Jayendra's Cloud Certification Blog

■ ■ ■

□ MENU

AWS Certified Solutions Architect – Professional (SAP-C02) Exam Learning Path

DECEMBER 21, 2022 ~ LAST UPDATED ON : OCTOBER 4, 2023 ~ JAYENDRAPATIL

Table of Contents [hide]

AWS Certified Solutions Architect – Professional (SAP-C02) Exam Learning Path

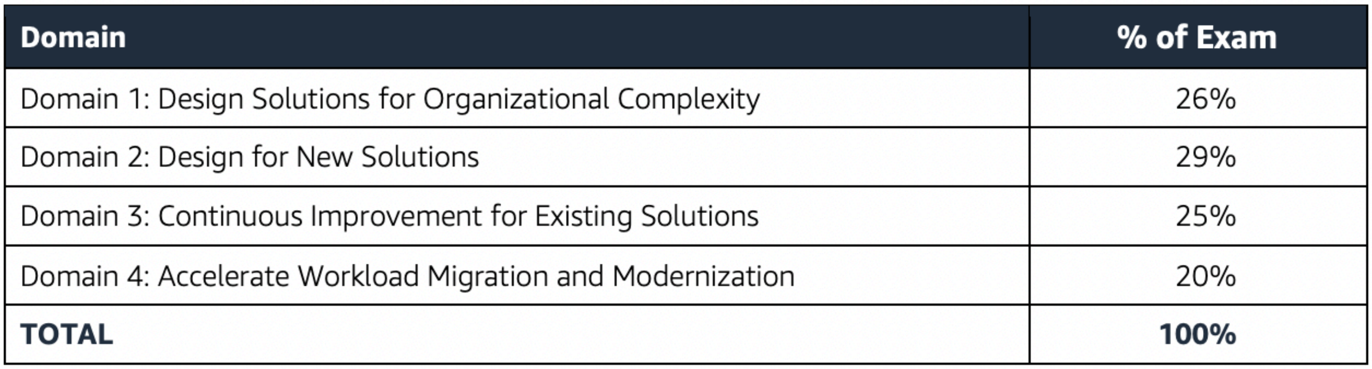
- AWS Certified Solutions Architect – Professional (SAP-C02) exam is the upgraded pattern of the previous Solution Architect – Professional SAP-C01 exam and was released in Nov. 2022.
- SAP-C02 is quite similar to SAP-C01 but has included some new services.

AWS Certified Solutions Architect – Professional (SAP-C02) Exam Content

- AWS Certified Solutions Architect – Professional (SAP-C02) exam validates the ability to complete tasks within the scope of the AWS Well-Architected Framework
  - Design for organizational complexity
  - Design for new solutions

- Continuously improve existing solutions
- Accelerate workload migration and modernization

Refer to AWS Certified Solutions Architect – Professional Exam Guide



Domain	% of Exam
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%
TOTAL	**100%**

AWS Certified Solutions Architect – Professional (SAP-C02) Exam Resources

- Online Courses
  - Stephane Maarek – Ultimate AWS Certified Solutions Architect Professional
  - Adrian Cantrill – AWS Certified Solutions Architect – Professional
  - Adrian Cantrill – AWS Professional Bundle
  - DolfinEd AWS Certified Solutions Architect Professional (E-Study Guide & Lab Guides Included)
  - Whizlabs – AWS Solutions Architect Professional Online Course
  - Coursera – AWS Cloud Solutions Architect Professional Certificate
- Practice tests
  - Braincert AWS Certified Solutions Architect – Professional Practice Exams
  - Stephane Maarek – Practice Exam AWS Certified Solutions Architect Professional
  - Whizlabs – AWS Solutions Architect Professional Certification Exam Practice Tests

AWS Certified Solutions Architect – Professional (SAP-C02) Exam Summary

- Professional exams are tough, lengthy, and tiresome. Most of the questions and answers options have a lot of prose and a lot of reading that needs to be done, so be sure you are prepared and manage your time well.
- Each solution involves multiple AWS services.
- AWS Certified Solutions Architect – Professional (SAP-C02) exam has 65 questions to be solved in 170 minutes.
- SAP-C02 exam includes two types of questions, multiple-choice and multiple-response.
- SAP-C02 has a scaled score between 100 and 1,000. The scaled score needed to pass the exam is 750.
- Each question mainly touches multiple AWS services.
- Associate exams currently cost $ 300 + tax.
- You can get an additional 30 minutes if English is your second language by requesting Exam Accommodations. It might not be needed for Associate exams but is helpful for Professional and Specialty ones.
- As always, mark the questions for review and move on and come back to them after you are done with all.
- As always, having a rough architecture or mental picture of the setup helps focus on the areas that you need to improve. Trust me, you will be able to eliminate 2 answers for sure and then need to focus on only the other two. Read the other 2 answers to check the difference area and that would help you reach the right answer or at least have a 50% chance of getting it right.
- AWS exams can be taken either remotely or online, I prefer to take them online as it provides a lot of flexibility. Just make sure you have a proper place to take the exam with no disturbance and nothing around you.
- Also, if you are taking the AWS Online exam for the first time try to join at least 30 minutes before the actual time as I have had issues with both PSI and Pearson with long wait times.

AWS Certified Solutions Architect – Professional (SAP-C02) Exam Topics

AWS Certified Solutions Architect – Professional (SAP-C02) focuses a lot on concepts and services related to Architecture & Design, Scalability, High Availability, Disaster Recovery, Migration, Security, and Cost Control.

Storage

- Simple Storage Service – S3
    - S3 Permissions & S3 Data Protection
        - S3 bucket policies to control access to VPC Endpoints and provide cross-account access.
    - S3 Storage Classes & Lifecycle policies
        - covers S3 Standard, Infrequent access, intelligent tier, and Glacier for archival and object transitions & deletions for cost management.
    - S3 Performance
        - S3 Transfer Acceleration can be used for fast, easy, and secure transfers of files over long distances between the client and an S3 bucket.
        - S3 Multi-part upload can help improve upload performance and resiliency.
        - S3 can be used for static website hosting and integrates with CloudFront to improve performance and latency.
    - S3 Security
        - S3 supports encryption using KMS
        - S3 supports Object Lock and Glacier supports Vault lock to prevent the deletion of objects, especially required for compliance requirements.
        - CORS allows client web applications loaded in one domain access to the restricted resources to be requested from another domain.
    - S3 supports the same and cross-region replication for disaster recovery.

  - S3 Access Logs enable tracking access requests to an S3 bucket.
  - supports S3 Select feature to query selective data from a single object.
  - S3 Event Notification enables notifications to be triggered when certain events happen in the bucket and support SNS, SQS, and Lambda as the destination.
- Elastic Block Store
  - EBS Backup using snapshots for HA and Disaster recovery
  - Data Lifecycle Manager can be used to automate the creation, retention, and deletion of snapshots taken to back up the EBS volumes.
- Storage Gateway
  - supports File Gateways and Volume Gateways

  - File Gateways provides a file interface into S3 and allows storing and retrieving of objects in S3 using industry-standard file protocols such as NFS and SMB.
- Elastic File System – EFS
  - provides fully managed, scalable, serverless, shared, and cost-optimized file storage for use with AWS and on-premises resources.
  - supports cross-region replication for disaster recovery
  - supports storage classes like S3
  - supports only Linux-based AMIs

- AWS Transfer Family
  - provides a secure transfer service (FTP, SFTP, FTPs) that helps transfer files into and out of AWS storage services.
  - supports transferring data from or to S3 and EFS.
- FSx for Lustre
  - managed, cost-effective service to launch and run the HPC high-performance Lustre file system.
- Understand different use cases for S3 vs EBS vs EFS

Database

- DynamoDB
  - provides a fully managed NoSQL database service with fast and predictable performance with seamless scalability.
  - supports following capacity modes
    - Provisioned – the maximum amount of capacity in terms of reads/writes per second that an application can consume from a table or index
    - On-demand – serves thousands of requests per second without capacity planning.
  - DynamoDB Auto Scaling can be used to handle peaks or bursts.
  - DynamoDB Streams for tracking changes
  - TTL to expire objects automatically and cost-effectively.
  - Global tables for multi-master, active-active inter-region storage needs.

    - Global tables do not support strong global consistency
    - DynamoDB Accelerator – DAX for seamless caching to reduce the load on DynamoDB for read-heavy requirements.
- RDS
    - supports cross-region read replicas ideal for disaster recovery with low RTO and RPO.
    - provides RDS proxy for effective database connection polling
    - RDS Multi-AZ vs Read Replicas
- Aurora
    - fully managed, MySQL- and PostgreSQL-compatible, relational database engine
    - Aurora Serverless provides on-demand, autoscaling configuration.

  - Aurora Global Database consists of one primary AWS Region where the data is mastered, and up to five read-only, secondary AWS Regions.
- Understand DynamoDB Global Tables vs Aurora Global Databases

- DocumentDB as a replacement for MongoDB
- Keyspaces as a replacement for Cassandra

Data Migration & Transfer

- Cloud Migration Services
  - Cloud Migration (*hint: make sure you understand the difference between rehost, replatform, and rearchitect*)
  - Server Migration Service helps to migrate servers and applications.
  - Database Migration Service
    - enables quick and secure data migration with minimal to zero downtime
    - supports Full and Change Data Capture – CDC migration to support continuous replication for zero downtime migration.

    - homogeneous migrations such as Oracle to Oracle, as well as heterogeneous migrations (using SCT) between different database platforms, such as Oracle or Microsoft SQL Server to Aurora.
- Snow Family
    - Ideal for one-time huge data transfers usually for use cases with limited bandwidth from on-premises to AWS.
- Understand use cases for data transfer using VPN (quick, slow, uses the Internet), Direct Connect (time to set up, private, recurring transfers), Snow Family (moderate time, private, one-time huge data transfers)

- Application Discovery Service
  - Agent ones can be used for hyper-v and physical services
  - Agentless can be used for VMware but does not track processes

- AWS Migration Hub provides a central location to collect server and application inventory data for the assessment, planning, and tracking of migrations to AWS and also helps accelerate application modernization following migration.

Networking & Content Delivery

- VPC – Virtual Private Cloud
  - Security Groups, NACLs
    - NACLs are stateless and need to open ephemeral ports for response traffic.
  - VPC Gateway Endpoints to provide access to S3 and DynamoDB
  - VPC Interface Endpoints or PrivateLink provide access to a variety of services like SQS, Kinesis, or Private APIs exposed through NLB.
  - VPC Peering to enable communication between VPCs within the same or different regions.
  - VPC Peering does not support overlapping CIDRs while PrivateLink does as only the endpoint is exposed.
  - VPC Flow Logs to track network traffic
  - NAT Gateway provides managed NAT service that provides better availability, higher bandwidth, and requires less administrative effort.
- Route 53
  - Routing Policies
    - focus on Weighted, Latency, and failover routing policies
    - failover routing provides active-passive configuration for disaster recovery while the others are active-active configurations.

■ ■ ■

    - Route 53 Resolver
        - Outbound endpoint for AWS -> On-premises DNS query resolution
        - Inbound endpoint for On-premises DNS query resolution
- CloudFront
    - fully managed, fast CDN service that speeds up the distribution of static, dynamic web or streaming content to end-users.

    - supports Origin Groups for multiple origins providing failover capability with primary and secondary origins.

  - does not support Auto Scaling as an origin
  - supports Geo-restriction
  - supports Lambda@Edge and Cloud Functions to execute code closer to the user.
  - Lambda@Edge can be used for quick auth checks, and redirect users based on request data.
  - Security can be enhanced by whitelisting CloudFront IPs or adding a custom header in CloudFront and verifying it in ALB.
- API Gateway
  - supports throttling, caching and helps define usage plans with API keys to identify clients
  - provides regional and edge-optimized endpoint types
  - supports CORS for cross-domain calls.
  - supports authentication mechanisms, such as AWS IAM policies, Lambda authorizer functions, and Amazon Cognito user pools.
  - provide serverless architecture with Lambda.

- Load Balancer – ELB, ALB and NLB
  - ELB with Auto Scaling to provide scalable and highly available applications
  - Understand ALB vs NLB and their use cases.

- Global Accelerator
  - optimizes the path to applications to keep packet loss, jitter, and latency consistently low.
  - helps improve the performance of the applications by lowering first-byte latency

  - provides 2 static IP addresses
  - does not preserve the client’s IP address with NLB

- Transit Gateway or Transit VPC
  - is a network transit hub that can be used to interconnect VPCs and on-premises networks via Direct Connect or VPN.
  - Transit Gateway is regional and Transit Gateway Peering needs to be configured to peer regional Transit gateways.

- Placement Groups
  - Cluster placement group with Enhanced Networking for HPC
  - Spread placement group for fault tolerance and high availability.
- Direct Connect & VPN
  - provide on-premises to AWS connectivity
  - Understand Direct Connect vs VPN
  - VPN can provide a cost-effective, quick failover for Direct Connect.
  - VPN over Direct Connect provides a secure dedicated connection and requires a public virtual interface.
  - Direct Connect Gateway is a global network device that helps establish connectivity that spans VPCs spread across multiple AWS Regions with a single Direct Connect connection.

Security, Identity & Compliance

- AWS Identity and Access Management
  - IAM Roles and use cases
  - IAM Web Identity & Federation
  - IAM Best Practices
- AWS Shield & Shield Advanced
  - for DDoS protection and integrates with Route 53, CloudFront, ALB, and Global Accelerator.
- AWS WAF
  - protects from common attack techniques like SQL injection and XSS, Conditions based include IP addresses, HTTP headers, HTTP body, and URI strings.
  - integrates with CloudFront, ALB, and API Gateway.
  - supports Web ACLs and can block traffic based on IPs, Rate limits, and specific countries as well.
- ACM – AWS Certificate Manager
  - helps easily provision, manage, and deploy public and private SSL/TLS certificates
  - is regional and you need to request certificates in all regions and associate individually in all regions.
  - does not provide certificates for EC2 instances.
- AWS KMS – Key Management Service
  - managed encryption service that allows the creation and control of encryption keys to enable data encryption.
  - KMS Multi-region keys
    - are AWS KMS keys in different AWS Regions that can be used interchangeably – as though having the same key in multiple Regions.
    - are not global and each multi-region key needs to be replicated and managed independently.
- Secrets Manager
  - helps protect secrets needed to access applications, services, and IT resources.
  - Secrets Manager vs SSM Parameter Store.

    - Secrets Manager supports random generation and automatic rotation of secrets, which is not provided by SSM Parameter Store.
    - Costs more than SSM Parameter Store.
- Amazon Macie is a data security and data privacy service that uses ML and pattern matching to discover and protect sensitive data in S3.
- AWS Security Hub is a cloud security posture management service that performs security best practice checks, aggregates alerts, and enables automated remediation.

Compute

- EC2
  - EC2 Instance Types & EC2 Instance Purchase Types
- Auto Scaling provides the ability to ensure a correct number of EC2 instances are always running to handle the load of the application
- Lambda
  - offers Serverless computing
  - Lambda running in VPC requires NAT Gateway to communicate with external public services
  - Lambda CPU can be increased by increasing memory only.
  - helps define reserved concurrency limits to reduce the impact
  - Lambda Alias now supports canary deployments
  - Lambda supports docker containers
  - Reserved Concurrency guarantees the maximum number of concurrent instances for the function
  - Provisioned Concurrency provides greater control over the performance of serverless applications and helps keep functions initialized and hyper-ready to respond in double-digit milliseconds.
  - Lambda Best Practices esp. handling the database connection code.
- Step Functions helps developers use AWS services to build distributed applications, automate processes, orchestrate microservices, and create data and machine learning (ML) pipelines.
- ECS – Elastic Container Service
  - container management service that supports Docker containers
  - supports two launch types
    - EC2 and
    - Fargate which provides the serverless capability
  - For least privilege, the role should be assigned to the Task.
  - `awsvpc` network mode gives ECS tasks the same networking properties as EC2 instances.

Disaster Recovery

- Disaster Recovery whitepaper, although outdated, make sure you understand the differences and implementation for each type esp. pilot light, warm standby w.r.t RTO, and RPO.
- Compute

  - Make components available in an alternate region,
  - Backup and Restore using either snapshots or AMIs that can be restored.
  - Use minimal low-scale capacity running which can be scaled once the failover happens
  - Use fully running compute in active-active confirmation with health checks.
  - CloudFormation to create, and scale infra as needed
- Storage
  - S3 and EFS support cross-region replication
  - DynamoDB supports Global tables for multi-master, active-active inter-region storage needs.
  - Aurora Global Database provides cross-region read replicas and failover capabilities.
  - RDS supports cross-region read replicas which can be promoted to master in case of a disaster. This can be done using Route 53, CloudWatch, and lambda functions.
- Network
  - Route 53 failover routing with health checks to failover across regions.
  - CloudFront Origin Groups support primary and secondary endpoints with failover.

Management & Governance tools

- AWS Organizations
  - Difference between Service Control Policies and IAM Policies
  - SCP provides the maximum permission that a user can have, however, the user still needs to be explicitly given IAM policy.
- Systems Manager
  - AWS Systems Manager and its various services like parameter store, patch manager
  - Parameter Store provides secure, scalable, centralized, hierarchical storage for configuration data and secret management. Does not support secrets rotation. Use Secrets Manager instead
  - Session Manager provides secure and auditable instance management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys.
  - Patch Manager helps automate the process of patching managed instances with both security-related and other types of updates.

- CloudWatch
  - CloudWatch logs
  - CloudWatch Subscription Filters and their integration with other services.
  - CloudWatch Events or EventBridge
- CloudTrail
  - for audit and governance
  - With Organizations, the trail can be configured to log CloudTrail from all accounts to a central account.
- CloudFormation
  - Handle disaster Recovery by automating the infra to replicate the environment across regions.
  - Deletion Policy to prevent, retain, or backup RDS, EBS Volumes
  - Stack policy can prevent stack resources from being unintentionally updated or deleted during a stack update. Stack Policy only applies for Stack updates and not stack deletion.
  - StackSets helps to create, update, or delete stacks across multiple accounts and Regions with a single operation.
- Control Tower
  - to setup, govern, and secure a multi-account environment
  - strongly recommended guardrails cover EBS encryption
- Service Catalog
  - allows organizations to create and manage catalogues of IT services that are approved for use on AWS with minimal permissions.
- Trusted Advisor
  - helps with cost optimization and service limits in addition to security, performance and fault tolerance.
- Compute Optimizer recommends optimal AWS resources for the workloads to reduce costs and improve performance by using machine learning to analyze historical utilization metrics.
- AWS Budgets to see usage-to-date and current estimated charges from AWS, set limits and provide alerts or notifications.
- Cost Allocation Tags can be used to organize AWS resources, and cost allocation tags to track the AWS costs on a detailed level.
- Cost Explorer helps visualize, understand, manage and forecast the AWS costs and usage over time.
- Amazon WorkSpaces provides a virtual workspace for varied worker types, especially hybrid and remote workers.

Integration Tools

- SQS in terms of loose coupling and scaling.
  - Difference between SQS Standard and FIFO esp. with throughput and order

  - SQS supports dead letter queues
- CloudWatch integration with SNS and Lambda for notifications.

Analytics

- Kinesis
  - for real-time data ingestion and analytics.
  - Difference between Kinesis Data Streams and Kinesis Firehose
  - Kinesis Data Firehose integrates with S3, Redshift, and OpenSearch.
- OpenSearch (Elasticsearch) provides a managed search solution.
- Amazon Timestream is a fast, scalable, and serverless time-series database service that makes it easier to store and analyze trillions of events per day.
- Amazon Connect is an omnichannel cloud contact center.
- Amazon Pinpoint is a flexible, scalable marketing communications service that helps connects customers over email, SMS, push notifications or voice
- Amazon Rekognition offers pre-trained and customizable computer vision capabilities to extract information and insights from images and videos
- Amazon Transcribe to Voice to Text conversion

Architecture & Design Flows

- Disaster Recovery
- Multi-Region Compute and Security
- Multi-Region Storage and Data
  - S3, EFS cross-region replication
  - DynamoDB Global Tables – Multi-Master
  - Aurora Global Database, RDS – Cross-region read replica
- WAF/AWS Shield -> CloudFront -> S3 with WAF-managed Amazon IP reputation rule group or country-specific rule
- Kinesis Data Streams -> Kinesis Data Firehose -> ES/S3/Redshift
- Kinesis Data Agent -> Kinesis Data Firehose -> ES/S3/Redshift
- CloudWatch Logs -> (Subscription Filter) -> Kinesis Data Streams
- Quota Monitor & Solution Definition
- Enhance Security with CloudFront + WAF
- S3 Event Notification -> SNS/SQS/Lambda
- Analysing SES data – SES Logs -> Kinesis Data Firehose -> S3 -> Athena
- Centralized Networking using Network Firewall
- Multi-Account Strategy
  - Identity account for role and users
  - Infosec account
  - Logging account

- Direct Connect with VPN – Low latency, Secure Connectivity
- Detect/Remediate Security/Compliance Rules with AWS Config -> Systems Manager Automation/Lambda to remediate findings
- Real-time Leadership Dashboard with ElastiCache
- RDS/S3 -> Glue Crawler -> Glue Catalog -> Athena
- Lambda@Edge + CloudFront to dynamically route requests
- AppSync Mobile Architecture
- Centralized Logging
- Multi-region API Gateway with CloudFront
- Accessing VPC Endpoints from On-premises
- Migrate Oracle to Amazon Redshift
- Monitor IAM Root User Activity
- Migrate an Oracle database to Aurora MySQL using AWS DMS and SCT
- Archive DynamoDB data to S3 using TTL
- Encrypt Existing and New EBS Volumes
- Building Fault-Tolerant Applications on AWS

On the Exam Day

- Make sure you are relaxed and get some good night's sleep. The exam is not tough if you are well-prepared.
- If you are taking the AWS Online exam
  - Try to join at least 30 minutes before the actual time as I have had issues with both PSI and Pearson with long wait times.
  - The online verification process does take some time and usually, there are glitches.
  - Remember, you would not be allowed to take the take if you are late by more than 30 minutes.
  - Make sure you have your desk clear, no hand-watches, or external monitors, keep your phones away, and nobody can enter the room.

Finally, All the Best 🙂

POSTED IN AWS, LEARNING PATH

CERTIFICATION PROFESSIONAL SAP-C02 SOLUTIONS ARCHITECT

SOLUTIONS ARCHITECT - PROFESSIONAL

...

< PREVIOUS
AWS Secrets Manager vs Systems Manager Parameter Store

NEXT >
AWS VPC Peering

Follow

DISCLOSURE

This post may contain affiliate links, meaning when you click the links and make a purchase, we receive a commission.

Recent Posts

AWS Certified Machine Learning -Specialty (MLS-C01) Exam Learning Path

AWS SageMaker Built-in Algorithms Summary

AWS Machine Learning Services – Cheat Sheet

AWS SageMaker

Machine Learning Concepts – Cheat Sheet

Categories

Select Category