

Amazon

Exam Questions AWS-SysOps

Amazon AWS Certified SysOps Administrator - Associate



NEW QUESTION 1

- (Exam Topic 1)

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

How should a SysOps administrator meet these requirements?

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

Answer: D

Explanation:

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

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

NEW QUESTION 2

- (Exam Topic 1)

A company needs to restrict access to an Amazon S3 bucket to Amazon EC2 instances in a VPC only. All traffic must be over the AWS private network.

What actions should the SysOps administrator take to meet these requirements?

- A. Create a VPC endpoint for the S3 bucket, and create an IAM policy that conditionally limits all S3 actions on the bucket to the VPC endpoint as the source.
- B. Create a VPC endpoint for the S3 bucket, and create an S3 bucket policy that conditionally limits all S3 actions on the bucket to the VPC endpoint as the source.
- C. Create a service-linked role for Amazon EC2 that allows the EC2 instances to interact directly with Amazon S3, and attach an IAM policy to the role that allows the EC2 instances full access to the S3 bucket.
- D. Create a NAT gateway in the VPC, and modify the VPC route table to route all traffic destined for Amazon S3 through the NAT gateway.

Answer: B

Explanation:

While IAM policy (letter A) also can be used, it does not enforce everyone. The only option that enforces everyone is policy configured directly in the bucket S3.

NEW QUESTION 3

- (Exam Topic 1)

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

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

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

Answer: A

NEW QUESTION 4

- (Exam Topic 1)

A SysOps administrator is deploying an application on 10 Amazon EC2 instances. The application must be highly available. The instances must be placed on distinct underlying hardware.

What should the SysOps administrator do to meet these requirements?

- A. Launch the instances into a cluster placement group in a single AWS Region.
- B. Launch the instances into a partition placement group in multiple AWS Regions.
- C. Launch the instances into a spread placement group in multiple AWS Regions.
- D. Launch the instances into a spread placement group in single AWS Region

Answer: D

Explanation:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

NEW QUESTION 5

- (Exam Topic 1)

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

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

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

Answer: A

NEW QUESTION 6

- (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 7

- (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 8

- (Exam Topic 1)

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

What should the SysOps administrator do to troubleshoot this issue?

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

Answer: B

NEW QUESTION 9

- (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 10

- (Exam Topic 1)

A company has an initiative to reduce costs associated with Amazon EC2 and AWS Lambda. Which action should a SysOps administrator take to meet these requirements?

- A. Analyze the AWS Cost and Usage Report by using Amazon Athena to identify cost savings.
- B. Create an AWS Budgets alert to alarm when account spend reaches 80% of the budget.
- C. Purchase Reserved Instances through the Amazon EC2 console.
- D. Use AWS Compute Optimizer and take action on the provided recommendations.

Answer: D

NEW QUESTION 10

- (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 14

- (Exam Topic 1)

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

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

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

Answer: B

Explanation:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html

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

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

NEW QUESTION 16

- (Exam Topic 1)

A SysOps administrator is using AWS Systems Manager Patch Manager to patch a fleet of Amazon EC2 instances. The SysOps administrator has configured a patch baseline and a maintenance window. The SysOps administrator also has used an instance tag to identify which instances to patch.

The SysOps administrator must give Systems Manager the ability to access the EC2 instances. Which additional action must the SysOps administrator perform to meet this requirement?

- A. Add an inbound rule to the instances' security group.
- B. Attach an IAM instance profile with access to Systems Manager to the instances.
- C. Create a Systems Manager activation Then activate the fleet of instances.
- D. Manually specify the instances to patch Instead of using tag-based selection.

Answer: A

NEW QUESTION 20

- (Exam Topic 1)

A company uses an Amazon Elastic File System (Amazon EFS) file system to share files across many Linux Amazon EC2 instances. A SysOps administrator notices that the file system's PercentIOLimit metric is consistently at 100% for 15 minutes or longer. The SysOps administrator also notices that the application that reads and writes to that file system is performing poorly. The application requires high throughput and IOPS while accessing the file system.

What should the SysOps administrator do to remediate the consistently high PercentIOLimit metric?

- A. Create a new EFS file system that uses Max I/O performance mod
- B. Use AWS DataSync to migrate data to the new EFS file system.
- C. Create an EFS lifecycle policy to transition future files to the Infrequent Access (IA) storage class to improve performance
- D. Use AWS DataSync to migrate existing data to IA storage.
- E. Modify the existing EFS file system and activate Max I/O performance mode.
- F. Modify the existing EFS file system and activate Provisioned Throughput mode.

Answer: A

Explanation:

To support a wide variety of cloud storage workloads, Amazon EFS offers two performance modes, General Purpose mode and Max I/O mode. You choose a file system's performance mode when you create it, and it cannot be changed. If the PercentIOLimit percentage returned was at or near 100 percent for a significant amount of time during the test, your application should use the Max I/O performance mode. <https://docs.aws.amazon.com/efs/latest/ug/performance.html>

NEW QUESTION 23

- (Exam Topic 1)

A recent organizational audit uncovered an existing Amazon RDS database that is not currently configured for high availability. Given the critical nature of this database, it must be configured for high availability as soon as possible.

How can this requirement be met?

- A. Switch to an active/passive database pair using the create-db-instance-read-replica with the --availability-zone flag.
- B. Specify high availability when creating a new RDS instance, and live-migrate the data.
- C. Modify the RDS instance using the console to include the Multi-AZ option.
- D. Use the modify-db-instance command with the --na flag.

Answer: C

NEW QUESTION 26

- (Exam Topic 1)

An environment consists of 100 Amazon EC2 Windows instances. The Amazon CloudWatch agent is deployed and running on all EC2 instances with a baseline configuration file to capture log files. There is a new requirement to capture the DHCP log files that exist on 50 of the instances.

What is the MOST operational efficient way to meet this new requirement?

- A. Create an additional CloudWatch agent configuration file to capture the DHCP logs. Use the AWS Systems Manager Run Command to restart the CloudWatch agent on each EC2 instance with the append-config option to apply the additional configuration file.
- B. Log in to each EC2 instance with administrator rights. Create a PowerShell script to push the needed baseline log files and DHCP log files to CloudWatch.
- C. Run the CloudWatch agent configuration file wizard on each EC2 instance. Verify that the base log files are included and add the DHCP log files during the wizard creation process.
- D. Run the CloudWatch agent configuration file wizard on each EC2 instance and select the advanced detail level.
- E. This will capture the operating system log files.

Answer: A

NEW QUESTION 31

- (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:*",

```



```
{
  "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 36

- (Exam Topic 1)

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

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

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

Answer: A

NEW QUESTION 40

- (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 44

- (Exam Topic 1)

A SysOps administrator has an AWS CloudFormation template of the company's existing infrastructure in us-west-2. The administrator attempts to use the template to launch a new stack in eu-west-1, but the stack only partially deploys, receives an error message, and then rolls back.

Why would this template fail to deploy? (Select TWO.)

- A. The template referenced an IAM user that is not available in eu-west-1.
- B. The template referenced an Amazon Machine Image (AMI) that is not available in eu-west-1.
- C. The template did not have the proper level of permissions to deploy the resources.
- D. The template requested services that do not exist in eu-west-1.
- E. CloudFormation templates can be used only to update existing services.

Answer: BD

NEW QUESTION 47

- (Exam Topic 1)

A SysOps administrator is evaluating Amazon Route 53 DNS options to address concerns about high availability for an on-premises website. The website consists of two servers: a primary active server and a secondary passive server. Route 53 should route traffic to the primary server if the associated health check returns 2xx or 3xx HTTP codes. All other traffic should be directed to the secondary passive server. The failover record type, set ID, and routing policy have been set appropriately for both primary and secondary servers.

Which next step should be taken to configure Route 53?

- A. Create an A record for each serve
- B. Associate the records with the Route 53 HTTP health check.
- C. Create an A record for each serve
- D. Associate the records with the Route 53 TCP health check.
- E. Create an alias record for each server with evaluate target health set to ye
- F. Associate the records with the Route 53 HTTP health check.
- G. Create an alias record for each server with evaluate target health set to ye
- H. Associate the records with the Route 53 TCP health check.

Answer: A

NEW QUESTION 48

- (Exam Topic 1)

A company is running an application on a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). The EC2 instances are launched by an Auto Scaling group and are automatically registered in a target group. A SysOps administrator must set up a notification to alert application owners when targets fail health checks.

What should the SysOps administrator do to meet these requirements?

- A. Create an Amazon CloudWatch alarm on the UnHealthyHostCount metri
- B. Configure an action to send an Amazon Simple Notification Service (Amazon SNS) notification when the metric is greater than 0.
- C. Configure an Amazon EC2 Auto Scaling custom lifecycle action to send an Amazon Simple Notification Service (Amazon SNS) notification when an instance is in the Pending:Wait state.
- D. Update the Auto Scaling grou
- E. Configure an activity notification to send an Amazon Simple Notification Service (Amazon SNS) notification for the Unhealthy event type.
- F. Update the ALB health check to send an Amazon Simple Notification Service (Amazon SNS) notification when an instance is unhealthy.

Answer: A

NEW QUESTION 49

- (Exam Topic 1)

A SysOps administrator must ensure that a company's Amazon EC2 instances auto scale as expected. The SysOps administrator configures an Amazon EC2 Auto Scaling Lifecycle hook to send an event to Amazon EventBridge (Amazon CloudWatch Events), which then invokes an AWS Lambda function to configure the EC2 instances. When the configuration is complete, the Lambda function calls the complete Lifecycle-action event to put the EC2 instances into service. In testing, the SysOps administrator discovers that the Lambda function is not invoked when the EC2 instances auto scale.

What should the SysOps administrator do to resolve this issue?

- A. Add a permission to the Lambda function so that it can be invoked by the EventBridge (CloudWatch Events) rule.
- B. Change the lifecycle hook action to CONTINUE if the lifecycle hook experiences a failure or timeout.
- C. Configure a retry policy in the EventBridge (CloudWatch Events) rule to retry the Lambda function invocation upon failure.
- D. Update the Lambda function execution role so that it has permission to call the complete lifecycle-action event

Answer: D

NEW QUESTION 53

- (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 55

- (Exam Topic 1)

A company uses Amazon Elasticsearch Service (Amazon ES) to analyze sales and customer usage data. Members of the company's geographically dispersed sales team are traveling. They need to log in to Kibana by using their existing corporate credentials that are stored in Active Directory. The company has deployed Active Directory Federation Services (AD FS) to enable authentication to cloud services. Which solution will meet these requirements?

- A. Configure Active Directory as an authentication provider in Amazon ES
- B. Add the Active Directory server's domain name to Amazon ES
- C. Configure Kibana to use Amazon ES authentication.
- D. Deploy an Amazon Cognito user pool
- E. Configure Active Directory as an external identity provider for the user pool
- F. Enable Amazon Cognito authentication for Kibana on Amazon ES.
- G. Enable Active Directory user authentication in Kibana
- H. Create an IP-based custom domain access policy in Amazon ES that includes the Active Directory server's IP address.
- I. Establish a trust relationship with Kibana on the Active Directory server

- J. Enable Active Directory user authentication in Kiban
- K. Add the Active Directory server's IP address to Kibana.

Answer: B

Explanation:

<https://aws.amazon.com/blogs/security/how-to-enable-secure-access-to-kibana-using-aws-single-sign-on/> <https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-cognito-auth.html>

NEW QUESTION 57

- (Exam Topic 1)

A company has an Amazon CloudFront distribution that uses an Amazon S3 bucket as its origin. During a review of the access logs, the company determines that some requests are going directly to the S3 bucket by using the website hosting endpoint. A SysOps administrator must secure the S3 bucket to allow requests only from CloudFront.

What should the SysOps administrator do to meet this requirement?

- A. Create an origin access identity (OAI) in CloudFron
- B. Associate the OAI with the distributio
- C. Remove access to and from other principals in the S3 bucket polic
- D. Update the S3 bucket policy to allow accessonly from the OAI.
- E. Create an origin access identity (OAI) in CloudFron
- F. Associate the OAI with the distributio
- G. Update the S3 bucket policy to allow access only from the OA
- H. Create a new origin, and specify the S3 bucket as the new origi
- I. Update the distribution behavior to use the new origi
- J. Remove the existing origin.
- K. Create an origin access identity (OAI) in CloudFron
- L. Associate the OAI with the distributio
- M. Update the S3 bucket policy to allow access only from the OA
- N. Disable website hostin
- O. Create a new origin, and specify the S3 bucket as the new origi
- P. Update the distribution behavior to use the new origi
- Q. Remove the existing origin.
- R. Update the S3 bucket policy to allow access only from the CloudFront distributio
- S. Remove access to and from other principals in the S3 bucket polic
- T. Disable website hostin
- . Create a new origin, and specify the S3 bucket as the new origi
- . Update the distribution behavior to use the new origi
- . Remove the existing origin.

Answer: A

NEW QUESTION 62

- (Exam Topic 1)

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

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

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

Answer: D

NEW QUESTION 67

- (Exam Topic 1)

A SysOps administrator is configuring an application on Amazon EC2 instances for a company Teams in other countries will use the application over the internet. The company requires the application endpoint to have a static pubic IP address.

How should the SysOps administrator deploy the application to meet this requirement?

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

Answer: C

NEW QUESTION 70

- (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 71

- (Exam Topic 1)

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

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

What should a SysOps administrator do to resolve this problem?

- A. Examine the expiration date on the certificate on the origin site
- B. Validate that the certificate has not expired
- C. Replace the certificate if necessary.
- D. Examine the hostname on the certificate on the origin site
- E. Validate that the hostname matches one of the hostnames on the CloudFront distribution
- F. Replace the certificate if necessary.
- G. Examine the firewall rules that are associated with the origin server
- H. Validate that port 443 is open for inbound traffic from the internet
- I. Create an inbound rule if necessary.
- J. Examine the network ACL rules that are associated with the CloudFront distribution
- K. Validate that port 443 is open for outbound traffic to the origin server
- L. Create an outbound rule if necessary.

Answer: A

Explanation:

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

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

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

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

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

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

NEW QUESTION 74

- (Exam Topic 1)

A company hosts its website on Amazon EC2 instances behind an Application Load Balancer. The company manages its DNS with Amazon Route 53, and wants to point its domain's zone apex to the website.

Which type of record should be used to meet these requirements?

- A. A CNAME record for the domain's zone apex
- B. An A record for the domain's zone apex
- C. An AAAA record for the domain's zone apex
- D. An alias record for the domain's zone apex

Answer: D

Explanation:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.htm>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-elb-load-balancer.html>

NEW QUESTION 77

- (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 81

- (Exam Topic 1)

A company's SysOps administrator needs to change the AWS Support plan for one of the company's AWS accounts. The account has multi-factor authentication (MFA) activated, and the MFA device is lost.

What should the SysOps administrator do to sign in?

- A. Sign in as a root user by using email and phone verification
- B. Set up a new MFA device
- C. Change the root user password.
- D. Sign in as an IAM user with administrator permission
- E. Resynchronize the MFA token by using the IAM console.
- F. Sign in as an IAM user with administrator permission
- G. Reset the MFA device for the root user by adding a new device.
- H. Use the forgot-password process to verify the email address
- I. Set up a new password and MFA device.

Answer: A

NEW QUESTION 86

- (Exam Topic 1)

A company hosts an internal application on Amazon EC2 instances. All application data and requests route through an AWS Site-to-Site VPN connection between the on-premises network and AWS. The company must monitor the application for changes that allow network access outside of the corporate network. Any change that exposes the application externally must be restricted automatically.

Which solution meets these requirements in the MOST operationally efficient manner?

- A. Create an AWS Lambda function that updates security groups that are associated with the elastic network interface to remove inbound rules with noncorporate CIDR range
- B. Turn on VPC Flow Logs, and send the logs to Amazon CloudWatch Log
- C. Create an Amazon CloudWatch alarm that matches traffic from noncorporate CIDR ranges, and publish a message to an Amazon Simple Notification Service (Amazon SNS) topic with the Lambda function as a target.
- D. Create a scheduled Amazon EventBridge (Amazon CloudWatch Events) rule that targets an AWS Systems Manager Automation document to check for public IP addresses on the EC2 instance
- E. If public IP addresses are found on the EC2 instances, initiate another Systems Manager Automation document to terminate the instances.
- F. Configure AWS Config and a custom rule to monitor whether a security group allows inbound requests from noncorporate CIDR range
- G. Create an AWS Systems Manager Automation document to remove any noncorporate CIDR ranges from the application security groups.
- H. Configure AWS Config and the managed rule for monitoring public IP associations with the EC2 instances by tag
- I. Tag the EC2 instances with an identifier
- J. Create an AWS Systems Manager Automation document to remove the public IP association from the EC2 instances.

Answer: C

Explanation:

<https://aws.amazon.com/blogs/security/how-to-auto-remediate-internet-accessible-ports-with-aws-config-and-aws-lambda/>

NEW QUESTION 90

- (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 93

- (Exam Topic 1)

A company hosts a database on an Amazon RDS Multi-AZ DB instance. The database is not encrypted. The company's new security policy requires all AWS resources to be encrypted at rest and in transit.

What should a SysOps administrator do to encrypt the database?

- A. Configure encryption on the existing DB instance.
- B. Take a snapshot of the DB instance
- C. Encrypt the snapshot
- D. Restore the snapshot to the same DB instance.
- E. Encrypt the standby replica in a secondary Availability Zone
- F. Promote the standby replica to the primary DB instance.
- G. Take a snapshot of the DB instance
- H. Copy and encrypt the snapshot
- I. Create a new DB instance by restoring the encrypted copy.

Answer: B

NEW QUESTION 97

- (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 100

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 105

- (Exam Topic 1)

A company uses Amazon Route 53 to manage the public DNS records for the domain example.com. The company deploys an Amazon CloudFront distribution to deliver static assets for a new corporate website. The company wants to create a subdomain that is named "static" and must route traffic for the subdomain to the CloudFront distribution.

How should a SysOps administrator create a new record for the subdomain in Route 53?

- A. Create a CNAME record.
- B. Enter static.cloudfront.net as the record name.
- C. Enter the CloudFront distribution's public IP address as the value.
- D. Create a CNAME record.
- E. Enter static.example.com as the record name.
- F. Enter the CloudFront distribution's private IP address as the value.
- G. Create an A record.
- H. Enter static.cloudfront.net as the record name.
- I. Enter the CloudFront distribution's ID as an alias target.
- J. Create an A record.
- K. Enter static.example.com as the record name.
- L. Enter the CloudFront distribution's domain name as an alias target.

Answer: D

Explanation:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html>

NEW QUESTION 109

- (Exam Topic 1)

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

What should the SysOps administrator do to meet these requirements?

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

Answer: C

Explanation:

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

NEW QUESTION 113

- (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 118

- (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 120

- (Exam Topic 1)

A company wants to use only IPv6 for all its Amazon EC2 instances. The EC2 instances must not be accessible from the internet, but the EC2 instances must be able to access the internet. The company creates a dual-stack VPC and IPv6-only subnets.

How should a SysOps administrator configure the VPC to meet these requirements?

- A. Create and attach a NAT gateway
- B. Create a custom route table that includes an entry to point all IPv6 traffic to the NAT gateway
- C. Attach the custom route table to the IPv6-only subnets.
- D. Create and attach an internet gateway
- E. Create a custom route table that includes an entry to point all IPv6 traffic to the internet gateway
- F. Attach the custom route table to the IPv6-only subnets.
- G. Create and attach an egress-only internet gateway
- H. Create a custom route table that includes an entry to point all IPv6 traffic to the egress-only internet gateway
- I. Attach the custom route table to the IPv6-only subnets.
- J. Create and attach an internet gateway and a NAT gateway
- K. Create a custom route table that includes an entry to point all IPv6 traffic to the internet gateway and all IPv4 traffic to the NAT gateway
- L. Attach the custom route table to the IPv6-only subnets.

Answer: C

NEW QUESTION 121

- (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

NEW QUESTION 122

- (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 123

- (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 124

- (Exam Topic 1)

An ecommerce company uses an Amazon ElastiCache for Memcached cluster for in-memory caching of popular product queries on the shopping site. When viewing recent Amazon CloudWatch metrics data for the ElastiCache cluster, the SysOps administrator notices a large number of evictions.

Which of the following actions will reduce these evictions? (Choose two.)

- A. Add an additional node to the ElastiCache cluster.
- B. Increase the ElastiCache time to live (TTL).
- C. Increase the individual node size inside the ElastiCache cluster.
- D. Put an Elastic Load Balancer in front of the ElastiCache cluster.
- E. Use Amazon Simple Queue Service (Amazon SQS) to decouple the ElastiCache cluster.

Answer: AC

Explanation:

<https://d1.awsstatic.com/training-and-certification/docs-sysops-associate/AWS-Certified-SysOps-Administrator>

NEW QUESTION 125

- (Exam Topic 1)

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

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

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

Answer: D

Explanation:

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

Every hour, CloudTrail also creates and delivers a file that references the log files for the last hour and contains a hash of each. This file is called a digest file.

Validated log files are invaluable in security and forensic investigations"

NEW QUESTION 126

- (Exam Topic 1)

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

What change should be made to alleviate the performance problem?

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

Answer: B

NEW QUESTION 131

- (Exam Topic 1)

A SysOps administrator is unable to authenticate an AWS CLI call to an AWS service Which of the following is the cause of this issue?

- A. The IAM password is incorrect
- B. The server certificate is missing
- C. The SSH key pair is incorrect
- D. There is no access key

Answer: C

NEW QUESTION 132

- (Exam Topic 1)

A company has an AWS Cloud Formation template that creates an Amazon S3 bucket. A user authenticates to the corporate AWS account with their Active Directory credentials and attempts to deploy the Cloud Formation template. However, the stack creation fails. Which factors could cause this failure? (Select TWO.)

- A. The user's IAM policy does not allow the cloudformation:CreateStack action.
- B. The user's IAM policy does not allow the cloudformation:CreateStackSet action.
- C. The user's IAM policy does not allow the s3:CreateBucket action.
- D. The user's IAM policy explicitly denies the s3:ListBucket action.
- E. The user's IAM policy explicitly denies the s3:PutObject action

Answer: AC

NEW QUESTION 133

- (Exam Topic 1)

A software company runs a workload on Amazon EC2 instances behind an Application Load Balancer (ALB) A SysOcs 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 HeathCheckPath setting s correct
- C. Set up Amazon ElasticCache to track the EC2 instances as they scale in and out
- D. Configure an Amazon API Gateway health check to ensure custom checks on aw of the EC2 instances

Answer: B

NEW QUESTION 134

- (Exam Topic 1)

A company needs to upload gigabytes of files every day. The company need to achieve higher throughput and upload speeds to Amazon S3 Which action should a SysOps administrator take to meet this requirement?

- A. Create an Amazon CloudFront distribution with the GET HTTP method allowed and the S3 bucket as an origin.
- B. Create an Amazon ElastiCache duster and enable caching for the S3 bucket
- C. Set up AWS Global Accelerator and configure it with the S3 bucket
- D. Enable S3 Transfer Acceleration and use the acceleration endpoint when uploading files

Answer: D

Explanation:

Enable Amazon S3 Transfer Acceleration Amazon S3 Transfer Acceleration can provide fast and secure transfers over long distances between your client and Amazon S3. Transfer Acceleration uses Amazon CloudFront's globally distributed edge locations.

<https://aws.amazon.com/premiumsupport/knowledge-center/s3-upload-large-files/>

NEW QUESTION 139

- (Exam Topic 1)

A company has an existing web application that runs on two Amazon EC2 instances behind an Application Load Balancer (ALB) across two Availability Zones The application uses an Amazon RDS Multi-AZ DB Instance Amazon Route 53 record sets route requests tor dynamic content to the load balancer and requests for static content to an Amazon S3 bucket Site visitors are reporting extremely long loading times. Which actions should be taken to improve the performance of the website? (Select TWO)

- A. Add Amazon CloudFront caching for static content
- B. Change the load balancer listener from HTTPS to TCP
- C. Enable Amazon Route 53 latency-based routing
- D. Implement Amazon EC2 Auto Scaling for the web servers
- E. Move the static content from Amazon S3 to the web servers

Answer: AD

NEW QUESTION 144

- (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 147

- (Exam Topic 1)

A SysOps administrator noticed that the cache hit ratio for an Amazon CloudFront distribution is less than 10%. Which collection of configuration changes will increase the cache hit ratio for the distribution? (Select TWO.)

- A. Ensure that only required cookies, query strings, and headers are forwarded in the Cache Behavior Settings.
- B. Change the Viewer Protocol Policy to use HTTPS only.
- C. Configure the distribution to use presigned cookies and URLs to restrict access to the distribution.
- D. Enable automatic compression of objects in the Cache Behavior Settings.
- E. Increase the CloudFront time to live (TTL) settings in the Cache Behavior Settings.

Answer: AE

Explanation:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cache-hit-ratio.html#cache-hit-ratio-ht>

NEW QUESTION 150

- (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 152

- (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 1AM credential
- B. Change the support plan.
- C. Sign in to the new account by using root user credential
- 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

NEW QUESTION 154

- (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 157

- (Exam Topic 1)

A SysOps administrator receives an alert from Amazon GuardDuty about suspicious network activity on an Amazon EC2 instance. The GuardDuty finding lists a new external IP address as a traffic destination. The SysOps administrator does not recognize the external IP address. The SysOps administrator must block traffic to the external IP address that GuardDuty identified.

Which solution will meet this requirement?

- A. Create a new security group to block traffic to the external IP address
- B. Assign the new security group to the EC2 instance.
- C. Use VPC flow logs with Amazon Athena to block traffic to the external IP address.
- D. Create a network ACL
- E. Add an outbound deny rule for traffic to the external IP address.
- F. Create a new security group to block traffic to the external IP address
- G. Assign the new security group to the entire VPC.

Answer: C

Explanation:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

NEW QUESTION 160

- (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 164

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

AWS-SysOps Practice Exam Features:

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

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