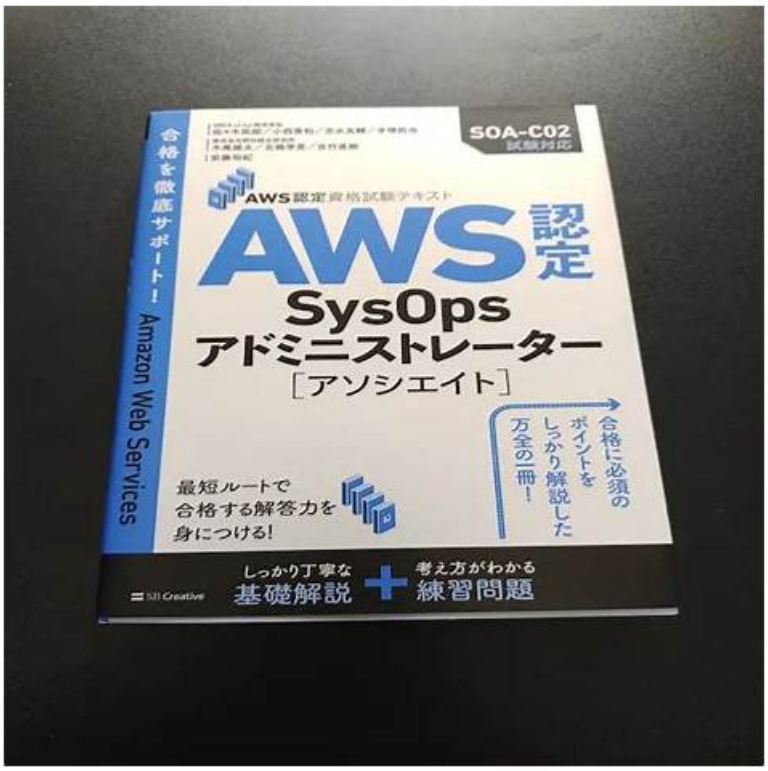
SOA-C02最新問題 & SOA-C02復習問題集



P.S. CertJukenがGoogle Driveで共有している無料かつ新しいSOA-C02ダンプ：https://drive.google.com/open?id=1K-qvu0yRg28eBo8TSST7mwES7farPZZc

CertJukenのAmazonのSOA-C02試験トレーニング資料は正確性が高くて、カバー率も広いです。それは君の文化知識を増強でき、君の実践水準も増強でき、君をIT業種での本当のエリートになって、君に他人に羨ましい給料のある仕事をもたらすことができます。うちのAmazonのSOA-C02試験トレーニング資料を購入する前に、CertJukenのサイトで、一部分のフリーな試験問題と解答をダンロードでき、試用してみます。

Amazon SOA-C02試験は、AWSで働くITプロフェッショナルにとって有価値な認定資格です。この試験では、AWSアーキテクチャとサービスの理解、およびAWS上でのアプリケーションの展開と管理におけるベストプラクティスの適用能力が評価されます。試験に合格することは、候補者がAWSシステムの管理と運用における専門知識を持っていることを証明し、3年間有効です。試験の準備には、AWS Certified SysOps Administrator - Associateトレーニングコースを受講することを推奨します。

SOA-C02試験は、65の多肢選択および多肢回答の問題から構成されるコンピューターベースの試験です。候補者は130分以内に試験を完了する必要があり、合格点は1000点中720点です。試験は英語、日本語、および簡体字中国語で利用可能です。

>> SOA-C02最新問題 <<

試験の準備方法-正確的なSOA-C02最新問題試験-認定するSOA-C02復習問題集

社会と経済の発展につれて、多くの人はIT技術を勉強します。なぜならば、IT職員にとって、AmazonのSOA-C02資格証明書があるのは肝心な指標であると言えます。自分の能力を証明するために、SOA-C02試験に合格するのは不可欠なことです。弊社のSOA-C02真題を入手して、試験に合格する可能性が大きくなります。

Amazon SOA-C02 試験は、65の多肢選択と多答式問題を含んだ130分間の試験です。この試験は英語、日本語、韓国語、簡体字中国語で利用可能です。この試験はテストセンターで対面で受験することも、自宅やオフィスからオンラインで受験することもできます。オンライン監視のオプションは、一部の地域で利用可能です。

Amazon AWS Certified SysOps Administrator - Associate (SOA-C02) 認定 SOA-C02 試験問題 (Q80-Q85):

質問 # 80
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.
  Use signed cookies for restricted delivery of the content through CloudFront.
- B. Store the digital content in an Amazon S3 bucket that has public access blocked.
  Use an origin access identity (OAI) to deliver the content through CloudFront.
  Restrict S3 bucket access with signed URLs in CloudFront.
- C. Store the digital content in an Amazon S3 bucket that does not have public access blocked.
  Use signed URLs to access the S3 bucket through CloudFront.
- D. Store the digital content in an Amazon S3 bucket that has public access blocked.
  Use an origin access identity (OAI) to deliver the content through CloudFront. Enable field- level encryption.

正解：B

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

質問 # 81
A company has an initiative to reduce costs associated with Amazon EC2 and AWS Lambd a. Which action should a SysOps administrator take to meet these requirements?

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

正解：A

解説：
AWS Compute Optimizer recommends optimal AWS resources for your workloads to reduce costs and improve performance. It provides actionable recommendations to help you choose the right EC2 instances and AWS Lambda configurations.
Access AWS Compute Optimizer:
Open the AWS Compute Optimizer console at AWS Compute Optimizer Console.
Review the recommendations for your EC2 instances and AWS Lambda functions.
Implement Recommendations:
Analyze the recommendations, which might include resizing instances, changing instance types, or modifying Lambda memory settings.
Apply the recommendations to optimize your resources and reduce costs.
Reference:
AWS Compute Optimizer
Getting Started with AWS Compute Optimizer

質問 # 82
A company runs an application on Amazon EC2 instances. The EC2 instances are in an Auto Scaling group and run behind an Application Load Balancer (ALB). The application experiences errors when total requests exceed 100 requests per second. A SysOps administrator must collect information about total requests for a 2-week period to determine when requests exceeded this threshold.
What should the SysOps administrator do to collect this data?

- A. Use the ALB's RequestCount metric. Configure a time range of 2 weeks and a period of 1 minute. Examine the chart to determine peak traffic times and volumes.
- B. Create Amazon CloudWatch custom metrics on the EC2 launch configuration templates to create aggregated request

metrics across all the EC2 instances.

- C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule. Configure an EC2 event matching pattern that creates a metric that is based on EC2 requests. Display the data in a graph.
- D. Use Amazon CloudWatch metric math to generate a sum of request counts for all the EC2 instances over a 2-week period. Sort by a 1-minute interval.

正解：A

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

質問 # 83
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. Use signed URLs to access the S3 bucket through CloudFront.
- B. Store the digital content in an Amazon S3 bucket that has public access blocked. Use an origin access identity (OAI) to deliver the content through CloudFront. Enable field-level encryption.
- C. Store the digital content in an Amazon S3 bucket that does not have public access blocked. Use signed cookies for restricted delivery of the content through CloudFront.
- D. Store the digital content in an Amazon S3 bucket that has public access blocked. Use an origin access identity (OAI) to deliver the content through CloudFront. Restrict S3 bucket access with signed URLs in CloudFront.

正解：D

解説：
To deliver digital content to authorized users through CloudFront while restricting unauthorized access, you can use an origin access identity (OAI) with signed URLs.
Store Content in S3 with Public Access Blocked:
Ensure the S3 bucket has public access blocked.
Navigate to the S3 console, select the bucket, and configure the "Block Public Access" settings.
Reference:
Create an OAI for CloudFront:
In the CloudFront console, create an OAI to securely access the S3 bucket.
Associate the OAI with the CloudFront distribution.
Restrict S3 Bucket Access to the OAI:
Update the S3 bucket policy to grant access to the OAI.
Example bucket policy:
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity <OAI-ID>"
},
"Action": "s3:GetObject",
"Resource": "arn:aws:s3:::bucket-name/*"
}
]
}
Use Signed URLs for Restricted Access:
Configure CloudFront to use signed URLs to control access to the content.
This setup ensures that only authorized users can access the content through CloudFront using signed URLs, while the S3 bucket remains private and secure.

質問 # 84
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. Deploy an Amazon Cognito user pool. Configure Active Directory as an external identity provider for the user pool. Enable Amazon Cognito authentication for Kibana on Amazon ES.
- B. Establish a trust relationship with Kibana on the Active Directory server. Enable Active Directory user authentication in Kibana. Add the Active Directory server's IP address to Kibana.
- C. Configure Active Directory as an authentication provider in Amazon ES. Add the Active Directory server's domain name to Amazon ES. Configure Kibana to use Amazon ES authentication.
- D. Enable Active Directory user authentication in Kibana. Create an IP-based custom domain access policy in Amazon ES that includes the Active Directory server's IP address.

正解： A

解説：
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

質問 # 85
......

myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

2026年CertJukenの最新SOA-C02 PDFダンプおよびSOA-C02試験エンジンの無料共有：https://drive.google.com/open?id=1K-qvu0yRg28eBo8TSST7mwES7farPZZc