

SOA-C02 Dumps

AWS Certified SysOps Administrator - Associate (SOA-C02)

<https://www.certleader.com/SOA-C02-dumps.html>



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 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 3

- (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 4

- (Exam Topic 1)

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

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

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

Answer: D

NEW QUESTION 5

- (Exam Topic 1)

A company website contains a web tier and a database tier on AWS. The web tier consists of Amazon EC2 instances that run in an Auto Scaling group across two Availability Zones. The database tier runs on an Amazon RDS for MySQL Multi-AZ DB instance. The database subnet network ACLs are restricted to only the web subnets that need access to the database. The web subnets use the default network ACL with the default rules.

The company's operations team has added a third subnet to the Auto Scaling group configuration. After an Auto Scaling event occurs, some users report that they intermittently receive an error message. The error message states that the server cannot connect to the database. The operations team has confirmed that the route tables are correct and that the required ports are open on all security groups.

Which combination of actions should a SysOps administrator take so that the web servers can communicate with the DB instance? (Select TWO.)

- A. On the default AC

- B. create inbound Allow rules of type TCP with the ephemeral port range and the source as the database subnets.
- C. On the default ACL, create outbound Allow rules of type MySQL/Aurora (3306). Specify the destinations as the database subnets.
- D. On the network ACLs for the database subnets, create an inbound Allow rule of type MySQL/Aurora (3306). Specify the source as the third web subnet.
- E. On the network ACLs for the database subnets, create an outbound Allow rule of type TCP with the ephemeral port range and the destination as the third web subnet.
- F. On the network ACLs for the database subnets, create an outbound Allow rule of type MySQL/Aurora (3306). Specify the destination as the third web subnet.

Answer: CD

NEW QUESTION 6

- (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 domain
- 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 VPC
- H. Create a security group that allows inbound traffic from the branch office CIDR blocks.

Answer: B

NEW QUESTION 7

- (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 Add an outbound deny rule for traffic to the external IP address
- E. Create a new security group to block traffic to the external IP address Assign the new security group to the entire VPC

Answer: A

NEW QUESTION 8

- (Exam Topic 1)

A SysOps administrator needs to create alerts that are based on the read and write metrics of Amazon Elastic Block Store (Amazon EBS) volumes that are attached to an Amazon EC2 instance. The SysOps administrator creates and enables Amazon CloudWatch alarms for the DiskReadBytes metric and the DiskWriteBytes metric.

A custom monitoring tool that is installed on the EC2 instance with the same alarm configuration indicates that the volume metrics have exceeded the threshold. However, the CloudWatch alarms were not in ALARM state.

Which action will ensure that the CloudWatch alarms function correctly?

- A. Install and configure the CloudWatch agent on the EC2 instance to capture the desired metrics.
- B. Install and configure AWS Systems Manager Agent on the EC2 instance to capture the desired metrics.
- C. Reconfigure the CloudWatch alarms to use the VolumeReadBytes metric and the VolumeWriteBytes metric for the EBS volumes.
- D. Reconfigure the CloudWatch alarms to use the VolumeReadBytes metric and the VolumeWriteBytes metric for the EC2 instance.

Answer: A

NEW QUESTION 9

- (Exam Topic 1)

A company needs to implement a managed file system to host Windows file shares for users on premises. Resources in the AWS Cloud also need access to the data on these file shares. A SysOps administrator needs to present the user file shares on premises and make the user file shares available on AWS with minimum latency.

What should the SysOps administrator do to meet these requirements?

- A. Set up an Amazon S3 File Gateway.
- B. Set up an AWS Direct Connect connection.
- C. Use AWS DataSync to automate data transfers between the existing file servers and AWS.
- D. Set up an Amazon FSx File Gateway.

Answer: D

Explanation:

Amazon FSx provides a fully managed file system that is optimized for Windows-based workloads and can be used to create file shares that can be accessed both on premises and in the AWS Cloud. The file shares that are created in Amazon FSx are highly available and can be accessed with low latency. Additionally, Amazon FSx supports Windows-based authentication, making it easy to integrate with existing Windows user accounts.

References:

[1] <https://aws.amazon.com/fsx/>

[2] <https://aws.amazon.com/storage/file-storage/>

[3] <https://docs.aws.a>

NEW QUESTION 10

- (Exam Topic 1)

A company wants to build a solution for its business-critical Amazon RDS for MySQL database. The database requires high availability across different geographic locations. A SysOps administrator must build a solution to handle a disaster recovery (DR) scenario with the lowest recovery time objective (RTO) and recovery point objective (RPO).

Which solution meets these requirements?

- A. Create automated snapshots of the database on a schedule.
- B. Copy the snapshots to the DR Region.
- C. Create a cross-Region read replica for the database.
- D. Create a Multi-AZ read replica for the database.
- E. Schedule AWS Lambda functions to create snapshots of the source database and to copy the snapshots to a DR Region.

Answer: B

NEW QUESTION 10

- (Exam Topic 1)

A company wants to create an automated solution for all accounts managed by AWS Organizations to detect any security groups that have 0.0.0.0/0 as the source address for inbound traffic. The company also wants to automatically remediate any noncompliant security groups by restricting access to a specific CIDR block that corresponds with the company's intranet.

- A. Create an AWS Config rule to detect noncompliant security groups.
- B. Set up automatic remediation to change the 0.0.0.0/0 source address to the approved CIDR block.
- C. Create an IAM policy to deny the creation of security groups that have 0.0.0.0/0 as the source address. Attach this IAM policy to every user in the company.
- D. Create an AWS Lambda function to inspect new and existing security groups. Check for a noncompliant 0.0.0.0/0 source address and change the source address to the approved CIDR block.
- E. Create a service control policy (SCP) for the organizational unit (OU) to deny the creation of security groups that have the 0.0.0.0/0 source address.
- F. Set up automatic remediation to change the 0.0.0.0/0 source address to the approved CIDR block.

Answer: A

NEW QUESTION 14

- (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 Operations.
- 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 tags.
- 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 18

- (Exam Topic 1)

A company with multiple AWS accounts needs to obtain recommendations for AWS Lambda functions and identify optimal resource configurations for each Lambda function. How should a SysOps administrator provide these recommendations?

- A. Create an AWS Serverless Application Repository and export the Lambda function recommendations.
- B. Enable AWS Compute Optimizer and export the Lambda function recommendations.
- C. Enable all features of AWS Organization and export the recommendations from AWS CloudTrail Insights.
- D. Run AWS Trusted Advisor and export the Lambda function recommendations.

Answer: B

NEW QUESTION 23

- (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 25

- (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 26

- (Exam Topic 1)

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 31

- (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 33

- (Exam Topic 1)

An organization created an Amazon Elastic File System (Amazon EFS) volume with a file system ID of `fs-85ba4Kc`, and it is actively used by 10 Amazon EC2 hosts. The organization has become concerned that the file system is not encrypted. How can this be resolved?

- A. Enable encryption on each host's connection to the Amazon EFS volume. Each connection must be recreated for encryption to take effect.
- B. Enable encryption on the existing EFS volume by using the AWS Command Line Interface.
- C. Enable encryption on each host's local drive. Restart each host to encrypt the drive.
- D. Enable encryption on a newly created volume and copy all data from the original volume. Reconnect each host to the new volume.

Answer: D

Explanation:

<https://docs.aws.amazon.com/efs/latest/ug/encryption.html>

Amazon EFS supports two forms of encryption for file systems, encryption of data in transit and encryption at rest. You can enable encryption of data at rest when creating an Amazon EFS file system. You can enable encryption of data in transit when you mount the file system.

NEW QUESTION 34

- (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 35

- (Exam Topic 1)

A SysOps administrator is unable to launch Amazon EC2 instances into a VPC because there are no available private IPv4 addresses in the VPC. Which combination of actions must the SysOps administrator take to launch the instances? (Select TWO.)

- A. Associate a secondary IPv4 CIDR block with the VPC
- B. Associate a primary IPv6 CIDR block with the VPC
- C. Create a new subnet for the VPC
- D. Modify the CIDR block of the VPC
- E. Modify the CIDR block of the subnet that is associated with the instances

Answer: AD

NEW QUESTION 38

- (Exam Topic 1)

A company has a stateless application that is hosted on a fleet of 10 Amazon EC2 On-Demand Instances in an Auto Scaling group. A minimum of 6 instances are needed to meet service requirements.

Which action will maintain uptime for the application MOST cost-effectively?

- A. Use a Spot Fleet with an On-Demand capacity of 6 instances.
- B. Update the Auto Scaling group with a minimum of 6 On-Demand Instances and a maximum of 10 On-Demand Instances.
- C. Update the Auto Scaling group with a minimum of 1 On-Demand Instance and a maximum of 6 On-Demand Instances.
- D. Use a Spot Fleet with a target capacity of 6 instances.

Answer: A

NEW QUESTION 39

- (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 43

- (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 that if the process stalls, the entire stack will 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 45

- (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 49

- (Exam Topic 1)

A company has mandated the use of multi-factor authentication (MFA) for all IAM users, and requires users to make all API calls using the CLI. However, users are not prompted to enter MFA tokens, and are able to run CLI commands without MFA. In an attempt to enforce MFA, the company attached an IAM policy to all users that denies API calls that have not been authenticated with MFA.

What additional step must be taken to ensure that API calls are authenticated using MFA?

- A. Enable MFA on IAM roles, and require IAM users to use role credentials to sign API calls.
- B. Ask the IAM users to log into the AWS Management Console with MFA before making API calls using the CLI.
- C. Restrict the IAM users to use of the console, as MFA is not supported for CLI use.
- D. Require users to use temporary credentials from the get-session token command to sign API calls.

Answer: D

NEW QUESTION 53

- (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 58

- (Exam Topic 1)

A company's SysOps administrator has created an Amazon EC2 instance with custom software that will be used as a template for all new EC2 instances across multiple AWS accounts. The Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the EC2 instance are encrypted with AWS managed keys. The SysOps administrator creates an Amazon Machine Image (AMI) of the custom EC2 instance and plans to share the AMI with the company's other AWS accounts. The company requires that all AMIs are encrypted with AWS Key Management Service (AWS KMS) keys and that only authorized AWS accounts can access the shared AMIs.

Which solution will securely share the AMI with the other AWS accounts?

- A. In the account where the AMI was created, create a customer master key (CMK). Modify the key policy to provide kms:DescribeKey, kms:ReEncrypt, kms:CreateGrant, and kms:Decrypt permissions to the AWS accounts that the AMI will be shared with
- B. Modify the AMI permissions to specify the AWS account numbers that the AMI will be shared with.
- C. In the account where the AMI was created, create a customer master key (CMK). Modify the key policy to provide kms:DescribeKey, kms:ReEncrypt*, kms:CreateGrant, and kms:Decrypt permissions to the AWS accounts that the AMI will be shared with
- D. Create a copy of the AMI
- E. and specify the CM
- F. Modify the permissions on the copied AMI to specify the AWS account numbers that the AMI will be shared with.
- G. In the account where the AMI was created, create a customer master key (CMK). Modify the key policy to provide kms:DescribeKey, kms:ReEncrypt, kms:CreateGrant, and kms:Decrypt permissions to the AWS accounts that the AMI will be shared with
- H. Create a copy of the AMI
- I. and specify the CM
- J. Modify the permissions on the copied AMI to make it public.
- K. In the account where the AMI was created, modify the key policy of the AWS managed key to provide kms:DescribeKey
- L. kms:ReEncrypt, kms:CreateGrant, and kms:Decrypt permissions to the AWS accounts that the AMI will be shared with
- M. Modify the AMI permissions to specify the AWS account numbers that the AMI will be shared with.

Answer: B

Explanation:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sharingamis-explicit.html>

NEW QUESTION 60

- (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 65

- (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 70

- (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 72

- (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 75

- (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 78

- (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 80

- (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 82

- (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 83

- (Exam Topic 1)

A SysOps administrator is attempting to download patches from the internet into an instance in a private subnet. An internet gateway exists for the VPC, and a NAT gateway has been deployed on the public subnet; however, the instance has no internet connectivity. The resources deployed into the private subnet must be inaccessible directly from the public internet.

Public Subnet (10.0.1.0/24) Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	IGW

Private Subnet (10.0.2.0/24) Route Table

Destination	Target
10.0.0.0/16	local

What should be added to the private subnet's route table in order to address this issue, given the information provided?

- A. 0.0.0.0/0 IGW
- B. 0.0.0.0/0 NAT
- C. 10.0.1.0/24 IGW
- D. 10.0.1.0/24 NAT

Answer: B

NEW QUESTION 88

- (Exam Topic 1)

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

How should the SysOps administrator implement this solution?

- A. Create an AWS Step Functions workflow to identify IAM users that have not been active for 90 days. Run an AWS Lambda function when a scheduled Amazon

EventBridge (Amazon CloudWatch Events) rule is invoked to automatically remove the AWS access keys and passwords for these IAM users

B. Configure an AWS Config rule to identify IAM users that have not been active for 90 days Set up an automatic weekly batch process on an Amazon EC2 instance to disable the AWS access keys and passwords for these IAM users

C. Develop and run a Python script on an Amazon EC2 instance to programmatically identify IAM users that have not been active for 90 days Automatically delete these IAM users

D. Set up an AWS Config managed rule to identify IAM users that have not been active for 90 days Set up an AWS Systems Manager automation runbook to disable the AWS access keys for these IAM users

Answer: D

NEW QUESTION 90

- (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 95

- (Exam Topic 1)

A SysOps administrator has enabled AWS CloudTrail in an AWS account. If CloudTrail is disabled, it must be re-enabled immediately. What should the SysOps administrator do to meet these requirements WITHOUT writing custom code?

- A. Add the AWS account to AWS Organization
- B. Enable CloudTrail in the management account.
- C. Create an AWS Config rule that is invoked when CloudTrail configuration change
- D. Apply the AWS-ConfigureCloudTrailLogging automatic remediation action.
- E. Create an AWS Config rule that is invoked when CloudTrail configuration change
- F. Configure the rule to invoke an AWS Lambda function to enable CloudTrail.
- G. Create an Amazon EventBridge (Amazon CloudWatch Events) hourly rule with a schedule pattern to run an AWS Systems Manager Automation document to enable CloudTrail.

Answer: D

NEW QUESTION 96

- (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 100

- (Exam Topic 1)

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

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

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

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

Answer: CD

NEW QUESTION 101

- (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 created with 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 102

- (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 105

- (Exam Topic 1)

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 108

- (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 110

- (Exam Topic 1)

A company needs to automatically monitor an AWS account for potential unauthorized AWS Management Console logins from multiple geographic locations. Which solution will meet this requirement?

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

Answer: D

NEW QUESTION 113

- (Exam Topic 1)

A data storage company provides a service that gives users the ability to upload and download files as needed. The files are stored in Amazon S3 Standard and must be immediately retrievable for 1 year. Users access files frequently during the first 30 days after the files are stored. Users rarely access files after 30 days. The company's SysOps administrator must use S3 Lifecycle policies to implement a solution that maintains object availability and minimizes cost.

Which solution will meet these requirements?

- A. Move objects to S3 Glacier after 30 days.
- B. Move objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.
- C. Move objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
- D. Move objects to S3 Standard-Infrequent Access (S3 Standard-IA) immediately.

Answer: C

Explanation:

<https://aws.amazon.com/s3/storage-classes/>

NEW QUESTION 118

- (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 119

- (Exam Topic 1)

A SysOps administrator is required to monitor free space on Amazon EBS volumes attached to Microsoft Windows-based Amazon EC2 instances within a company's account. The administrator must be alerted to potential issues.

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

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

Answer: C

NEW QUESTION 121

- (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 124

- (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 126

- (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 130

- (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 SecretsManager.
- 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 133

- (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 136

- (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. AWS Config
- D. AWS Systems Manager

Answer: C

NEW QUESTION 137

- (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 139

- (Exam Topic 1)

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

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

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

Answer: B

NEW QUESTION 140

- (Exam Topic 1)

A company hosts a web portal on Amazon EC2 instances. The web portal uses an Elastic Load Balancer (ELB) and Amazon Route 53 for its public DNS service. The ELB and the EC2 instances are deployed by way of a single AWS CloudFormation stack in the us-east-1 Region. The web portal must be highly available across multiple Regions.

Which configuration will meet these requirements?

- A. Deploy a copy of the stack in the us-west-2 Region
- B. Create a single start of authority (SOA) record in Route 53 that includes the IP address from each ELB
- C. Configure the SOA record with health check
- D. Use the ELB in us-east-1 as the primary record and the ELB in us-west-2 as the secondary record.
- E. Deploy a copy of the stack in the us-west-2 Region
- F. Create an additional A record in Route 53 that includes the ELB in us-west-2 as an alias target
- G. Configure the A records with a failover routing policy and health check
- H. Use the ELB in us-east-1 as the primary record and the ELB in us-west-2 as the secondary record.
- I. Deploy a new group of EC2 instances in the us-west-2 Region
- J. Associate the new EC2 instances with the existing ELB, and configure load balancer health checks on all EC2 instances
- K. Configure the ELB to update Route 53 when EC2 instances in us-west-2 fail health checks.
- L. Deploy a new group of EC2 instances in the us-west-2 Region
- M. Configure EC2 health checks on all EC2 instances in each Region
- N. Configure a peering connection between the VPC
- O. Use the VPC in us-east-1 as the primary record and the VPC in us-west-2 as the secondary record.

Answer: B

Explanation:

When you create a hosted zone, Route 53 automatically creates a name server (NS) record and a start of authority (SOA) record for the zone.

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/migrate-dns-domain-in-use.html#migrate-dns-crea>

https://en.wikipedia.org/wiki/SOA_record

NEW QUESTION 141

- (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 145

- (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 146

- (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 148

- (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 ALB.
- E. Choose a failover routing policy.
- F. Set Evaluate Target Health to Yes.
- G. Configure Elastic Load Balancing (ELB) health checks for the Auto Scaling group.
- H. Add a target group to the ALB in the primary Region.
- I. Include the EC2 instances in the secondary Region as targets.
- J. Configure EC2 health checks for the Auto Scaling group.
- K. Add a target group to the ALB in the primary Region.
- L. Include the EC2 instances in the secondary Region as targets.

Answer: A

NEW QUESTION 149

- (Exam Topic 1)

A company has a compliance requirement that no security groups can allow SSH ports to be open to all IP addresses. A SysOps administrator must implement a solution that will notify the company's SysOps team when a security group rule violates this requirement. The solution also must remediate the security group rule automatically.

Which solution will meet these requirements?

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function when a security group changes.
- B. Configure the Lambda function to evaluate the security group for compliance, remove all inbound security group rules on all ports, and notify the SysOps team if the security group is noncompliant.
- C. Create an AWS CloudTrail metric filter for security group changes.
- D. Create an Amazon CloudWatch alarm to notify the SysOps team through an Amazon Simple Notification Service (Amazon SNS) topic when the metric is greater than 0. Subscribe an AWS Lambda function to the SNS topic to remediate the security group rule by removing the rule.
- E. Activate the AWS Config restricted-ssh managed rule.
- F. Add automatic remediation to the AWS Config rule by using the AWS Systems Manager Automation AWS-DisablePublicAccessForSecurityGroup runbook.
- G. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to notify the SysOps team when the rule is noncompliant.
- H. Create an AWS CloudTrail metric filter for security group changes.
- I. Create an Amazon CloudWatch alarm for when the metric is greater than 0. Add an AWS Systems Manager action to the CloudWatch alarm to suspend the security group by using the Systems Manager Automation AWS-DisablePublicAccessForSecurityGroup runbook when the alarm is in ALARM state.
- J. Add an Amazon Simple Notification Service (Amazon SNS) topic as a second target to notify the SysOps team.

Answer: C

NEW QUESTION 153

- (Exam Topic 1)

A SysOps administrator is configuring AWS Client VPN to connect users on a corporate network to AWS resources that are running in a VPC. According to compliance requirements, only traffic that is destined for the VPC can travel across the VPN tunnel. How should the SysOps administrator configure Client VPN to meet these requirements?

- A. Associate the Client VPN endpoint with a private subnet that has an internet route through a NAT gateway.
- B. On the Client VPN endpoint, turn on the split-tunnel option.
- C. On the Client VPN endpoint, specify DNS server IP addresses.
- D. Select a private certificate to use as the identity certificate for the VPN client.

Answer: C

NEW QUESTION 157

- (Exam Topic 1)

A company's SysOps administrator must ensure that all Amazon EC2 Windows instances that are launched in an AWS account have a third-party agent installed. The third-party agent has an MSI package. The company uses AWS Systems Manager for patching, and the Windows instances are tagged appropriately. The third-party agent requires periodic updates as new versions are released. The SysOps administrator must deploy these updates automatically. Which combination of steps will meet these requirements with the LEAST operational effort? (Select TWO.) Create a Systems Manager Distributor package for the third-party agent.

- A. Make sure that Systems Manager Inventory is configured
- B. If Systems Manager Inventory is not configured, set up a new inventory for instances that is based on the appropriate tag value for Windows.
- C. Create a Systems Manager State Manager association to run the AWS-RunRemoteScript document. Populate the details of the third-party agent package
- D. Specify instance tags based on the appropriate tag value for Windows with a schedule of 1 day
- E. Create a Systems Manager State Manager association to run the AWS-ConfigureAWSPackage document
- F. Populate the details of the third-party agent package
- G. Specify instance tags based on the appropriate tag value for Windows with a schedule of 1 day
- H. Create a Systems Manager OpsItem with the tag value for Windows. Attach the Systems Manager Distributor package to the OpsItem
- I. Create a maintenance window that is specific to the package deployment. Configure the maintenance window to cover 24 hours a day.

Answer: AD

Explanation:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/distributor-working-with-packages-deploy.html>

NEW QUESTION 159

- (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 a single AWS Region.

Answer: D

Explanation:

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

NEW QUESTION 162

- (Exam Topic 1)

A compliance requirement 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 163

- (Exam Topic 1)

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

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

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

Answer: B

NEW QUESTION 168

- (Exam Topic 1)

An Amazon S3 Inventory report reveals that more than 1 million objects in an S3 bucket are not encrypted. These objects must be encrypted, and all future objects must be encrypted at the time they are written.

Which combination of actions should a SysOps administrator take to meet these requirements? (Select TWO.)

- A. Create an AWS Config rule that runs evaluations against configuration changes to the S3 bucket. When an unencrypted object is found, run an AWS Systems

Manager Automation document to encrypt the object in place

B. Edit the properties of the S3 bucket to enable default server-side encryption

C. Filter the S3 Inventory report by using S3 Select to find all objects that are not encrypted Create an S3 Batch Operations job to copy each object in place with encryption enabled

D. Filter the S3 Inventory report by using S3 Select to find all objects that are not encrypted Send each object name as a message to an Amazon Simple Queue Service (Amazon SQS) queue Use the SQS queue to invoke an AWS Lambda function to tag each object with a key of "Encryption" and a value of "SSE-KMS"

E. Use S3 Event Notifications to invoke an AWS Lambda function on all new object-created events for the S3 bucket Configure the Lambda function to check whether the object is encrypted and to run an AWS Systems Manager Automation document to encrypt the object in place when an unencrypted object is found

Answer: BC

Explanation:

<https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/>

NEW QUESTION 170

- (Exam Topic 1)

A SysOps administrator is using Amazon EC2 instances to host an application. The SysOps administrator needs to grant permissions for the application to access an Amazon DynamoDB table.

Which solution will meet this requirement?

A. Create access keys to access the DynamoDB table

B. Assign the access keys to the EC2 instance profile.

C. Create an EC2 key pair to access the DynamoDB table

D. Assign the key pair to the EC2 instance profile.

E. Create an IAM user to access the DynamoDB table

F. Assign the IAM user to the EC2 instance profile.

G. Create an IAM role to access the DynamoDB table

H. Assign the IAM role to the EC2 instance profile.

Answer: D

NEW QUESTION 171

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SOA-C02 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SOA-C02-dumps.html>