SAA-C03認證：AWS Certified Solutions Architect - Associate考試即時下載|更新的Amazon SAA-C03

順便提一下，可以從雲存儲中下載PDFExamDumps SAA-C03考試題庫的完整版：https://drive.google.com/open?id=1a-slBlumOIiccrY7UAl0Kz-QDBSyqFf5

PDFExamDumps是一個你可以完全相信的網站。PDFExamDumps的Amazon技術專家為了讓大家可以學到更加高效率的資料一直致力於各種SAA-C03認證考試的研究，從而開發出了更多的考試資料。只要你使用過一次PDFExamDumps的資料，你就肯定還想用第二次。因為PDFExamDumps不但給你提供最好的資料，而且為你提供最優質的服務。如果你對我們的產品有任何意見都可以隨時提出，因為我們不僅以讓廣大考生輕鬆通過SAA-C03考試為宗旨，更把為大家提供最好的服務作為我們的目標。

Amazon AWS 認證解決方案架構師 - 副（SAA-C03）考試是一個認證，驗證個人在 Amazon Web Services（AWS）平台上設計和部署可擴展，高可用性和容錯的系統的專業知識。此認證適用於具有對 AWS 服務的充分理解能力，並能設計和實施滿足業務需求的解決方案的專業人士。SAA-C03 考試考試了設計和部署安全，具有成本效益和高可用性的 AWS 服務所必須的知識和技能。

>> SAA-C03認證 <<

SAA-C03熱門考題 & 最新SAA-C03題庫資源

伴隨著 Amazon 認證，越來越多的客戶注意到 Amazon 的重要性，目前是經濟衰退的時期，找一份工作不容易，考取 Amazon 認證的證書當然是有用的，能夠幫助你穩定你的位置，增加求職的法碼。如果你正在準備 SAA-C03 考試題目和答案的電子圖書的形式或自我測試軟體，以獲得適當的知識和技能，急需通過 SAA-C03 考試，可以憑藉 PDFExamDumps 考題網最新的題庫順利通過該考試。

為了準備亞馬遜SAA-C03認證考試，候選人可以利用各種資源，包括AWS培訓課程，白皮書和練習考試。 AWS提供一系列培訓課程，包括基於課堂的培訓，虛擬講師主導的培訓以及自定進度的在線培訓，旨在幫助候選人為考試做準備。候選人還可以參加練習考試以測試他們的知識並確定需要改進的領域。

Amazon SAA-C03 認證考試是為那些希望在 Amazon Web Services (AWS) 雲上設計和部署可擴展、容錯和高可用系統的人而設計的。這個認證非常適合解決方案架構師、系統管理員和開發人員，他們希望驗證自己在 AWS 基礎架構、服務和最佳實踐方面的知識和專業能力。SAA-C03 考試是以前的 SAA-C02 認證考試的更新版本，被認為是雲計算行業中最受追捧的認證之一。

最新的 AWS Certified Solutions Architect SAA-C03 免費考試真題 (Q132-Q137):

問題 #132
A company is migrating a new application from an on-premises data center to a new VPC in the AWS Cloud.
The company has multiple AWS accounts and VPCs that share many subnets and applications.

The company wants to have fine-grained access control for the new application. The company wants to ensure that all network resources across accounts and VPCs that are granted permission to access the new application can access the application.

- A. Set up a VPC peering connection for each VPC that needs access to the new application VPC. Update route tables in each VPC to enable connectivity.
- B. Deploy a transit gateway in the account that hosts the new application. Share the transit gateway with each account that needs to connect to the application. Update route tables in the VPC that hosts the new application and in the transit gateway to enable connectivity.
- C. Use an AWS PrivateLink endpoint service to make the new application accessible to other VPCs. Control access to the application by using an endpoint policy.
- D. Use an Application Load Balancer (ALB) to expose the new application to the internet. Configure authentication and authorization processes to ensure that only specified VPCs can access the application.

答案：C

解題說明：
AWS PrivateLink is the most suitable solution for providing fine-grained access control while allowing multiple VPCs, potentially across multiple accounts, to access the new application. This approach offers the following advantages:
* Fine-grained control: Endpoint policies can restrict access to specific services or principals.
* No need for route table updates: Unlike VPC peering or transit gateways, AWS PrivateLink does not require complex route table management.
* Scalable architecture: PrivateLink scales to support traffic from multiple VPCs.
* Secure connectivity: Ensures private connectivity over the AWS network, without exposing resources to the internet.
Why Other Options Are Not Ideal:
* Option A:
* VPC peering is not scalable when connecting multiple VPCs or accounts.
* Route table management becomes complex as the number of VPCs increases.Not scalable.
* Option B:
* While transit gateways provide scalable VPC connectivity, they are not ideal for fine-grained access control.
* Transit gateways allow connectivity but do not inherently restrict access to specific applications.
Not ideal for fine-grained access control.
* Option D:
* Exposing the application through an ALB over the internet is not secure and does not align with the requirement to use private network resources.Security risk.
AWS References:
* AWS PrivateLink:AWS Documentation - PrivateLink
* AWS Networking Services Comparison:AWS Whitepaper - Networking Services

問題 #133
A disaster response team is using drones to collect images of recent storm damage. The response team's laptops lack the storage and compute capacity to transfer the images and process the data.
While the team has Amazon EC2 instances for processing and Amazon S3 buckets for storage, network connectivity is intermittent and unreliable. The images need to be processed to evaluate the damage.
What should a solutions architect recommend?

- A. Configure Amazon Data Firehose to create multiple delivery streams aimed separately at the S3 buckets for storage and the EC2 instances for processing images.
- B. Upload the images to Amazon Simple Queue Service (Amazon SQS) during intermittent connectivity to EC2 instances.
- C. Use AWS Storage Gateway pre-installed on a hardware appliance to cache the images locally for Amazon S3 to process the images when connectivity becomes available.
- D. Use AWS Snowball Edge devices to process and store the images.

答案：D

解題說明：
AWS Snowball Edge is specifically designed for use cases that involve limited or unreliable network connectivity. It enables data transfer and local compute processing at edge locations.
* It comes in two options: Snowball Edge Storage Optimized and Snowball Edge Compute Optimized.
* The Compute Optimized model allows the disaster response team to both store images locally and process data on the device using Amazon EC2-compatible compute resources.

This removes the need for constant network connectivity. After processing, the device can be shipped back to AWS, where data is uploaded to S3.
Other options fail due to:
* SQS not being suitable for large binary image data (Option B)
* Kinesis Data Firehose needing steady connectivity (Option C)
* Storage Gateway is for hybrid cloud environments with ongoing connection, not rugged field use (Option D)
# References:
* AWS Snowball Edge Overview
* Snowball Edge Use Cases

問題 #134
A company needs to ensure that an IAM group that contains database administrators can perform operations only within Amazon RDS. The company must ensure that the members of the IAM group cannot access any other AWS services.

- A. Create an IAM policy with a statement that includes the Effect "Allow" and the Action "rds:". Include a permissions boundary that has the Effect "Allow" and the Action "rds:". Attach the IAM policy to the IAM group.
- B. Create an IAM policy that includes a statement that has the Effect "Allow" and the Action "rds:". Attach the IAM policy to the IAM group.
- C. Create an IAM policy that includes a statement that has the Effect "Deny" and the NotAction "rds:". Attach the IAM policy to the IAM group.
- D. Create an IAM policy that includes two statements. Configure the first statement to have the Effect "Allow" and the Action "rds:". Configure the second statement to have the Effect "Deny" and the Action "". Attach the IAM policy to the IAM group.

答案：C

解題說明：
To enforce that IAM users can only access Amazon RDS and no other AWS services, the recommended approach is to use a Deny statement with NotAction. This ensures that all actions are denied except RDS actions. Options A and B do not fully achieve the restriction: A only allows RDS but does not explicitly deny access to other services if another policy grants access; B's explicit Deny for "*" would override all other permissions, including the intended RDS Allow, which would result in no access at all. Option D with permissions boundaries still allows other attached policies to grant access outside RDS. Therefore, C is the correct approach to enforce RDS-only access.
References:* IAM JSON Policy Elements - Effect, Action, NotAction, and Deny* AWS Well-Architected Framework - Security Pillar: Least privilege

問題 #135
A company is developing an application that will run on a production Amazon Elastic Kubernetes Service (Amazon EKS) cluster The EKS cluster has managed node groups that are provisioned with On-Demand Instances.
The company needs a dedicated EKS cluster for development work. The company will use the development cluster infrequently to test the resiliency of the application. The EKS cluster must manage all the nodes.
Which solution will meet these requirements MOST cost-effectively?

- A. Create a managed node group that contains only Spot Instances.
- B. Create two managed node groups. Provision one node group with On-Demand Instances. Provision the second node group with Spot Instances.
- C. Create a managed node group that contains only On-Demand Instances.
- D. Create an Auto Scaling group that has a launch configuration that uses Spot Instances. Configure the user data to add the nodes to the EKS cluster.

答案：A

解題說明：
Spot Instances are EC2 instances that are available at up to a 90% discount compared to On-Demand prices.
Spot Instances are suitable for stateless, fault-tolerant, and flexible workloads that can tolerate interruptions.
Spot Instances can be reclaimed by EC2 when the demand for On-Demand capacity increases, but they provide a two-minute warning before termination. EKS managed node groups automate the provisioning and lifecycle management of nodes for EKS clusters. Managed node groups can use Spot Instances to reduce costs and scale the cluster based on demand. Managed node groups also support features such as Capacity Rebalancing and Capacity Optimized allocation strategy to improve the availability

and resilience of Spot Instances. This solution will meet the requirements most cost-effectively, as it leverages the lowest-priced EC2 capacity and does not require any manual intervention.
References:
1 explains how to create and use managed node groups with EKS.
2 describes how to use Spot Instances with managed node groups.
3 provides an overview of Spot Instances and their benefits.

問題 #136
A company has a multi-tier web application. The application's internal service components are deployed on Amazon EC2 instances. The internal service components need to access third-party software as a service (SaaS) APIs that are hosted on AWS.
The company needs to provide secure and private connectivity from the application's internal services to the third-party SaaS application. The company needs to ensure that there is minimal public internet exposure.
Which solution will meet these requirements?

- A. Use AWS PrivateLink to create a private connection between the application's VPC and the third-party SaaS provider.
- B. Deploy AWS Transit Gateway to manage and route traffic between the application's VPC and the third-party SaaS provider.
- C. Implement an AWS Site-to-Site VPN to establish a secure connection with the third-party SaaS provider.
- D. Configure AWS PrivateLink to allow only outbound traffic from the VPC without enabling the third-party SaaS provider to establish a return path to the network.

答案：A

解題說明：
AWS PrivateLink enables private connectivity between VPCs and supported AWS or third-party services without exposing traffic to the public internet. It ensures secure and private communications, making it ideal for connecting internal services to SaaS applications hosted in AWS.
Reference:

問題 #137
.....

2026 PDFExamDumps最新的SAA-C03 PDF版考試題庫和SAA-C03考試問題和答案免費分享：https://drive.google.com/open?id=1a-slBlumOIiccrY7UAl0Kz-QDBSyqFf5