Free Questions for SOA-C02 by braindumpscollection

Shared by Colon on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

update an existing AWS CloudFormation stack. If needed, a copy 0t the CloudFormation template is available in an Amazon SB bucket named cloudformation-bucket

1. Use the us-east-2 Region for all resources.

2. Unless specified below, use the default configuration settings.

3. update the Amazon EQ instance named Devinstance by making the following changes to the stack named 1700182:

a) Change the EC2 instance type to us-east-t2.nano.

b) Allow SSH to connect to the EC2 instance from the IP address range

192.168.100.0/30.

c) Replace the instance profile IAM role with IamRoleB.

4. Deploy the changes by updating the stack using the CFServiceR01e role.

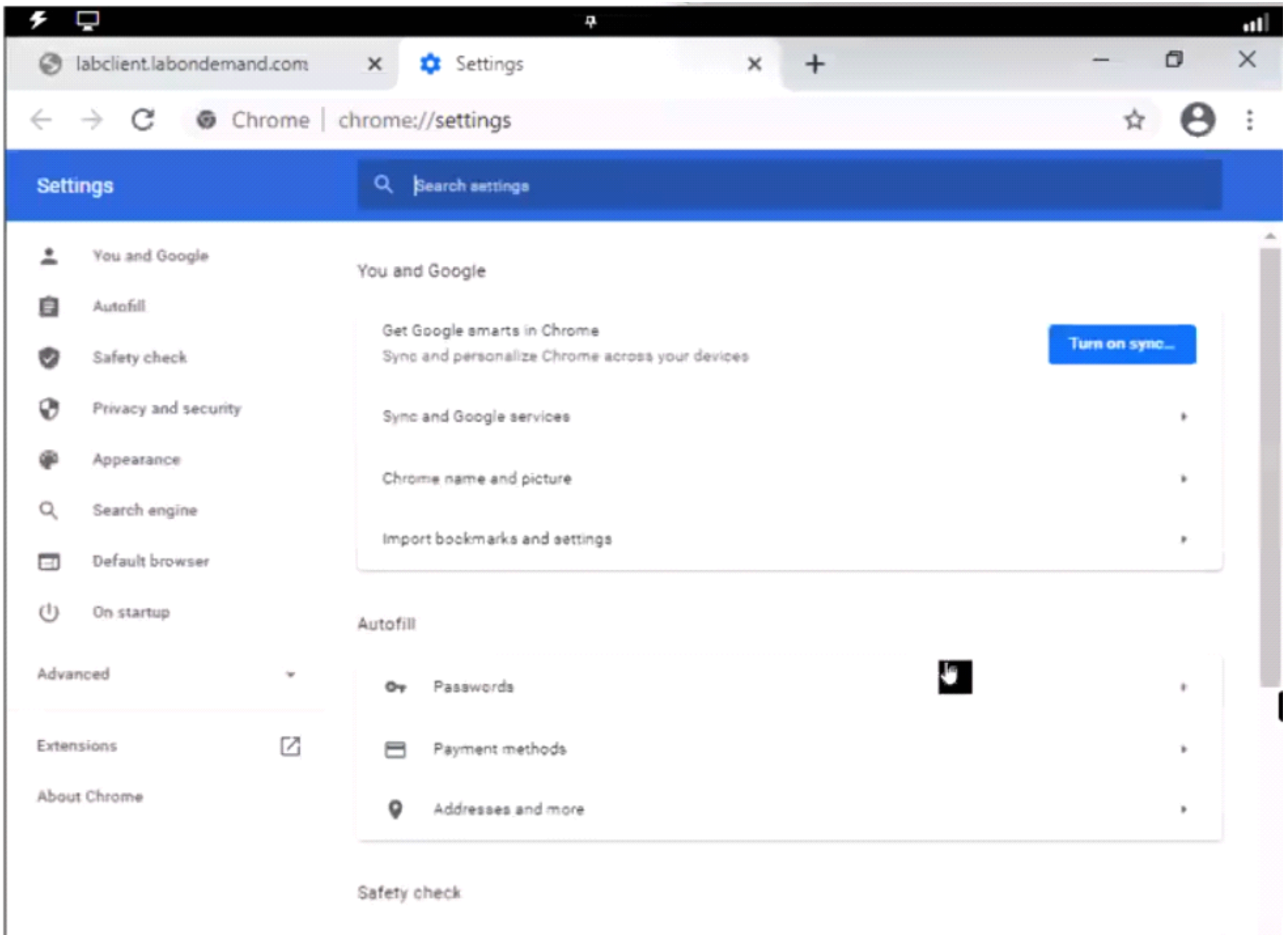
5. Edit the stack options to prevent accidental deletion.

6. Using the output from the stack, enter the value of the ProdInstanceId in the text box below:

Options:

A- Explanation:

Solution as given below.


labclient.labondemand.com
Settings
Chrome | chrome://settings
Settings
Search settings
You and Google
Autofill
Safety check
Privacy and security
Appearance
Search engine
Default browser
On startup
Advanced
Extensions
About Chrome
You and Google
Get Google smarts in Chrome
Sync and personalize Chrome across your devices
Turn on sync...
Sync and Google services
Chrome name and picture
Import bookmarks and settings
Autofill
Passwords
Payment methods
Addresses and more
Safety check

Answer:

A

Question 2

Question Type: MultipleChoice

A SysOps administrator receives an alert from Amazon GuardDuty about suspicious network activity on an Amazon FC2 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?

Options:

A- Create a new security group to block traffic to the external IP address. Assign the new security group to the EC2 instance

B- Use VPC flow logs with Amazon Athena to block traffic to the external IP address

C- Create a network ACL Add an outbound deny rule tor traffic to the external IP address

D- Create a new security group to block traffic to the external IP address Assign the new security group to the entire VPC

Answer:

A

Question 3

Question Type: MultipleChoice

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?

Options:

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-rejected

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

Question 4

Question Type: MultipleChoice

A company must ensure that any objects uploaded to an S3 bucket are encrypted.

Which of the following actions will meet this requirement? (Choose two.)

Options:

A- Implement AWS Shield to protect against unencrypted objects stored in S3 buckets.

B- Implement Object access control list (ACL) to deny unencrypted objects from being uploaded to the S3 bucket.

C- Implement Amazon S3 default encryption to make sure that any object being uploaded is encrypted before it is stored.

D- Implement Amazon Inspector to inspect objects uploaded to the S3 bucket to make sure that they are encrypted.

E- Implement S3 bucket policies to deny unencrypted objects from being uploaded to the buckets.

Answer:

C, E

Explanation:

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

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

https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/

How to Prevent Uploads of Unencrypted Objects to Amazon S3#

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

Question 5

Question Type: MultipleChoice

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

CloudFormation stack, it fails to deploy.

What is likely to be the problem?

Options:

A- The Amazon Machine image used is not available in that region.

B- The AWS CloudFormation template needs to be updated to the latest version.

C- The VPC configuration parameters have changed and must be updated in the template.

D- The account has reached the default limit for VPCs allowed.

Answer:

D

Question 6

Question Type: MultipleChoice

A SysOps administrator is deploying a test site running on Amazon EC2 instances. The application requires both incoming and outgoing connectivity to the internet.

Which combination of steps are required to provide internet connectivity to the EC2 instances? (Choose two.)

Options:

A- Add a NAT gateway to a public subnet.

B- Attach a private address to the elastic network interface on the EC2 instance.

C- Attach an Elastic IP address to the internet gateway.

D- Add an entry to the route table for the subnet that points to an internet gateway.

E- Create an internet gateway and attach it to a VPC.

Answer:

D, E

Explanation:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

Question 7

Question Type: **MultipleChoice**

A SysOps administrator is maintaining a web application using an Amazon CloudFront web distribution, an Application Load Balancer (ALB), Amazon RDS, and

Amazon EC2 in a VPC. All services have logging enabled. The administrator needs to investigate HTTP Layer 7 status codes from the web application.

Which log sources contain the status codes? (Choose two.)

Options:

A- VPC Flow Logs

B- AWS CloudTrail logs

C- ALB access logs

D- CloudFront access logs

E- RDS logs

Answer:

C, D

Explanation:

'C' because Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html

'D' because 'you can configure CloudFront to create log files that contain detailed information about every user request that CloudFront receives'

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html

Question 8

Question Type: MultipleChoice

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

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

Options:

A- Configure the CloudFront distribution behavior to forward the User-Agent header.

B- Configure the CloudFront distribution origin settings. Add a User-Agent header to the list of origin custom headers.

C- Enable IPv6 on the ALB. Update the CloudFront distribution origin settings to use the dualstack endpoint.

D- Enable IPv6 on the CloudFront distribution. Update the Route 53 record to use the dualstack endpoint.

Answer:

A

Explanation:

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

Question 9

Question Type: MultipleChoice

A company wants to be alerted through email when IAM CreateUser API calls are made within its AWS account.

Which combination of actions should a SysOps administrator take to meet this requirement? (Choose two.)

Options:

A- Create an Amazon EventBridge (Amazon CloudWatch Events) rule with AWS CloudTrail as the event source and IAM CreateUser as the specific API call for the event pattern.

B- Create an Amazon EventBridge (Amazon CloudWatch Events) rule with Amazon CloudSearch as the event source and IAM CreateUser as the specific API call for the event pattern.

C- Create an Amazon EventBridge (Amazon CloudWatch Events) rule with AWS IAM Access Analyzer as the event source and IAM CreateUser as the specific API call for the event pattern.

D- Use an Amazon Simple Notification Service (Amazon SNS) topic as an event target with an email subscription.

E- Use an Amazon Simple Email Service (Amazon SES) notification as an event target with an email subscription.

Answer:

A, D

Explanation:

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

Question 10

Question Type: MultipleChoice

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?

Options:

A- Create a CNAME record. Enter static.cloudfront.net as the record name. Enter the CloudFront distribution's public IP address as the value.

B- Create a CNAME record. Enter static.example.com as the record name. Enter the CloudFront distribution's private IP address as the value.

C- Create an A record. Enter static.cloudfront.net as the record name. Enter the CloudFront distribution's ID as an alias target.

D- Create an A record. Enter static.example.com as the record name. 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

Question 11

Question Type: MultipleChoice

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?

Options:

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/

Question 12

Question Type: MultipleChoice

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?

Options:

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/