JON BONSO

AWS CERTIFIED

SOLUTIONS ARCHITECT PROFESSIONAL

Tutorials Dojo
Study Guide and Cheat Sheets

TABLE OF CONTENTS

INTRODUCTION

In the fast-paced IT industry today, there will always be a growing demand for certified IT Professionals that can design highly available, fault-tolerant, resilient and cost-effective solutions. Companies are spending millions of dollars to optimize the performance of their applications and scale their infrastructure globally to serve customers around the world. They need a reliable and skillful IT staff to migrate their on-premises workload to AWS, reduce their total operating costs, effectively manage complex organizational accounts globally and design new solutions to meet customer demands.

This Study Guide eBook aims to equip you with the necessary knowledge and practical skill sets needed to pass the latest version of the AWS Certified Solutions Architect – Professional exam. We included the essential concepts, exam domains, exam tips, sample questions, cheat sheets, and other relevant information about the latest AWS Certified Solutions Architect – Professional SAP-C02 exam. It begins with the presentation of the exam structure to give you an insight into the question types, exam domains, scoring scheme, and the list of benefits you'll receive once you pass the exam.

We used the official SAP-C02 exam guide for the AWS Certified Solutions Architect Professional exam to structure the contents of this guide, covering all the relevant AWS topics for every exam domain. Various AWS concepts, related AWS services, and technical implementations are covered to provide you with an idea of what to expect on the actual exam.

> **i Solutions Architect Professional Exam Notes:**
>
> Don't forget to read the boxed "**exam tips**" (like this one) scattered throughout the eBook, as these are the key concepts that you will likely encounter on your test. The last part of this guide includes a collection of articles that compares two or more similar AWS services to supplement your knowledge.

The AWS Certified Solutions Architect - Professional certification exam is a difficult test to pass; therefore, anyone who wants to take it must allocate ample time for review. The exam registration costs hundreds of dollars, which is why we spent considerable time and effort to ensure that this study guide provides you with the essential and relevant knowledge to increase your chances of passing the Solutions Architect Professional exam.

*** **Note:** This eBook is meant to be just a supplementary resource when preparing for the exam. We highly recommend working on your hands-on labs and practice exams to further expand your knowledge and improve your test taking skills.*

AWS CERTIFIED SOLUTIONS ARCHITECT PROFESSIONAL EXAM OVERVIEW

SAP-C02 Exam Details

The AWS Certified Solutions Architect – Professional (SAP-C02) exam is one of the two Professional-level certification tests of the AWS Certification program. This particular exam is meant for individuals who perform a solutions architect role in their current company/organization. The SAP-C02 exam validates the person's general IT knowledge, advanced technical skills, and experience in designing optimized AWS solutions that are based on the AWS Well-Architected Framework.

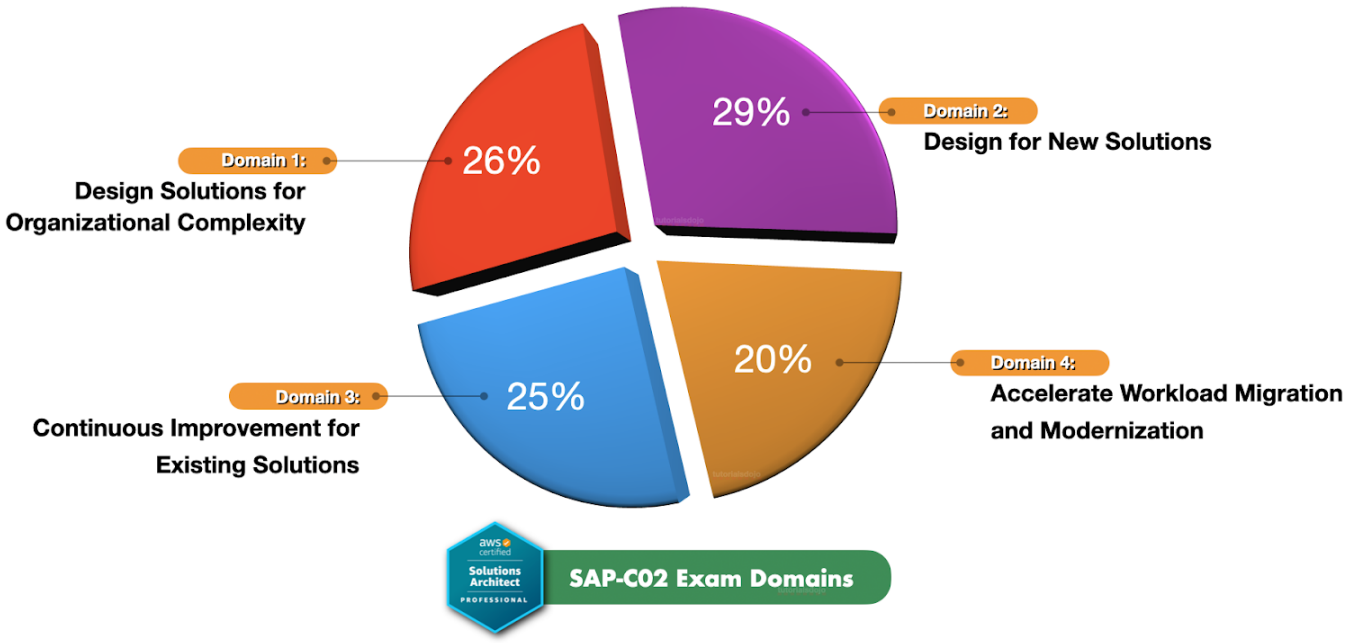
This Pro-level certification exam is composed of 75 multiple-choice or multiple-response scenario-based questions that you must complete within 180 minutes or 3 hours. The "multiple-choice" question type has one correct answer and three incorrect responses, while the "multiple response" item has two or more right responses out of five or more options. Like other AWS certification exams, you can take the SAP-C02 exam from a local testing center or online from your home.

Exam Code:	SAP-C02
Release Date:	November 2022
Prerequisites:	None
No. of Questions:	75
Score Range:	100 - 1000
Cost:	300 USD
Passing Score:	750/1000
Time Limit:	3 hours (180 minutes)
Format:	Scenario-based. Multiple choice/multiple answers.
Delivery Method:	Testing center or online proctored exam.

The AWS Certified Solutions Architect – Professional (SAP-C02) exam has no prerequisites, so you can take this exam directly. The score range is from 100 to 1000 and you need to score at least 750 to pass the test. Thus, the passing score is at 75% (750/1000) compared with just 72% for the Associate-level exams.

Exam Domains

The AWS Certified Solutions Architect Professional (SAP-C02) exam has 4 different domains, each with corresponding weight and topic coverage. The exam domains are as follows: Design Solutions for Organizational Complexity (26%), Design for New Solutions (29%), Continuous Improvement for Existing Solutions (25%) and lastly, Accelerate Workload Migration and Modernization (20%):



The list of exam domains can be found on the official Exam Guide for the AWS Certified Solutions Architect - Professional exam. Each exam domain is comprised of several task statements. A task statement is a sub-category of the exam domain that contains the necessary topics, knowledge, concepts, and skills for you to accomplish a particular task or activity in AWS.

As seen in the above pie graph, the first domain covers 26% of the overall test while the second domain covers 29%, which represents the biggest chunk of the exam. This is followed by the third and fourth domains with 25% and 20% coverage, respectively.

Let's look at each of these domains one by one.

Domain 1: Design Solutions for Organizational Complexity

The first exam domain is all about checking your knowledge in properly setting up cloud architectures for large organizations with multiple business units. You have to be knowledgeable in launching and maintaining a centralized cloud organization with multiple AWS accounts across several geographical regions using the AWS Organizations service as well the other governance and management services. This includes the skill of setting up cost-effective, resilient and reliable network connectivity for your hybrid cloud and shared AWS resources.

This is the second biggest domain in the exam with 26% percent coverage; therefore, you must allocate significant time to study the various concepts covered in this domain. It also includes the security posture of your cloud solutions to ensure that they conform with the guardrails and regulations of your organization.

The series of scenarios that you will encounter in this domain checks your know-how in doing these tasks:

- Architect network connectivity strategies.
- Prescribe security controls.
- Design reliable and resilient architectures.
- Design a multi-account AWS environment.
- Determine cost optimization and visibility strategies.

Domain 2: Design for New Solutions

The second exam domain (“Design Resilient Architectures”) is all about designing resilient architectures in AWS. It is the biggest domain in the exam, with 29% percent coverage so you must also allocate a lot of time to understand the different concepts covered in this domain.

The questions that you will encounter in this domain will challenge your knowledge in:

- Design a deployment strategy to meet business requirements.
- Design a solution to ensure business continuity.
- Determine security controls based on requirements.
- Design a strategy to meet reliability requirements.
- Design a solution to meet performance objectives.
- Determine a cost optimization strategy to meet solution goals and objectives.

Domain 3: Continuous Improvement for Existing Solutions

The third domain is all about continuously improving your existing cloud solutions in AWS. This has an exam coverage of 25 percent and revolves around improving the security, performance, reliability and overall operational excellence of your solutions. It also includes the topic of cost optimization and the skill involved to easily identify them on an existing cloud architecture. You should prepare for:

- Determine a strategy to improve overall operational excellence.
- Determine a strategy to improve security.
- Determine a strategy to improve performance.
- Determine a strategy to improve reliability
- Identify opportunities for cost optimizations.

Domain 4: Accelerate Workload Migration and Modernization

The last exam domain revolves around designing cost-optimized architectures. It comprises 20% of the exam coverage, so you have to limit the time you spend reviewing the concepts under this domain. As you might have guessed, this domain is all about the costs of your cloud architecture and the different ways to reduce operational expenditures. This domain checks if you possess the knowledge in doing following tasks:

- Select existing workloads and processes for potential migration
- Determine the optimal migration approach for existing workloads.
- Determine a new architecture for existing workloads.
- Determine opportunities for modernization and enhancements.

These are the four exam domains that you should be familiar with when you start your exam preparations. Again, the SAP-C02 exam is primarily focused on security so make sure that you focus on the “Design Secure Architectures” domain and all the related knowledge areas in its task statements.

I highly recommend that you read the official exam guide for the AWS Certified Solutions Architect Professional exam from cover to cover. Pay close attention to the topics included, and don't forget to read the Appendix section, which contains a list of related AWS services that will appear in the exam.

The Old SAP-C01 and New SAP-C02 Exam Difference

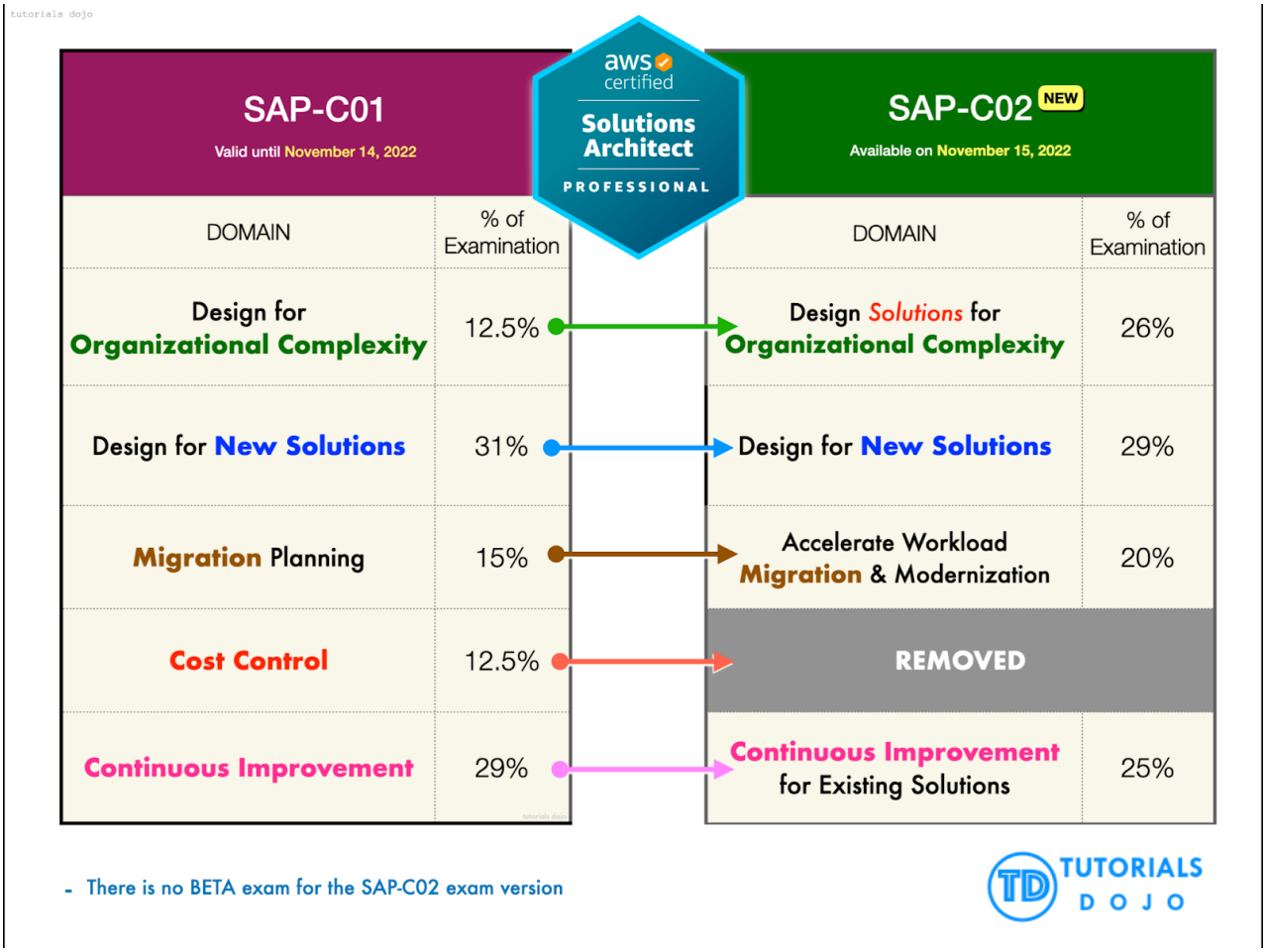
The SAP-C02 is the 3rd iteration of the AWS Certified Solutions Architect Professional exam, which was initially launched about a decade ago. The very first version of this certification test was released on May 2014 with an exam code of SAP-C00. AWS released the second version on February 2019, which is 5 years from the first one, with an exam code of SAP-C01. The third, and also the latest, exam version of the AWS Certified Solutions Architect – Professional exam has an exam code of SAP-C02 which became available on November 15, 2022.

I've already taken and passed the previous versions of this exam in the past, but this week, I took the latest exam version to ensure that our SAP-C02 reviewers here at Tutorials Dojo are still on par with the actual exam. I took the first version of this test (SAP-C00) on April 2018, which is almost 5 years from today, and then the second exam version (SAP-C01) on February 2019. I took the recently launched SAP-C02 exam version on November 2022.

It's noticeable that the length of time for the SAP-C01 version to be replaced with the new SAP-C02 is 3 years. Based on this trend, I'm assuming that the 4th iteration of this certification test will be coming in 2025, with an exam code of SAP-C03. This is just a rough estimation as it depends on the number of feature changes and brand-new services that AWS releases.

Through all these exam iterations, I would say that there were significant changes from the first SAP-C00 exam compared with the second version (SAP-C01). Back in 2018, when I took the SAP-C00 exam, the questions were long, but the number of AWS services included was not that extensive. It was when AWS released the SAP-C01 exam version where the AWS Certified Solutions Architect Professional exam topics covered a wide range of AWS services and other 3rd party systems.

The SAP-C02 still resembles the old format of the recently decommissioned SAP-C01 exam. It has a mix of long questions (with 3-4 paragraphs) and short ones (1-2 paragraphs). The same goes for the answers as well, with multiple-response questions where you have to select 2 or 3 items out of 5 or 6 options. In comparison with the SAA-C03 and other Associate-level exams, the AWS Certified Solutions Architect Professional exam has significantly more multiple-response questions than multiple-choice items.



The table above shows the difference between the SAP-C01 exam domains versus the new SAP-C02 exam. From 5 exam domains, it is now down to 4, with changes in the coverage percentage on each domain. The Design for Organizational Complexity domain was renamed to Design Solutions for Organizational Complexity, and its exam coverage was bumped up from 12.5% to 26% while the Migration Planning domain was upgraded from 15% to 20% and was also renamed to Accelerate Workload Migration & Modernization. Speaking of Modernization, expect to see a lot of containerized architectures in the exam, which involves Kubernetes, Amazon ECS, Amazon EKS, Serverless, and other related services.

You can also see here that the Cost Control domain was removed. Don't think that there will be no cost-related questions in the exam. It only means that the cost factor has been distributed to other exam domains. So, for example, the Design Solutions for Organizational Complexity domain includes cost management and billing setup topics for multi-account AWS environments using AWS Organizations. The exam coverage for the Design for New Solutions domain was reduced from 31% to 29% only. The same goes for the Continuous Improvement domain, which was at 29% before but is now at 25%, including a slight name change to "Continuous Improvement for Existing Solutions" as well.

Exam Topics for SAP-C02

This list of the AWS services covered for the AWS Certified Solutions Architect Professional exam is quite long which simply proves how wide the topics are covered in the test. Don't get scared by the sheer length of list but rather, start in reviewing the AWS services based on its section. With proper training and study strategy, you would be able to adequately cover these topics on your review:

Analytics:
- Amazon Athena
- AWS Data Exchange
- AWS Data Pipeline
- Amazon EMR
- AWS Glue
- Amazon Kinesis Data Analytics
- Amazon Kinesis Data Firehose
- Amazon Kinesis Data Streams
- AWS Lake Formation
- Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- Amazon OpenSearch Service
- Amazon QuickSight

Application Integration:
- Amazon AppFlow
- AWS AppSync
- Amazon EventBridge (Amazon CloudWatch Events)
- Amazon MQ
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Queue Service (Amazon SQS)
- AWS Step Functions

Business Applications:
- Alexa for Business
- Amazon Simple Email Service (Amazon SES)

Blockchain:
- Amazon Managed Blockchain

Machine Learning:
- Amazon Comprehend
- Amazon Forecast
- Amazon Fraud Detector
- Amazon Kendra
- Amazon Lex
- Amazon Personalize
- Amazon Polly
- Amazon Rekognition
- Amazon SageMaker
- Amazon Textract
- Amazon Transcribe
- Amazon Translate

Management and Governance:
- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch Logs
- AWS Command Line Interface (AWS CLI)
- AWS Compute Optimizer
- AWS Config
- AWS Control Tower
- AWS License Manager
- Amazon Managed Grafana
- Amazon Managed Service for Prometheus
- AWS Management Console
- AWS Organizations
- AWS Personal Health Dashboard
- AWS Proton
- AWS Service Catalog
- Service Quotas
- AWS Systems Manager
- AWS Trusted Advisor
- AWS Well-Architected Tool

Cloud Financial Management:
AWS Budgets
AWS Cost and Usage Report
AWS Cost Explorer
Savings Plans

Compute:
AWS App Runner
AWS Auto Scaling
AWS Batch
Amazon EC2
Amazon EC2 Auto Scaling
AWS Elastic Beanstalk
Amazon Elastic Kubernetes Service (Amazon EKS)
Elastic Load Balancing
AWS Fargate
AWS Lambda
Amazon Lightsail
AWS Outposts
AWS Wavelength

Containers:
Amazon Elastic Container Registry (Amazon ECR)
Amazon Elastic Container Service (Amazon ECS)
Amazon ECS Anywhere
Amazon Elastic Kubernetes Service (Amazon EKS)
Amazon EKS Anywhere
Amazon EKS Distro

Database:
Amazon Aurora
Amazon Aurora Serverless
Amazon DocumentDB (with MongoDB compatibility)
Amazon DynamoDB
Amazon ElastiCache
Amazon Keyspaces (for Apache Cassandra)
Amazon Neptune
Amazon RDS
Amazon Redshift
Amazon Timestream

Migration and Transfer:
AWS Application Discovery Service
AWS Application Migration Service (CloudEndure Migration)
AWS Database Migration Service (AWS DMS)
AWS DataSync
AWS Migration Hub
AWS Schema Conversion Tool (AWS SCT)
AWS Snow Family
AWS Transfer Family

Security, Identity, and Compliance:
AWS Artifact
AWS Audit Manager
AWS Certificate Manager (ACM)
AWS CloudHSM
Amazon Cognito
Amazon Detective
AWS Directory Service
AWS Firewall Manager
Amazon GuardDuty
AWS Identity and Access Management (IAM)
Amazon Inspector
AWS Key Management Service (AWS KMS)
Amazon Macie
AWS Network Firewall
AWS Resource Access Manager (AWS RAM)
AWS Secrets Manager
AWS Security Hub
AWS Security Token Service (AWS STS)
AWS Shield
AWS Single Sign-On
AWS WAF

Media Services:
- Amazon Elastic Transcoder
- Amazon Kinesis Video Streams

Developer Tools:
AWS Cloud9
AWS CodeArtifact
AWS CodeBuild
AWS CodeCommit
AWS CodeDeploy
Amazon CodeGuru
AWS CodePipeline
AWS CodeStar
AWS X-Ray

Frontend Web and Mobile:
AWS Amplify
Amazon API Gateway
AWS Device Farm
Amazon Pinpoint

Internet of Things:
AWS IoT Analytics
AWS IoT Core
AWS IoT Device Defender
AWS IoT Device Management
AWS IoT Events
AWS IoT Greengrass
AWS IoT SiteWise
AWS IoT Things Graph
AWS IoT 1-Click

Networking and Content Delivery:
- Amazon CloudFront
- AWS Direct Connect
- Elastic Load Balancing (ELB)
- AWS Global Accelerator
- AWS PrivateLink
- Amazon Route 53
- AWS Transit Gateway
- Amazon VPC
- AWS VPN

Storage:
- AWS Backup
- Amazon Elastic Block Store (Amazon EBS)
- AWS Elastic Disaster Recovery (CloudEndure Disaster Recovery)
- Amazon Elastic File System (Amazon EFS)
- Amazon FSx (for all types)
- Amazon S3
- Amazon S3 Glacier
- AWS Storage Gateway

End User Computing:
- Amazon AppStream 2.0
- Amazon WorkSpaces

Exam Scoring System

You can get a score from 100 to 1,000 with a minimum passing score of **750** when you take the Solutions Architect Professional exam. AWS uses a scaled scoring model to equate scores across multiple exam types that may have different difficulty levels. The complete score report will be sent to you by email after a few days.

Individuals who unfortunately do not pass the AWS exam must wait 14 days before they are allowed to retake the exam. Fortunately, there is no hard limit on exam attempts until you pass the exam. Take note that on each attempt, the full registration price of the AWS exam must be paid. Within 5 business days of completing your exam, your AWS Certification Account will have a record of your complete exam results.

		Score Performance	
Section	**% of Scored Items**	**Needs Improvement**	**Meets Competencies**
Domain 1: Design Solutions for Organizational Complexity	26%		
Domain 2: Design for New Solutions	29%		
Domain 3: Continuous Improvement for Existing Solutions	25%		
Domain 4: Accelerate Workload Migration and Modernization	20%		

Disclaimer: AWS Certification exams are designed to make pass/fail decisions based on the total exam score. Section level results are designed to provide direction on areas where a candidate may be weak. Candidates should exercise caution when interpreting the above section level score information as it is less reliable than the total exam score and not intended to guide future test performance.

The score report, as shown above, contains a table of your performance at each section/domain, which indicates whether you met the competency level required for these domains or not. AWS uses a compensatory scoring model, which means that you do not necessarily need to pass each and every individual section, only the overall examination. Each section has a specific score weighting that translates to the number of questions; hence, some sections have more questions than others. The Score Performance table highlights your strengths and weaknesses that you need to improve on.

AWS CERTIFIED SOLUTIONS ARCHITECT PROFESSIONAL EXAM - STUDY GUIDE AND TIPS

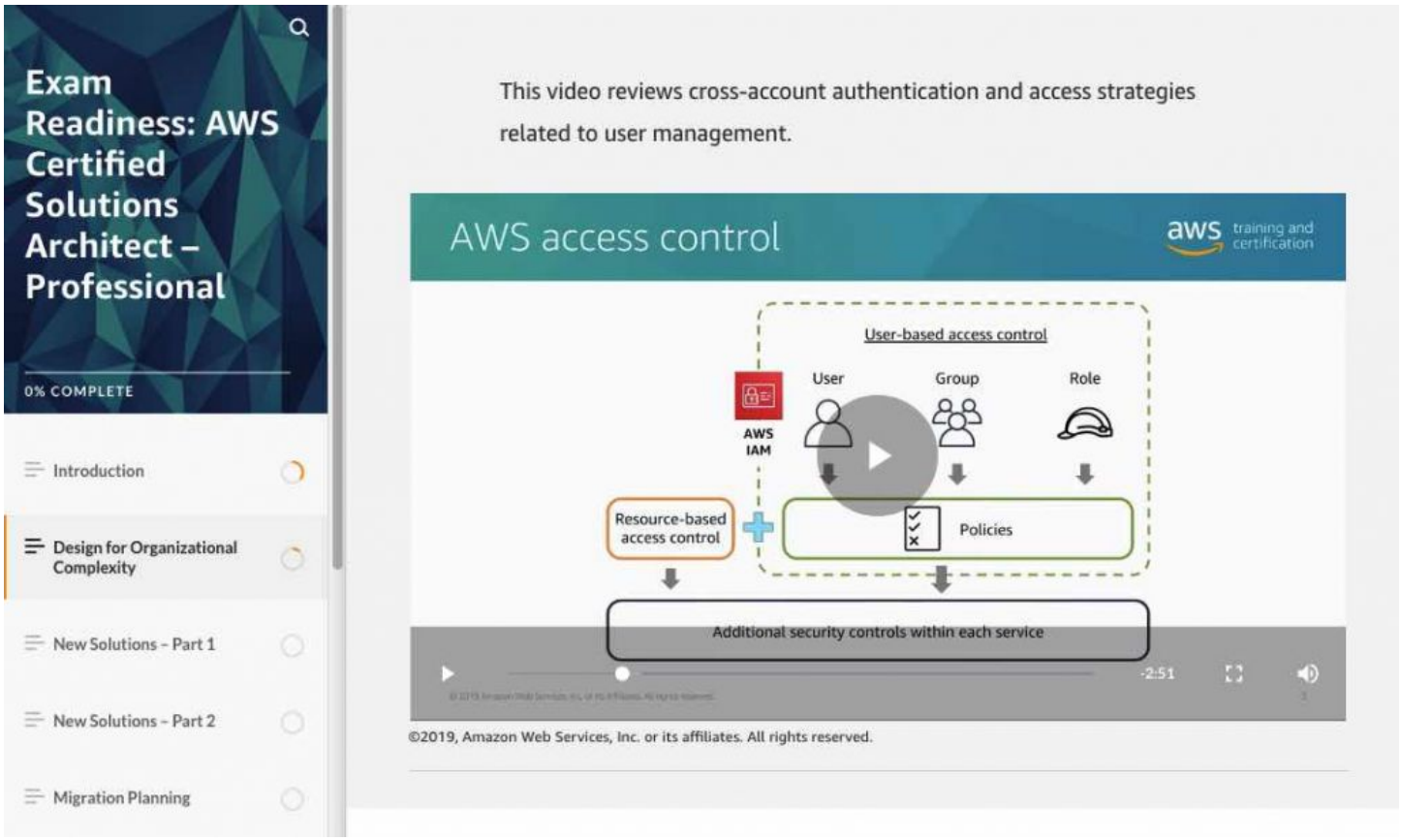
Few years ago, before you can take the AWS Certified Solutions Architect Professional exam (or SA Pro for short), you would first have to pass the associate level exam of this track. This is to ensure that you have sufficient knowledge and understanding on architecting in AWS, before tackling the more difficult certification. In October 2018, AWS removed this ruling so that there are no more prerequisites for taking the Professional level exams. You now have the freedom to directly pursue this certification if you wish to.

This certification is truly a levelled-up version of the AWS Solutions Architect Associate certification. It examines your capability to create well-architected solutions in AWS, but on a grander scale and with more difficult requirements. Because of this, we recommend that you go through our exam preparation guide for the AWS Certified Solutions Architect Associate and even the AWS Certified Cloud Practitioner if you have not done so yet. These study guides contain important materials that will be crucial for passing the SAP-C02 exam.

Study Materials

The official AWS sample questions, Whitepapers, FAQs, AWS Documentation, Re:Invent videos, forums, labs, AWS cheat sheets, AWS practice exams, and your own personal technical experiences are what you will need to pass the exam. Since the SA Pro is one of the most difficult AWS certification exams out there, you have to prepare yourself with every study material you can get your hands on. To learn more details regarding your exam, go through this AWS exam blueprint as it discusses the various domains they will test you on.

AWS has a digital course called Exam Readiness: AWS Certified Solutions Architect – Professional, which is a short video lecture that discusses what to expect on the AWS Certified Solutions Architect – Professional exam. It should sufficiently provide an overview of the different concepts and practices that you'll need to know about. Each topic in the course will also contain a short quiz right after you finish its lecture to help you lock in the important information.



For whitepapers, aside from the ones listed down in our Solutions Architect Associate and Cloud Practitioner exam guides, you should also study the following:

- Security best practices for AWS Key Management Service
- Encryption of Data at Rest
- Web Application Hosting in the AWS Cloud
- Practicing Continuous Integration and Continuous Delivery on AWS
- Microservices architecture on AWS
- AWS Well-Architected Framework
- Using Amazon Web Services for Disaster Recovery
- AWS Architecture Center architecture whitepapers

Also check out this article: **Top 5 FREE AWS Review Materials**.

AWS Services to Focus On

Generally, as a soon-to-be AWS Certified SA Pro, you should already have a thorough understanding of every service and feature in AWS. But for the purpose of this review, give more attention on the following services since they are common topics in the SA Pro exams:

1. AWS Organizations
    1. Know how to create organizational units (OUs), service control policies (SCPs), and any additional parameters in AWS Organizations.
    2. There might be scenarios where the master account needs access to member accounts. Your options can include setting up OUs and SCPs, delegating an IAM role, or providing cross account access.
    3. Differentiate SCP from IAM policies.
    4. You should also know how to integrate AWS Organizations with other services such as CloudFormation, Service Catalog, and IAM to manage resources and user access.
    5. Lastly, read how you can save on costs by enabling consolidated billing in your organizations, and what would be the benefits of enabling all features.
2. AWS Server Migration Services
    1. Study the different ways to migrate on-premises servers to the AWS Cloud.
    2. Also study how you can perform the migration in a secure and reliable manner.
    3. You should be aware of what types of objects AWS SMS can migrate for you i.e. VMs, and what is the output of the migration process.
3. AWS Database Migration Service + Schema Conversion Tool
    1. Aside from server and application migration, you should also know how you can move on-premises databases to AWS, and not just to RDS but to other services as well as Aurora and RedShift.
    2. Read over what schemas can be converted by SCT.
4. AWS Serverless Application Model
    1. The AWS SAM has a syntax of its own. Study the syntax and how AWS SAM is used to deploy serverless applications through code.
    2. Know the relationship between SAM and CloudFormation. **Hint:** You can use these two together.
5. AWS Systems Manager
    1. Study the different features under Systems Manager and how each feature can automate EC2-related processes. Patch Manager and Maintenance Windows are often used together to perform automated patching. It allows for easier setup and better control over patch baselines, rather than using a cron job within an EC2 instance or using Cloudwatch Events.
    2. It is also important to know how you can troubleshoot EC2 issues using Systems Manager.
    3. Parameter Store allows you to securely store a string in AWS, which can be retrieved anywhere in your environment. You can use this service instead of AWS Secrets Manager if you don't need to rotate your secrets.

6. AWS CI/CD - Study the different CI/CD tools in AWS, from function to features to implementation. It would be very helpful if you can create your own CI/CD pipeline as well using the services below.
    1. CodeCommit
    2. CodeBuild
    3. CodeDeploy
    4. CodePipeline
7. AWS Service Catalog
    1. This service is also part of the automation toolkit in AWS. Study how you can create and manage portfolios of approved services in Service Catalog, and how you can integrate these with other technologies such as AWS Organizations.
    2. You can enforce tagging on services using service catalog. This way, users can only launch resources that have the tags you defined.
    3. Know when Service Catalog is a better option for resource control rather than AWS Cloudformation. A good example is when you want to create a customized portfolio for each type of user in an organization and selectively grant access to the appropriate portfolio.
8. AWS Direct Connect (DX)
    1. You should have a deep understanding of this service. Questions commonly include Direct Connect Gateway, public and private VIFs and LAGs.
    2. Direct Connect is commonly used for connecting on-premises networks to AWS, but it can also be used to connect different AWS Regions to a central datacenter. For these kinds of scenarios, take note of the benefits of Direct Connect such as dedicated bandwidth, network security, multi-Region and multi-VPC connection support.
    3. Direct Connect is also used along with a failover connection, such as a secondary DX line or IPsec VPN. The correct answer will depend on specific requirements like cost, speed, ease of management, etc.
    4. Another combination that can be used to link different VPCs is Transit Gateway + DX.
9. AWS CloudFormation - Your AWS exam might include a lot of scenarios that involve Cloudformation, so take note of the following:
    1. You can use CloudFormation to enforce tagging by requiring users to only use resources that CloudFormation launched.
    2. CloudFormation can be used for managing resources across different AWS accounts in an Organization using StackSets.
    3. CloudFormation is often compared to AWS Service Catalog and AWS SAM. The way to approach this in the exam is to know what features are supported by CloudFormation that cannot be performed in a similar fashion with Service Catalog or SAM.
10. Amazon VPC (in depth)
    1. Know the ins and outs of NAT Gateways and NAT instances, such as supported IP protocols, which types of packets are dropped in a cut connection, etc.
    2. Study about transit gateway and how it can be used together with Direct Connect.
    3. Remember longest prefix routing.

4. Compare VPC peering to other options such as Site to Site VPN. Know what components are in use: Customer gateway, Virtual Private Gateway, etc.

11. Amazon ECS
    1. Differentiate task role from task execution role.
    2. Compare using ECS compute instances from Fargate serverless model.
    3. Study how to link together ECS and ECR with CI/CD tools to automate deployment of updates to your Docker containers.
12. Elastic Load Balancer (in depth)
    1. Differentiate the internet protocols used by each type of ELB for listeners and target groups: HTTP, HTTPS, TCP, UDP, TLS.
    2. Know how you can configure load balancers to forward client IP to target instances.
    3. Know how you can secure your ELB traffic through the use of SSL and WAF. SSL can be offloaded on either the ELB or CloudHSM.
13. Elastic Beanstalk
    1. Study the different deployment options for Elastic Beanstalk.
    2. Know the steps in performing a blue/green deployment.
    3. Know how you can use traffic splitting deployment to perform canary testing
    4. Compare Elastic Beanstalk's deployment options to CodeDeploy.
14. WAF and Shield
    1. Know at what network layer WAF and Shield operate in
    2. Differentiate security capabilities of WAF and Shield Advanced, especially with regards to DDoS protection. A great way to determine which one to use is to look at the services that need the protection and if cost is a factor. You may also visit this AWS documentation for additional details.
15. Amazon Workspaces vs Amazon Appstream
    1. Workspaces is best for virtual desktop environments. You can use it to provision either Windows or Linux desktops in just a few minutes and quickly scale to provide thousands of desktops to workers across the globe.
    2. Appstream is best for standalone desktop applications. You centrally manage your desktop applications on AppStream 2.0 and securely deliver them to any computer.
16. Amazon Workdocs - It is important to determine what features makes Workdocs unique compared to using S3 and EFS. Choose this service if you need a secure document storage where you can collaborate in real-time with others and manage access to the documents.
17. Elasticache vs DAX vs Aurora Read Replicas
    1. Know your caching options especially when it comes to databases.
    2. If there is a feature that is readily integrated with the database, it would be better to use that integrated features instead for less overhead.
18. Snowball Edge vs Direct Connect vs S3 Acceleration - These three services are heavily used for data migration purposes. Read the exam scenario properly to determine which service is best used. Factors in choosing the correct answer are cost, time allotted for the migration, and how much data is needed to be transported.

19. Using Resource Tags with IAM - Study how you can use resource tags to manage access via IAM policies.

We also recommend checking out **Tutorials Dojo's AWS Cheat Sheets** which provides a summarized but highly informative set of notes and tips for your review on these services. These **cheat sheets** are presented mostly in bullet points which will help you retain the knowledge much better vs reading the lengthy FAQs.

We expect that you already have vast knowledge on the AWS services that a Solutions Architect commonly use, such as those listed in our SA Associate review guide. It is also not enough to just know the service and its features. You should also have a good understanding on how to integrate these services with one another to build large-scale infrastructures and applications. It's why it is generally recommended to have hands-on experience managing and operating systems on AWS.

Common Exam Scenarios

Scenario	Solution
Design Solutions for Organizational Complexity	
You are managing multiple accounts and you need to ensure that each account can only use resources that it is supposed to. What is a simple and reusable method of doing so?	AWS Organizations is a given here. It simplifies a lot of the account management and controls that you would use for this scenario. For resource control, you may use AWS CloudFormation Stacksets to define a specific stack and limit your developers to the created resources. You may also use AWS Service Catalog if you like to define specific product configurations or CloudFormation stacks, and give your developers freedom to deploy them. For permission controls, a combination of IAM policies and SCPs should suffice.
You are creating a CloudFormation stack and uploading it to AWS Service Catalog so you may share this stack with other AWS accounts in your organization. How can your end-users access the product/portfolio while still granting the least privilege?	Your end-users require appropriate IAM permissions to access AWS Service Catalog and launch a CloudFormation stack. The **AWSServiceCatalogEndUserFullAccess** and **AWSServiceCatalogEndUserReadOnlyAccess** policies grant access to the AWS Service Catalog end-user console view. When a user who has either of these policies chooses AWS Service Catalog in the AWS Management Console, the end-user console view displays the products that they have permission to launch. You should also provide the user the permission to pass IAM role to CloudFormation so that

	the CloudFormation stack can launch the necessary resources.
How can you provide access to users in a different account to resources in your account?	Use cross-account IAM roles and attach the permissions necessary to access your resources. Have the users in the other account reference this IAM role.
How do you share or link two networks together? (VPCs, VPNs, routes, etc) What if you have restrictions on your traffic e.g. it cannot traverse through the public Internet?	Sharing networks or linking two networks is a common theme in a very large organization. This ensures that your networks adhere to the best practices all the time. For VPCs, you can use VPC sharing, VPC Peering, or Transit Gateways. VPNs can utilize Site-to-Site VPN for cross-region or cross-account connections. For strict network compliance, you can access some of your AWS resources privately through shared VPC endpoints. This way, your traffic does not need to traverse through the public Internet. More information on that can be found in this article:
You have multiple accounts under AWS Organizations. Previously, each account can purchase their own RIs, but now, they have to request it from one central account for procurement. What steps should be done to satisfy this requirement in the most secure way?	Ensure that all AWS accounts are part of an AWS Organizations structure operating in all features mode. Then create an SCP that contains a deny rule to the ec2:PurchaseReservedInstancesOffering and ec2:ModifyReservedInstances actions. Attach the SCP to each organizational unit (OU) of the AWS Organizations' structure.
Can you connect multiple VPCs that belong to different AWS accounts and have overlapping CIDRs? If so, how can you manage your route tables so that the correct traffic is routed to the correct VPC?	You can connect multiple VPCs together even if they have overlapping CIDRs. What is important is that you are aware of how routing works in AWS. AWS uses longest prefix matching to determine where traffic is delivered to. So to make sure that your traffic is routed properly, be as specific as possible with your routes.
Members of a department will need access to your AWS Management Console. Without having to create IAM Users for each member, how can you provide long-term access?	You can use your on-premises SAML 2.0-compliant identity provider to grant your members federated access to the AWS Management Console via the AWS single sign-on (SSO) endpoint. This will provide them long term access to the console as long as they can authenticate with the IdP.

Is it possible for one account to monitor all API actions executed by each member account in an AWS Organization? If so, how does it work?	You can configure AWS CloudTrail to create a trail that will log all events for all AWS accounts in that organization. When you create an organization trail, a trail with the name that you give it will be created in every AWS account that belongs to your organization. Users with CloudTrail permissions in member accounts will be able to see this trail. However, users in member accounts will not have sufficient permissions to delete the organization trail, turn logging on or off, change what types of events are logged, or otherwise alter the organization trail in any way. When you create an organization trail in the console, or when you enable CloudTrail as a trusted service in the Organizations, this creates a service-linked role to perform logging tasks in your organization's member accounts. This role is named AWSServiceRoleForCloudTrail, and is required for CloudTrail to successfully log events for an organization. Log files for an account removed from the organization that were created prior to the account's removal will still remain in the Amazon S3 bucket where log files are stored for the trail.
You have 50 accounts joined to your AWS Organizations and you will require a central, internal DNS solution to help reduce the network complexity. Each account has its own VPC that will rely on the private DNS solution for resolving different AWS resources (servers, databases, AD domains, etc). What is the least complex network architecture that you can create?	Create a shared services VPC in your central account, and connect the other VPCs to yours using VPC peering or AWS Transit Gateway. Set up a private hosted zone in Amazon Route 53 on your shared services VPC and add in the necessary domains/subdomains. Associate the rest of the VPCs to this private hosted zone.
How can you easily deploy a basic infrastructure to different AWS regions while at the same time allowing your developers to optimize (but not delete) the launched infrastructures?	Use CloudFormation Stacksets to deploy your infrastructure to different regions. Deploy the stack in an administrator account. Create an IAM role that developers can assume so they can optimize the infrastructure. Make sure that the IAM role has a policy that denies deletion for cloudformation-launched resources.

You have multiple VPCs in your organization that are using the same Direct Connect line to connect back to your corporate datacenter. This setup does not account for line failure which will affect the business greatly if something were to happen to the network. How do you make the network more highly available? What if the VPCs span multiple regions?	Utilize Site-To-Site VPN between the VPCs and your datacenter and terminate the VPN tunnel at a virtual private gateway. Setup BGP routing. An alternative solution is to provision another Direct Connect line in another location if you require constant network performance, at the expense of additional cost. If the VPCs span multiple regions, you can use a Direct Connect Gateway.
Design for New Solutions	
You have production instances running in the same account as your dev environment. Your developers occasionally mistakenly stop/terminate production instances. How can you prevent this from happening?	You can leverage resource tagging and create an explicit deny IAM policy that would prevent developers from stopping or terminating instances tagged under production.
If you have documents that need to be collaborated upon, and you also need strict access controls over who gets to view and edit these documents, what service should you use?	AWS has a suite of services similar to Microsoft Office or Gsuite, and one of those services is called Amazon Workdocs. Amazon Workdocs is a fully managed, secure content creation, storage, and collaboration service.
You have objects in an S3 bucket that have different retrieval frequencies. To optimize cost and retrieval times, what change should you make?	S3 has a new storage class called "S3 Intelligent-Tiering". S3 IT moves data between two access tiers — frequent access and infrequent access — when access patterns change and is ideal for data with unknown or changing access patterns. What makes this relatively cost-effective is that there are no retrieval fees in S3 Intelligent-Tiering, unlike the S3 IA storage class.
How can you quickly scale your applications in AWS while keeping costs low?	While EC2 instances are perfectly fine compute option, they tend to be pricey if they are not right-sized or if the capacity consumption is fluctuating. If you can, re-architect your applications to use Containers or Serverless compute options such as ECS, Fargate, Lambda and API Gateway.

You would like to automate your application deployments and use blue-green deployment to properly test your updates. Code updates are submitted to an S3 bucket you own. You wish to have a consistent environment where you can test your changes. Which services will help you fulfill this scenario?	Create a deployment pipeline using CodePipeline. Use AWS Lambda to invoke the stages in your pipeline. Use AWS CodeBuild to compile your code, before sending it to AWS Elastic Beanstalk in a blue environment. Have AWS Codebuild test the update in the blue environment. Once testing has succeeded, trigger AWS Lambda to swap the URLs between your blue and green Elastic Beanstalk environments. More information here.
Your company only allows the use of pre-approved AMIs for all your teams. However, users should not be prevented from launching unauthorized AMIs as it might affect some of their automation. How can you monitor all EC2 instances launched to make sure they are compliant with your approved AMI list, and that you are informed when someone uses an incompliant AMI?	Utilize AWS Config to monitor AMI compliance across all AWS accounts. Configure Amazon SNS to notify you when an EC2 instance was launched using an un-approved AMI. You can also use Amazon EventBridge to monitor each RunInstance event. Use it to trigger a Lambda function that will cross check the launch configuration to your AMI list and send you a notification via SNS if the AMI used was un-approved. This will give you more information such as who launched the instance.
How can you build a fully automated call center in AWS?	Utilize Amazon Connect, Amazon Lex, Amazon Polly, and AWS Lambda.
You have a large number of video files that are being processed locally by your custom AI application for facial detection and recognition. These video files are kept in a tape library for long term storage. Video metadata and timestamps of detected faces are stored in MongoDB. You decided to use AWS to further enhance your operations, but the migration procedure should have minimal disruption to the existing process. What should be your setup?	Use Amazon Storage Gateway Tape Gateway to store your video files in an Amazon S3 bucket. Start importing the video files to your tape gateway after you've configured the appliance. Create a Lambda function that will extract the videos from Tape Gateway and forward them to Amazon Rekognition. Use Amazon Rekognition for facial detection and timestamping. Once finished, have Rekognition trigger a Lambda function that will store the resulting information in Amazon DynamoDB.
Is it possible in AWS for you to enlist the help of other people to complete tasks that only humans can do?	Yes, you can submit tasks in AWS Mechanical Turk and have other people complete them in exchange for a fee.
You have a requirement to enforce HTTPS for all your connections but you would like to offload the SSL/TLS to a separate server to reduce the impact on application performance. Unfortunately, the	You cannot use ACM in another region for this purpose since ACM is a regional service. Generate your own certificate and upload it to AWS IAM. Associate the

region you are using does not support AWS ACM. What can be your alternative?	imported certificate with an elastic load balancer. More information here.
Accelerate Workload Migration and Modernization	
You are using a database engine on-premises that is not currently supported by RDS. If you wish to bring your database to AWS, how do you migrate it?	AWS has two tools to help you migrate your database workloads to the cloud: database migration service and schema conversion tool. First, collect information on your source database and have SCT convert your database schema and database code. You may check the supported source engines here. Once the conversion is finished, you can launch an RDS database and apply the converted schema, and use database migration service to safely migrate your database.
You have thousands of applications running on premises that need to be migrated to AWS. However, they are too intertwined with each other and may cause issues if the dependencies are not mapped properly. How should you proceed?	Use AWS Application Discovery Service to collect server utilization data and perform dependency mapping. Then send the result to AWS Migration Hub where you can initiate the migration of the discovered servers.
You have to migrate a large amount of data (TBs) over the weekend to an S3 bucket and you are not sure how to proceed. You have a 500Mbps Direct Connect line from your corporate data center to AWS. You also have a 1Gbps Internet connection. What should be your mode of migration?	One might consider using Snow hardware to perform the migration, but the time constraint does not allow you to ship the hardware in time. Your Direct Connect line is only 500Mbps as well. So you should instead enable S3 Transfer Acceleration and dedicate all your available bandwidth for the data transfer.
You have a custom-built application that you'd like to migrate to AWS. Currently, you don't have enough manpower or money to rewrite the application to be cloud-optimized, but you would still like to optimize whatever you can on the application. What should be your migration strategy?	Rehosting is out of the question since there are no optimizations done in a lift-and-shift scenario. Re-architecting is also out of the question since you do not have the budget and manpower for it. You cannot retire nor repurchase since this is a custom production application. So your only option would be to re-platform it to utilize scaling and load balancing for example.

How can you leverage AWS as a cost-effective solution for offsite backups of mission-critical objects that have short RTO and RPO requirements?	For hybrid cloud architectures, you may use AWS Storage Gateway to continuously store file backups onto Amazon S3. Since you have short RTO and RPO, the best storage type to use is File Gateway. File Gateway allows you to mount Amazon S3 onto your server, and by doing so you can quickly retrieve the files you need. Volume Gateway does not work here since you will have to restore entire volumes before you can retrieve your files. Enable versioning on your S3 bucket to maintain old copies of an object. You can then create lifecycle policies in Amazon S3 to achieve even lower costs.
You have hundreds of EC2 Linux servers concurrently accessing files in your local NAS. The communication is kept private by AWS Direct Connect and IPsec VPN. You notice that the NAS is not able to sufficiently serve your EC2 instances, thus leading to huge slowdowns. You consider migrating to an AWS storage service as an alternative. What should be your service and how do you perform the migration?	Since you have hundreds of EC2 servers, the best storage for concurrent access would be Amazon EFS. To migrate your data to EFS, you may use AWS DataSync. Create a VPC endpoint for your EFS so that the data migration is performed quickly and securely over your Direct Connect.
If you have a piece of software (e.g. CRM) that you want to bring to the cloud, and you have an allocated budget but not enough manpower to re-architect it, what is your next best option to make sure the software is still able to take advantage of the cloud?	Check in the AWS Marketplace and verify if there is a similar tool that you can use -- Repurchasing strategy.
Continuous Improvement for Existing Solutions	
You have a running EMR cluster that has erratic utilization and task processing takes longer as time goes on. What can you do to keep costs to a minimum?	Add additional task nodes, but use instance fleets with the master node in on-Demand mode and a mix of On-Demand and Spot Instances for the core and task nodes. Purchase Reserved Instances for the master node.
A company has multiple AWS accounts in AWS Organizations that has full features enabled. How do you track AWS costs in Organizations and alert if costs from a business unit exceed a specific budget threshold?	Use Cost Explorer to monitor the spending of each account. Create a budget in AWS Budgets for each OU by grouping linked accounts, then configure SNS notification to alert you if the budget has been exceeded.

You have a Serverless stack running for your mobile application (Lambda, API Gateway, DynamoDB). Your Lambda costs are getting expensive due to the long wait time caused by high network latency when communicating with the SQL database in your on-premises environment. Only a VPN solution connects your VPC to your on-premises network. What steps can you make to reduce your costs?	If possible, migrate your database to AWS for lower latency. If this is not an option, consider purchasing a Direct Connect line with your VPN on top of it for a secure and fast network. Consider caching frequently retrieved results on API Gateway. Continuously monitor your Lambda execution time and reduce it gradually up to an acceptable duration.
You have a set of EC2 instances behind a load balancer and an autoscaling group, and they connect to your RDS database. Your VPC containing the instances uses NAT gateways to retrieve patches periodically. Everything is accessible only within the corporate network. What are some ways to lower your cost?	If your EC2 instances are production workloads, purchase Reserved instances. If they are not, schedule the autoscaling to scale in when they are not in use and scale out when you are about to use them. Consider a caching layer for your database reads if the same queries often appear. Consider using NAT instances instead, or better yet, remove the NAT gateways if you are only using them for patching. You can easily create a new NAT instance or NAT gateway when you need them again.
You need to generate continuous database and server backups in your primary region and have them available in your disaster recovery region as well. Backups need to be made available immediately in the primary region while the disaster region allows more leniency, as long as they can be restored in a few hours. A single backup is kept only for a month before it is deleted. A dedicated team conducts game days every week in the primary region to test the backups. You need to keep storage costs as low as possible.	Store the backups in Amazon S3 Standard and configure cross-region replication to the DR region S3 bucket. Create a lifecycle policy in the DR region to move the backups to S3 Glacier. S3 IA is not applicable since you need to wait fo 30 days before you can transition to IA from Standard.
Determine the most cost-effective infrastructure: a) Data is constantly being delivered to a file storage at a constant rate. Storage should have enough capacity to accommodate growth. b) The data is extracted and worked upon by worker nodes. A job can take a few hours to finish. c) This is not a mission-critical workload, so interruptions are acceptable as long as they are reprocessed. d) The jobs only need to run during evenings.	You may use Amazon Kinesis Firehose to continuously stream the data into Amazon S3. Then configure AWS Batch with spot pricing for your worker nodes. Use Amazon Cloudwatch Events to schedule your jobs at night. More information here.

If you are cost-conscious about the charges incurred by external users who frequently access your S3 objects, what change can you introduce to shift the charges to the users?	Ensure that the external users have their own AWS accounts. Enable S3 Requester Pays on the S3 buckets. Create a bucket policy that will allow these users read/write access to the buckets.
You have a Direct Connect line from an AWS partner data center to your on-premises data center. Webservers are running in EC2, and they connect back to your on-premises databases/data warehouse. How can you increase the reliability of your connection?	There are multiple ways to increase the reliability of your network connection. You can order another Direct Connect line for redundancy, which AWS recommends for critical workloads. You may also create an IPSec VPN connection over public Internet, but that will require additional configuration since you need to monitor the health of both networks.
You have a set of instances behind a Network Load Balancer and an autoscaling group. If you are to protect your instances from DDoS, what changes should you make?	Since AWS WAF does not integrate with NLB directly, you can create a CloudFront and attach the WAF there, and use your NLB as the origin. You can also enable AWS Shield Advanced so you get the full suite of features against DDoS and other security attacks.
You have a critical production workload (servers + databases) running in one region, and your RTO is 5 minutes while your RPO is 15 minutes. What is your most cost-efficient disaster recovery option?	If you have the option to choose warm standby, make sure that the DR infrastructure is able to automatically detect failure on the primary infrastructure (through health checks), and it can automatically scale up/scale out (autoscaling + scripts) and perform an immediate failover (Route 53 failover routing) in response. If your warm standby option does not state that it can do so then you might not be able to meet your RTO/RPO, which means you must use multi-site DR solution instead even though it is costly.
You use RDS to store data collected by hundreds of IoT robots. You know that these robots can produce up to tens of KBs of data per minute. It is expected that in a few years, the number of robots will continuously increase, and so database storage should be able to scale to handle the amount of data coming in and the IOPS required to match performance. How can you re-architect your solution to better suit this upcoming growth?	Instead of using a database, consider using a data warehousing solution such as Amazon Redshift instead. That way, your data storage can scale much larger and the database performance will not take that much of a hit.

You have a stream of data coming into your AWS environment that is being delivered by multiple sensors around the world. You need real-time processing for these data and you have to make sure that they are processed in the order in which they came in. What should be your architecture?	One might consider using SQS FIFO for this scenario, but since it also requires you to have real-time processing capabilities, Amazon Kinesis is a better solution. You can configure the data to have a specific partition key so that it is processed by the same Kinesis shard, thereby giving you similar FIFO capabilities.
You want to use your AWS Direct Connect to access S3 and DynamoDB endpoints while using your Internet provider for other types of traffic. How should you configure this?	Create a public interface on your AWS Direct Connect link. Advertise specific routes for your network to AWS, so that S3 traffic and DynamoDB traffic pass through your AWS Direct Connect.
You have a web application leveraging Cloudfront for caching frequently accessed objects. However, parts of the application are reportedly slow in some countries. What cost-effective improvement can you make?	Utilize Lambda@edge to run parts of the application closer to the users.
If you are running Amazon Redshift and you have a tight RTO and RPO requirement, what improvement can you make so that your Amazon Redshift is more highly available and durable in case of a regional disaster?	Amazon Redshift allows you to copy snapshots to other regions by enabling cross-region snapshots. Snapshots to S3 are automatically created on active clusters every 8 hours or when an amount of data equal to 5 GB per node changes. Depending on the snapshot policy configured on the primary cluster, the snapshot updates can either be scheduled, or based upon data change, and then any updates are automatically replicated to the secondary/DR region.
You have multiple EC2 instances distributed across different AZs depending on their function, and each of the AZ has its own m5.large NAT instance. A set of EC2 servers in one AZ occasionally cannot reach an API that is external to AWS when there is a high volume of traffic. This is unacceptable for your organization. What is the most cost-effective solution for your problem?	It would be better if you transition your NAT Instances to NAT Gateways since they provide faster network speeds. Resizing the NAT instance to something higher is not cost-effective anymore since the network speed increase is gradual as you go up. Adding more NAT instances to a single AZ makes your environment too complex.

Most of your vendors' applications use IPv4 to communicate with your private AWS resources. However, a newly acquired vendor will only be supporting IPv6. You will be creating a new VPC dedicated for this vendor, and you need to make sure that all of your private EC2 instances can communicate using IPv6. What are the configurations that you need to do?	Provide your EC2 instances with IPv6 addresses. Create security groups that will allow IPv6 addresses for inbound and outbound. Create an egress-only Internet gateway to allow your private instances to reach the vendor.

Validate Your Knowledge

After your review, you should take some practice tests to measure your preparedness for the real exam. AWS offers a sample practice test for free which you can find here. You can also opt to buy the longer AWS sample practice test at aws.training, and use the discount coupon you received from any previously taken certification exams. Be aware though that the sample practice tests do not mimic the difficulty of the real SA Pro exam. You should not rely solely on them to gauge your preparedness. It is better to take more **practice tests** to fully understand if you are prepared to pass the certification exam.

Fortunately, **Tutorials Dojo** also offers a great set of practice questions for you to take **here**. It is kept updated by the creators to ensure that the questions match what you'll be expecting in the real exam. The practice tests will help fill in any important details that you might have missed or skipped in your review. You can pair our practice exams with this study guide eBook to further help in your exam preparations.

Sample Practice Test Questions:

Question 1

A company has multiple AWS resources in its production account that are shared among various business units. Each business unit may have one or more AWS accounts which have resources in the production account. There were a lot of incidents in which the developers from a specific business unit accidentally terminated the EC2 instances owned by another business unit. You are tasked to come up with a solution to only allow a specific business unit who own the EC2 instances, and other AWS resources, to terminate their own resources.

Which of the following is the most suitable multi-account strategy that you should implement?

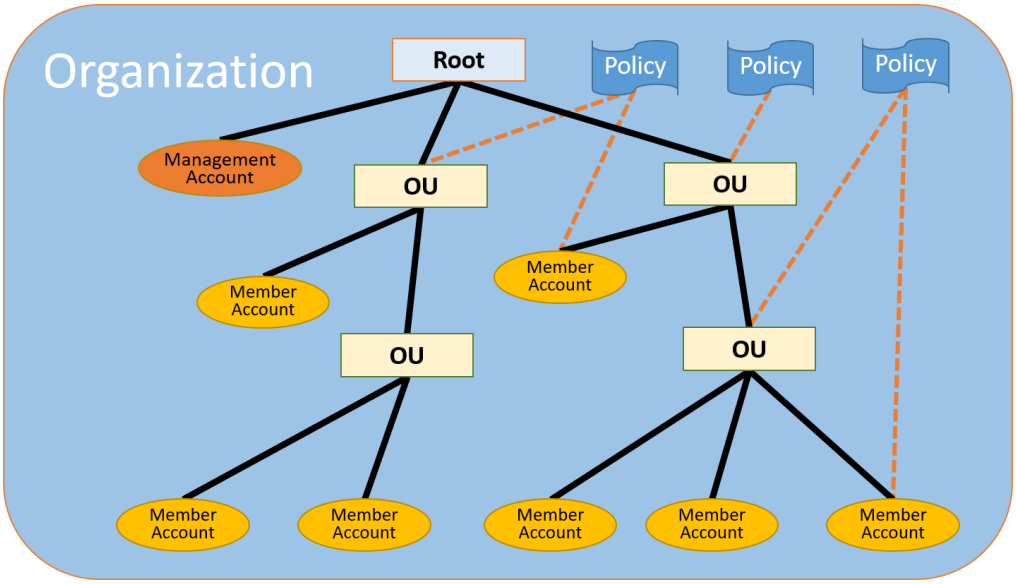
1. Use AWS Organizations to centrally manage all of your accounts. Group your accounts, which belongs to a specific business unit, to individual Organization Unit (OU). Create an IAM Role in the production account for each business unit which has a policy that allows access to the EC2 instances including a resource-level permission to terminate the instances that it owns. Create an

AWSServiceRoleForOrganizations service-linked role to the individual member accounts of the OU to enable **trusted access**.

2. Use AWS Organizations to centrally manage all of your accounts. Group your accounts, which belongs to a specific business unit, to individual Organization Unit (OU). Create a Service Control Policy in the production account for each business unit which has a policy that allows access to the EC2 instances including a resource-level permission to terminate the instances that it owns. Provide the cross-account access and the SCP to the individual member accounts to tightly control who can terminate the EC2 instances.
3. Use AWS Organizations to centrally manage all of your accounts. Group your accounts, which belong to a specific business unit, to individual Organization Units (OU). Create an IAM Role in the production account which has a policy that allows access to the EC2 instances including a resource-level permission to terminate the instances owned by a particular business unit. Provide the cross-account access and the IAM policy to every member accounts of the OU.
4. Use AWS Control Tower to centrally manage all of your accounts. Group your accounts, which belongs to a specific business unit, to individual Organization Unit (OU). Create a Service Control Policy in the production account which has a policy that allows access to the EC2 instances including a resource-level permission to terminate the instances owned by a particular business unit. Provide the cross-account access and the SCP to the OUs, which will then be automatically inherited by its member accounts.

Correct Answer: 3

AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an *organization* that you create and centrally manage. AWS Organizations includes account management and consolidated billing capabilities that enable you to better meet the budgetary, security, and compliance needs of your business. As an administrator of an organization, you can create accounts in your organization and invite existing accounts to join the organization.



You can use organizational units (OUs) to group accounts together to administer as a single unit. This greatly simplifies the management of your accounts. For example, you can attach a policy-based control to an OU, and all accounts within the OU automatically inherit the policy. You can create multiple OUs within a single organization, and you can create OUs within other OUs. Each OU can contain multiple accounts, and you can move accounts from one OU to another. However, OU names must be unique within a parent OU or root.

Resource-level permissions refers to the ability to specify which resources users are allowed to perform actions on. Amazon EC2 has partial support for resource-level permissions. This means that for certain Amazon EC2 actions, you can control when users are allowed to use those actions based on conditions that have to be fulfilled, or specific resources that users are allowed to use. For example, you can grant users permissions to launch instances, but only of a specific type, and only using a specific AMI.

The scenario on this question has a lot of AWS Accounts that need to be managed. AWS Organization solves this problem and provides you with control by assigning the different business units as individual Organization Units (OU). Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization. However, SCPs alone are not sufficient for allowing access in the accounts in your organization. Attaching an SCP to an AWS Organizations entity just defines a guardrail for what actions the principals can perform. You still need to attach identity-based or resource-based policies to principals or resources in your organization's accounts to actually grant permission to them.
Since SCPs only allow or deny the use of an AWS service, you don't want to block OUs from completely using the EC2 service. Thus, you will need to provide cross-account access and the IAM policy to every member accounts of the OU.

Hence, the correct answer is: **Use AWS Organizations to centrally manage all of your accounts. Group your accounts, which belong to a specific business unit, to individual Organization Units (OU). Create an IAM Role**

in the production account which has a policy that allows access to the EC2 instances including a resource-level permission to terminate the instances owned by a particular business unit. Provide the cross-account access and the IAM policy to every member accounts of the OU.

The option that says: **Use AWS Organizations to centrally manage all of your accounts. Group your accounts, which belongs to a specific business unit, to individual Organization Unit (OU). Create an IAM Role in the production account for each business unit which has a policy that allows access to the EC2 instances including a resource-level permission to terminate the instances that it owns. Create an AWSServiceRoleForOrganizations service-linked role to the individual member accounts of the OU to enable trusted access** is incorrect because **AWSServiceRoleForOrganizations** service-linked role is primarily used to only allow AWS Organizations to create service-linked roles for other AWS services. This service-linked role is present in all organizations and not just in a specific OU. SCPs are similar to IAM permission policies except that they don't grant any permissions.

The following options are incorrect because an SCP policy simply specifies the services and actions that users and roles can use in the accounts:

1. Use AWS Organizations to centrally manage all of your accounts. Group your accounts, which belongs to a specific business unit, to individual Organization Unit (OU). Create a Service Control Policy in the production account for each business unit which has a policy that allows access to the EC2 instances including a resource-level permission to terminate the instances that it owns. Provide the cross-account access and the SCP to the individual member accounts to tightly control who can terminate the EC2 instances.

2. Use AWS Control Tower to centrally manage all of your accounts. Group your accounts, which belongs to a specific business unit, to individual Organization Unit (OU). Create a Service Control Policy in the production account which has a policy that allows access to the EC2 instances including a resource-level permission to terminate the instances owned by a particular business unit. Provide the cross-account access and the SCP to the OUs, which will then be automatically inherited by its member accounts.

References:
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_ous.html
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-supported-iam-actions-resources.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

Check out this AWS Organizations Cheat Sheet:
https://tutorialsdojo.com/aws-organizations/

Service Control Policies (SCP) vs IAM Policies:
https://tutorialsdojo.com/service-control-policies-scp-vs-iam-policies/

Comparison of AWS Services Cheat Sheets:
https://tutorialsdojo.com/comparison-of-aws-services/

Question 2

A company provides big data services to enterprise clients around the globe. One of the clients has 60 TB of raw data from their on-premises Oracle data warehouse. The data is to be migrated to Amazon Redshift. However, the database receives minor updates on a daily basis while major updates are scheduled every end of the month. The migration process must be completed within approximately 30 days before the next major update on the Redshift database. The company can only allocate 50 Mbps of Internet connection for this activity to avoid impacting business operations.

Which of the following actions will satisfy the migration requirements of the company while keeping the costs low?

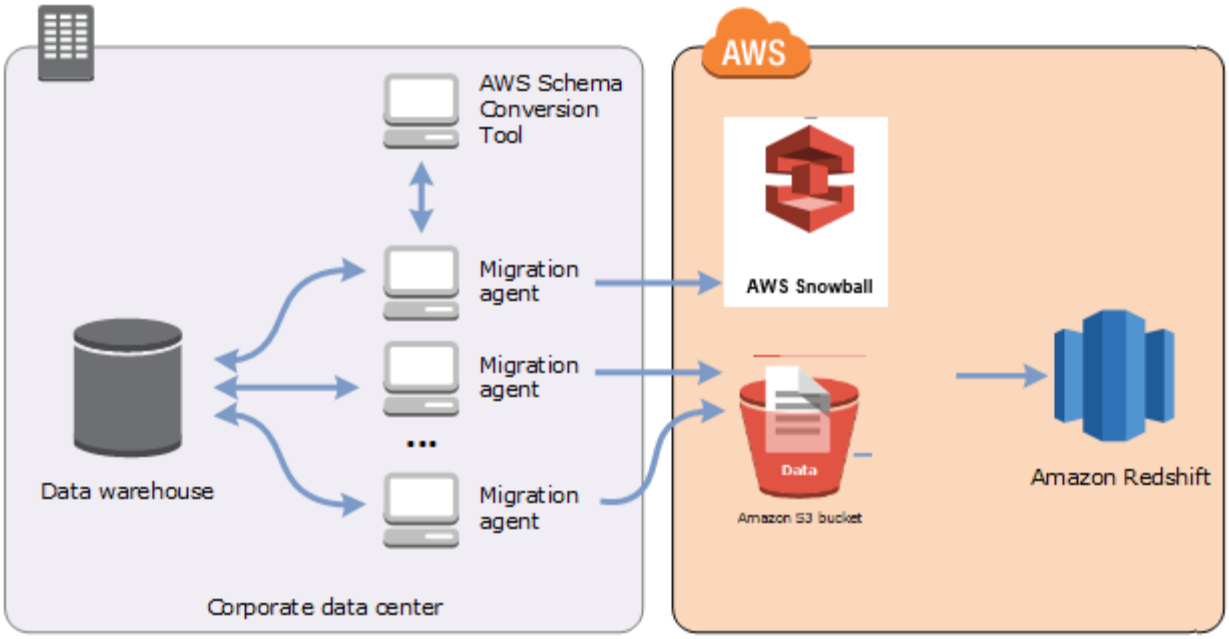
1. Create a new Oracle Database on Amazon RDS. Configure Site-to-Site VPN connection from the on-premises data center to the Amazon VPC. Configure replication from the on-premises database to Amazon RDS. Once replication is complete, create an AWS Schema Conversion Tool (SCT) project with AWS DMS task to migrate the Oracle database to Amazon Redshift. Monitor and verify if the data migration is complete before the cut-over.
2. Create an AWS Snowball Edge job using the AWS Snowball console. Export all data from the Oracle data warehouse to the Snowball Edge device. Once the Snowball device is returned to Amazon and data is imported to an S3 bucket, create an Oracle RDS instance to import the data. Create an AWS Schema Conversion Tool (SCT) project with AWS DMS task to migrate the Oracle database to Amazon Redshift. Copy the missing daily updates from Oracle in the data center to the RDS for Oracle database over the Internet. Monitor and verify if the data migration is complete before the cut-over.
3. Since you have a 30-day window for migration, configure VPN connectivity between AWS and the company's data center by provisioning a 1 Gbps AWS Direct Connect connection. Launch an Oracle Real Application Clusters (RAC) database on an EC2 instance and set it up to fetch and synchronize the data from the on-premises Oracle database. Once replication is complete, create an AWS DMS task on an AWS SCT project to migrate the Oracle database to Amazon Redshift. Monitor and verify if the data migration is complete before the cut-over.
4. Create an AWS Snowball import job to request for a Snowball Edge device. Use the AWS Schema Conversion Tool (SCT) to process the on-premises data warehouse and load it to the Snowball Edge device. Install the extraction agent on a separate on-premises server and register it with AWS SCT. Once the Snowball Edge imports data to the S3 bucket, use AWS SCT to migrate the data to Amazon Redshift. Configure a local task and AWS DMS task to replicate the ongoing updates to the data warehouse. Monitor and verify that the data migration is complete.

Correct Answer: 4

You can use an **AWS SCT** agent to extract data from your on-premises data warehouse and migrate it to Amazon Redshift. The agent extracts your data and uploads the data to either Amazon S3 or, for large-scale migrations, an AWS Snowball Edge device. You can then use AWS SCT to copy the data to Amazon Redshift.

Large-scale data migrations can include many terabytes of information and can be slowed by network performance and by the sheer amount of data that has to be moved. AWS Snowball Edge is an AWS service you can use to transfer data to the cloud at faster-than-network speeds using an AWS-owned appliance. An AWS Snowball Edge device can hold up to 100 TB of data. It uses 256-bit encryption and an industry-standard Trusted Platform Module (TPM) to ensure both security and full chain-of-custody for your data. AWS SCT works with AWS Snowball Edge devices.

When you use AWS SCT and an AWS Snowball Edge device, you migrate your data in two stages. First, you use the AWS SCT to process the data locally and then move that data to the AWS Snowball Edge device. You then send the device to AWS using the AWS Snowball Edge process, and then AWS automatically loads the data into an Amazon S3 bucket. Next, when the data is available on Amazon S3, you use AWS SCT to migrate the data to Amazon Redshift. Data extraction agents can work in the background while AWS SCT is closed. You manage your extraction agents by using AWS SCT. The extraction agents act as listeners. When they receive instructions from AWS SCT, they extract data from your data warehouse.



Therefore, the correct answer is: **Create an AWS Snowball import job to request for a Snowball Edge device. Use the AWS Schema Conversion Tool (SCT) to process the on-premises data warehouse and load it to the Snowball Edge device. Install the extraction agent on a separate on-premises server and register it with AWS SCT. Once the Snowball Edge imports data to the S3 bucket, use AWS SCT to migrate the data to Amazon Redshift. Configure a local task and AWS DMS task to replicate the ongoing updates to the data warehouse. Monitor and verify that the data migration is complete.**

The option that says: **Create a new Oracle Database on Amazon RDS. Configure Site-to-Site VPN connection from the on-premises data center to the Amazon VPC. Configure replication from the on-premises database to Amazon RDS. Once replication is complete, create an AWS Schema Conversion Tool (SCT) project with AWS DMS task to migrate the Oracle database to Amazon Redshift. Monitor and verify if the data migration is complete before the cut-over** is incorrect. Replicating 60 TB worth of data over the public Internet will take several days over the 30-day migration window. It is also stated in the scenario that the company can only allocate 50 Mbps of Internet connection for the migration activity. Sending the data over the Internet could potentially affect business operations.

The option that says: **Create an AWS Snowball Edge job using the AWS Snowball console. Export all data from the Oracle data warehouse to the Snowball Edge device. Once the Snowball device is returned to Amazon and data is imported to an S3 bucket, create an Oracle RDS instance to import the data. Create an AWS Schema Conversion Tool (SCT) project with AWS DMS task to migrate the Oracle database to Amazon Redshift. Copy the missing daily updates from Oracle in the data center to the RDS for Oracle database over the internet. Monitor and verify if the data migration is complete before the cut-over** is incorrect. You need to configure the data extraction agent first on your on-premises server. In addition, you don't need the data to be imported and exported via Amazon RDS. AWS DMS can directly migrate the data to Amazon Redshift.

The option that says: **Since you have a 30-day window for migration, configure VPN connectivity between AWS and the company's data center by provisioning a 1 Gbps AWS Direct Connect connection. Install Oracle database on an EC2 instance that is configured to synchronize with the on-premises Oracle database. Once replication is complete, create an AWS DMS task on an AWS SCT project to migrate the Oracle database to Amazon Redshift. Monitor and verify if the data migration is complete before the cut-over Since you have a 30-day window for migration, configure VPN connectivity between AWS and the company's data center by provisioning a 1 Gbps AWS Direct Connect connection. Launch an Oracle Real Application Clusters (RAC) database on an EC2 instance and set it up to fetch and synchronize the data from the on-premises Oracle database. Once replication is complete, create an AWS DMS task on an AWS SCT project to migrate the Oracle database to Amazon Redshift. Monitor and verify if the data migration is complete before the cut-over** is incorrect. Although this is possible, the company wants to keep the cost low. Using a Direct Connect connection for a one-time migration is not a cost-effective solution.

References:
https://aws.amazon.com/getting-started/hands-on/migrate-oracle-to-amazon-redshift/
https://docs.aws.amazon.com/SchemaConversionTool/latest/userguide/agents.dw.html
https://docs.aws.amazon.com/SchemaConversionTool/latest/userguide/agents.html

Tutorials Dojo's AWS Certified Solutions Architect Professional Exam Study Guide:
https://tutorialsdojo.com/aws-certified-solutions-architect-professional/

Click **here** for more **AWS Certified Solutions Architect Professional practice exam questions**.

More AWS reviewers can be found **here**:

Additional Training Materials: High-Quality Video Courses

There are a few top-rated AWS Certified Solutions Architect Professional video courses that you can check out as well, which can complement your exam preparations especially if you are the type of person who can learn better through visual courses instead of reading long whitepapers:

- AWS Certified Solutions Architect Professional by Adrian Cantrill

Based on user feedback, any of these video courses plus our **practice test course** and this study guide eBook were enough to pass this tough exam.

In general, what you should have learned from your review are the following:

- Features and use cases of the AWS services and how they integrate with each other
- AWS networking, security, billing and account management
- The AWS CLI, APIs and SDKs
- Automation, migration planning, and troubleshooting
- The best practices in designing solutions in the AWS Cloud
- Building CI/CD solutions using different platforms
- Resource management in a multi-account organization
- Multi-level security

All these factors are essentially the domains of your certification exam. It is because of this difficult hurdle that AWS Certified Solutions Architect Professionals are highly respected in the industry. They are capable of architecting ingenious solutions that solve customer problems in AWS. They are also constantly improving themselves by learning all the new services and features that AWS produces each year to make sure that they can provide the best solutions to their customers. Let this challenge be your motivation to dream high and strive further in your career as a Solutions Architect!

Final notes regarding your exam

The SA Professional exam questions always ask for highly available, fault tolerant, cost-effective and secure solutions. Be sure to understand the choices provided to you, and verify that they have accurate explanations. Some choices are very misleading such that they seem to be the most natural answer to the question, but actually contain incorrect information, such as the incorrect use of a service. Always place accuracy above all else.

When unsure of which options are correct in a multi-select question, try to eliminate some of the choices that you believe are false. This will help narrow down the feasible answers to that question. The same goes for multiple choice type questions. Be extra careful as well when selecting the number of answers you submit.

Since an SA Professional has responsibilities in creating large-scale architectures, be wary of the different ways AWS services can be integrated with one another. Common combinations include:

- AWS Security Hub, AWS Control Tower, AWS Organizations and AWS Resource Access Manager
- Amazon ECS Anywhere, Amazon ECS and AWS Fargate
- Amazon EKS Anywhere, Amazon EKS and AWS Fargate
- Lambda, API Gateway, Amazon SNS, and DynamoDB
- EC2, EBS/EFS/Elasticache, Auto Scaling, ELB, and SQS
- Amazon S3, Amazon Cloudfront, AWS WAF
- Amazon S3, Kinesis
- On-premises servers with Direct Connect/VPN/VPC Endpoints/Transit Gateway
- On-premises DNS servers and Amazon Route 53 with inbound/outbound DNS resolvers
- AWS Organizations, AWS IAM Identity Center, IAM roles, Config, Cloudformation and Service Catalog
- Mobile apps with Cognito, API Gateway, and DynamoDB
- CodeCommit, CodePipeline, CodeBuild, CodeDeploy
- ECR, ECS/Fargate and S3
- EMR + Spot Fleets/Combinations of different instance types for master node and task nodes
- Amazon Connect + Alexa + Amazon Lex

Lastly, be on the lookout for “key terms” that will help you realize the answer faster. Words such as millisecond latency, serverless, managed, highly available, most cost effective, fault tolerant, mobile, streaming, object storage, archival, polling, push notifications, etc are commonly seen in the exam. Time management is very important when taking AWS certification exams, so be sure to monitor the time you consume for each question.

Domain 1: Design Solutions for Organizational Complexity

Overview

The first domain of the AWS Certified Solutions Architect Professional exam evaluates your capability to implement solutions that allow different accounts and business units to operate in an AWS environment securely and reliably. As you become part of a larger organization, the number of users and stakeholders involved in your cloud architecture becomes more complex. You need to be able to segregate these user groups and business units according to their respective purpose and simplify their responsibilities within your AWS environments. Consequently, you also need to make sure that each group is given access to what they should and what they only need. This is to avoid any unnecessary access that could result in security leaks for the organization.

26% of questions in the actual SAP-C02 exam revolve around designing an organizational setup that involves the use of multiple AWS accounts, AWS Regions, VPCs, and billing configuration. This is the second biggest domain in the AWS Certified Solutions Architect Professional exam so expect to see a lot of questions that involve a variety of management and governance services in AWS. You have to focus on the following AWS services: AWS Organizations, AWS Control Tower, AWS Direct Connect, Amazon Route 53, AWS Security Hub, and others. Make sure that you know how Consolidated Billing works for multiple AWS accounts that are under an AWS Organization, especially the right configuration of enabling or disabling the Reserved Instance (RI) Sharing option for one or more AWS accounts.

This domain checks your know-how in doing these tasks:

- Architecting network connectivity strategies
- Prescribing security controls
- Designing reliable and resilient architectures.
- Designing a multi-account AWS environment
- Determining cost optimization and visibility strategies.

In this chapter, we will cover the related topics for organizational designs and strategies in AWS that will likely show up in your Solutions Architect Professional exam.

Managing of Multiple AWS Accounts in an Organization

As a company grows larger and the number of AWS users and resources increase, it becomes extraordinarily difficult to manage such a huge, complex ecosystem in just a single AWS account. Various teams will have different workloads, different stakeholders will have different objectives, and different environments will have different priorities. And much like in a software development lifecycle wherein you have a dedicated environment for development, for QA or staging, for UAT, and for production, AWS allows you to set up a similar structure at no cost through account organizations.

In an ideal scenario, you should be using one account per development lifecycle environment. You should also have a separate account for centrally storing logs, another separate account for facilitating security between the different accounts under your organization, and a separate account for billing and administration tasks. This is known as a **Landing Zone** setup.

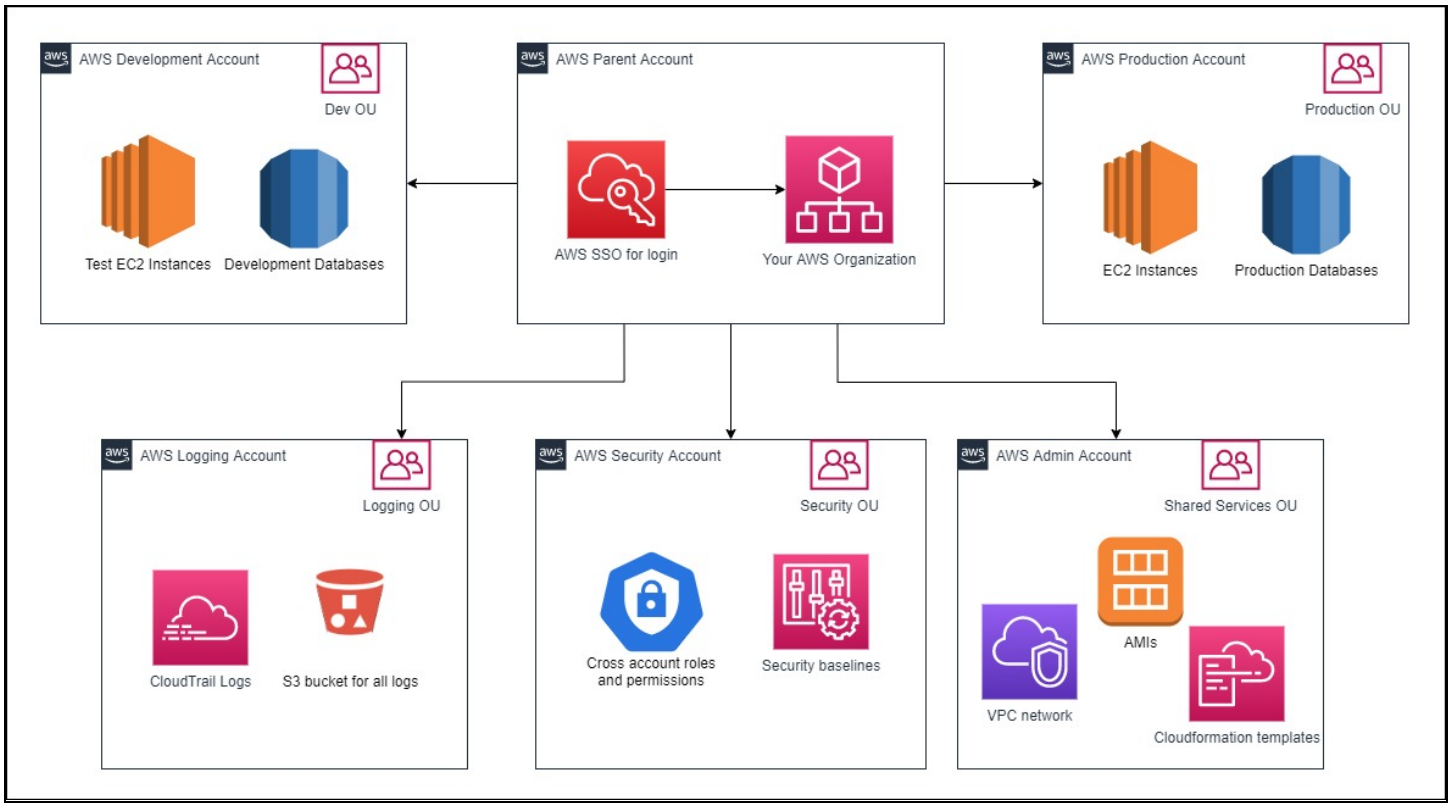


Figure: Example Setup of Landing Zone

Through this structure, you can experiment and develop faster since you have achieved a degree of isolation and flexibility. You can create an exact copy of an environment setup of another account and not have to worry about affecting the other account's processes while you define your own.

There are many ways to manage multiple accounts in AWS, but the most common and simplest method is by using AWS Organizations. This service allows you to govern and centrally manage your different AWS accounts under one account. It also provides many features for implementing security, cost management, and infrastructure compliance which we will also discuss along the way. The main components in AWS Organizations are the **master account** and the **member accounts**. As the name implies, the master account is where you'll be creating your organization. You can then invite other accounts to join your organization as members and manage them from your end. Take note that a member account can be a part of only one AWS Organization at a time. Once you have all your necessary accounts joined to the organization, you can start grouping them together into **Organization Units** (OUs), which will allow you to create a hierarchy. Making use of OUs will not only simplify account management, but also enable you to easily deploy security policies and shared resources across multiple accounts in an OU at the same time.

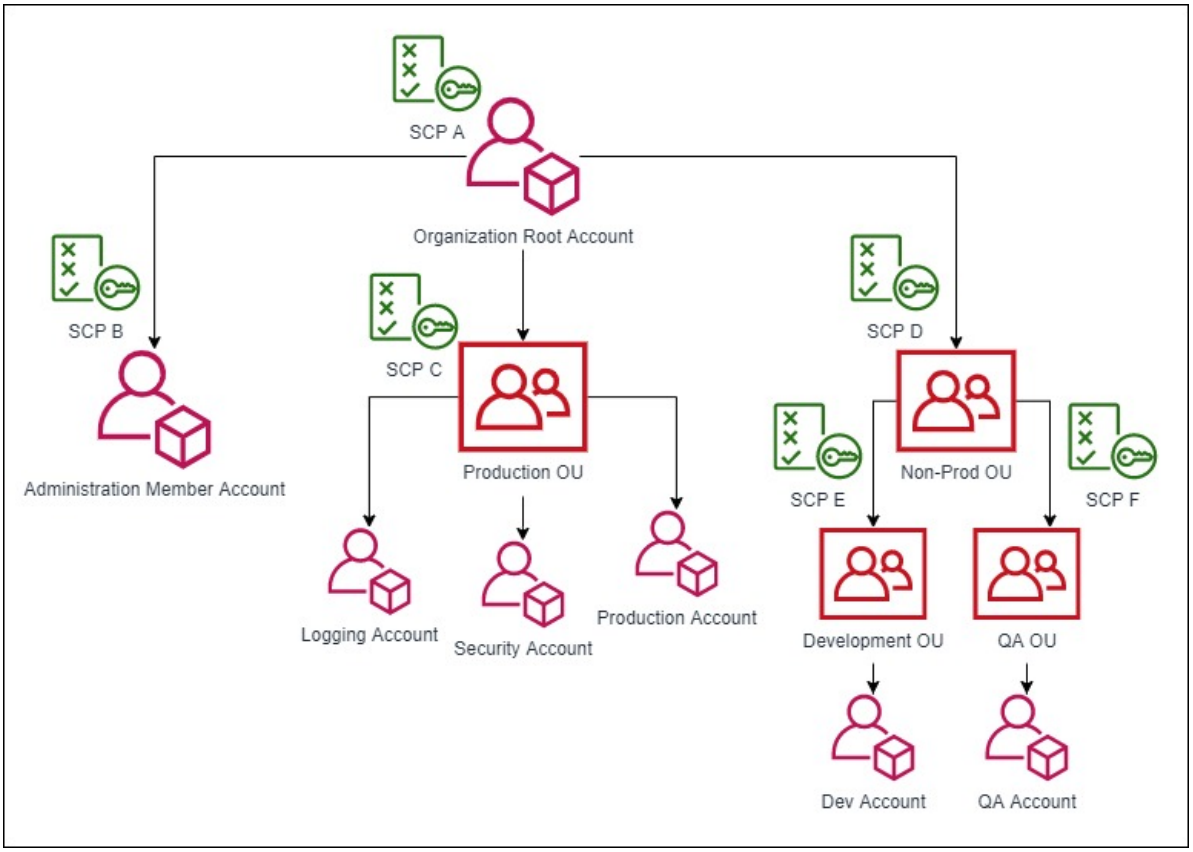


Figure: Example Structure of an AWS Organization with Multiple Accounts, OUs and SCPs

References:
https://aws.amazon.com/solutions/implementations/aws-landing-zone/
https://aws.amazon.com/blogs/mt/tag/aws-multi-account-management/
https://aws.amazon.com/organizations/

Security and Access Controls for a Multi-Account Structure

Since there can be hundreds of users and services interacting with one another in a multi-account structure, configuring security properly is vital in ensuring that you adhere to the principle of least privilege. There are different strategies that you can implement for multi-account security, depending on your business needs. There are also a few best practices that we will be discussing while you leverage these strategies. Sometimes, there can be questions in your exam that utilize more than one strategy for implementing security. The best way to know which to choose is to determine the assets involved in the accounts.

Cross-account roles

In a standalone account, IAM roles are a great way to provide access to your resources without having to create dedicated user credentials. They can also be attached to AWS services to allow interaction with one another in a secure manner. But what you might not have known is that you can also use IAM roles to provide access to users in another account. These are known as **cross-account roles**. Cross-account roles save you from the tedious task of creating and managing dedicated IAM Users in each account.

To get started with cross-account roles, you need to go to the IAM service and create a role meant for cross-account access. For convenience, imagine that you administer account A and the one requiring access to your environment is account B. During role creation, you input the Account ID of account B. At this point, you can also require users of account B to be MFA authenticated before they can assume the role.

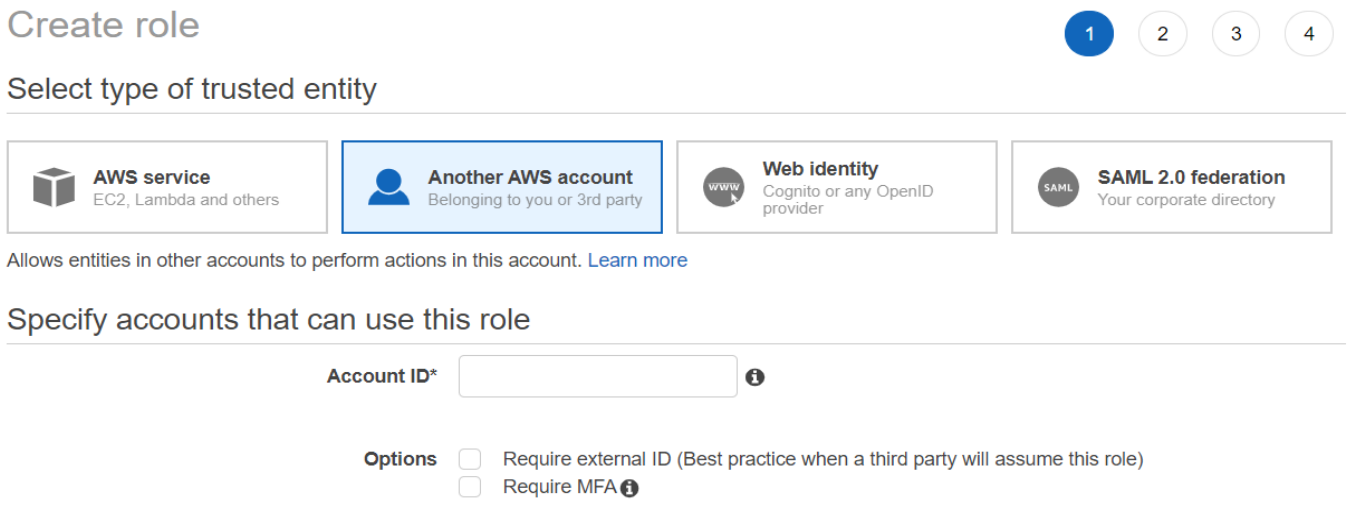


Figure: Create a cross-account role in IAM

On the final step, you provide the role with the necessary permissions to your account A via IAM Policies. Once this cross-account role has been created, IAM Users in account B can switch to or assume this role and gain

the permissions to do what they need to do in your account. To limit who can assume this role in account B, the admin of account B can create a policy that allows only specific users to assume the cross-account role.

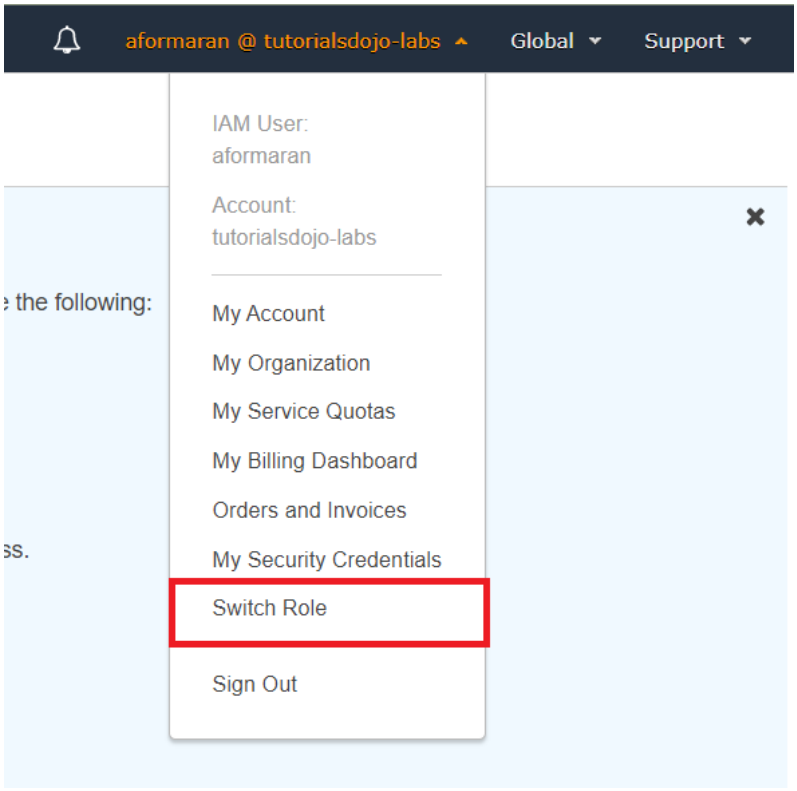


Figure: How to switch role in the AWS Console

AWS Organizations Service Control Policies

When you are the administrator of multiple accounts in an AWS Organization, you need to make sure that each account will function the way they are intended to. You can use Service Control Policies (SCPs) to restrict the actions that entities can perform in an account. SCPs are written in similar syntax as IAM Policies. SCPs apply account-wide, so it affects both IAM Users and IAM Roles managed by that account, but it does not affect resource-based policies/service-linked roles. Do keep in mind that you can only use SCPs if you have enabled **all features** in your AWS Organization.

SCPs can be attached to individual accounts and OUs. Attaching an SCP to an OU cascades the policy to member accounts of that OU. This means that any SCP you attach at the root of a hierarchy also applies to everything below it. An explicit deny overrules an explicit allow. An explicit allow overrules an implicit deny. By default, an SCP named *FullAWSAccess* is attached to every organization root, OU, and account. This default SCP allows all actions and all services.

i Solutions Architect Professional Exam Notes:

Remember that an SCP can only define what actions are available in an account. It does not delegate the actual permissions unlike IAM Policies. If you need to do something in your environment, you need to have the necessary policies attached first. In terms of permission hierarchy, the *deny* rule always takes precedence. This means that even if you have an IAM Policy that allows you to perform an action, if the SCP attached to that account implicitly or explicitly denies this action then you cannot perform it. Same goes with having an allow in the SCP but being implicitly or explicitly denied in the IAM Policy.

There are two common approaches to SCPs: *whitelisting* and *blacklisting*.

- **Blacklisting** applies the FullAWSAccess SCP, which doesn't filter out any AWS service APIs, then filters out specific APIs by blacklisting them in subsequent SCPs attached to OUs at various points in your organization's structure.
- **Whitelisting** is about modifying your SCPs to be more restrictive in allow permissions. All other actions are therefore implicitly denied. Users and roles in the affected accounts can then exercise only that level of access, even if their IAM policies allow all actions.

Shared Directory Services

If you are using AWS Managed Microsoft AD Directory, you can share this directory to other VPCs and AWS accounts within the same Region. This makes it convenient to manage different directory-aware services such as EC2 instances or local Windows servers across different VPCs and accounts. To share your directory, you first need to configure the network between the VPCs that will be communicating. You have multiple options on how to do this, such as VPC Peering, Direct Connect, Transit Gateway, VPN and so on. Once you have configured your route tables and security groups, you have two ways to share your directory:

1) If you are in an AWS Organization, you only need to select the accounts that you want to share the directory to. Your AWS Organization must have all features enabled and the directory must be in the organization's master account for this to work.
2) If you are sharing the directory to an external account, you need to initiate a handshake request and the recipient needs to accept your request.

If you have an external AD that you want to use as an authentication method for your AWS account (which is common in a hybrid environment), you can do so by using **SAML Federation**. Federation is the practice of establishing trust between a system acting as an identity provider and other systems, often called service providers, that accept authentication tokens from that identity provider. You have options on how to implement federation in AWS:

1) You may use AWS IAM Identity Center which works with your identity provider to handle access for your federated users and roles.

2) You may use IAM identity providers instead of creating IAM users in your AWS account. IAM supports providers that are compatible with OpenID Connect (OIDC) or SAML 2.0. OIDC calls the *AssumeRoleWithWebIdentity* API to trade the authentication token you get from those IdPs for AWS temporary security credentials. SAML calls AWS STS *AssumeRoleWithSAML* API, passing the ARN of the SAML provider, the ARN of the role to assume, and the SAML assertion from IdP.
3) You may use third-party SAML solution providers and manually configure a solution to work with AWS federation.

References:
https://d0.awsstatic.com/aws-answers/AWS_Multi_Account_Security_Strategy.pdf
https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_type-auth.html
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_directory_sharing.html