subnets in a VPC, and import a snapshot from the old domai
- F. Create a security group that allows inbound traffic from the branch office CIDR blocks.
- G. Reconfigure the Amazon ES domain in private subnets in a VP
- H. Create a security group that allows inbound traffic from the branch office CIDR blocks.

**Answer: B**

**NEW QUESTION 17**

- (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 21

- (Exam Topic 1)

A company has deployed AWS Security Hub and AWS Config in a newly implemented organization in AWS Organizations. A SysOps administrator must implement a solution to restrict all member accounts in the organization from deploying Amazon EC2 resources in the ap-southeast-2 Region. The solution must be implemented from a single point and must govern an current and future accounts. The use of root credentials also must be restricted in member accounts. Which AWS feature should the SysOps administrator use to meet these requirements?

- A. AWS Config aggregator
- B. IAM user permissions boundaries
- C. AWS Organizations service control policies (SCPs)
- D. AWS Security Hub conformance packs

**Answer: C**

#### NEW QUESTION 22

- (Exam Topic 1)

A company runs a stateless application that is hosted on an Amazon EC2 instance. Users are reporting performance issues. A SysOps administrator reviews the Amazon CloudWatch metrics for the application and notices that the instance's CPU utilization frequently reaches 90% during business hours. What is the MOST operationally efficient solution that will improve the application's responsiveness?

- A. Configure CloudWatch logging on the EC2 instanc
- B. Configure a CloudWatch alarm for CPU utilization to alert the SysOps administrator when CPU utilization goes above 90%.
- C. Configure an AWS Client VPN connection to allow the application users to connect directly to the EC2 instance private IP address to reduce latency.
- D. Create an Auto Scaling group, and assign it to an Application Load Balance
- E. Configure a target tracking scaling policy that is based on the average CPU utilization of the Auto Scaling group.
- F. Create a CloudWatch alarm that activates when the EC2 instance's CPU utilization goes above 80%.Configure the alarm to invoke an AWS Lambda function that vertically scales the instance.

**Answer: C**

#### NEW QUESTION 23

- (Exam Topic 1)

A company has two VPC networks named VPC A and VPC B. The VPC A CIDR block is 10.0.0.0/16 and the VPC B CIDR block is 172.31.0.0/16. The company wants to establish a VPC peering connection named

pcx-12345 between both VPCs.

Which rules should appear in the route table of VPC A after configuration? (Select TWO.)

- A. Destination: 10.0.0.0/16, Target: Local
- B. Destination: 172.31.0.0/16, Target: Local
- C. Destination: 10.0.0.0/16, Target: pcx-12345
- D. Destination: 172.31.0.0/16, Target: pcx-12345
- E. Destination: 10.0.0.0/16. Target: 172.31.0.0/16

**Answer: AD**

#### Explanation:

<https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-routing.html>

#### NEW QUESTION 25

- (Exam Topic 1)

A company uses an Amazon S3 bucket to store data files. The S3 bucket contains hundreds of objects. The company needs to replace a tag on all the objects in the S3 bucket with another tag.

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

- A. Use S3 Batch Operation
- B. Specify the operation to replace all object tags.

- C. Use the AWS CLI to get the tags for each object
- D. Save the tags in a list
- E. Use S3 Batch Operations. Specify the operation to delete all object tags
- F. Use the AWS CLI and the list to retag the objects.
- G. Use the AWS CLI to get the tags for each object
- H. Save the tags in a list
- I. Use the AWS CLI and the list to remove the object tag
- J. Use the AWS CLI and the list to retag the objects.
- K. Use the AWS CLI to copy the objects to another S3 bucket
- L. Add the new tag to the copied objects. Delete the original objects.

**Answer:** A

**Explanation:**

Ref. <https://aws.amazon.com/es/blogs/storage/adding-and-removing-object-tags-with-s3-batch-operations/>

**NEW QUESTION 27**

- (Exam Topic 1)

A company uses AWS Organizations to manage multiple AWS accounts with consolidated billing enabled. Organization member account owners want the benefits of Reserved Instances (RIs) but do not want to share RIs with other accounts. Which solution will meet these requirements?

- A. Purchase RIs in individual member account
- B. Disable RI discount sharing in the management account.
- C. Purchase RIs in individual member account
- D. Disable RI discount sharing in the member accounts.
- E. Purchase RIs in the management account
- F. Disable RI discount sharing in the management account.
- G. Purchase RIs in the management account
- H. Disable RI discount sharing in the member accounts.

**Answer:** A

**Explanation:**

<https://aws.amazon.com/premiumsupport/knowledge-center/ec2-ri-consolidated-billing/>

RI discounts apply to accounts in an organization's consolidated billing family depending upon whether RI sharing is turned on or off for the accounts. By default, RI sharing for all accounts in an organization is turned on. The management account of an organization can change this setting by turning off RI sharing for an account. The capacity reservation for an RI applies only to the account the RI was purchased on, no matter whether RI sharing is turned on or off.

**NEW QUESTION 31**

- (Exam Topic 1)

A gaming application is deployed on four Amazon EC2 instances in a default VPC. The SysOps administrator has noticed consistently high latency in responses as data is transferred among the four instances. There is no way for the administrator to alter the application code. The MOST effective way to reduce latency is to relaunch the EC2 instances in:

- A. a dedicated VPC.
- B. a single subnet inside the VPC.
- C. a placement group.
- D. a single Availability Zone.

**Answer:** C

**NEW QUESTION 33**

- (Exam Topic 1)

A company is hosting applications on Amazon EC2 instances. The company is hosting a database on an Amazon RDS for PostgreSQL DB instance. The company requires all connections to the DB instance to be encrypted. What should a SysOps administrator do to meet this requirement?

- A. Allow SSL connections to the database by using an inbound security group rule.
- B. Encrypt the database by using an AWS Key Management Service (AWS KMS) encryption key.
- C. Enforce SSL connections to the database by using a custom parameter group.
- D. Patch the database with SSL/TLS by using a custom PostgreSQL extension.

**Answer:** C

**Explanation:**

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/PostgreSQL.Concepts.General.SSL.htm> Amazon RDS supports SSL/TLS encryption for connections to the database, and this can be enabled by creating a custom parameter group and setting the `rds.force_ssl` parameter to 1. This will ensure that all connections to the database are encrypted, protecting the data and maintaining compliance with the company's requirements.

**NEW QUESTION 37**

- (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 38

- (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 43

- (Exam Topic 1)

A development team recently deployed a new version of a web application to production. After the release, penetration testing revealed a cross-site scripting vulnerability that could expose user data. Which AWS service will mitigate this issue?

- A. AWS Shield Standard
- B. AWS WAF
- C. Elastic Load Balancing
- D. Amazon Cognito

**Answer:** B

#### Explanation:

<https://www.imperva.com/learn/application-security/cross-site-scripting-xss-attacks/>

#### NEW QUESTION 46

- (Exam Topic 1)

A company uses AWS CloudFormation to deploy its application infrastructure. Recently, a user accidentally changed a property of a database in a CloudFormation template and performed a stack update that caused an interruption to the application. A SysOps administrator must determine how to modify the deployment process to allow the DevOps team to continue to deploy the infrastructure, but prevent against accidental modifications to specific resources. Which solution will meet these requirements?

- A. Set up an AWS Config rule to alert based on changes to any CloudFormation stack. An AWS Lambda function can then describe the stack to determine if any protected resources were modified and cancel the operation.
- B. Set up an Amazon CloudWatch Events event with a rule to trigger based on any CloudFormation API call. An AWS Lambda function can then describe the stack to determine if any protected resources were modified and cancel the operation.
- C. Launch the CloudFormation templates using a stack policy with an explicit allow for all resources and an explicit deny of the protected resources with an action of Update.
- D. Attach an IAM policy to the DevOps team role that prevents a CloudFormation stack from updating, with a condition based on the specific Amazon Resource Names (ARNs) of the protected resources.

**Answer:** B

#### NEW QUESTION 48

- (Exam Topic 1)

A SysOps administrator is tasked with analyzing database performance. The database runs on a single Amazon RDS D6 instance. The SysOps administrator finds that, during times of peak traffic, resources on the database are over utilized due to the amount of read traffic. Which actions should the SysOps administrator take to improve RDS performance? (Select TWO.)

- A. Add a read replica.
- B. Modify the application to use Amazon ElastiCache for Memcached.
- C. Migrate the database from RDS to Amazon DynamoDB.
- D. Migrate the database to Amazon EC2 with enhanced networking enabled.
- E. Upgrade the database to a Multi-AZ deployment.

**Answer:** AB

### NEW QUESTION 50

- (Exam Topic 1)

A SysOps administrator launches an Amazon EC2 Linux instance in a public subnet. When the instance is running, the SysOps administrator obtains the public IP address and attempts to remotely connect to the instance multiple times. However, the SysOps administrator always receives a timeout error. Which action will allow the SysOps administrator to remotely connect to the instance?

- A. Add a route table entry in the public subnet for the SysOps administrator's IP address.
- B. Add an outbound network ACL rule to allow TCP port 22 for the SysOps administrator's IP address.
- C. Modify the instance security group to allow inbound SSH traffic from the SysOps administrator's IP address.
- D. Modify the instance security group to allow outbound SSH traffic to the SysOps administrator's IP address.

**Answer: C**

### NEW QUESTION 53

- (Exam Topic 1)

A software company runs a workload on Amazon EC2 instances behind an Application Load Balancer (ALB). A SysOps administrator needs to define a custom health check for the EC2 instances. What is the MOST operationally efficient solution?

- A. Set up each EC2 Instance so that it writes its healthy/unhealthy status into a shared Amazon S3 bucket for the ALB to read
- B. Configure the health check on the ALB and ensure that the HealthCheckPath setting is correct
- C. Set up Amazon ElastiCache to track the EC2 instances as they scale in and out
- D. Configure an Amazon API Gateway health check to ensure custom checks on each of the EC2 instances

**Answer: B**

### NEW QUESTION 57

- (Exam Topic 1)

A SysOps administrator has successfully deployed a VPC with an AWS CloudFormation template. The SysOps administrator wants to deploy the same template across multiple accounts that are managed through AWS Organizations.

Which solution will meet this requirement with the LEAST operational overhead?

- A. Assume the OrganizationAccountAccessRole IAM role from the management account
- B. Deploy the template in each of the accounts
- C. Create an AWS Lambda function to assume a role in each account. Deploy the template by using the AWS CloudFormation CreateStack API call
- D. Create an AWS Lambda function to query for a list of accounts. Deploy the template by using the AWS CloudFormation CreateStack API call.
- E. Use AWS CloudFormation StackSets from the management account to deploy the template in each of the accounts

**Answer: D**

#### Explanation:

AWS CloudFormation StackSets extends the capability of stacks by enabling you to create, update, or delete stacks across multiple accounts and AWS Regions.

### NEW QUESTION 61

- (Exam Topic 1)

A company's reporting job that used to run in 15 minutes is now taking an hour to run. An application generates the reports. The application runs on Amazon EC2 instances and extracts data from an Amazon RDS for MySQL database.

A SysOps administrator checks the Amazon CloudWatch dashboard for the RDS instance and notices that the Read IOPS metrics are high, even when the reports are not running. The SysOps administrator needs to improve the performance and the availability of the RDS instance.

Which solution will meet these requirements?

- A. Configure an Amazon ElastiCache cluster in front of the RDS instance
- B. Update the reporting job to query the ElastiCache cluster.
- C. Deploy an RDS read replica
- D. Update the reporting job to query the reader endpoint.
- E. Create an Amazon CloudFront distribution
- F. Set the RDS instance as the origin
- G. Update the reporting job to query the CloudFront distribution.
- H. Increase the size of the RDS instance.

**Answer: B**

#### Explanation:

Using an RDS read replica will improve the performance and availability of the RDS instance by offloading read queries to the replica. This will also ensure that the reporting job completes in a timely manner and does not affect the performance of other queries that might be running on the RDS instance. Additionally, updating the reporting job to query the reader endpoint will ensure that all read queries are directed to the read replica.

Reference: [1] [https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_ReadRepl.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html)

### NEW QUESTION 62

- (Exam Topic 1)

A SysOps administrator is troubleshooting an AWS CloudFormation template whereby multiple Amazon EC2 instances are being created. The template is working in us-east-1, but it is failing in us-west-2 with the error code:

```
AMI [ami-12345678] does not exist
```

How should the administrator ensure that the AWS CloudFormation template is working in every region?

- A. Copy the source region's Amazon Machine Image (AMI) to the destination region and assign it the same ID.
- B. Edit the AWS CloudFormation template to specify the region code as part of the fully qualified AMI ID.
- C. Edit the AWS CloudFormation template to offer a drop-down list of all AMIs to the user by using the `aws::EC2::ami::imageId` control.

- D. Modify the AWS CloudFormation template by including the AMI IDs in the "Mappings" section
- E. Refer to the proper mapping within the template for the proper AMI ID.

**Answer:** A

#### NEW QUESTION 67

- (Exam Topic 1)

A SysOps administrator is creating an Amazon EC2 Auto Scaling group in a new AWS account. After adding some instances, the SysOps administrator notices that the group has not reached the minimum number of instances. The SysOps administrator receives the following error message:

```
Launching a new EC2 instance. Status Reason: Your quota allows for 0 more running instance(s).  
You requested at least 1. Launching EC2 instance failed.
```

Which action will resolve this issue?

- A. Adjust the account spending limits for Amazon EC2 on the AWS Billing and Cost Management console
- B. Modify the EC2 quota for that AWS Region in the EC2 Settings section of the EC2 console.
- C. Request a quota increase for the Instance type family by using Service Quotas on the AWS Management Console.
- D. Use the Rebalance action in the Auto Scaling group on the AWS Management Console.

**Answer:** C

#### NEW QUESTION 68

- (Exam Topic 1)

A company creates custom AMI images by launching new Amazon EC2 instances from an AWS CloudFormation template it installs and configures necessary software through AWS OpsWorks and takes images of each EC2 instance. The process of installing and configuring software can take between 2 to 3 hours but at times the process stalls due to installation errors.

The SysOps administrator must modify the CloudFormation template so if the process stalls, the entire stack will fail and roll back.

Based on these requirements, what should be added to the template?

- A. Conditions with a timeout set to 4 hours.
- B. CreationPolicy with timeout set to 4 hours.
- C. DependsOn a timeout set to 4 hours.
- D. Metadata with a timeout set to 4 hours

**Answer:** B

#### NEW QUESTION 69

- (Exam Topic 1)

A company recently acquired another corporation and all of that corporation's AWS accounts. A financial analyst needs the cost data from these accounts. A SysOps administrator uses Cost Explorer to generate cost and usage reports. The SysOps administrator notices that "No Tagkey" represents 20% of the monthly cost.

What should the SysOps administrator do to tag the "No Tagkey" resources?

- A. Add the accounts to AWS Organization
- B. Use a service control policy (SCP) to tag all the untagged resources.
- C. Use an AWS Config rule to find the untagged resource
- D. Set the remediation action to terminate the resources.
- E. Use Cost Explorer to find and tag all the untagged resources.
- F. Use Tag Editor to find and tag all the untagged resources.

**Answer:** D

#### Explanation:

"You can add tags to resources when you create the resource. You can use the resource's service console or API to add, change, or remove those tags one resource at a time. To add tags to—or edit or delete tags of—multiple resources at once, use Tag Editor. With Tag Editor, you search for the resources that you want to tag, and then manage tags for the resources in your search results." <https://docs.aws.amazon.com/ARG/latest/userguide/tag-editor.html>

#### NEW QUESTION 71

- (Exam Topic 1)

A SysOps administrator must create a solution that automatically shuts down any Amazon EC2 instances that have less than 10% average CPU utilization for 60 minutes or more.

Which solution will meet this requirement in the MOST operationally efficient manner?

- A. Implement a cron job on each EC2 instance to run once every 60 minutes and calculate the current CPU utilization
- B. Initiate an instance shutdown if CPU utilization is less than 10%.
- C. Implement an Amazon CloudWatch alarm for each EC2 instance to monitor average CPU utilization. Set the period at 1 hour, and set the threshold at 10%. Configure an EC2 action on the alarm to stop the instance.
- D. Install the unified Amazon CloudWatch agent on each EC2 instance, and enable the Basic level predefined metric set
- E. Log CPU utilization every 60 minutes, and initiate an instance shutdown if CPU utilization is less than 10%.
- F. Use AWS Systems Manager Run Command to get CPU utilization from each EC2 instance every 60 minutes
- G. Initiate an instance shutdown if CPU utilization is less than 10%.

**Answer:** B

#### Explanation:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html>

#### NEW QUESTION 75

- (Exam Topic 1)

An organization is running multiple applications for their customers. Each application is deployed by running a base AWS CloudFormation template that configures a new VPC. All applications are run in the same AWS account and AWS Region. A SysOps administrator has noticed that when trying to deploy the same AWS CloudFormation stack, it fails to deploy. What is likely to be the problem?

- A. The Amazon Machine image used is not available in that region.
- B. The AWS CloudFormation template needs to be updated to the latest version.
- C. The VPC configuration parameters have changed and must be updated in the template.
- D. The account has reached the default limit for VPCs allowed.

**Answer: D**

#### NEW QUESTION 78

- (Exam Topic 1)

A Sysops administrator has created an Amazon EC2 instance using an AWS CloudFormation template in the us-east-1 Region. The administrator finds that this template has failed to create an EC2 instance in the us-west-2 Region. What is one cause for this failure?

- A. Resource tags defined in the CloudFormation template are specific to the us-east-1 Region.
- B. The Amazon Machine Image (AMI) ID referenced in the CloudFormation template could not be found in the us-west-2 Region.
- C. The cfn-init script did not run during resource provisioning in the us-west-2 Region.
- D. The IAM user was not created in the specified Region.

**Answer: B**

#### Explanation:

One possible cause for the failure of the CloudFormation template to create an EC2 instance in the us-west-2 Region is that the Amazon Machine Image (AMI) ID referenced in the template could not be found in the us-west-2 Region. This could be due to the fact that the AMI is not available in that region, or the credentials used to access the AMI were not configured properly. The other options (resource tags defined in the CloudFormation template are specific to the us-east-1 Region, the cfn-init script did not run during resource provisioning in the us-west-2 Region, and the IAM user was not created in the specified Region) are not valid causes for this failure.

#### NEW QUESTION 81

- (Exam Topic 1)

A company hosts a web application on an Amazon EC2 instance. The web server logs are published to Amazon CloudWatch Logs. The log events have the same structure and include the HTTP response codes that are associated with the user requests. The company needs to monitor the number of times that the web server returns an HTTP 404 response.

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

- A. Create a CloudWatch Logs metric filter that counts the number of times that the web server returns an HTTP 404 response.
- B. Create a CloudWatch Logs subscription filter that counts the number of times that the web server returns an HTTP 404 response.
- C. Create an AWS Lambda function that runs a CloudWatch Logs Insights query that counts the number of 404 codes in the log events during the past hour.
- D. Create a script that runs a CloudWatch Logs Insights query that counts the number of 404 codes in the log events during the past hour.

**Answer: A**

#### Explanation:

This is the most operationally efficient solution that meets the requirements, as it will allow the company to monitor the number of times that the web server returns an HTTP 404 response in real-time. The other solutions (creating a CloudWatch Logs subscription filter, an AWS Lambda function, or a script) will require additional steps and resources to monitor the number of times that the web server returns an HTTP 404 response.

A metric filter allows you to search for specific terms, phrases, or values in your log events, and then to create a metric based on the number of occurrences of those search terms. This allows you to create a CloudWatch Metric that can be used to create alarms and dashboards, which can be used to monitor the number of HTTP 404 responses returned by the web server.

#### NEW QUESTION 85

- (Exam Topic 1)

A company stores files on 50 Amazon S3 buckets in the same AWS Region. The company wants to connect to the S3 buckets securely over a private connection from its Amazon EC2 instances. The company needs a solution that produces no additional cost.

Which solution will meet these requirements?

- A. Create a gateway VPC endpoint for each S3 bucket. Attach the gateway VPC endpoints to each subnet inside the VPC.
- B. Create an interface VPC endpoint for each S3 bucket. Attach the interface VPC endpoints to each subnet inside the VPC.
- C. Create one gateway VPC endpoint for all the S3 buckets. Add the gateway VPC endpoint to the VPC route table.
- D. Create one interface VPC endpoint for all the S3 buckets. Add the interface VPC endpoint to the VPC route table.

**Answer: C**

#### NEW QUESTION 86

- (Exam Topic 1)

A company is running a flash sale on its website. The website is hosted on burstable performance Amazon EC2 instances in an Auto Scaling group. The Auto Scaling group is configured to launch instances when the CPU utilization is above 70%.

A couple of hours into the sale, users report slow load times and error messages for refused connections. A SysOps administrator reviews Amazon CloudWatch metrics and notices that the CPU utilization is at 20% across the entire fleet of instances.

The SysOps administrator must restore the website's functionality without making changes to the network infrastructure.

Which solution will meet these requirements?

- A. Activate unlimited mode for the instances in the Auto Scaling group.
- B. Implement an Amazon CloudFront distribution to offload the traffic from the Auto Scaling group.
- C. Move the website to a different AWS Region that is closer to the users.

D. Reduce the desired size of the Auto Scaling group to artificially increase CPU average utilization.

**Answer:** B

**Explanation:**

Implement an Amazon CloudFront distribution to offload the traffic from the Auto Scaling group does not breach the requirement of no changes in the network infrastructure. Reason is that cloudfront is a distribution that allows you to distribute content using a worldwide network of edge locations that provide low latency and high data transfer speeds. It plug in to existing setup, not changes to it.

**NEW QUESTION 87**

- (Exam Topic 1)

A company has an application that customers use to search for records on a website. The application's data is stored in an Amazon Aurora DB cluster. The application's usage varies by season and by day of the week.

The website's popularity is increasing, and the website is experiencing slower performance because of increased load on the DB cluster during periods of peak activity. The application logs show that the performance issues occur when users are searching for information. The same search is rarely performed multiple times.

A SysOps administrator must improve the performance of the platform by using a solution that maximizes resource efficiency. Which solution will meet these requirements?

- A. Deploy an Amazon ElastiCache for Redis cluster in front of the DB cluster
- B. Modify the application to check the cache before the application issues new queries to the database
- C. Add the results of any queries to the cache.
- D. Deploy an Aurora Replica for the DB cluster
- E. Modify the application to use the reader endpoint for search operation
- F. Use Aurora Auto Scaling to scale the number of replicas based on load
- G. Most Voted
- H. Use Provisioned IOPS on the storage volumes that support the DB cluster to improve performance sufficiently to support the peak load on the application.
- I. Increase the instance size in the DB cluster to a size that is sufficient to support the peak load on the application
- J. Use Aurora Auto Scaling to scale the instance size based on load.

**Answer:** B

**Explanation:**

[https://docs.amazonaws.cn/en\\_us/AmazonRDS/latest/AuroraUserGuide/aurora-replicas-adding.html](https://docs.amazonaws.cn/en_us/AmazonRDS/latest/AuroraUserGuide/aurora-replicas-adding.html)

**NEW QUESTION 92**

- (Exam Topic 1)

A company plans to deploy a database on an Amazon Aurora MySQL DB cluster. The database will store data for a demonstration environment. The data must be reset on a daily basis.

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

- A. Create a manual snapshot of the DB cluster after the data has been populated
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function on a daily basis
- C. Configure the function to restore the snapshot and then delete the previous DB cluster.
- D. Enable the Backtrack feature during the creation of the DB cluster
- E. Specify a target backtrack window of 48 hours
- F. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function on a daily basis
- G. Configure the function to perform a backtrack operation.
- H. Export a manual snapshot of the DB cluster to an Amazon S3 bucket after the data has been populated. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function on a daily basis
- I. Configure the function to restore the snapshot from Amazon S3.
- J. Set the DB cluster backup retention period to 2 days
- K. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function on a daily basis
- L. Configure the function to restore the DB cluster to a point in time and then delete the previous DB cluster.

**Answer:** D

**Explanation:**

Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function on a daily basis. Configure the function to restore the DB cluster to a point in time and then delete the previous DB cluster. This is the most operationally efficient solution that meets the requirements, as it will allow the company to reset the database on a daily basis without having to manually take and restore snapshots. The other solutions (creating a manual snapshot of the DB cluster, enabling the Backtrack feature, or exporting a manual snapshot of the DB cluster to Amazon S3) will require additional steps and resources to reset the database on a daily basis.

**NEW QUESTION 95**

- (Exam Topic 1)

A company is using an Amazon DynamoDB table for data. A SysOps administrator must configure replication of the table to another AWS Region for disaster recovery.

What should the SysOps administrator do to meet this requirement?

- A. Enable DynamoDB Accelerator (DAX).
- B. Enable DynamoDB Streams, and add a global secondary index (GSI).
- C. Enable DynamoDB Streams, and add a global table Region.
- D. Enable point-in-time recovery.

**Answer:** C

**NEW QUESTION 99**

- (Exam Topic 1)

A company's IT department noticed an increase in the spend of their developer AWS account. There are over 50 developers using the account, and the finance team wants to determine the service costs incurred by each developer. What should a SysOps administrator do to collect this information? (Select TWO.)

- A. Activate the createdBy tag in the account.
- B. Analyze the usage with Amazon CloudWatch dashboards.
- C. Analyze the usage with Cost Explorer.
- D. Configure AWS Trusted Advisor to track resource usage.
- E. Create a billing alarm in AWS Budgets.

**Answer: AC**

#### NEW QUESTION 104

- (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 107

- (Exam Topic 1)

A SysOps administrator must configure a resilient tier of Amazon EC2 instances for a high performance computing (HPC) application. The HPC application requires minimum latency between nodes. Which actions should the SysOps administrator take to meet these requirements? (Select TWO.)

- A. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the file system to the EC2 instances by using user data.
- B. Create a Multi-AZ Network Load Balancer in front of the EC2 instances.
- C. Place the EC2 instances in an Auto Scaling group within a single subnet.
- D. Launch the EC2 instances into a cluster placement group.
- E. Launch the EC2 instances into a partition placement group.

**Answer: AD**

#### NEW QUESTION 111

- (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 112

- (Exam Topic 1)

A company is storing media content in an Amazon S3 bucket and uses Amazon CloudFront to distribute the content to its users. Due to licensing terms, the company is not authorized to distribute the content in some countries. A SysOps administrator must restrict access to certain countries. What is the MOST operationally efficient solution that meets these requirements?

- A. Configure the S3 bucket policy to deny the GetObject operation based on the S3:LocationConstraint condition.
- B. Create a secondary origin access identity (OAI). Configure the S3 bucket policy to prevent access from unauthorized countries.
- C. Enable the geo restriction feature in the CloudFront distribution to prevent access from unauthorized countries.
- D. Update the application to generate signed CloudFront URLs only for IP addresses in authorized countries.

**Answer: C**

#### NEW QUESTION 116

- (Exam Topic 1)

A company plans to launch a static website on its domain example.com and subdomain www.example.com using Amazon S3. How should the SysOps

administrator meet this requirement?

- A. Create one S3 bucket named example.com for both the domain and subdomain.
- B. Create one S3 bucket with a wildcard named \*.example.com for both the domain and subdomain.
- C. Create two S3 buckets named example.com and www.example.com.
- D. Configure the subdomain bucket to redirect requests to the domain bucket.
- E. Create two S3 buckets named http://example.com and http://www.example.com.
- F. Configure the wildcard (\*) bucket to redirect requests to the domain bucket.

**Answer: C**

#### NEW QUESTION 121

- (Exam Topic 1)

A company runs its Infrastructure on Amazon EC2 Instances that run in an Auto Scaling group. Recently, the company promoted faulty code to the entire EC2 fleet. This faulty code caused the Auto Scaling group to scale the instances before any of the application logs could be retrieved.

What should a SysOps administrator do to retain the application logs after instances are terminated?

- A. Configure an Auto Scaling lifecycle hook to create a snapshot of the ephemeral storage upon termination of the instances.
- B. Create a new Amazon Machine Image (AMI) that has the Amazon CloudWatch agent installed and configured to send logs to Amazon CloudWatch Log
- C. Update the launch template to use the new AMI.
- D. Create a new Amazon Machine Image (AMI) that has a custom script configured to send logs to AWS CloudTrail
- E. Update the launch template to use the new AMI.
- F. Install the Amazon CloudWatch agent on the Amazon Machine Image (AMI) that is defined in the launch template
- G. Configure the CloudWatch agent to back up the logs to ephemeral storage.

**Answer: B**

#### NEW QUESTION 126

- (Exam Topic 1)

A company is trying to connect two applications. One application runs in an on-premises data center that has a hostname of host1.onprem.private. The other application runs on an Amazon EC2 instance that has a hostname of host1.awscloud.private. An AWS Site-to-Site VPN connection is in place between the on-premises network and AWS.

The application that runs in the data center tries to connect to the application that runs on the EC2 instance, but DNS resolution fails. A SysOps administrator must implement DNS resolution between on-premises and AWS resources.

Which solution allows the on-premises application to resolve the EC2 instance hostname?

- A. Set up an Amazon Route 53 inbound resolver endpoint with a forwarding rule for the onprem.private hosted zone
- B. Associate the resolver with the VPC of the EC2 instance
- C. Configure the on-premises DNS resolver to forward onprem.private DNS queries to the inbound resolver endpoint.
- D. Set up an Amazon Route 53 inbound resolver endpoint
- E. Associate the resolver with the VPC of the EC2 instance
- F. Configure the on-premises DNS resolver to forward awscloud.private DNS queries to the inbound resolver endpoint.
- G. Set up an Amazon Route 53 outbound resolver endpoint with a forwarding rule for the onprem.private hosted zone
- H. Associate the resolver with the AWS Region of the EC2 instance
- I. Configure the on-premises DNS resolver to forward onprem.private DNS queries to the outbound resolver endpoint.
- J. Set up an Amazon Route 53 outbound resolver endpoint
- K. Associate the resolver with the AWS Region of the EC2 instance
- L. Configure the on-premises DNS resolver to forward awscloud.private DNS queries to the outbound resolver endpoint.

**Answer: C**

#### NEW QUESTION 131

- (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 132

- (Exam Topic 1)

A SysOps administrator is setting up a fleet of Amazon EC2 instances in an Auto Scaling group for an application. The fleet should have 50% CPU available at that times to accommodate bursts of traffic. The load will increase significantly between the hours of 09:00 and 17:00, 7 days a week

How should the SysOps administrator configure the scaling of the EC2 instances to meet these requirements?

- A. Create a target tracking scaling policy that runs when the CPU utilization is higher than 90%
- B. Create a target tracking scaling policy that runs when the CPU utilization is higher than 50%. Create a scheduled scaling policy that ensures that the fleet is available at 09:00 Create a second scheduled scaling policy that scales in the fleet at 17:00
- C. Set the Auto Scaling group to start with 2 instances by setting the desired instances maximum instances, and minimum instances to 2 Create a scheduled

scaling policy that ensures that the fleet is available at 09:00

D. Create a scheduled scaling policy that ensures that the fleet is available at 09.00. Create a second scheduled scaling policy that scales in the fleet at 17:00

**Answer:** B

#### NEW QUESTION 135

- (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 139

- (Exam Topic 1)

A company is implementing a monitoring solution that is based on machine learning. The monitoring solution consumes Amazon EventBridge (Amazon CloudWatch Events) events that are generated by Amazon EC2 Auto Scaling. The monitoring solution provides detection of anomalous behavior such as unanticipated scaling events and is configured as an EventBridge (CloudWatch Events) API destination.

During initial testing, the company discovers that the monitoring solution is not receiving events. However, Amazon CloudWatch is showing that the EventBridge (CloudWatch Events) rule is being invoked. A SysOps administrator must implement a solution to retrieve client error details to help resolve this issue.

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

- A. Create an EventBridge (CloudWatch Events) archive for the event pattern to replay the event
- B. Increase the logging on the monitoring solution
- C. Use replay to invoke the monitoring solution
- D. Examine the error details.
- E. Add an Amazon Simple Queue Service (Amazon SQS) standard queue as a dead-letter queue for the target
- F. Process the messages in the dead-letter queue to retrieve error details.
- G. Create a second EventBridge (CloudWatch Events) rule for the same event pattern to target an AWS Lambda function
- H. Configure the Lambda function to invoke the monitoring solution and to record the results to Amazon CloudWatch Log
- I. Examine the errors in the logs.
- J. Configure the EventBridge (CloudWatch Events) rule to send error messages to an Amazon Simple Notification Service (Amazon SNS) topic.

**Answer:** A

#### Explanation:

"In EventBridge, you can create an archive of events so that you can easily replay them at a later time. For example, you might want to replay events to recover from errors or to validate new functionality in your application." <https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-archive.html>

#### NEW QUESTION 140

- (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 144

- (Exam Topic 1)

A company has a critical serverless application that uses multiple AWS Lambda functions. Each Lambda function generates 1 GB of log data daily in its own Amazon CloudWatch Logs log group. The company's security team asks for a count of application errors, grouped by type, across all of the log groups.

What should a SysOps administrator do to meet this requirement?

- A. Perform a CloudWatch Logs Insights query that uses the stats command and count function.
- B. Perform a CloudWatch Logs search that uses the groupby keyword and count function.
- C. Perform an Amazon Athena query that uses the SELECT and GROUP BY keywords.
- D. Perform an Amazon RDS query that uses the SELECT and GROUP BY keywords.

**Answer:** A

#### NEW QUESTION 148

- (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 152

- (Exam Topic 1)

A company is undergoing an external audit of its systems, which run wholly on AWS. A SysOps administrator must supply documentation of Payment Card Industry Data Security Standard (PCI DSS) compliance for the infrastructure managed by AWS.

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

- A. Download the applicable reports from the AWS Artifact portal and supply these to the auditors.
- B. Download complete copies of the AWS CloudTrail log files and supply these to the auditors.
- C. Download complete copies of the AWS CloudWatch logs and supply these to the auditors.
- D. Provide the auditors with administrative access to the production AWS account so that the auditors can determine compliance.

**Answer:** A

#### NEW QUESTION 153

- (Exam Topic 1)

A SysOps administrator noticed that a large number of Elastic IP addresses are being created on the company's AWS account, but they are not being associated with Amazon EC2 instances, and are incurring Elastic IP address charges in the monthly bill.

How can the administrator identify who is creating the Elastic IP addresses?

- A. Attach a cost-allocation tag to each requested Elastic IP address with the IAM user name of the developer who creates it.
- B. Query AWS CloudTrail logs by using Amazon Athena to search for Elastic IP address events.
- C. Create a CloudWatch alarm on the EIPCreated metric and send an Amazon SNS notification when the alarm triggers.
- D. Use Amazon Inspector to get a report of all Elastic IP addresses created in the last 30 days.

**Answer:** B

#### NEW QUESTION 154

- (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 158

- (Exam Topic 1)

A company stores sensitive data in an Amazon S3 bucket. The company must log all access attempts to the S3 bucket. The company's risk team must receive immediate notification about any delete events.

Which solution will meet these requirements?

- A. Enable S3 server access logging for audit log
- B. Set up an Amazon Simple Notification Service (Amazon SNS) notification for the S3 bucket
- C. Select DeleteObject for the event type for the alert system.
- D. Enable S3 server access logging for audit log
- E. Launch an Amazon EC2 instance for the alert system. Run a cron job on the EC2 instance to download the access logs each day and to scan for a DeleteObject event.
- F. Use Amazon CloudWatch Logs for audit log
- G. Use Amazon CloudWatch alarms with an Amazon Simple Notification Service (Amazon SNS) notification for the alert system.
- H. Use Amazon CloudWatch Logs for audit log
- I. Launch an Amazon EC2 instance for the alert system. Run a cron job on the EC2 instance each day to compare the list of the items with the list from the previous day
- J. Configure the cron job to send a notification if an item is missing.

**Answer:** A

#### Explanation:

To meet the requirements of logging all access attempts to the S3 bucket and receiving immediate notification about any delete events, the company can enable S3 server access logging and set up an Amazon Simple Notification Service (Amazon SNS) notification for the S3 bucket. The S3 server access logs will record all access attempts to the bucket, including delete events, and the SNS notification can be configured to send an alert when a DeleteObject event occurs.

#### NEW QUESTION 159

- (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 160

- (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 162

- (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 164

- (Exam Topic 1)

A company runs its entire suite of applications on Amazon EC2 instances. The company plans to move the applications to containers and AWS Fargate. Within 6 months, the company plans to retire its EC2 instances and use only Fargate. The company has been able to estimate its future Fargate costs.

A SysOps administrator needs to choose a purchasing option to help the company minimize costs. The SysOps administrator must maximize any discounts that are available and must ensure that there are no unused reservations.

Which purchasing option will meet these requirements?

- A. Compute Savings Plans for 1 year with the No Upfront payment option
- B. Compute Savings Plans for 1 year with the Partial Upfront payment option
- C. EC2 Instance Savings Plans for 1 year with the All Upfront payment option
- D. EC2 Reserved Instances for 1 year with the Partial Upfront payment option

**Answer: C**

#### NEW QUESTION 168

- (Exam Topic 1)

A development team recently deployed a new version of a web application to production. After the release, penetration testing revealed a cross-site scripting vulnerability that could expose user data.

Which AWS service will mitigate this issue?

- A. AWS Shield Standard
- B. AWS WAF
- C. Elastic Load Balancing
- D. Amazon Cognito

**Answer: A**

#### NEW QUESTION 169

- (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**

#### NEW QUESTION 171

- (Exam Topic 1)

A SysOps administrator must manage the security of an AWS account. Recently, an IAM user's access key was mistakenly uploaded to a public code repository. The SysOps administrator must identify anything that was changed by using this access key.

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to send all IAM events to an AWS Lambda function for analysis.
- B. Query Amazon EC2 logs by using Amazon CloudWatch Logs Insights for all events related to the compromised access key within the suspected timeframe.
- C. Search AWS CloudTrail event history for all events initiated with the compromised access key within the suspected timeframe.
- D. Search VPC Flow Logs for all events initiated with the compromised access key within the suspected timeframe.

**Answer: C**

#### NEW QUESTION 175

- (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 177

- (Exam Topic 1)

A new website will run on Amazon EC2 instances behind an Application Load Balancer. Amazon Route 53 will be used to manage DNS records.

What type of record should be set in Route 53 to point the website's apex domain name (for example, company.com) to the Application Load Balancer?

- A. CNAME
- B. SOA
- C. TXT
- D. ALIAS

**Answer: D**

#### NEW QUESTION 178

- (Exam Topic 1)

A company is running a website on Amazon EC2 instances that are in an Auto Scaling group. When the website traffic increases, additional instances take several minutes to become available because of a

long-running user data script that installs software. A SysOps administrator must decrease the time that is required (or new instances to become available).

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

- A. Reduce the scaling thresholds so that instances are added before traffic increases.
- B. Purchase Reserved Instances to cover 100% of the maximum capacity of the Auto Scaling group.
- C. Update the Auto Scaling group to launch instances that have a storage optimized instance type.
- D. Use EC2 Image Builder to prepare an Amazon Machine Image (AMI) that has pre-installed software.

**Answer: D**

#### Explanation:

Automated way to update your image. Have a pipeline to update your image. When you boot from your AMI, updates/scripts are already pre-installed, so no need to complete boot scripts in boot process. <https://aws.amazon.com/image-builder/>

#### NEW QUESTION 182

- (Exam Topic 1)

A company is using Amazon Elastic File System (Amazon EFS) to share a file system among several Amazon EC2 instances. As usage increases, users report that file retrieval from the EFS file system is slower than normal.

Which action should a SysOps administrator take to improve the performance of the file system?

- A. Configure the file system for Provisioned Throughput.
- B. Enable encryption in transit on the file system.

- C. Identify any unused files in the file system, and remove the unused files.
- D. Resize the Amazon Elastic Block Store (Amazon EBS) volume of each of the EC2 instances.

**Answer:** A

#### NEW QUESTION 186

- (Exam Topic 1)

A Sysops administrator needs to configure automatic rotation for Amazon RDS database credentials. The credentials must rotate every 30 days. The solution must integrate with Amazon RDS.

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

- A. Store the credentials in AWS Systems Manager Parameter Store as a secure string
- B. Configure automatic rotation with a rotation interval of 30 days.
- C. Store the credentials in AWS Secrets Manager
- D. Configure automatic rotation with a rotation interval of 30 days.
- E. Store the credentials in a file in an Amazon S3 bucket
- F. Deploy an AWS Lambda function to automatically rotate the credentials every 30 days.
- G. Store the credentials in AWS Secrets Manager
- H. Deploy an AWS Lambda function to automatically rotate the credentials every 30 days.

**Answer:** B

#### Explanation:

Storing the credentials in AWS Secrets Manager and configuring automatic rotation with a rotation interval of 30 days is the most efficient way to meet the requirements with the least operational overhead. AWS Secrets Manager automatically rotates the credentials at the specified interval, so there is no need for an additional AWS Lambda function or manual rotation. Additionally, Secrets Manager is integrated with Amazon RDS, so the credentials can be easily used with the RDS database.

#### NEW QUESTION 190

- (Exam Topic 1)

A company's customers are reporting increased latency while accessing static web content from Amazon S3. A SysOps administrator observed a very high rate of read operations on a particular S3 bucket.

What will minimize latency by reducing load on the S3 bucket?

- A. Migrate the S3 bucket to a region that is closer to end users' geographic locations
- B. Use cross-region replication to replicate all of the data to another region
- C. Create an Amazon CloudFront distribution with the S3 bucket as the origin.
- D. Use Amazon ElastiCache to cache data being served from Amazon S3

**Answer:** C

#### NEW QUESTION 192

- (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 enabled
- 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 197

- (Exam Topic 1)

A SysOps administrator configures an Amazon S3 gateway endpoint in a VPC. The private subnets inside the VPC do not have outbound internet access. A user logs in to an Amazon EC2 instance in one of the private subnets and cannot upload a file to an Amazon S3 bucket in the same AWS Region.

Which solution will solve this problem?

- A. Update the EC2 instance role policy to allow s3:PutObject access to the target S3 bucket.
- B. Update the EC2 security group to allow outbound traffic to 0.0.0.0/0 for port 80.
- C. Update the EC2 subnet route table to include the S3 prefix list destination routes to the S3 gateway endpoint.
- D. Update the S3 bucket policy to allow s3:PutObject access from the private subnet CIDR block.

**Answer:** C

#### NEW QUESTION 199

- (Exam Topic 1)

A company has an application that runs only on Amazon EC2 Spot Instances. The instances run in an Amazon EC2 Auto Scaling group with scheduled scaling actions.

However, the capacity does not always increase at the scheduled times, and instances terminate many times a day. A Sysops administrator must ensure that the instances launch on time and have fewer interruptions.

Which action will meet these requirements?

- A. Specify the capacity-optimized allocation strategy for Spot Instance
- B. Add more instance types to the Auto Scaling group.
- C. Specify the capacity-optimized allocation strategy for Spot Instance
- D. Increase the size of the instances in the Auto Scaling group.
- E. Specify the lowest-price allocation strategy for Spot Instance
- F. Add more instance types to the Auto Scaling group.
- G. Specify the lowest-price allocation strategy for Spot Instance
- H. Increase the size of the instances in the Auto Scaling group.

**Answer:** A

**Explanation:**

Specifying the capacity-optimized allocation strategy for Spot Instances and adding more instance types to the Auto Scaling group is the best action to meet the requirements. Increasing the size of the instances in the Auto Scaling group will not necessarily help with the launch time or reduce interruptions, as the Spot Instances could still be interrupted even with larger instance sizes.

**NEW QUESTION 201**

- (Exam Topic 1)

A company needs to create a daily Amazon Machine Image (AMI) of an existing Amazon Linux EC2 instance that hosts the operating system, application, and database on multiple attached Amazon Elastic Block Store (Amazon EBS) volumes. File system integrity must be maintained.

Which solution will meet these requirements?

- A. Create an AWS Lambda function to call the CreateImage API operation with the EC2 instance ID and the no-reboot parameter enable
- B. Create a daily scheduled Amazon EventBridge (Amazon CloudWatch Events) rule that invokes the function.
- C. Create an AWS Lambda function to call the CreateImage API operation with the EC2 instance ID and the reboot parameter enable
- D. Create a daily scheduled Amazon EventBridge (Amazon CloudWatch Events) rule that invokes the function.
- E. Use AWS Backup to create a backup plan with a backup rule that runs dail
- F. Assign the resource ID of the EC2 instance with the no-reboot parameter enabled.
- G. Use AWS Backup to create a backup plan with a backup rule that runs dail
- H. Assign the resource ID of the EC2 instance with the reboot parameter enabled.

**Answer:** B

**Explanation:**

[https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/Creating\\_EBSbacked\\_WinAMI.html](https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/Creating_EBSbacked_WinAMI.html) "NoReboot By default, Amazon EC2 attempts to shut down and reboot the instance before creating the image.

If the No Reboot option is set, Amazon EC2 doesn't shut down the instance before creating the image. When this option is used, file system integrity on the created image can't be guaranteed." Besides, we can use AWS EventBridge to invoke Lambda function

[https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API\\_CreateImage.html](https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_CreateImage.html)

**NEW QUESTION 204**

- (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 1AM credentials.
- B. Set up Amazon Inspector
- C. Scan and monitor resources for unauthorized logins.
- D. Set up AWS Confi
- 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 209**

- (Exam Topic 1)

A company is planning to host its stateful web-based applications on AWS A SysOps administrator is using an Auto Scaling group of Amazon EC2 instances The web applications will run 24 hours a day 7 days a week throughout the year The company must be able to change the instance type within the same instance family later in the year based on the traffic and usage patterns

Which EC2 instance purchasing option will meet these requirements MOST cost-effectively?

- A. Convertible Reserved Instances
- B. On-Demand instances
- C. Spot instances
- D. Standard Reserved instances

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ri-convertible-exchange.html>

**NEW QUESTION 214**

- (Exam Topic 1)

An Amazon EC2 instance needs to be reachable from the internet. The EC2 instance is in a subnet with the following route table:

| Destination   | Target         |
|---------------|----------------|
| 10.0.0.0/16   | Local          |
| 172.31.0.0/16 | pcx-1122334455 |

Which entry must a SysOps administrator add to the route table to meet this requirement?

- A. A route for 0.0.0.0/0 that points to a NAT gateway
- B. A route for 0.0.0.0/0 that points to an egress-only internet gateway
- C. A route for 0.0.0.0/0 that points to an internet gateway
- D. A route for 0.0.0.0/0 that points to an elastic network interface

**Answer: C**

#### NEW QUESTION 219

- (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 221

- (Exam Topic 1)

A company uses an Amazon Simple Queue Service (Amazon SQS) standard queue with its application. The application sends messages to the queue with unique message bodies. The company decides to switch to an SQS FIFO queue.

What must the company do to migrate to an SQS FIFO queue?

- A. Create a new SQS FIFO queue. Turn on content-based deduplication on the new FIFO queue. Update the application to include a message group ID in the messages.
- B. Create a new SQS FIFO queue. Update the application to include the DelaySeconds parameter in the messages.
- C. Modify the queue type from SQS standard to SQS FIFO. Turn off content-based deduplication on the queue. Update the application to include a message group ID in the messages.
- D. Modify the queue type from SQS standard to SQS FIFO. Update the application to send messages with identical message bodies and to include the DelaySeconds parameter in the messages.

**Answer: A**

#### Explanation:

FIFO queues don't support per-message delays, only per-queue delays. If your application sets the same value of the DelaySeconds parameter on each message, you must modify your application to remove the per-message delay and set DelaySeconds on the entire queue instead.

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues-moving.html>

#### NEW QUESTION 224

- (Exam Topic 1)

A company has attached the following policy to an IAM user:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "rds:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:Region": "us-east-1"
        }
      }
    },
    {
      "Effect": "Deny",
      "NotAction": [
        "ec2:*",
        "s3:GetObject"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:Region": "us-east-1"
        }
      }
    },
    {
      "Effect": "Deny",
      "NotAction": [
        "ec2:*",
        "s3:GetObject"
      ],
      "Resource": "*"
    }
  ]
}
```

Which of the following actions are allowed for the IAM user?

- A. Amazon RDS DescribeDBInstances action in the us-east-1 Region
- B. Amazon S3 Putobject operation in a bucket named testbucket
- C. Amazon EC2 Describe Instances action in the us-east-1 Region
- D. Amazon EC2 AttachNetworkinterface action in the eu-west-1 Region

**Answer: C**

#### NEW QUESTION 225

- (Exam Topic 1)

A company plans to migrate several of its high performance computing (MPC) virtual machines (VMs) to Amazon EC2 instances on AWS. A SysOps administrator must identify a placement group for this deployment. The strategy must minimize network latency and must maximize network throughput between the HPC VMs. Which strategy should the SysOps administrator choose to meet these requirements?

- A. Deploy the instances in a cluster placement group in one Availability Zone.
- B. Deploy the instances in a partition placement group in two Availability Zones
- C. Deploy the instances in a partition placement group in one Availability Zone
- D. Deploy the instances in a spread placement group in two Availability Zones

**Answer: A**

#### NEW QUESTION 230

- (Exam Topic 1)

A company updates its security policy to clarify cloud hosting arrangements for regulated workloads. Workloads that are identified as sensitive must run on hardware that is not shared with other customers or with other AWS accounts within the company. Which solution will ensure compliance with this policy?

- A. Deploy workloads only to Dedicated Hosts.
- B. Deploy workloads only to Dedicated Instances.
- C. Deploy workloads only to Reserved Instances.
- D. Place all instances in a dedicated placement group.

**Answer:** A

**Explanation:**

Dedicated Hosts are physical servers that are dedicated to a single customer, ensuring that the customer's workloads are not shared with other customers or with other AWS accounts within the company. This will ensure that the company's security policy is followed and that sensitive workloads are running on hardware that is not shared with other customers or with other AWS accounts within the company.

**NEW QUESTION 231**

- (Exam Topic 1)

A company runs an application on Amazon EC2 instances. The EC2 instances are in an Auto Scaling group and run behind an Application Load Balancer (ALB). The application experiences errors when total requests exceed 100 requests per second. A SysOps administrator must collect information about total requests for a 2-week period to determine when requests exceeded this threshold.

What should the SysOps administrator do to collect this data?

- A. Use the ALB's RequestCount metri
- B. Configure a time range of 2 weeks and a period of 1 minute.Examine the chart to determine peak traffic times and volumes.
- C. Use Amazon CloudWatch metric math to generate a sum of request counts for all the EC2 instances over a 2-week perio
- D. Sort by a 1-minute interval.
- E. Create Amazon CloudWatch custom metrics on the EC2 launch configuration templates to create aggregated request metrics across all the EC2 instances.
- F. Create an Amazon EventBridge (Amazon CloudWatch Events) rul
- G. Configure an EC2 event matching pattern that creates a metric that is based on EC2 request
- H. Display the data in a graph.

**Answer:** A

**Explanation:**

Using the ALB's RequestCount metric will allow the SysOps administrator to collect information about total requests for a 2-week period and determine when requests exceeded the threshold of 100 requests per second. Configuring a time range of 2 weeks and a period of 1 minute will ensure that the data can be accurately examined to determine peak traffic times and volumes.

**NEW QUESTION 232**

- (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 instanc
- 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:AuthoflzeSecurityGroupIngress 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 VP
- G. Add a statement to the IAM role policy to allow the ec2:CreateVpnConnection action on the bastion hos
- H. Instruct the team to use the bastion host endpoint to connect to the instances.D Create an internet-facing Network Load Balance
- I. Use two listener
- 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 234**

- (Exam Topic 1)

With the threat of ransomware viruses encrypting and holding company data hostage, which action should be taken to protect an Amazon S3 bucket?

- A. Deny Pos
- B. Pu
- C. and Delete on the bucket.
- D. Enable server-side encryption on the bucket.
- E. Enable Amazon S3 versioning on the bucket.
- F. Enable snapshots on the bucket.

**Answer:** B

**NEW QUESTION 238**

- (Exam Topic 1)

A SysOps administrator created an AWS Cloud Formation template that provisions Amazon EC2 instances, an Elastic Load Balancer (ELB), and an Amazon RDS DB instance. During stack creation, the creation of the EC2 instances and the creation of the ELB are successful. However, the creation of the DB instance fails.

What is the default behavior of CloudFormation in this scenario?

- A. CloudFormation will roll back the stack and delete the stack.
- B. CloudFormation will roll back the stack but will not delete the stack.
- C. CloudFormation will prompt the user to roll back the stack or continue.
- D. CloudFormation will successfully complete the stack but will report a failed status for the DB instance.

**Answer:** C

#### NEW QUESTION 242

- (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 244

- (Exam Topic 1)

An Amazon EC2 instance is running an application that uses Amazon Simple Queue Service (Amazon SQS) queues. A SysOps administrator must ensure that the application can read, write, and delete messages from the SQS queues.

Which solution will meet these requirements in the MOST secure manner?

- A. Create an IAM user with an IAM policy that allows the sqs SendMessage permission, the sqs ReceiveMessage permission, and the sqs DeleteMessage permission to the appropriate queues. Embed the IAM user's credentials in the application's configuration.
- B. Create an IAM user with an IAM policy that allows the sqs SendMessage permission, the sqs ReceiveMessage permission, and the sqs DeleteMessage permission to the appropriate queues. Export the IAM user's access key and secret access key as environment variables on the EC2 instance.
- C. Create and associate an IAM role that allows EC2 instances to call AWS services. Attach an IAM policy to the role that allows sqs.\* permissions to the appropriate queues.
- D. Create and associate an IAM role that allows EC2 instances to call AWS services. Attach an IAM policy to the role that allows the sqs SendMessage permission, the sqs ReceiveMessage permission, and the sqs DeleteMessage permission to the appropriate queues.

**Answer:** D

#### NEW QUESTION 247

- (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 248

- (Exam Topic 1)

A company has a stateful web application that is hosted on Amazon EC2 instances in an Auto Scaling group. The instances run behind an Application Load Balancer (ALB) that has a single target group. The ALB is configured as the origin in an Amazon CloudFront distribution. Users are reporting random logouts from the web application.

Which combination of actions should a SysOps administrator take to resolve this problem? (Select TWO.)

- A. Change to the least outstanding requests algorithm on the ALB target group.
- B. Configure cookie forwarding in the CloudFront distribution cache behavior.
- C. Configure header forwarding in the CloudFront distribution cache behavior.
- D. Enable group-level stickiness on the ALB listener rule.
- E. Enable sticky sessions on the ALB target group.

**Answer:** BE

**Explanation:**

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Cookies.html>

You can configure each cache behavior to do one of the following: Forward all cookies to your origin – CloudFront includes all cookies sent by the viewer when it forwards requests to the origin. <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/sticky-sessions.html>

By default, an Application Load Balancer routes each request independently to a registered target based on the chosen load-balancing algorithm.

**NEW QUESTION 251**

- (Exam Topic 1)

A manufacturing company uses an Amazon RDS DB instance to store inventory of all stock items. The company maintains several AWS Lambda functions that interact with the database to add, update, and delete items. The Lambda functions use hardcoded credentials to connect to the database.

A SysOps administrator must ensure that the database credentials are never stored in plaintext and that the password is rotated every 30 days.

Which solution will meet these requirements in the MOST operationally efficient manner?

- A. Store the database password as an environment variable for each Lambda function.
- B. Create a new Lambda function that is named PasswordRotate.
- C. Use Amazon EventBridge (Amazon CloudWatch Events) to schedule the PasswordRotate function every 30 days to change the database password and update the environment variable for each Lambda function.
- D. Use AWS Key Management Service (AWS KMS) to encrypt the database password and to store the encrypted password as an environment variable for each Lambda function.
- E. Grant each Lambda function access to the KMS key so that the database password can be decrypted when required.
- F. Create a new Lambda function that is named PasswordRotate to change the password every 30 days.
- G. Use AWS Secrets Manager to store credentials for the databases.
- H. Create a Secrets Manager secret, and select the database so that Secrets Manager will use a Lambda function to update the database password automatically.
- I. Specify an automatic rotation schedule of 30 days.
- J. Update each Lambda function to access the database password from Secrets Manager.
- K. Use AWS Systems Manager Parameter Store to create a secure string to store credentials for the databases.
- L. Create a new Lambda function called PasswordRotate.
- M. Use Amazon EventBridge (Amazon CloudWatch Events) to schedule the PasswordRotate function every 30 days to change the database password and to update the secret within Parameter Store.
- N. Update each Lambda function to access the database password from Parameter Store.

**Answer:** C

**Explanation:**

When you choose to enable rotation, Secrets Manager supports the following Amazon Relational Database Service (Amazon RDS) databases with AWS written and tested Lambda rotation function templates, and full configuration of the rotation process:

Amazon Aurora on Amazon RDS MySQL on Amazon RDS PostgreSQL on Amazon RDS Oracle on Amazon RDS MariaDB on Amazon RDS

Microsoft SQL Server on Amazon RDS <https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html>

**NEW QUESTION 252**

- (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 255**

- (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 258**

- (Exam Topic 1)

A company hosts a web application on an Amazon EC2 instance in a production VPC. Client connections to the application are failing. A SysOps administrator

inspects the VPC flow logs and finds the following entry:

```
2 111122223333 eni-####> 192.0.2.15 203.0.113.56 40711 443 6 1 40 1418530010 1418530070 REJECT OK
```

What is a possible cause of these failed connections?

- A. A security group is denying traffic on port 443.
- B. The EC2 instance is shut down.
- C. The network ACL is blocking HTTPS traffic.
- D. The VPC has no internet gateway attached.

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-records-examples.html#flow-log-example-accepted>

<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-records-examples.html#>

Accepted and rejected traffic: In this example, RDP traffic (destination port 3389, TCP protocol) to network interface eni-1235b8ca123456789 in account 123456789010 was rejected. 2 123456789010

```
eni-1235b8ca123456789 172.31.9.69 172.31.9.12 49761 3389 6 20 4249 1418530010 1418530070 REJECT OK
```

**NEW QUESTION 260**

- (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 265**

- (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 267**

- (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 AVVS 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 270**

- (Exam Topic 1)

A SysOps administrator is notified that an Amazon EC2 instance has stopped responding. The AWS Management Console indicates that the system status checks are failing. What should the administrator do first to resolve this issue?

- A. Reboot the EC2 instance so it can be launched on a new host
- B. Stop and then start the EC2 instance so that it can be launched on a new host
- C. Terminate the EC2 instance and relaunch it
- D. View the AWS CloudTrail log to investigate what changed on the EC2 instance

**Answer:** B

**Explanation:**

<https://aws.amazon.com/premiumsupport/knowledge-center/ec2-windows-system-status-check-fail/>

**NEW QUESTION 271**

- (Exam Topic 1)

A company uses AWS Organizations. A SysOps administrator wants to use AWS Compute Optimizer and AWS tag policies in the management account to govern all member accounts in the billing family. The SysOps administrator navigates to the AWS Organizations console but cannot activate tag policies through the management account.

What could be the reason for this issue?

- A. All features have not been enabled in the organization.

- B. Consolidated billing has not been enabled.
- C. The member accounts do not have tags enabled for cost allocation.
- D. The member accounts have not manually enabled trusted access for Compute Optimizer.

**Answer:** C

#### NEW QUESTION 274

- (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

#### Explanation:

"An Auto Scaling group can contain EC2 instances in one or more Availability Zones within the same Region. However, Auto Scaling groups cannot span multiple Regions". As stated in <https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-benefits.htm>

#### NEW QUESTION 279

- (Exam Topic 1)

A company has an organization in AWS Organizations. The company uses shared VPCs to provide networking resources across accounts. A SysOps administrator has been able to successfully launch and manage Amazon EC2 instances in a participant account. However, the SysOps administrator is now receiving an InstanceLimitExceeded error when the SysOps administrator tries to launch a new EC2 instance. What should the SysOps administrator do to resolve this error?

- A. Request an instance quota increase from the account that owns the VPC.
- B. Launch additional EC2 instances in a different AWS Region.
- C. Request an instance quota increase from the parent account.
- D. Launch additional EC2 instances by using a different Amazon Machine Image (AMI).

**Answer:** A

#### NEW QUESTION 284

- (Exam Topic 1)

An errant process is known to use an entire processor and run at 100%. A SysOps administrator wants to automate restarting the instance once the problem occurs for more than 2 minutes. How can this be accomplished?

- A. Create an Amazon CloudWatch alarm for the Amazon EC2 instance with basic monitoring.
- B. Enable an action to restart the instance.
- C. Create a CloudWatch alarm for the EC2 instance with detailed monitoring.
- D. Enable an action to restart the instance.
- E. Create an AWS Lambda function to restart the EC2 instance, triggered on a scheduled basis every 2 minutes.
- F. Create a Lambda function to restart the EC2 instance, triggered by EC2 health checks.

**Answer:** B

#### NEW QUESTION 285

- (Exam Topic 1)

A company plans to run a public web application on Amazon EC2 instances behind an Elastic Load Balancer (ELB). The company's security team wants to protect the website by using AWS Certificate Manager (ACM) certificates. The ELB must automatically redirect any HTTP requests to HTTPS. Which solution will meet these requirements?

- A. Create an Application Load Balancer that has one HTTPS listener on port 80. Attach an SSL/TLS certificate to listener port 80. Create a rule to redirect requests from HTTP to HTTPS.
- B. Create an Application Load Balancer that has one HTTP listener on port 80 and one HTTPS protocol listener on port 443. Attach an SSL/TLS certificate to listener port 443. Create a rule to redirect requests from port 80 to port 443.
- C. Create an Application Load Balancer that has two TCP listeners on port 80 and port 443. Attach an SSL/TLS certificate to listener port 443. Create a rule to redirect requests from port 80 to port 443.
- D. Create a Network Load Balancer that has two TCP listeners on port 80 and port 443. Attach an SSL/TLS certificate to listener port 443. Create a rule to redirect requests from port 80 to port 443.

**Answer:** B

#### NEW QUESTION 290

- (Exam Topic 1)

A company has an application that is deployed in two AWS Regions in an active-passive configuration. The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB) in each Region. The instances are in an Amazon EC2 Auto Scaling group in each Region. The application uses an Amazon Route 53 hosted zone (or DNS). A SysOps administrator needs to configure automatic failover to the secondary Region. What should the SysOps administrator do to meet these requirements?

- A. Configure Route 53 alias records that point to each ALB.
- B. Choose a failover routing policy.

- C. Set Evaluate Target Health to Yes.
- D. Configure CNAME records that point to each AL
- E. Choose a failover routing polic
- F. Set Evaluate Target Health to Yes.
- G. Configure Elastic Load Balancing (ELB) health checks for the Auto Scaling grou
- H. Add a target group to the ALB in the primary Regio
- I. Include the EC2 instances in the secondary Region as targets.
- J. Configure EC2 health checks for the Auto Scaling grou
- K. Add a target group to the ALB in the primary Regio
- L. Include the EC2 instances in the secondary Region as targets.

**Answer:** A

#### NEW QUESTION 295

- (Exam Topic 1)

A SysOps administrator is tasked with deploying a company's infrastructure as code. The SysOps administrator want to write a single template that can be reused for multiple environments.

How should the SysOps administrator use AWS CloudFormation to create a solution?

- A. Use Amazon EC2 user data in a CloudFormation template
- B. Use nested stacks to provision resources
- C. Use parameters in a CloudFormation template
- D. Use stack policies to provision resources

**Answer:** C

#### Explanation:

Reuse templates to replicate stacks in multiple environments After you have your stacks and resources set up, you can reuse your templates to replicate your infrastructure in multiple environments. For example, you can create environments for development, testing, and production so that you can test changes before implementing them into production. To make templates reusable, use the parameters, mappings, and conditions sections so that you can customize your stacks when you create them. For example, for your development environments, you can specify a lower-cost instance type compared to your production environment, but all other configurations and settings remain the same. <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html#reuse>

#### NEW QUESTION 299

- (Exam Topic 1)

A company has a memory-intensive application that runs on a fleet of Amazon EC2 instances behind an Elastic Load Balancer (ELB). The instances run in an Auto Scaling group. A Sysops administrator must ensure that the application can scale based on the number of users that connect to the application.

Which solution will meet these requirements?

- A. Create a scaling policy that will scale the application based on the ActiveConnectionCount Amazon CloudWatch metric that is generated from the ELB.
- B. Create a scaling policy that will scale the application based on the mem used Amazon CloudWatch metric that is generated from the ELB.
- C. Create a scheduled scaling policy to increase the number of EC2 instances in the Auto Scaling group to support additional connections.
- D. Create and deploy a script on the ELB to expose the number of connected users as a custom Amazon CloudWatch metri
- E. Create a scaling policy that uses the metric.

**Answer:** D

#### Explanation:

This solution will allow the application to scale based on the number of users that connect to the application. The other solutions (creating a scaling policy that uses the ActiveConnectionCount Amazon CloudWatch metric generated from the ELB, creating a scaling policy that uses the mem used Amazon CloudWatch metric generated from the ELB, or creating a scheduled scaling policy to increase the number of EC2 instances in the Auto Scaling group to support additional connections) will not meet the requirements, as they do not allow the application to scale based on the number of users that connect to the application.

#### NEW QUESTION 302

- (Exam Topic 1)

A SysOps administrator has created an AWS Service Catalog portfolio and has shared the portfolio with a second AWS account in the company. The second account is controlled by a different administrator.

Which action will the administrator of the second account be able to perform?

- A. Add a product from the imported portfolio to a local portfolio.
- B. Add new products to the imported portfolio.
- C. Change the launch role for the products contained in the imported portfolio.
- D. Customize the products in the imported portfolio.

**Answer:** A

#### NEW QUESTION 305

- (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-balancer> [https://aws.amazon.com/global-accelerator/faqs/?nc1=h\\_ls](https://aws.amazon.com/global-accelerator/faqs/?nc1=h_ls)

**NEW QUESTION 310**

- (Exam Topic 2)

If your AWS Management Console browser does not show that you are logged in to an AWS account, close the browser and relaunch the console by using the AWS Management Console shortcut from the VM desktop.

If the copy-paste functionality is not working in your environment, refer to the instructions file on the VM desktop and use Ctrl+C, Ctrl+V or Command-C, Command-V.

Configure Amazon EventBridge to meet the following requirements.

- \* 1. use the us-east-2 Region for all resources,
- \* 2. Unless specified below, use the default configuration settings.
- \* 3. Use your own resource naming unless a resource name is specified below.
- \* 4. Ensure all Amazon EC2 events in the default event bus are replayable for the past 90 days.
- \* 5. Create a rule named RunFunction to send the exact message every 15 minutes to an existing AWS Lambda function named LogEventFunction.
- \* 6. Create a rule named SpotWarning to send a notification to a new standard Amazon SNS topic named TopicEvents whenever an Amazon EC2 Spot Instance is interrupted. Do NOT create any topic subscriptions. The notification must match the following structure:

Input path:

```
{"instance": "$.detail.instance-id"}
```

Input Path:

```
{"instance": "$.detail.instance-id"}
```

Input template:

"The EC2 Spot Instance <instance> has been on account."

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Here are the steps to configure Amazon EventBridge to meet the above requirements:

- Log in to the AWS Management Console by using the AWS Management Console shortcut from the VM desktop. Make sure that you are logged in to the desired AWS account.
- Go to the EventBridge service in the us-east-2 Region.
- In the EventBridge service, navigate to the "Event buses" page.
- Click on the "Create event bus" button.
- Give a name to your event bus, and select "default" as the event source type.
- Navigate to "Rules" page and create a new rule named "RunFunction"
- In the "Event pattern" section, select "Schedule" as the event source and set the schedule to run every 15 minutes.
- In the "Actions" section, select "Send to Lambda" and choose the existing AWS Lambda function named "LogEventFunction"
- Create another rule named "SpotWarning"
- In the "Event pattern" section, select "EC2" as the event source, and filter the events on "EC2 Spot Instance interruption"
- In the "Actions" section, select "Send to SNS topic" and create a new standard Amazon SNS topic named "TopicEvents"
- In the "Input Transformer" section, set the Input Path to {"instance": "\$.detail.instance-id"} and Input template to "The EC2 Spot Instance <instance> has been interrupted on account."
- Now all Amazon EC2 events in the default event bus will be replayable for past 90 days. Note:
- You can use the AWS Management Console, AWS CLI, or SDKs to create and manage EventBridge resources.
- You can use CloudTrail event history to replay events from the past 90 days.
- You can refer to the AWS EventBridge documentation for more information on how to configure and use the service: <https://aws.amazon.com/eventbridge/>

**NEW QUESTION 313**

.....

## Relate Links

**100% Pass Your AWS-SysOps Exam with ExamBible Prep Materials**

<https://www.exambible.com/AWS-SysOps-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>