Certified Data Engineer -
Domain 1: Data Ingestion and Transformation Task Statement 1.1: Perform data ingestion. Knowledge of: • Throughput and latency characteristics for AWS services that ingest data • Data ingestion patterns (for example, frequency and data history) • Streaming data ingestion • Batch data ingestion (for example, scheduled ingestion, event-driven ingestion) • Replayability of data ingestion pipelines • Stateful and stateless data transactions Skills in: • Reading data from streaming sources (for example, Amazon Kinesis, Amazon Managed Streaming for Apache Kafka [Amazon MSK], Amazon DynamoDB Streams, AWS Database Migration Service [AWS DMS], AWS Glue, Amazon Redshift) • Reading data from batch sources (for example, Amazon S3, AWS Glue, Amazon EMR, AWS DMS, Amazon Redshift, AWS Lambda, Amazon AppFlow) • Implementing appropriate configuration options for batch ingestion • Consuming data APIs
Setting up schedulers by using Amazon EventBridge, Apache Airflow, or time-based schedules for jobs and crawlers • Setting up event triggers (for example, Amazon S3 Event Notifications, EventBridge) • Calling a Lambda function from Amazon Kinesis • Creating allowlists for IP addresses to allow connections to data sources • Implementing throttling and overcoming rate limits (for example, DynamoDB, Amazon RDS, Kinesis) • Managing fan-in and fan-out for streaming data distribution
Task Statement 1.2: Transform and process data. Knowledge of: • Creation of ETL pipelines based on business requirements • Volume, velocity, and variety of data (for example, structured data, unstructured data) • Cloud computing and distributed computing • How to use Apache Spark to process data • Intermediate data staging locations Skills in: • Optimizing container usage for performance needs (for example, Amazon Elastic Kubernetes Service [Amazon EKS], Amazon Elastic Container Service [Amazon ECS]) • Connecting to different data sources (for example, Java Database Connectivity [JDBC], Open Database Connectivity [ODBC]) • Integrating data from multiple sources • Optimizing costs while processing data • Implementing data transformation services based on requirements (for example, Amazon EMR, AWS Glue, Lambda, Amazon Redshift) • Transforming data between formats (for example, from .csv to Apache Parquet) • Troubleshooting and debugging common transformation failures and performance issues • Creating data APIs to make data available to other systems by using AWS services
Task Statement 1.3: Orchestrate data pipelines. Knowledge of: • How to integrate various AWS services to create ETL pipelines • Event-driven architecture • How to configure AWS services for data pipelines based on schedules or dependencies • Serverless workflows Skills in: • Using orchestration services to build workflows for data ETL pipelines (for example, Lambda, EventBridge, Amazon Managed Workflows for Apache Airflow [Amazon MWAA], AWS Step Functions, AWS Glue workflows) • Building data pipelines for performance, availability, scalability, resiliency, and fault tolerance • Implementing and maintaining serverless workflows • Using notification services to send alerts (for example, Amazon Simple Notification Service [Amazon SNS], Amazon Simple Queue Service [Amazon SQS])
Task Statement 1.4: Apply programming concepts. Knowledge of: • Continuous integration and continuous delivery (CI/CD) (implementation, testing, and deployment of data pipelines) • SQL queries (for data source queries and data transformations) • Infrastructure as code (IaC) for repeatable deployments (for example, AWS Cloud Development Kit [AWS CDK], AWS CloudFormation) • Distributed computing • Data structures and algorithms (for example, graph data structures and tree data structures) • SQL query optimization
Skills in: • Optimizing code to reduce runtime for data ingestion and transformation • Configuring Lambda functions to meet concurrency and performance needs • Performing SQL queries to transform data (for example, Amazon Redshift stored procedures) • Structuring SQL queries to meet data pipeline requirements • Using Git commands to

perform actions such as creating, updating, cloning, and branching repositories • Using the AWS Serverless Application Model (AWS SAM) to package and deploy serverless data pipelines (for example, Lambda functions, Step Functions, DynamoDB tables) • Using and mounting storage volumes from within Lambda functions Domain 2: Data Store Management Task Statement 2.1: Choose a data store. Knowledge of: • Storage platforms and their characteristics • Storage services and configurations for specific performance demands • Data storage formats (for example, .csv, .txt, Parquet) • How to align data storage with data migration requirements • How to determine the appropriate storage solution for specific access patterns • How to manage locks to prevent access to data (for example, Amazon Redshift, Amazon RDS) Skills in: • Implementing the appropriate storage services for specific cost and performance requirements (for example, Amazon Redshift, Amazon EMR, AWS Lake Formation, Amazon RDS, DynamoDB, Amazon Kinesis Data Streams, Amazon MSK) • Configuring the appropriate storage services for specific access patterns and requirements (for example, Amazon Redshift, Amazon EMR, Lake Formation, Amazon RDS, DynamoDB)
Applying storage services to appropriate use cases (for example, Amazon S3) • Integrating migration tools into data processing systems (for example, AWS Transfer Family) • Implementing data migration or remote access methods (for example, Amazon Redshift federated queries, Amazon Redshift materialized views, Amazon Redshift Spectrum) Task Statement 2.2: Understand data cataloging systems. Knowledge of: • How to create a data catalog • Data classification based on requirements • Components of metadata and data catalogs Skills in: • Using data catalogs to consume data from the data's source • Building and referencing a data catalog (for example, AWS Glue Data Catalog, Apache Hive metastore) • Discovering schemas and using AWS Glue crawlers to populate data catalogs • Synchronizing partitions with a data catalog • Creating new source or target connections for cataloging (for example, AWS Glue) Task Statement 2.3: Manage the lifecycle of data. Knowledge of: • Appropriate storage solutions to address hot and cold data requirements • How to optimize the cost of storage based on the data lifecycle • How to delete data to meet business and legal requirements • Data retention policies and archiving strategies • How to protect data with appropriate resiliency and availability
Skills in: • Performing load and unload operations to move data between Amazon S3 and Amazon Redshift • Managing S3 Lifecycle policies to change the storage tier of S3 data • Expiring data when it reaches a specific age by using S3 Lifecycle policies • Managing S3 versioning and DynamoDB TTL Task Statement 2.4: Design data models and schema evolution. Knowledge of: • Data modeling concepts • How to ensure accuracy and trustworthiness of data by using data lineage • Best practices for indexing, partitioning strategies, compression, and other data optimization techniques • How to model structured, semi-structured, and unstructured data • Schema evolution techniques Skills in: • Designing schemas for Amazon Redshift, DynamoDB, and Lake Formation • Addressing changes to the characteristics of data • Performing schema conversion (for example, by using the AWS Schema Conversion Tool [AWS SCT] and AWS DMS Schema Conversion) • Establishing data lineage by using AWS tools (for example, Amazon SageMaker ML Lineage Tracking) Domain 3: Data Operations and Support Task Statement 3.1: Automate data processing by using AWS services. Knowledge of: • How to maintain and troubleshoot data processing for repeatable business outcomes • API calls for data processing • Which services accept scripting (for example, Amazon EMR, Amazon Redshift, AWS Glue)
Skills in: • Orchestrating data pipelines (for example, Amazon MWAA, Step Functions) • Troubleshooting Amazon managed workflows • Calling SDKs to access Amazon features from code • Using the features of AWS services to process data (for example, Amazon EMR, Amazon Redshift, AWS Glue) • Consuming and maintaining data APIs • Preparing data

transformation (for example, AWS Glue DataBrew) • Querying data (for example, Amazon Athena) • Using Lambda to automate data processing • Managing events and schedulers (for example, EventBridge) Task Statement 3.2: Analyze data by using AWS services. Knowledge of: • Tradeoffs between provisioned services and serverless services • SQL queries (for example, SELECT statements with multiple qualifiers or JOIN clauses) • How to visualize data for analysis • When and how to apply cleansing techniques • Data aggregation, rolling average, grouping, and pivoting Skills in: • Visualizing data by using AWS services and tools (for example, AWS Glue DataBrew, Amazon QuickSight) • Verifying and cleaning data (for example, Lambda, Athena, QuickSight, Jupyter Notebooks, Amazon SageMaker Data Wrangler) • Using Athena to query data or to create views • Using Athena notebooks that use Apache Spark to explore data Task Statement 3.3: Maintain and monitor data pipelines. Knowledge of: • How to log application data • Best practices for performance tuning • How to log access to AWS services • Amazon Macie, AWS CloudTrail, and Amazon CloudWatch
Skills in: • Extracting logs for audits • Deploying logging and monitoring solutions to facilitate auditing and traceability • Using notifications during monitoring to send alerts • Troubleshooting performance issues • Using CloudTrail to track API calls • Troubleshooting and maintaining pipelines (for example, AWS Glue, Amazon EMR) • Using Amazon CloudWatch Logs to log application data (with a focus on configuration and automation) • Analyzing logs with AWS services (for example, Athena, Amazon EMR, Amazon OpenSearch Service, CloudWatch Logs Insights, big data application logs) Task Statement 3.4: Ensure data quality. Knowledge of: • Data sampling techniques • How to implement data skew mechanisms • Data validation (data completeness, consistency, accuracy, and integrity) • Data profiling Skills in: • Running data quality checks while processing the data (for example, checking for empty fields) • Defining data quality rules (for example, AWS Glue DataBrew) • Investigating data consistency (for example, AWS Glue DataBrew) Domain 4: Data Security and Governance Task Statement 4.1: Apply authentication mechanisms. Knowledge of: • VPC security networking concepts • Differences between managed services and unmanaged services • Authentication methods (password-based, certificate-based, and role-based) • Differences between AWS managed policies and customer managed policies Skills in: • Updating VPC security groups • Creating and updating IAM groups, roles, endpoints, and services • Creating and rotating credentials for password management (for example, AWS Secrets Manager) • Setting up IAM roles for access (for example, Lambda, Amazon API Gateway, AWS CLI, CloudFormation) • Applying IAM policies to roles, endpoints, and services (for example, S3 Access Points, AWS PrivateLink) Task Statement 4.2: Apply authorization mechanisms. Knowledge of: • Authorization methods (role-based, policy-based, tag-based, and attributebased) • Principle of least privilege as it applies to AWS security • Role-based access control and expected access patterns • Methods to protect data from unauthorized access across services Skills in: • Creating custom IAM policies when a managed policy does not meet the needs • Storing application and database credentials (for example, Secrets Manager, AWS Systems Manager Parameter Store) • Providing database users, groups, and roles access and authority in a database (for example, for Amazon Redshift) • Managing permissions through Lake Formation (for Amazon Redshift, Amazon EMR, Athena, and Amazon S3) Task Statement 4.3: Ensure data encryption and masking. Knowledge of: • Data encryption options available in AWS analytics services (for example, Amazon Redshift, Amazon EMR, AWS Glue) • Differences between client-side encryption and server-side encryption • Protection of sensitive data • Data anonymization, masking, and key salting
Skills in: • Applying data masking and anonymization according to compliance laws or company policies • Using encryption keys to encrypt or decrypt data (for example, AWS Key

Management Service [AWS KMS]) • Configuring encryption across AWS account boundaries • Enabling encryption in transit for data. Task Statement 4.4: Prepare logs for audit. Knowledge of: • How to log application data • How to log access to AWS services • Centralized AWS logs Skills in: • Using CloudTrail to track API calls • Using CloudWatch Logs to store application logs • Using AWS CloudTrail Lake for centralized logging queries • Analyzing logs by using AWS services (for example, Athena, CloudWatch Logs Insights, Amazon OpenSearch Service) • Integrating various AWS services to perform logging (for example, Amazon EMR in cases of large volumes of log data) Task Statement 4.5: Understand data privacy and governance. Knowledge of: • How to protect personally identifiable information (PII) • Data sovereignty Skills in: • Granting permissions for data sharing (for example, data sharing for Amazon Redshift) • Implementing PII identification (for example, Macie with Lake Formation) • Implementing data privacy strategies to prevent backups or replications of data to disallowed AWS Regions • Managing configuration changes that have occurred in an account (for example, AWS Config)

AWS Certified Developer
Domain 1: Development with AWS Services Task Statement 1: Develop code for applications hosted on AWS. Knowledge of: • Architectural patterns (for example, event-driven, microservices, monolithic, choreography, orchestration, fanout) • Idempotency • Differences between stateful and stateless concepts • Differences between tightly coupled and loosely coupled components • Fault-tolerant design patterns (for example, retries with exponential backoff and jitter, dead-letter queues) • Differences between synchronous and asynchronous patterns Skills in: • Creating fault-tolerant and resilient applications in a programming language (for example, Java, C#, Python, JavaScript, TypeScript, Go) • Creating, extending, and maintaining APIs (for example, response/request transformations, enforcing validation rules, overriding status codes) • Writing and running unit tests in development environments (for example, using AWS Serverless Application Model [AWS SAM]) • Writing code to use messaging services • Writing code that interacts with AWS services by using APIs and AWS SDKs • Handling data streaming by using AWS services Task Statement 2: Develop code for AWS Lambda. Knowledge of: • Event source mapping • Stateless applications • Unit testing • Event-driven architecture • Scalability • The access of private resources in VPCs from Lambda code Skills in: • Configuring Lambda functions by defining environment variables and parameters (for example, memory, concurrency, timeout, runtime, handler, layers, extensions, triggers, destinations) • Handling the event lifecycle and errors by using code (for example, Lambda Destinations, dead-letter queues) • Writing and running test code by using AWS services and tools • Integrating Lambda functions with AWS services • Tuning Lambda functions for optimal performance Task Statement 3: Use data stores in application development. Knowledge of: • Relational and non-relational databases • Create, read, update, and delete (CRUD) operations • High-cardinality partition keys for balanced partition access • Cloud storage options (for example, file, object, databases) • Database consistency models (for example, strongly consistent, eventually consistent) • Differences between query and scan operations • Amazon DynamoDB keys and indexing • Caching strategies (for example, write-through, read-through, lazy loading, TTL) • Amazon S3 tiers and lifecycle management • Differences between ephemeral and persistent data storage patterns Skills in: • Serializing and deserializing data to provide persistence to a data store • Using, managing, and maintaining data stores • Managing data lifecycles • Using data caching services Domain 2: Security Task Statement 1: Implement authentication and/or authorization for applications and AWS services. Knowledge of: • Identity federation (for example, Security Assertion Markup Language [SAML], OpenID Connect [OIDC], Amazon Cognito) • Bearer tokens (for example, JSON Web Token [JWT], OAuth, AWS Security Token Service [AWS STS]) • The comparison of user pools and identity pools in Amazon Cognito • Resource-based policies, service policies, and principal policies • Role-based access control (RBAC) • Application authorization that uses ACLs • The principle of least privilege • Differences between AWS managed policies and customer-managed policies • Identity and access management Skills in: • Using an identity provider to implement federated access (for example, Amazon Cognito, AWS Identity and Access Management [IAM]) • Securing applications by using bearer tokens • Configuring programmatic access to AWS • Making authenticated calls to AWS services • Assuming an IAM role • Defining permissions for principals Task Statement 2: Implement encryption by using AWS services. Knowledge of: • Encryption at rest and in transit • Certificate

management (for example, AWS Private Certificate Authority) • Key protection (for example, key rotation) • Differences between client-side encryption and server-side encryption • Differences between AWS managed and customer managed AWS Key Management Service (AWS KMS) keys Version 1.1 DVA-C02 7 | PAGE Skills in: • Using encryption keys to encrypt or decrypt data • Generating certificates and SSH keys for development purposes • Using encryption across account boundaries • Enabling and disabling key rotation Task Statement 3: Manage sensitive data in application code. Knowledge of: • Data classification (for example, personally identifiable information [PII], protected health information [PHI]) • Environment variables • Secrets management (for example, AWS Secrets Manager, AWS Systems Manager Parameter Store) • Secure credential handling Skills in: • Encrypting environment variables that contain sensitive data • Using secret management services to secure sensitive data • Sanitizing sensitive data Domain 3: Deployment Task Statement 1: Prepare application artifacts to be deployed to AWS. Knowledge of: • Ways to access application configuration data (for example, AWS AppConfig, Secrets Manager, Parameter Store) • Lambda deployment packaging, layers, and configuration options • Git-based version control tools (for example, Git, AWS CodeCommit) • Container images Skills in: • Managing the dependencies of the code module (for example, environment variables, configuration files, container images) within the package • Organizing files and a directory structure for application deployment • Using code repositories in deployment environments • Applying application requirements for resources (for example, memory, cores) Task Statement 2: Test applications in development environments. Knowledge of: • Features in AWS services that perform application deployment • Integration testing that uses mock endpoints • Lambda versions and aliases Skills in: • Testing deployed code by using AWS services and tools • Performing mock integration for APIs and resolving integration dependencies • Testing applications by using development endpoints (for example, configuring stages in Amazon API Gateway) • Deploying application stack updates to existing environments (for example, deploying an AWS SAM template to a different staging environment) Task Statement 3: Automate deployment testing. Knowledge of: • API Gateway stages • Branches and actions in the continuous integration and continuous delivery (CI/CD) workflow • Automated software testing (for example, unit testing, mock testing) Skills in: • Creating application test events (for example, JSON payloads for testing Lambda, API Gateway, AWS SAM resources) • Deploying API resources to various environments • Creating application environments that use approved versions for integration testing (for example, Lambda aliases, container image tags, AWS Amplify branches, AWS Copilot environments) • Implementing and deploying infrastructure as code (IaC) templates (for example, AWS SAM templates, AWS CloudFormation templates) • Managing environments in individual AWS services (for example, differentiating between development, test, and production in API Gateway) Version 1.1 DVA-C02 9 | PAGE Task Statement 4: Deploy code by using AWS CI/CD services. Knowledge of: • Git-based version control tools (for example, Git, AWS CodeCommit) • Manual and automated approvals in AWS CodePipeline • Access application configurations from AWS AppConfig and Secrets Manager • CI/CD workflows that use AWS services • Application deployment that uses AWS services and tools (for example, CloudFormation, AWS Cloud Development Kit [AWS CDK], AWS SAM, AWS CodeArtifact, AWS Copilot, Amplify, Lambda) • Lambda deployment packaging options • API Gateway stages and custom domains • Deployment strategies (for example, canary, blue/green, rolling) Skills in: • Updating existing IaC templates (for

example, AWS SAM templates, CloudFormation templates) • Managing application environments by using AWS services • Deploying an application version by using deployment strategies • Committing code to a repository to invoke build, test, and deployment actions • Using orchestrated workflows to deploy code to different environments • Performing application rollbacks by using existing deployment strategies • Using labels and branches for version and release management • Using existing runtime configurations to create dynamic deployments (for example, using staging variables from API Gateway in Lambda functions) Domain 4: Troubleshooting and Optimization Task Statement 1: Assist in a root cause analysis. Knowledge of: • Logging and monitoring systems • Languages for log queries (for example, Amazon CloudWatch Logs Insights) • Data visualizations • Code analysis tools • Common HTTP error codes • Common exceptions generated by SDKs • Service maps in AWS X-Ray Skills in: • Debugging code to identify defects • Interpreting application metrics, logs, and traces • Querying logs to find relevant data • Implementing custom metrics (for example, CloudWatch embedded metric format [EMF]) • Reviewing application health by using dashboards and insights • Troubleshooting deployment failures by using service output logs Task Statement 2: Instrument code for observability. Knowledge of: • Distributed tracing • Differences between logging, monitoring, and observability • Structured logging • Application metrics (for example, custom, embedded, built-in) Skills in: • Implementing an effective logging strategy to record application behavior and state • Implementing code that emits custom metrics • Adding annotations for tracing services • Implementing notification alerts for specific actions (for example, notifications about quota limits or deployment completions) • Implementing tracing by using AWS services and tools Task Statement 3: Optimize applications by using AWS services and features. Knowledge of: • Caching • Concurrency • Messaging services (for example, Amazon Simple Queue Service [Amazon SQS], Amazon Simple Notification Service [Amazon SNS]) Skills in: • Profiling application performance • Determining minimum memory and compute power for an application • Using subscription filter policies to optimize messaging • Caching content based on request headers

AWS Certified Solutions Architect :
Domain 1: Design Solutions for Organizational Complexity Task Statement 1.1: Architect network connectivity strategies. Knowledge of: • AWS Global Infrastructure • AWS networking concepts (for example, Amazon VPC, AWS Direct Connect, AWS VPN, transitive routing, AWS container services) • Hybrid DNS concepts (for example, Amazon Route 53 Resolver, on-premises DNS integration) • Network segmentation (for example, subnetting, IP addressing, connectivity among VPCs) • Network traffic monitoring Skills in: • Evaluating connectivity options for multiple VPCs • Evaluating connectivity options for on-premises, co-location, and cloud integration • Selecting AWS Regions and Availability Zones based on network and latency requirements • Troubleshooting traffic flows by using AWS tools • Using service endpoints for service integrations Task Statement 1.2: Prescribe security controls. Knowledge of: • AWS Identity and Access Management (IAM) and AWS IAM Identity Center (AWS Single Sign-On) • Route tables, security groups, and network ACLs • Encryption keys and certificate management (for example, AWS Key Management Service [AWS KMS], AWS Certificate Manager [ACM]) • AWS security, identity, and compliance tools (for example, AWS CloudTrail, AWS Identity and Access Management Access Analyzer, AWS Security Hub, Amazon Inspector) Skills

in: • Evaluating cross-account access management • Integrating with third-party identity providers • Deploying encryption strategies for data at rest and data in transit • Developing a strategy for centralized security event notifications and auditing Task Statement 1.3: Design reliable and resilient architectures. Knowledge of: • Recovery time objectives (RTOs) and recovery point objectives (RPOs) • Disaster recovery strategies (for example, using AWS Elastic Disaster Recovery, pilot light, warm standby, and multi-site) • Data backup and restoration Skills in: • Designing disaster recovery solutions based on RTO and RPO requirements • Implementing architectures to automatically recover from failure • Developing the optimal architecture by considering scale-up and scale-out options • Designing an effective backup and restoration strategy Task Statement 1.4: Design a multi-account AWS environment. Knowledge of: • AWS Organizations and AWS Control Tower • Multi-account event notifications • AWS resource sharing across environments Skills in: • Evaluating the most appropriate account structure for organizational requirements • Recommending a strategy for central logging and event notifications • Developing a multi-account governance model Task Statement 1.5: Determine cost optimization and visibility strategies. Knowledge of: • AWS cost and usage monitoring tools (for example, AWS Trusted Advisor, AWS Pricing Calculator, AWS Cost Explorer, AWS Budgets) • AWS purchasing options (for example, Reserved Instances, Savings Plans, Spot Instances) • AWS rightsizing visibility tools (for example, AWS Compute Optimizer, Amazon S3 Storage Lens) Skills in: • Monitoring cost and usage with AWS tools • Developing an effective tagging strategy that maps costs to business units • Understanding how purchasing options affect cost and performance Domain 2: Design for New Solutions Task Statement 2.1: Design a deployment strategy to meet business requirements. Knowledge of: • Infrastructure as code (IaC) (for example, AWS CloudFormation) • Continuous integration and continuous delivery (CI/CD) • Change management processes • Configuration management tools (for example, AWS Systems Manager) Skills in: • Determining an application or upgrade path for new services and features • Selecting services to develop deployment strategies and implement appropriate rollback mechanisms • Adopting managed services as needed to reduce infrastructure provisioning and patching overhead • Making advanced technologies accessible by delegating complex development and deployment tasks to AWS Task Statement 2.2: Design a solution to ensure business continuity. Knowledge of: • AWS Global Infrastructure • AWS networking concepts (for example, Route 53, routing methods) • RTOs and RPOs • Disaster recovery scenarios (for example, backup and restore, pilot light, warm standby, multi-site) • Disaster recovery solutions on AWS Skills in: • Configuring disaster recovery solutions • Configuring data and database replication • Performing disaster recovery testing • Architecting a backup solution that is automated, is cost-effective, and supports business continuity across multiple Availability Zones or Regions • Designing an architecture that provides application and infrastructure availability in the event of a disruption • Using processes and components for centralized monitoring to proactively recover from system failures Task Statement 2.3: Determine security controls based on requirements. Knowledge of: • IAM • Route tables, security groups, and network ACLs • Encryption options for data at rest and data in transit • AWS service endpoints • Credential management services • AWS managed security services (for example, AWS Shield, AWS WAF, Amazon GuardDuty, AWS Security Hub) Skills in: • Specifying IAM users and IAM roles that adhere to the principle of least privilege access • Specifying inbound and outbound network flows by using security group rules and network ACL rules • Developing

attack mitigation strategies for large-scale web applications • Developing encryption strategies for data at rest and data in transit • Specifying service endpoints for service integrations • Developing strategies for patch management to remain compliant with organizational standards Task Statement 2.4: Design a strategy to meet reliability requirements. Knowledge of: • AWS Global Infrastructure • AWS storage services and replication strategies (for example Amazon S3, Amazon RDS, Amazon ElastiCache) • Multi-AZ and multi-Region architectures • Auto scaling policies and events • Application integration (for example, Amazon Simple Notification Service [Amazon SNS], Amazon Simple Queue Service [Amazon SQS], AWS Step Functions) • Service quotas and limits Skills in: • Designing highly available application environments based on business requirements • Using advanced techniques to design for failure and ensure seamless system recoverability • Implementing loosely coupled dependencies • Operating and maintaining high-availability architectures (for example, application failovers, database failovers) • Using AWS managed services for high availability • Implementing DNS routing policies (for example, Route 53 latency-based routing, geolocation routing, simple routing) Task Statement 2.5: Design a solution to meet performance objectives. Knowledge of: • Performance monitoring technologies • Storage options on AWS • Instance families and use cases • Purpose-built databases Skills in: • Designing large-scale application architectures for a variety of access patterns • Designing an elastic architecture based on business objectives • Applying design patterns to meet performance objectives with caching, buffering, and replicas • Developing a process methodology for selecting purpose-built services for required tasks • Designing a rightsizing strategy Task Statement 2.6: Determine a cost optimization strategy to meet solution goals and objectives. Knowledge of: • AWS cost and usage monitoring tools (for example, Cost Explorer, Trusted Advisor, AWS Pricing Calculator) • Pricing models (for example, Reserved Instances, Savings Plans) • Storage tiering • Data transfer costs • AWS managed service offerings Skills in: • Identifying opportunities to select and rightsize infrastructure for cost-effective resources • Identifying appropriate pricing models • Performing data transfer modeling and selecting services to reduce data transfer costs • Developing a strategy and implementing controls for expenditure and usage awareness Domain 3: Continuous Improvement for Existing Solutions Task Statement 3.1: Determine a strategy to improve overall operational excellence. Knowledge of: • Alerting and automatic remediation strategies • Disaster recovery planning • Monitoring and logging solutions (for example, Amazon CloudWatch) • CI/CD pipelines and deployment strategies (for example, blue/green, all-at-once, rolling) • Configuration management tools (for example, Systems Manager) Skills in: • Determining the most appropriate logging and monitoring strategy • Evaluating current deployment processes for improvement opportunities • Prioritizing opportunities for automation within a solution stack • Recommending the appropriate AWS solution to enable configuration management automation • Engineering failure scenario activities to support and exercise an understanding of recovery actions Task Statement 3.2: Determine a strategy to improve security. Knowledge of: • Data retention, data sensitivity, and data regulatory requirements • Automated monitoring and remediation strategies (for example, AWS Config rules) • Secrets management (for example, Systems Manager, AWS Secrets Manager) • Principle of least privilege access • Security-specific AWS solutions • Patching practices • Backup practices and methods Skills in: • Evaluating a strategy for the secure management of secrets and credentials • Auditing an environment for least privilege access • Reviewing

implemented solutions to ensure security at every layer • Reviewing comprehensive traceability of users and services • Prioritizing automated responses to the detection of vulnerabilities • Designing and implementing a patch and update process • Designing and implementing a backup process • Employing remediation techniques Task Statement 3.3: Determine a strategy to improve performance. Knowledge of: • High-performing systems architectures (for example, auto scaling, instance fleets, placement groups) • Global service offerings (for example, AWS Global Accelerator, Amazon CloudFront, edge computing services) • Monitoring tool sets and services (for example, CloudWatch) • Service level agreements (SLAs) and key performance indicators (KPIs) Skills in: • Translating business requirements to measurable metrics • Testing potential remediation solutions and making recommendations • Proposing opportunities for the adoption of new technologies and managed services • Assessing solutions and applying rightsizing based on requirements • Identifying and examining performance bottlenecks Task Statement 3.4: Determine a strategy to improve reliability. Knowledge of: • AWS Global Infrastructure • Data replication methods • Scaling methodologies (for example, load balancing, auto scaling) • High availability and resiliency • Disaster recovery methods and tools • Service quotas and limits Skills in: • Understanding application growth and usage trends • Evaluating existing architecture to determine areas that are not sufficiently reliable • Remediating single points of failure • Enabling data replication, self-healing, and elastic features and services Task Statement 3.5: Identify opportunities for cost optimizations. Knowledge of: • Cost-conscious architecture choices (for example, using Spot Instances, scaling policies, and rightsizing resources) • Price model adoptions (for example, Reserved Instances, Savings Plans) • Networking and data transfer costs • Cost management, alerting, and reporting Skills in: • Analyzing usage reports to identify underutilized and overutilized resources • Using AWS solutions to identify unused resources • Designing billing alarms based on expected usage patterns • Investigating AWS Cost and Usage Reports at a granular level • Using tagging for cost allocation and reporting Domain 4: Accelerate Workload Migration and Modernization Task Statement 4.1: Select existing workloads and processes for potential migration. Knowledge of: • Migration assessment and tracking tools (for example, AWS Migration Hub) • Portfolio assessment • Asset planning • Prioritization and migration of workloads (for example, wave planning) Skills in: • Completing an application migration assessment • Evaluating applications according to the seven common migration strategies (7Rs) • Evaluating total cost of ownership (TCO) Task Statement 4.2: Determine the optimal migration approach for existing workloads. Knowledge of: • Data migration options and tools (for example, AWS DataSync, AWS Transfer Family, AWS Snow Family, S3 Transfer Acceleration) • Application migration tools (for example, AWS Application Discovery Service, AWS Application Migration Service) • AWS networking services and DNS (for example, Direct Connect, AWS Site-to-Site VPN, Route 53) • Identity services (for example, IAM Identity Center, AWS Directory Service) • Database migration tools (for example, AWS Database Migration Service [AWS DMS], AWS Schema Conversion Tool [AWS SCT]) • Governance tools (for example, AWS Control Tower, Organizations) Skills in: • Selecting the appropriate database transfer mechanism • Selecting the appropriate application transfer mechanism • Selecting the appropriate data transfer service and migration strategy • Applying the appropriate security methods to migration tools • Selecting the appropriate governance model Task Statement 4.3: Determine a new architecture for existing workloads. Knowledge of: • Compute services (for example, Amazon EC2, AWS Elastic Beanstalk) • Containers (for example, Amazon Elastic

Container Service [Amazon ECS], Amazon Elastic Kubernetes Service [Amazon EKS], AWS Fargate, Amazon Elastic Container Registry [Amazon ECR]) • AWS storage services (for example, Amazon Elastic Block Store [Amazon EBS], Amazon Elastic File System [Amazon EFS], Amazon FSx, Amazon S3, Volume Gateway) • Databases (for example, Amazon DynamoDB, Amazon OpenSearch Service, Amazon RDS, self-managed databases on Amazon EC2) Skills in: • Selecting the appropriate compute platform • Selecting the appropriate container hosting platform • Selecting the appropriate storage service • Selecting the appropriate database platform Task Statement 4.4: Determine opportunities for modernization and enhancements. Knowledge of: • Serverless compute offerings (for example, AWS Lambda) • Containers (for example, Amazon ECS, Amazon EKS, Fargate) • AWS storage services (for example, Amazon S3, Amazon EFS) • Purpose-built databases (for example, DynamoDB, Amazon Aurora Serverless, ElastiCache) • Integration services (for example, Amazon SQS, Amazon SNS, Amazon EventBridge, Step Functions) Skills in: • Identifying opportunities to decouple application components • Identifying opportunities for serverless solutions • Selecting the appropriate service for containers • Identifying opportunities for purpose-built databases • Selecting the appropriate application integration service

AWS Certified Machine Learning
Domain 1: Data Engineering Task Statement 1.1: Create data repositories for ML. ? Identify data sources (for example, content and location, primary sources such as user data). ? Determine storage mediums (for example, databases, Amazon S3, Amazon Elastic File System [Amazon EFS], Amazon Elastic Block Store [Amazon EBS]). Task Statement 1.2: Identify and implement a data ingestion solution. ? Identify data job styles and job types (for example, batch load, streaming). ? Orchestrate data ingestion pipelines (batch-based ML workloads and streaming-based ML workloads). o Amazon Kinesis o Amazon Kinesis Data Firehose o Amazon EMR o AWS Glue o Amazon Managed Service for Apache Flink ? Schedule jobs. Task Statement 1.3: Identify and implement a data transformation solution. ? Transform data in transit (ETL, AWS Glue, Amazon EMR, AWS Batch). ? Handle ML-specific data by using MapReduce (for example, Apache Hadoop, Apache Spark, Apache Hive). Domain 2: Exploratory Data Analysis Task Statement 2.1: Sanitize and prepare data for modeling. ? Identify and handle missing data, corrupt data, and stop words. ? Format, normalize, augment, and scale data. ? Determine whether there is sufficient labeled data. o Identify mitigation strategies. o Use data labelling tools (for example, Amazon Mechanical Turk). Task Statement 2.2: Perform feature engineering. ? Identify and extract features from datasets, including from data sources such as text, speech, image, public datasets. ? Analyze and evaluate feature engineering concepts (for example, binning, tokenization, outliers, synthetic features, one-hot encoding, reducing dimensionality of data). Task Statement 2.3: Analyze and visualize data for ML. ? Create graphs (for example, scatter plots, time series, histograms, box plots). ? Interpret descriptive statistics (for example, correlation, summary statistics, p-value). ? Perform cluster analysis (for example, hierarchical, diagnosis, elbow plot, cluster size). Domain 3: Modeling Task Statement 3.1: Frame business problems as ML problems. ? Determine when to use and when not to use ML. ? Know the difference between supervised and unsupervised learning. ? Select from among classification, regression, forecasting, clustering, and recommendation models. Task Statement 3.2: Select the appropriate model(s) for a given ML problem. ? XGBoost, logistic regression, k-means, linear regression,

decision trees, random forests, RNN, CNN, ensemble, transfer learning ? Express the intuition behind models. Task Statement 3.3: Train ML models. ? Split data between training and validation (for example, cross validation). ? Understand optimization techniques for ML training (for example, gradient decent, loss functions, convergence). ? Choose appropriate compute resources (for example GPU or CPU, distributed or non-distributed). o Choose appropriate compute platforms (Spark or non-Spark). ? Update and retrain models. o Batch or real-time/online Task Statement 3.4: Perform hyperparameter optimization. ? Perform regularization. o Drop out o L1/L2 ? Perform cross validation. ? Initialize models. ? Understand neural network architecture (layers and nodes), learning rate, and activation functions. ? Understand tree-based models (number of trees, number of levels). ? Understand linear models (learning rate). Task Statement 3.5: Evaluate ML models. ? Avoid overfitting or underfitting. o Detect and handle bias and variance. ? Evaluate metrics (area under curve [AUC]-receiver operating characteristics [ROC], accuracy, precision, recall, Root Mean Square Error [RMSE], F1 score). ? Interpret confusion matrices. ? Perform offline and online model evaluation (A/B testing). ? Compare models by using metrics (for example, time to train a model, quality of model, engineering costs). ? Perform cross validation. Domain 4: Machine Learning Implementation and Operations Task Statement 4.1: Build ML solutions for performance, availability, scalability, resiliency, and fault tolerance. ? Log and monitor AWS environments. o AWS CloudTrail and Amazon CloudWatch o Build error monitoring solutions. ? Deploy to multiple AWS Regions and multiple Availability Zones. ? Create AMIs and golden images. ? Create Docker containers. ? Deploy Auto Scaling groups. ? Rightsize resources (for example, instances, Provisioned IOPS, volumes). ? Perform load balancing. ? Follow AWS best practices. Task Statement 4.2: Recommend and implement the appropriate ML services and features for a given problem. ? ML on AWS (application services) o Amazon Polly o Amazon Lex o Amazon Transcribe ? Understand AWS service quotas. ? Determine when to build custom models and when to use Amazon SageMaker built-in algorithms. ? Understand AWS infrastructure (for example, instance types) and cost considerations. o Use Spot Instances to train deep learning models by using AWS Batch. Task Statement 4.3: Apply basic AWS security practices to ML solutions. ? AWS Identity and Access Management (IAM) ? S3 bucket policies ? Security groups ? VPCs ? Encryption and anonymization Task Statement 4.4: Deploy and operationalize ML solutions. ? Expose endpoints and interact with them. ? Understand ML models. ? Perform A/B testing. ? Retrain pipelines. ? Debug and troubleshoot ML models. o Detect and mitigate drops in performance. o Monitor performance of the model.

AWS Certified Data Analytics
Domain 1: Collection Task Statement 1.1: Determine the operational characteristics of the collection system. • Confirm that data loss is within tolerance limits in the event of failures. • Evaluate costs associated with data acquisition, transfer, and provisioning from various sources into the collection system (for example, networking, bandwidth, ETL, data migration). • Assess the failure scenarios that the collection system may experience, and take remediation actions based on impact. • Determine data persistence at various points of data capture. • Identify the latency characteristics of the collection system. Task Statement 1.2: Select a collection system that handles the frequency, volume, and source of data. • Describe and characterize the volume and flow characteristics of incoming data (for example,

streaming, transactional, batch). • Match the flow characteristics of data to potential solutions. • Assess the tradeoffs between various ingestion services, and take into account scalability, cost, fault tolerance, and latency. • Explain the throughput capability of a variety of types of data collection solutions, and identify bottlenecks. • Choose a collection solution that satisfies connectivity constraints of the source data system. Task Statement 1.3: Select a collection system that addresses the key properties of data, such as order, format, and compression. • Describe how to capture data changes at the source. • Discuss data structure and format, compression applied, and encryption requirements. • Distinguish the impact of out-of-order delivery of data, duplicate delivery of data, and the tradeoffs between at-most-once, exactly-once, and at-leastonce processing. • Describe how to transform and filter data during the collection process. Domain 2: Storage and Data Management Task Statement 2.1: Determine the operational characteristics of the storage solution for analytics. • Determine the appropriate storage service or services on the basis of cost compared to performance. • Understand the durability, reliability, and latency characteristics of the storage solution based on requirements. • Determine the requirements of a system for strong or eventual consistency of the storage system. • Determine the appropriate storage solution to address data freshness requirements. Task Statement 2.2: Determine data access and retrieval patterns. • Determine the appropriate storage solution based on update patterns (for example, bulk, transactional, micro batching). • Determine the appropriate storage solution based on access patterns (for example, sequential or random access, continuous usage or one-time usage). • Determine the appropriate storage solution to address change characteristics of data (append-only changes or updates). • Determine the appropriate storage solution for long-term storage and transient storage. • Determine the appropriate storage solution for structured data and semistructured data. • Determine the appropriate storage solution to address query latency requirements. Task Statement 2.3: Select appropriate data layout, schema, structure, and format. • Determine appropriate mechanisms to address schema evolution requirements. • Select the appropriate storage format for a specific task. • Select the appropriate compression and encoding strategies for a chosen storage format. • Select the appropriate data sorting and distribution strategies and the storage layout for efficient data access. • Explain the cost and performance implications of different data distributions, layouts, and formats (for example, size and number of files). • Implement data formatting and partitioning schemes for data-optimized analysis. Task Statement 2.4: Define data lifecycles based on usage patterns and business requirements. • Determine the appropriate strategy to address data lifecycle requirements. • Apply appropriate lifecycle and data retention policies to different storage solutions. Task Statement 2.5: Determine the appropriate system to catalog data and to manage metadata. • Evaluate mechanisms to discover new and updated data sources. • Evaluate mechanisms to create and update data catalogs and metadata. • Explain mechanisms to search and retrieve data catalogs and metadata. • Explain mechanisms to tag and classify data. Domain 3: Processing Task Statement 3.1: Determine appropriate data processing solution requirements. • Understand data preparation and usage requirements. • Understand different types of data sources and targets. • Evaluate performance and orchestration needs. • Evaluate appropriate services for cost, scalability, and availability. Task Statement 3.2: Design a solution to transform and prepare data for analysis. • Apply appropriate ETL and ELT techniques for batch workloads and realtime workloads. • Implement failover, scaling, and replication mechanisms. • Implement techniques to address

concurrency needs. • Implement techniques to improve cost-optimization efficiencies. • Orchestrate workflows. • Aggregate and enrich data for downstream consumption. Task Statement 3.3: Automate and operationalize data processing solutions. • Implement automated techniques for repeatable workflows. • Apply methods to identify and recover from processing failures. • Deploy logging and monitoring solutions to enable auditing and traceability. Domain 4: Analysis and Visualization Task Statement 4.1: Determine the operational characteristics of an analysis and visualization solution. • Determine costs associated with analysis and visualization. • Determine scalability associated with analysis. • Determine failover recovery and fault tolerance within the RPO and RTO. • Determine the availability characteristics of an analysis tool. • Evaluate dynamic, interactive, and static presentations of data. • Translate performance requirements to an appropriate visualization approach (for example, pre-compute and consume static data, consume dynamic data). Task Statement 4.2: Select the appropriate data analysis solution for a given scenario. • Evaluate and compare analysis solutions. • Select the right type of analysis based on the customer use case (for example, streaming, interactive, collaborative, operational). Task Statement 4.3: Select the appropriate data visualization solution for a given scenario. • Evaluate output capabilities for a given analysis solution (for example, metrics, KPIs, tabular, API). • Choose the appropriate method for data delivery (for example, web, mobile, email, collaborative notebooks). • Choose and define the appropriate data refresh schedule. • Choose appropriate tools for different data freshness requirements (for example, Amazon OpenSearch Service, Amazon QuickSight, Amazon EMR notebooks). • Understand the capabilities of visualization tools for interactive use cases (for example, drill down, drill through, pivot). • Implement the appropriate data access mechanism (for example, in memory, direct access). • Implement an integrated solution from multiple heterogeneous data sources. Domain 5: Security Task Statement 5.1: Select appropriate authentication and authorization mechanisms. • Implement appropriate authentication methods (for example, federated access, SSO, AWS Identity and Access Management [IAM]). • Implement appropriate authorization methods (for example, policies, ACLs, table and column level permissions). • Implement appropriate access control mechanisms (for example, security groups, role-based controls). Task Statement 5.2: Apply data protection and encryption techniques. • Determine data encryption and masking needs. • Apply different encryption approaches (for example, server-side encryption, client-side encryption, AWS Key Management Service [AWS KMS], AWS CloudHSM). • Implement at-rest and in-transit encryption mechanisms. • Implement data obfuscation and masking techniques. • Apply basic principles of key rotation and secrets management. Task Statement 5.3: Apply data governance and compliance controls. • Determine data governance and compliance requirements. • Understand and configure access, and audit logging across data analytics services. • Implement appropriate controls to meet compliance requirements.

AWS Certified Database :
Domain 1: Workload-Specific Database Design Task Statement 1.1: Select appropriate database services for specific types of data and workloads. ? Differentiate between ACID and BASE workloads. ? Explain appropriate uses of types of databases (for example, relational, key-value, document, in-memory, graph, time series, ledger). ? Identify use cases for persisted data compared with ephemeral data. Task Statement 1.2: Determine strategies for disaster recovery and

high availability. ? Select Region and Availability Zone placement to optimize database performance. ? Determine implications of Regions and Availability Zones on disaster recovery and high availability strategies. ? Differentiate use cases for read replicas and Multi-AZ deployments.
Task Statement 1.3: Design database solutions for performance, compliance, and scalability. ? Recommend serverless compared with instance-based database architecture. ? Evaluate requirements for scaling read replicas. ? Define database caching solutions. ? Evaluate the implications of partitioning, sharding, and indexing. ? Determine appropriate instance types and storage options. ? Determine auto scaling capabilities for relational and NoSQL databases. ? Determine the implications of Amazon DynamoDB adaptive capacity. ? Determine data locality based on compliance requirements. Task Statement 1.4: Compare the costs of database solutions. ? Determine cost implications of DynamoDB capacity units, including on-demand capacity compared with provisioned capacity. ? Determine costs associated with instance types and automatic scaling. ? Design for costs, including high availability, backups, multi-Region, Multi-AZ, and storage type options. ? Compare data access costs. Domain 2: Deployment and Migration Task Statement 2.1: Automate database solution deployments. ? Evaluate application requirements to determine components to deploy. ? Choose appropriate deployment tools and services (for example, AWS CloudFormation, AWS CLI). Task Statement 2.2: Determine data preparation and migration strategies. ? Determine the data migration method (for example, snapshots, replication, restore). ? Evaluate database migration tools and services (for example, AWS Database Migration Service [AWS DMS], native database tools). ? Prepare data sources and targets. ? Determine schema conversion methods (for example, AWS Schema Conversion Tool [AWS SCT]). ? Determine heterogeneous compared with homogeneous migration strategies.
Task Statement 2.3: Perform and validate data migration. ? Design and script data migration. ? Run data extraction and migration scripts. ? Verify the successful load of data. Domain 3: Management and Operations Task Statement 3.1: Determine maintenance tasks and processes. ? Account for the AWS shared responsibility model for database services. ? Determine appropriate maintenance window strategies. ? Differentiate between major and minor engine upgrades. Task Statement 3.2: Determine backup and restore strategies. ? Identify the need for automatic and manual backups and snapshots. ? Differentiate backup and restore strategies (for example, full backup, point-in-time, encrypting backups cross-Region). ? Define retention policies. ? Correlate the backup and restore to recovery point objective (RPO) and recovery time objective (RTO) requirements. Task Statement 3.3: Manage the operational environment of a database solution. ? Orchestrate the refresh of lower environments. ? Implement configuration changes (for example, in Amazon RDS option groups and parameter groups, or DynamoDB indexing changes). ? Automate operational tasks. ? Take action based on AWS Trusted Advisor reports.
Domain 4: Monitoring and Troubleshooting Task Statement 4.1: Determine monitoring and alerting strategies. ? Evaluate monitoring tools (for example, Amazon CloudWatch, Amazon RDS Performance Insights, database native). ? Determine appropriate parameters and thresholds for alert conditions. ? Use tools to notify users when thresholds are breached (for example, Amazon Simple Notification Service [Amazon SNS], Amazon Simple Queue Service [Amazon SQS], CloudWatch dashboards). Task Statement 4.2: Troubleshoot and resolve common

database issues. ? Identify, evaluate, and respond to categories of failures (for example, troubleshoot connectivity; instance, storage, and partitioning issues). ? Automate responses when possible. Task Statement 4.3: Optimize database performance. ? Troubleshoot database performance issues. ? Identify appropriate AWS tools and services for database optimization. ? Evaluate the configuration, schema design, queries, and infrastructure to improve performance. Domain 5: Database Security Task Statement 5.1: Encrypt data at rest and in transit. ? Encrypt data in relational and NoSQL databases. ? Apply SSL connectivity to databases. ? Implement key management (for example, AWS Key Management Service [AWS KMS], AWS CloudHSM). Task Statement 5.2: Evaluate auditing solutions. ? Determine auditing strategies for structural and schema changes (for example, DDL). ? Determine auditing strategies for data changes (for example, DML). ? Determine auditing strategies for data access (for example, queries). ? Determine auditing strategies for infrastructure changes (for example, AWS CloudTrail). ? Enable the export of database logs to Amazon CloudWatch Logs. Task Statement 5.3: Determine access control and authentication mechanisms. ? Recommend authentication controls for users and roles (for example, IAM, native credentials, Active Directory). ? Recommend authorization controls for users (for example, policies). Task Statement 5.4: Recognize potential security vulnerabilities within database solutions. ? Determine security group rules and network ACLs for database access. ? Identify relevant VPC configurations (for example, VPC endpoints, public subnets compared with private subnets, perimeter zone). ? Determine appropriate storage methods for sensitive data.

Advanced Network

. Domain 1: Network Design

Task Statement 1.1: Design a solution that incorporates edge network services to optimize user performance and traffic management for global architectures. Knowledge of: •Design patterns for the usage of content distribution networks (for example, Amazon CloudFront) •Design patterns for global traffic management (for example, AWS Global

Accelerator) • Integration patterns for content distribution networks and global traffic

management with other services (for example, Elastic Load Balancing [ELB], Amazon API Gateway) Skills in:

• Evaluating requirements of global inbound and outbound traffic from the internet to design an appropriate content distribution solution Task Statement 1.2: Design DNS solutions that meet public, private, and hybrid requirements. Knowledge of: •

DNS protocol (for example, DNS records, TTL, DNSSEC, DNS delegation, zones) • DNS logging and monitoring • Amazon Route 53 features (for example, alias records, traffic policies,

resolvers, health checks) •Integration of Route 53 with other AWS networking services (for example,

Amazon VPC) •Integration of Route 53 with hybrid, multi-account, and multi-Region options • Domain registration

Skills in: • Using Route 53 public hosted zones • Using Route 53 private hosted zones • Using Route 53 Resolver endpoints in hybrid and AWS architectures •

Using Route 53 for global traffic management • Creating and managing domain registrations

Task Statement 1.3: Design solutions that integrate load balancing to meet high availability, scalability, and security requirements.
Knowledge of: • How load balancing works at layer 3, layer 4, and layer 7 of the OSI model • Different types of load balancers and how they meet requirements for network design, high availability, and security • Connectivity patterns that apply to load balancing based on the use case
(for example, internal load balancers, external load balancers) • Scaling factors for load balancers • Integrations of load balancers and other AWS services (for example, Global Accelerator, CloudFront, AWS WAF, Route 53, Amazon Elastic Kubernetes Service [Amazon EKS], AWS Certificate Manager [ACM]) • Configuration options for load balancers (for example, proxy protocol, cross-zone load balancing, session affinity [sticky sessions], routing algorithms) • Configuration options for load balancer target groups (for example, TCP, GENEVE, IP compared with instance) • AWS Load Balancer Controller for Kubernetes clusters • Considerations for encryption and authentication with load balancers (for
example, TLS termination, TLS passthrough)
Skills in: • Selecting an appropriate load balancer based on the use case • Integrating auto scaling with load balancing solutions • Integrating load balancers with existing application deployments
Task Statement 1.4: Define logging and monitoring requirements across AWS and hybrid networks.
Knowledge of: • Amazon CloudWatch metrics, agents, logs, alarms, dashboards, and insights
in AWS architectures to provide visibility • AWS Transit Gateway Network Manager in architectures to provide visibility • VPC Reachability Analyzer in architectures to provide visibility • Flow logs and traffic mirroring in architectures to provide visibility • Access logging (for example, load balancers, CloudFront)
Skills in: • Identifying the logging and monitoring requirements • Recommending appropriate metrics to provide visibility of the network
status • Capturing baseline network performance Task Statement 1.5: Design a routing strategy and connectivity architecture between on-premises networks and the AWS Cloud. Knowledge of: • Routing fundamentals (for example, dynamic compared with static, BGP) • Layer 1 and layer 2 concepts for physical interconnects (for example, VLAN,
link aggregation group [LAG], optics, jumbo frames) • Encapsulation and encryption technologies (for example, Generic Routing
Encapsulation [GRE], IPsec) • Resource sharing across AWS accounts • Overlay networks
Skills in: • Identifying the requirements for hybrid connectivity • Designing a redundant hybrid connectivity model with AWS services (for
example, AWS Direct Connect, AWS Site-to-Site VPN) • Designing BGP routing with BGP attributes to influence the traffic flows
based on the desired traffic patterns (load sharing, active/passive) • Designing for integration of a software-defined wide area network (SD-WAN) with AWS (for example, Transit Gateway Connect, overlay networks)
Task Statement 1.6: Design a routing strategy and connectivity architecture that include multiple AWS accounts, AWS Regions, and VPCs to support different connectivity patterns.
Knowledge of: • Different connectivity patterns and use cases (for example, VPC

peering,
Transit Gateway, AWS PrivateLink) • Capabilities and advantages of VPC sharing • IP subnets and solutions accounting for IP address overlaps
Skills in: • Connecting multiple VPCs by using the most appropriate services based on
requirements (for example, using VPC peering, Transit Gateway,
PrivateLink) • Using VPC sharing in a multi-account setup • Managing IP overlaps by using different available services and options (for example, NAT, PrivateLink, Transit Gateway routing) Domain 2: Network Implementation Task Statement 2.1: Implement routing and connectivity between on-premises networks and the AWS Cloud. Knowledge of: • Routing protocols (for example, static, dynamic) • VPNs (for example, security, accelerated VPN) • Layer 1 and types of hardware to use (for example, Letter of Authorization
[LOA] documents, colocation facilities, Direct Connect) • Layer 2 and layer 3 (for example, VLANs, IP addressing, gateways, routing,
switching) • Traffic management and SD-WAN (for example, Transit Gateway Connect) •DNS (for example, conditional forwarding, hosted zones, resolvers) • Security appliances (for example, firewalls) • Load balancing (for example, layer 4 compared with layer 7, reverse proxies,
layer 3) • Infrastructure automation •AWS Organizations and AWS Resource Access Manager (AWS RAM) (for
example, multi-account Transit Gateway, Direct Connect, Amazon VPC,
Route 53) • Test connectivity (for example, Route Analyzer, Reachability Analyzer) • Networking services of VPCs
Skills in: • Configuring the physical network requirements for hybrid connectivity solutions • Configuring static or dynamic routing protocols to work with hybrid connectivity solutions • Configuring existing on-premises networks to connect with the AWS Cloud •Configuring existing on-premises name resolution with the AWS Cloud • Configuring and implementing load balancing solutions • Configuring network monitoring and logging for AWS services • Testing and validating connectivity between environments
Task Statement 2.2: Implement routing and connectivity across multiple AWS accounts, Regions, and VPCs to support different connectivity patterns.
Knowledge of: • Inter-VPC and multi-account connectivity (for example, VPC peering, Transit
Gateway, VPN, third-party vendors, SD-WAN, multi-protocol label switching [MPLS]) • Private application connectivity (for example, PrivateLink) • Methods of expanding AWS networking connectivity (for example, Organizations, AWS RAM) • Host and service name resolution for applications and clients (for example,
DNS) • Infrastructure automation •Authentication and authorization (for example, SAML, Active Directory) • Security (for example, security groups, network ACLs, AWS Network
Firewall) • Test connectivity (for example, Route Analyzer, Reachability Analyzer, tooling)
Skills in: • Configuring network connectivity architectures by using AWS services in a single-VPC or multi-VPC design (for example, DHCP, routing, security
groups) • Configuring hybrid connectivity with existing third-party vendor solutions • Configuring a hub-and-spoke network architecture (for example, Transit Gateway, transit VPC) • Configuring a DNS solution to make hybrid connectivity

possible • Implementing security between network boundaries • Configuring network monitoring and logging by using AWS solutions Task Statement 2.3: Implement complex hybrid and multi-account DNS architectures. Knowledge of: • When to use private hosted zones and public hosted zones • Methods to alter traffic management (for example, based on latency, geography, weighting) • DNS delegation and forwarding (for example, conditional forwarding) • Different DNS record types (for example, A, AAAA, TXT, pointer records, alias records) • DNSSEC • How to share DNS services between accounts (for example, AWS RAM) • Requirements and implementation options for outbound and inbound endpoints Skills in: • Configuring DNS zones and conditional forwarding • Configuring traffic management by using DNS solutions • Configuring DNS for hybrid networks • Configuring appropriate DNS records • Configuring DNSSEC on Route 53 • Configuring DNS within a centralized or distributed network architecture • Configuring DNS monitoring and logging on Route 53 Task Statement 2.4: Automate and configure network infrastructure. Knowledge of: • Infrastructure as code (IaC) (for example, AWS Cloud Development Kit [AWS CDK], AWS CloudFormation, AWS CLI, AWS SDK, APIs) • Event-driven network automation • Common problems of using hardcoded instructions in IaC templates when provisioning cloud networking resources Skills in: • Creating and managing repeatable network configurations • Integrating event-driven networking functions • Integrating hybrid network automation options with AWS native IaC • Eliminating risk and achieving efficiency in a cloud networking environment while maintaining the lowest possible cost • Automating the process of optimizing cloud network resources with IaC Domain 3: Network Management and Operation Task Statement 3.1: Maintain routing and connectivity on AWS and hybrid networks. Knowledge of: • Industry-standard routing protocols that are used in AWS hybrid networks (for example, BGP over Direct Connect) • Connectivity methods for AWS and hybrid networks (for example, Direct Connect gateway, Transit Gateway, VIFs) • How limits and quotas affect AWS networking services (for example, bandwidth limits, route limits) • Available private and public access methods for custom services (for example, PrivateLink, VPC peering) • Available inter-Regional and intra-Regional communication patterns Skills in: • Managing routing protocols for AWS and hybrid connectivity options (for example, over a Direct Connect connection, VPN) • Maintaining private access to custom services (for example, PrivateLink, VPC peering) • Using route tables to direct traffic appropriately (for example, automatic propagation, BGP) • Setting up private access or public access to AWS services (for example, Direct Connect, VPN) • Optimizing routing over dynamic and static routing protocols (for example, summarizing routes, CIDR overlap) Task Statement 3.2: Monitor and analyze

network traffic to troubleshoot and optimize connectivity patterns. Knowledge of: • Network performance metrics and reachability constraints (for example, routing, packet size) • Appropriate logs and metrics to assess network performance and reachability issues (for example, packet loss) • Tools to collect and analyze logs and metrics (for example, CloudWatch, VPC Flow Logs, VPC Traffic Mirroring) • Tools to analyze routing patterns and issues (for example, Reachability Analyzer, Transit Gateway Network Manager)
Skills in: • Analyzing tool output to assess network performance and troubleshoot connectivity (for example, VPC Flow Logs, Amazon CloudWatch Logs) • Mapping or understanding network topology (for example, Transit Gateway Network Manager) • Analyzing packets to identify issues in packet shaping (for example, VPC Traffic Mirroring) • Troubleshooting connectivity issues that are caused by network misconfiguration (for example, Reachability Analyzer) • Verifying that a network configuration meets network design requirements (for example, Reachability Analyzer) • Automating the verification of connectivity intent as a network configuration changes (for example, Reachability Analyzer) • Troubleshooting packet size mismatches in a VPC to restore network connectivity
Task Statement 3.3: Optimize AWS networks for performance, reliability, and cost-effectiveness.
Knowledge of: •Situations in which a VPC peer or a transit gateway are appropriate • Different methods to reduce bandwidth utilization (for example, unicast compared with multicast, CloudFront) • Cost-effective connectivity options for data transfer between a VPC and on- premises environments • Different types of network interfaces on AWS • High-availability features in Route 53 (for example, DNS load balancing using health checks with latency and weighted record sets) • Availability of options from Route 53 that provide reliability • Load balancing and traffic distribution patterns •VPC subnet optimization • Frame size optimization for bandwidth across different connection types
Skills in: • Optimizing for network throughput • Selecting the right network interface for the best performance (for example, elastic network interface, Elastic Network Adapter [ENA], Elastic Fabric Adapter [EFA]) • Choosing between VPC peering, proxy patterns, or a transit gateway connection based on analysis of the network requirements provided • Implementing a solution on an appropriate network connectivity service (for example, VPC peering, Transit Gateway, VPN connection) to meet network requirements • Implementing a multicast capability within a VPC and on-premises environments • Creating Route 53 public hosted zones and private hosted zones and records to optimize application availability (for example, private zonal DNS entry to route traffic to multiple Availability Zones) • Updating and optimizing subnets for auto scaling configurations to support increased application load • Updating and optimizing subnets to prevent the

depletion of available IP
addresses within a VPC (for example, secondary CIDR) • Configuring jumbo frame support across connection types • Optimizing network connectivity by using Global Accelerator to improve
network performance and application availability Domain 4: Network Security, Compliance, and Governance Task Statement 4.1: Implement and maintain network features to meet security and compliance needs and requirements. Knowledge of: • Different threat models based on application architecture • Common security threats • Mechanisms to secure different application flows • AWS network architecture that meets security and compliance
requirements
Skills in: • Securing inbound traffic flows into AWS (for example, AWS WAF, AWS Shield, Network Firewall) •Securing outbound traffic flows from AWS (for example, Network Firewall,
proxies, Gateway Load Balancers) • Securing inter-VPC traffic within an account or across multiple accounts (for
example, security groups, network ACLs, VPC endpoint policies) • Implementing an AWS network architecture to meet security and compliance requirements (for example, untrusted network, perimeter VPC, three-tier architecture) • Developing a threat model and identifying appropriate mitigation strategies
for a given network architecture • Testing compliance with the initial requirements (for example, failover test,
resiliency) • Automating security incident reporting and alerting using AWS
Task Statement 4.2: Validate and audit security by using network monitoring and logging services.
Knowledge of: •Network monitoring and logging services that are available in AWS (for
example, CloudWatch, AWS CloudTrail, VPC Traffic Mirroring, VPC Flow Logs, Transit Gateway Network Manager) • Alert mechanisms (for example, CloudWatch alarms) • Log creation in different AWS services (for example, VPC flow logs, load balancer access logs, CloudFront access logs) • Log delivery mechanisms (for example, Amazon Kinesis, Route 53, CloudWatch) • Mechanisms to audit network security configurations (for example, security groups, AWS Firewall Manager, AWS Trusted Advisor)
Skills in: • Creating and analyzing a VPC flow log (including base and extended fields
of flow logs) • Creating and analyzing network traffic mirroring (for example, using VPC
Traffic Mirroring) • Implementing automated alarms by using CloudWatch • Implementing customized metrics by using CloudWatch • Correlating and analyzing information across single or multiple AWS log
sources • Implementing log delivery solutions • Implementing a network audit strategy across single or multiple AWS
network services and accounts (for example, Firewall Manager, security groups, network ACLs)
Task Statement 4.3: Implement and maintain confidentiality of data and communications of the network.
Knowledge of: •Network encryption options that are available on AWS • VPN connectivity over Direct Connect • Encryption methods for data in

transit (for example, IPsec) • Network encryption under the AWS shared responsibility model •Security methods for DNS communications (for example, DNSSEC)
Skills in: • Implementing network encryption methods to meet application compliance requirements (for example, IPsec, TLS) • Implementing encryption solutions to secure data in transit (for example, CloudFront, Application Load Balancers and Network Load Balancers, VPN over Direct Connect, AWS managed databases, Amazon S3, custom solutions on Amazon EC2, Transit Gateway) • Implementing a certificate management solution by using a certificate authority (for example, ACM, AWS Private Certificate Authority [ACM PCA]) • Implementing secure DNS communications

Devops

Devops Domain 1: SDLC Automation Task Statement 1.1: Implement CI/CD pipelines. Knowledge of: • Software development lifecycle (SDLC) concepts, phases, and models • Pipeline deployment patterns for single- and multi-account environments
Skills in: • Configuring code, image, and artifact repositories • Using version control to integrate pipelines with application environments • Setting up build processes (for example, AWS CodeBuild) • Managing build and deployment secrets (for example, AWS Secrets Manager, AWS Systems Manager Parameter Store) •Determining appropriate deployment strategies (for example, AWS CodeDeploy)
Task Statement 1.2: Integrate automated testing into CI/CD pipelines.
Knowledge of: •Different types of tests (for example, unit tests, integration tests, acceptance tests, user interface tests, security scans) • Reasonable use of different types of tests at different stages of the CI/CD pipeline
Skills in: • Running builds or tests when generating pull requests or code merges (for example, AWS CodeCommit, CodeBuild) •Running load/stress tests, performance benchmarking, and application testing at scale • Measuring application health based on application exit codes • Automating unit tests and code coverage •Invoking AWS services in a pipeline for testing Task Statement 1.3: Build and manage artifacts. Knowledge of: • Artifact use cases and secure management • Methods to create and generate artifacts • Artifact lifecycle considerations
Skills in: • Creating and configuring artifact repositories (for example, AWS CodeArtifact, Amazon S3, Amazon Elastic Container Registry [Amazon ECR]) • Configuring build tools for generating artifacts (for example, CodeBuild, AWS Lambda) • Automating Amazon EC2 instance and container image build processes (for example, EC2 Image Builder)
Task Statement 1.4: Implement deployment strategies for instance, container, and serverless environments.
Knowledge of: •Deployment methodologies for various platforms (for example, Amazon EC2, Amazon Elastic Container Service [Amazon ECS], Amazon Elastic

Kubernetes Service [Amazon EKS], Lambda) • Application storage patterns (for example, Amazon Elastic File System
[Amazon EFS], Amazon S3, Amazon Elastic Block Store [Amazon EBS]) • Mutable deployment patterns in contrast to immutable deployment patterns • Tools and services available for distributing code (for example, CodeDeploy,
EC2 Image Builder) Skills in: • Configuring security permissions to allow access to artifact repositories (for example, AWS Identity and Access Management [IAM], CodeArtifact) • Configuring deployment agents (for example, CodeDeploy agent) • Troubleshooting deployment issues • Using different deployment methods (for example, blue/green, canary) Domain 2: Configuration Management and IaC Task Statement 2.1: Define cloud infrastructure and reusable components to provision and manage systems throughout their lifecycle. Knowledge of: • Infrastructure as code (IaC) options and tools for AWS • Change management processes for IaC-based platforms • Configuration management services and strategies
Skills in: • Composing and deploying IaC templates (for example, AWS Serverless Application Model [AWS SAM], AWS CloudFormation, AWS Cloud
Development Kit [AWS CDK]) • Applying CloudFormation StackSets across multiple accounts and AWS
Regions • Determining optimal configuration management services (for example, AWS OpsWorks, AWS Systems Manager, AWS Config, AWS AppConfig) • Implementing infrastructure patterns, governance controls, and security standards into reusable IaC templates (for example, AWS Service Catalog, CloudFormation modules, AWS CDK)
Task Statement 2.2: Deploy automation to create, onboard, and secure AWS accounts in a multi-account or multi-Region environment.
Knowledge of: • AWS account structures, best practices, and related AWS services
Skills in: • Standardizing and automating account provisioning and configuration • Creating, consolidating, and centrally managing accounts (for example,
AWS Organizations, AWS Control Tower) •Applying IAM solutions for multi-account and complex organization
structures (for example, SCPs, assuming roles) • Implementing and developing governance and security controls at scale
(AWS Config, AWS Control Tower, AWS Security Hub, Amazon Detective, Amazon GuardDuty, AWS Service Catalog, SCPs) Task Statement 2.3: Design and build automated solutions for complex tasks and large-scale environments. Knowledge of:
• AWS services and solutions to automate tasks and processes • Methods and strategies to interact with the AWS software-defined infrastructure
Skills in: • Automating system inventory, configuration, and patch management (for example, Systems Manager, AWS Config) • Developing Lambda function automations for complex scenarios (for
example, AWS SDKs, Lambda, AWS Step Functions) • Automating the configuration of software applications to the desired state
(for example, OpsWorks, Systems Manager State Manager) • Maintaining software compliance (for example, Systems Manager)
Domain 3: Resilient Cloud Solutions
Task Statement 3.1: Implement highly available solutions to meet resilience and business requirements.
Knowledge of: •Multi-AZ and multi-Region deployments (for example, compute layer,

data
layer) • SLAs • Replication and failover methods for stateful services • Techniques to achieve high availability (for example, Multi-AZ, multi-Region)
Skills in: • Translating business requirements into technical resiliency needs • Identifying and remediating single points of failure in existing workloads • Enabling cross-Region solutions where available (for example, Amazon
DynamoDB, Amazon RDS, Amazon Route 53, Amazon S3, Amazon CloudFront) • Configuring load balancing to support cross-AZ services • Configuring applications and related services to support multiple
Availability Zones and Regions while minimizing downtime Task Statement 3.2: Implement solutions that are scalable to meet business requirements. Knowledge of:
• Appropriate metrics for scaling services • Loosely coupled and distributed architectures • Serverless architectures • Container platforms
Skills in: • Identifying and remediating scaling issues • Identifying and implementing appropriate auto scaling, load balancing, and
caching solutions • Deploying container-based applications (for example, Amazon ECS, Amazon
EKS) • Deploying workloads in multiple Regions for global scalability • Configuring serverless applications (for example, Amazon API Gateway, Lambda, AWS Fargate)
Task Statement 3.3: Implement automated recovery processes to meet RTO and RPO requirements.
Knowledge of: •Disaster recovery concepts (for example, RTO, RPO) • Backup and recovery strategies (for example, pilot light, warm standby) • Recovery procedures
Skills in: • Testing failover of Multi-AZ and multi-Region workloads (for example, Amazon RDS, Amazon Aurora, Route 53, CloudFront) • Identifying and implementing appropriate cross-Region backup and recovery strategies (for example, AWS Backup, Amazon S3, Systems
Manager) • Configuring a load balancer to recover from backend failure Domain 4: Monitoring and Logging Task Statement 4.1: Configure the collection, aggregation, and storage of logs and metrics. Knowledge of: • How to monitor applications and infrastructure • Amazon CloudWatch metrics (for example, namespaces, metrics, dimensions,
and resolution) • Real-time log ingestion • Encryption options for at-rest and in-transit logs and metrics (for example,
client-side and server-side, AWS Key Management Service [AWS KMS]) • Security configurations (for example, IAM roles and permissions to allow for log collection)
Skills in: • Securely storing and managing logs •Creating CloudWatch metrics from log events by using metric filters • Creating CloudWatch metric streams (for example, Amazon S3 or Amazon
Kinesis Data Firehose options) • Collecting custom metrics (for example, using the CloudWatch agent) • Managing log storage lifecycles (for example, S3 lifecycles, CloudWatch log
group retention) • Processing log data by using CloudWatch log subscriptions (for example,
Kinesis, Lambda, Amazon OpenSearch Service) • Searching log data by using filter and pattern syntax or CloudWatch Logs
Insights • Configuring encryption of log data (for example, AWS KMS) Task

Statement 4.2: Audit, monitor, and analyze logs and metrics to detect issues.
Knowledge of: • Anomaly detection alarms (for example, CloudWatch anomaly detection) • Common CloudWatch metrics and logs (for example, CPU utilization with
Amazon EC2, queue length with Amazon RDS, 5xx errors with an
Application Load Balancer [ALB]) • Amazon Inspector and common assessment templates • AWS Config rules • AWS CloudTrail log events
Skills in: • Building CloudWatch dashboards and Amazon QuickSight visualizations • Associating CloudWatch alarms with CloudWatch metrics (standard and custom) • Configuring AWS X-Ray for different services (for example, containers, API
Gateway, Lambda) • Analyzing real-time log streams (for example, using Kinesis Data Streams) •Analyzing logs with AWS services (for example, Amazon Athena, CloudWatch Logs Insights)
Task Statement 4.3: Automate monitoring and event management of complex environments.
Knowledge of: • Event-driven, asynchronous design patterns (for example, S3 Event Notifications or Amazon EventBridge events to Amazon Simple Notification
Service [Amazon SNS] or Lambda) • Capabilities of auto scaling for a variety of AWS services (for example, EC2
Auto Scaling groups, RDS storage auto scaling, DynamoDB, ECS capacity provider, EKS autoscalers) • Alert notification and action capabilities (for example, CloudWatch alarms
to Amazon SNS, Lambda, EC2 automatic recovery) • Health check capabilities in AWS services (for example, ALB target groups,
Route 53) Skills in: • Configuring solutions for auto scaling (for example, DynamoDB, EC2 Auto
Scaling groups, RDS storage auto scaling, ECS capacity provider) • Creating CloudWatch custom metrics and metric filters, alarms, and notifications (for example, Amazon SNS, Lambda) • Configuring S3 events to process log files (for example, by using Lambda)
and deliver log files to another destination (for example, OpenSearch
Service, CloudWatch Logs) • Configuring EventBridge to send notifications based on a particular event
pattern • Installing and configuring agents on EC2 instances (for example, AWS Systems Manager Agent [SSM Agent], CloudWatch agent) • Configuring AWS Config rules to remediate issues • Configuring health checks (for example, Route 53, ALB)
Domain 5: Incident and Event Response
Task Statement 5.1: Manage event sources to process, notify, and take action in response to events.
Knowledge of: • AWS services that generate, capture, and process events (for example, AWS
Health, EventBridge, CloudTrail) • Event-driven architectures (for example, fan out, event streaming, queuing)
Skills in: • Integrating AWS event sources (for example, AWS Health, EventBridge, CloudTrail) • Building event processing workflows (for example, Amazon Simple Queue
Service [Amazon SQS], Kinesis, Amazon SNS, Lambda, Step Functions) Task Statement 5.2: Implement configuration changes in response to events. Knowledge

of: • Fleet management services (for example, Systems Manager, AWS Auto Scaling) • Configuration management services (for example, AWS Config)
Skills in: • Applying configuration changes to systems • Modifying infrastructure configurations in response to events • Remediating a non-desired system state
Task Statement 5.3: Troubleshoot system and application failures.
Knowledge of: • AWS metrics and logging services (for example, CloudWatch, X-Ray) • AWS service health services (for example, AWS Health, CloudWatch, Systems Manager OpsCenter) • Root cause analysis
Skills in: • Analyzing failed deployments (for example, AWS CodePipeline, CodeBuild,
CodeDeploy, CloudFormation, CloudWatch synthetic monitoring) • Analyzing incidents regarding failed processes (for example, auto scaling, Amazon ECS, Amazon EKS)
Domain 6: Security and Compliance
Task Statement 6.1: Implement techniques for identity and access management at scale.
Knowledge of: • Appropriate usage of different IAM entities for human and machine access
(for example, users, groups, roles, identity providers, identity-based policies, resource-based policies, session policies) • Identity federation techniques (for example, using IAM identity providers
and AWS IAM Identity Center [AWS Single Sign-On]) • Permission management delegation by using IAM permissions boundaries • Organizational SCPs Skills in: • Designing policies to enforce least privilege access • Implementing role-based and attribute-based access control patterns • Automating credential rotation for machine identities (for example, Secrets
Manager) • Managing permissions to control access to human and machine identities
(for example, enabling multi-factor authentication [MFA], AWS Security Token Service [AWS STS], IAM profiles)
Task Statement 6.2: Apply automation for security controls and data protection.
Knowledge of: • Network security components (for example, security groups, network ACLs,
routing, AWS Network Firewall, AWS WAF, AWS Shield) • Certificates and public key infrastructure (PKI) • Data management (for example, data classification, encryption, key
management, access controls)
Skills in: • Automating the application of security controls in multi-account and multi-Region environments (for example, Security Hub, Organizations, AWS Control Tower, Systems Manager) • Combining security controls to apply defense in depth (for example, AWS
Certificate Manager [ACM], AWS WAF, AWS Config, AWS Config rules, Security Hub, GuardDuty, security groups, network ACLs, Amazon Detective, Network Firewall) • Automating the discovery of sensitive data at scale (for example, Amazon Macie) • Encrypting data in transit and data at rest (for example, AWS KMS, AWS CloudHSM, ACM) Task Statement 6.3: Implement security monitoring and auditing solutions. Knowledge of: • Security auditing services and features (for example, CloudTrail, AWS
Config, VPC Flow Logs, CloudFormation drift detection) • AWS services for identifying security vulnerabilities and events (for

example, GuardDuty, Amazon Inspector, IAM Access Analyzer, AWS Config) • Common cloud security threats (for example, insecure web traffic, exposed AWS access keys, S3 buckets with public access enabled or encryption disabled) Skills in: • Implementing robust security auditing • Configuring alerting based on unexpected or anomalous security events • Configuring service and application logging (for example, CloudTrail, CloudWatch Logs) • Analyzing logs, metrics, and security findings

AWS Certified Security -

. Domínio 1: Detecção de ameaças e resposta a incidentes
Declaração de tarefa 1.1: Projetar e implementar um plano de resposta a incidentes.
Conhecimento sobre: • Práticas recomendadas da AWS para resposta a incidentes • Incidentes na nuvem • Funções e responsabilidades no plano de resposta a incidentes • Formato de busca de segurança da AWS (ASFF)
Habilidades em: • Implementar estratégias de invalidação e de troca de credenciais em resposta a comprometimentos (por exemplo, usando o AWS Identity and Access Management [IAM] e o AWS Secrets Manager) • Isolar recursos da AWS • Projetar e implementar manuais e runbooks para respostas a incidentes de segurança • Implantar serviços de segurança (por exemplo, AWS Security Hub, Amazon Macie, Amazon GuardDuty, Amazon Inspector, AWS Config, Amazon Detective, AWS Identity and Access Management Access Analyzer) • Configurar integrações com serviços nativos da AWS e serviços de terceiros (por exemplo, usando o Amazon EventBridge e o ASFF)
Declaração de tarefa 1.2: Detectar ameaças e anomalias de segurança usando os serviços da AWS.
Conhecimento sobre: • Serviços de segurança gerenciados pela AWS que detectam ameaças • Técnicas de anomalia e correlação para unir dados entre serviços • Visualizações para identificar anomalias • Estratégias para centralizar as descobertas de segurança
Habilidades em: • Avaliar as descobertas dos serviços de segurança (por exemplo, GuardDuty, Security Hub, Macie, AWS Config, IAM Access Analyzer) • Pesquisar e correlacionar ameaças à segurança nos serviços da AWS (por exemplo, usando o Detective) • Realizar consultas para validar eventos de segurança (por exemplo, usando o Amazon Athena) • Criar painéis e filtros de métricas para detectar atividades anômalas (por exemplo, usando o Amazon CloudWatch)
Declaração de tarefa 1.3: Responder a recursos e cargas de trabalho comprometidos.
Conhecimento sobre: • Guia de resposta a incidentes de segurança da AWS • Mecanismos de isolamento de recursos • Técnicas para análise da causa raiz • Mecanismos de captura de dados • Análise de logs para validação de eventos Habilidades em: • Automatizar a correção usando serviços da AWS (por exemplo, AWS

Lambda, AWS Step Functions, EventBridge, runbooks do AWS Systems Manager, Security Hub, AWS Config) • Responder aos recursos comprometidos (por exemplo, isolando instâncias do Amazon EC2) • Investigar e analisar para realizar a análise da causa raiz (por exemplo, usando o Detective) • Capturar dados forenses relevantes de um recurso comprometido (por exemplo, snapshots de volume do Amazon Elastic Block Store [Amazon EBS], despejo de memória) • Consultar logs no Amazon S3 para coletar informações contextuais relacionadas a eventos de segurança (por exemplo, usando o Athena) • Proteger e preservar artefatos forenses (por exemplo, usando o bloqueio de objetos do S3, contas forenses isoladas, ciclo de vida do S3 e replicação do S3) • Preparar serviços para incidentes e recuperá-los após incidentes

Domínio 2: Registro e monitoramento de segurança

Declaração de tarefa 2.1: Projetar e implementar monitoramento e alertas para abordar eventos de segurança.

Conhecimento sobre: • Serviços da AWS que monitoram eventos e fornecem alarmes (por exemplo, CloudWatch, EventBridge) • Serviços da AWS que automatizam alertas (por exemplo, Lambda, Amazon Simple Notification Service [Amazon SNS], Security Hub) •Ferramentas que monitoram métricas e listas de referência (por exemplo, GuardDuty, Systems Manager)

Habilidades em: • Analisar arquiteturas para identificar requisitos de monitoramento e origens de dados para monitoramento de segurança • Analisar ambientes e cargas de trabalho para determinar os requisitos de monitoramento • Projetar o monitoramento do ambiente e o monitoramento da carga de trabalho com base nos requisitos de negócios e de segurança • Configurar ferramentas e scripts automatizados para realizar auditorias regulares (por exemplo, criando informações personalizadas no Security Hub) • Definir as métricas e os limites que geram alertas

Declaração de tarefa 2.2: Solucionar problemas de monitoramento e alertas de segurança.

Conhecimento sobre: • Configuração de serviços de monitoramento (por exemplo, Security Hub) • Dados relevantes que indicam eventos de segurança

Habilidades em: • Analisar a funcionalidade do serviço, as permissões e a configuração dos recursos após um evento que não forneceu visibilidade ou alerta • Analisar e corrigir a configuração de um aplicativo personalizado que não está relatando as respectivas estatísticas • Avaliar os serviços de registro e monitoramento para alinhamento com os requisitos de segurança

Declaração de tarefa 2.3: Projetar e implementar uma solução de registro em log.

Conhecimento sobre: • Serviços e recursos da AWS que fornecem funcionalidades de registro (por exemplo, logs de fluxo da VPC, logs de DNS, AWS CloudTrail, Amazon CloudWatch Logs) • Atributos das funcionalidades de registro (por exemplo, níveis de log, tipo,

verbosidade) • Destinos de log e gerenciamento do ciclo de vida (por exemplo, período de
retenção)
Habilidades em: • Configurar o registro para serviços e aplicativos • Identificar requisitos de registro e origens para ingestão de logs Implementar o armazenamento de logs e o gerenciamento do ciclo de vida de acordo com os requisitos organizacionais e as práticas recomendadas da AWS Declaração de tarefa 2.4: Solucionar problemas de registros em log. Conhecimento sobre: • Recursos e casos de uso de serviços da AWS que fornecem origens dos dados (por exemplo, nível de log, tipo, verbosidade, cadência, pontualidade, imutabilidade) • Serviços e recursos da AWS que fornecem funcionalidades de registro (por
exemplo, logs de fluxo da VPC, logs de DNS, CloudTrail, CloudWatch Logs) • Permissões de acesso necessárias para o registro
Habilidades em: • Identificar a configuração incorreta e determinar as etapas de correção para
permissões de acesso ausentes que são necessárias para o registro (por exemplo, gerenciar permissões de leitura/gravação, permissões de bucket do S3, acesso público e integridade) • Determinar a causa da falta de logs e executar as etapas de correção Declaração de tarefa 2.5: Projetar uma solução de análise de logs.
Conhecimento sobre: • Serviços e ferramentas para analisar logs capturados (por exemplo, Athena,
filtro do CloudWatch Logs) • Recursos de análise de logs dos serviços da AWS (por exemplo, CloudWatch
Logs Insights, CloudTrail Insights, Security Hub Insights) • Formato e componentes do log (por exemplo, logs do CloudTrail)
Habilidades em: • Identificar padrões em logs para indicar anomalias e ameaças conhecidas • Normalizar, analisar e correlacionar logs Domínio 3: Segurança de infraestrutura Declaração de tarefa 3.1: Projetar e implementar controles de segurança para serviços de borda. Conhecimento sobre: • Recursos de segurança em serviços de borda (por exemplo, AWS WAF,
balanceadores de carga, Amazon Route 53, Amazon CloudFront, AWS
Shield) • Ataques, ameaças e explorações comuns (por exemplo, Top 10 do Open Web Application Security Project [OWASP], DDoS) • Arquitetura de aplicativos web em camadas
Habilidades em: • Definir estratégias de segurança de borda para casos de uso comuns (por
exemplo, site público, aplicativo sem servidor, back-end de aplicativo
móvel) • Selecionar serviços de borda apropriados com base nas ameaças e ataques
previstos (por exemplo, Top 10 do OWASP, DDoS) • Selecionar proteções apropriadas com base nas vulnerabilidades e nos
riscos previstos (por exemplo, software, aplicativos e bibliotecas
vulneráveis) • Definir camadas de defesa combinando serviços de segurança de borda (por
exemplo, CloudFront com AWS WAF e balanceadores de carga) • Aplicar restrições na borda com base em vários critérios (por exemplo, geografia, geolocalização, limite de taxa) • Ativar logs, métricas e monitoramento de serviços de borda para indicar
ataques

Declaração de tarefa 3.2: Projetar e implementar controles de segurança de rede.
Conhecimento sobre: • Mecanismos de segurança da VPC (por exemplo, grupos de segurança, ACLs
de rede, AWS Network Firewall) • Conectividade entre VPC (por exemplo, AWS Transit Gateway, endpoints de
VPC) • Origens de telemetria de segurança (por exemplo, espelhamento de tráfego, logs de fluxo da VPC) • Tecnologia, terminologia e uso de VPN • Opções de conectividade on-premises (por exemplo, AWS VPN, AWS Direct Connect)
Habilidades em: • Implementar a segmentação de rede com base em requisitos de segurança
(por exemplo, sub-redes públicas, sub-redes privadas, VPCs sigilosas, conectividade on-premises) • Projetar controles de rede para permitir ou impedir o tráfego de rede
conforme necessário (por exemplo, usando grupos de segurança, ACLs de rede e firewall de rede) • Projetar fluxos de rede para manter os dados fora da Internet pública (por
exemplo, usando Transit Gateway, endpoints de VPC e Lambda em VPCs) • Determinar quais origens de telemetria monitorar com base no projeto, nas ameaças e nos ataques da rede (por exemplo, logs do balanceador de carga, logs de fluxo da VPC, espelhamento de tráfego) • Determinar os requisitos de redundância e de carga de trabalho de
segurança para comunicação entre ambientes on-premises e a nuvem AWS (por exemplo, usando AWS VPN, AWS VPN via Direct Connect e MACsec) • Identificar e remover o acesso desnecessário à rede • Gerenciar configurações de rede conforme os requisitos mudam (por
exemplo, usando o AWS Firewall Manager)
Declaração de tarefa 3.3: Projetar e implementar controles de segurança para cargas de trabalho de computação.
Conhecimento sobre: • Provisionamento e manutenção de instâncias do EC2 (por exemplo,
aplicação de patches, inspeção, criação de snapshots e AMIs, uso do EC2 Image Builder) • Perfis de instância do IAM e perfis de serviço do IAM • Serviços que verificam vulnerabilidades em cargas de trabalho de computação (por exemplo, Amazon Inspector, Amazon Elastic Container Registry [Amazon ECR]) Segurança baseada em host (por exemplo, firewalls, proteção)
Habilidades em: • Criar AMIs reforçadas do EC2 • Aplicar perfis de instância e perfis de serviço conforme apropriado para
autorizar cargas de trabalho de computação • Verificar instâncias do EC2 e imagens de contêineres em busca de
vulnerabilidades conhecidas • Aplicar patches em uma frota de instâncias do EC2 ou imagens de
contêineres • Ativar mecanismos de segurança baseados em host (por exemplo, firewalls
baseados em host) • Analisar as descobertas do Amazon Inspector e determinar as técnicas de
mitigação apropriadas • Transmitir segredos e credenciais com segurança para cargas de trabalho de
computação
Declaração de tarefa 3.4: Solucionar problemas de segurança de rede.

Conhecimento sobre: • Como analisar a acessibilidade (por exemplo, usando o VPC Reachability
Analyzer e o Amazon Inspector) • Conceitos fundamentais de redes TCP/IP (por exemplo, UDP comparado
com TCP, portas, modelo Open Systems Interconnection [OSI], utilitários do sistema operacional de rede) • Como ler origens de log relevantes (por exemplo, logs do Route 53, logs do
AWS WAF, logs de fluxo da VPC)
Habilidades em: • Identificar, interpretar e priorizar problemas na conectividade de rede (por
exemplo, usando o Amazon Inspector Network Reachability) • Determinar soluções para produzir o comportamento de rede desejado • Analisar origens de log para identificar problemas • Capturar amostras de tráfego para análise de problemas (por exemplo,
usando o espelhamento de tráfego) Domínio 4: Identity and Access Management
Declaração de tarefa 4.1: Projetar, implementar e solucionar problemas de autenticação de recursos da AWS. Conhecimento sobre: • Métodos e serviços para criar e gerenciar identidades (por exemplo,
federação, provedores de identidade, AWS IAM Identity Center [AWS Single Sign-On], Amazon Cognito) • Mecanismos de credenciamento temporários e de longo prazo • Como solucionar problemas de autenticação (por exemplo, usando o
CloudTrail, o IAM Access Advisor e o simulador de políticas do IAM)
Habilidades em: • Estabelecer identidade por meio de um sistema de autenticação, com base
nos requisitos • Habilitar a autenticação com multifator (MFA) • Determinar quando usar o AWS Security Token Service (AWS STS) para
emitir credenciais temporárias
Declaração de tarefa 4.2: Projetar, implementar e solucionar problemas de autorização de recursos da AWS.
Conhecimento sobre: • Políticas diferentes do IAM (por exemplo, políticas gerenciadas, políticas em
linha, políticas baseadas em identidade, políticas baseadas em recursos, políticas de controle de sessão) • Componentes e impacto de uma política (por exemplo, principal, ação,
recurso, condição) • Como solucionar problemas de autorização (por exemplo, usando o
CloudTrail, o IAM Access Advisor e o simulador de políticas do IAM)
Habilidades em: • Construir estratégias de controle de acesso baseado em atributos (ABAC) e
controle de acesso baseado em perfis (RBAC) •Avaliar os tipos de políticas do IAM para determinados requisitos e cargas
de trabalho • Interpretar o efeito de uma política do IAM em ambientes e cargas de trabalho • Aplicar o princípio de menor privilégio em um ambiente • Impor a separação adequada de deveres • Analisar erros de acesso ou de autorização para determinar causa ou efeito • Investigar permissões, autorizações ou privilégios não intencionais
concedidos a um recurso, um serviço ou uma entidade
Domínio 5: Proteção de dados
Declaração de tarefa 5.1: Projetar e implementar controles que promovam

confidencialidade e integridade aos dados em trânsito.
Conhecimento sobre: • Conceitos de TLS • Conceitos de VPN (por exemplo, IPsec) • Métodos de acesso remoto seguro (por exemplo, SSH, RDP sobre o gerenciador de sessões do Systems Manager) • Conceitos do gerenciador de sessões do Systems Manager • Como os certificados TLS funcionam com vários serviços e recursos de rede
(por exemplo, CloudFront, balanceadores de carga)
Habilidades em: • Projetar conectividade segura entre a AWS e redes on-premises (por
exemplo, usando o Direct Connect e gateways da VPN) • Projetar mecanismos para exigir criptografia ao se conectar a recursos (por
exemplo, Amazon RDS, Amazon Redshift, CloudFront, Amazon S3, Amazon DynamoDB, balanceadores de carga, Amazon Elastic File System [Amazon EFS], Amazon API Gateway) • Exigir TLS para chamadas de API da AWS (por exemplo, com o Amazon S3) • Projetar mecanismos para encaminhar tráfego por conexões seguras (por
exemplo, usando o Systems Manager e o EC2 Instance Connect) • Projetar redes entre regiões usando VIFs privadas e VIFs públicas Declaração de tarefa 5.2: Projetar e implementar controles que promovam confidencialidade e integridade para dados em repouso. Conhecimento sobre: • Seleção da técnicas de criptografia (por exemplo, do lado do cliente, do
lado do servidor, simétrica, assimétrica) • Técnicas de verificação de integridade (por exemplo, algoritmos de hashing,
assinaturas digitais) • Políticas de recursos (por exemplo, para DynamoDB, Amazon S3 e AWS Key
Management Service [AWS KMS]) • Perfis e políticas do IAM
Habilidades em: • Projetar políticas de recursos para restringir o acesso a usuários autorizados
(por exemplo, políticas de bucket do S3, políticas do DynamoDB) • Projetar mecanismos para impedir o acesso público não autorizado (por exemplo, bloqueio de acesso público do S3, prevenção de snapshots
públicos e AMIs públicas) • Configurar serviços para ativar a criptografia de dados em repouso (por
exemplo, Amazon S3, Amazon RDS, DynamoDB, Amazon Simple Queue Service [Amazon SQS], Amazon EBS, Amazon EFS) • Projetar mecanismos para proteger a integridade dos dados evitando
modificações (por exemplo, usando o bloqueio de objetos do S3, as políticas de chave do KMS, o Vault Lock do S3 Glacier e o Vault Lock do AWS Backup) • Projetar a criptografia em repouso usando o AWS CloudHSM para bancos de dados relacionais (por exemplo, Amazon RDS, RDS Custom, bancos de
dados em instâncias do EC2) • Escolher técnicas de criptografia com base nos requisitos de negócios
Declaração de tarefa 5.3: Projetar e implementar controles para gerenciar o ciclo de vida dos dados em repouso.
Conhecimento sobre: • Políticas de ciclo de vida • Padrões de retenção de dados
Habilidades em: • Projetar mecanismos de ciclo de vida do S3 para reter dados durante os
períodos de retenção necessários (por exemplo, bloqueio de objetos do S3, Vault Lock do S3 Glacier, política de ciclo de vida do S3) • Projetar o gerenciamento automático do ciclo de vida de serviços e recursos

da AWS (por exemplo, Amazon S3, snapshots de volume do EBS, snapshots de volume do RDS, AMIs, imagens de contêineres, grupos de logs do CloudWatch, Amazon Data Lifecycle Manager) • Estabelecer cronogramas e retenção para o AWS Backup nos serviços da AWS

Declaração de tarefa 5.4: Projetar e implementar controles para proteger credenciais, segredos e materiais de chaves criptográficas.

Conhecimento sobre: • Secrets Manager • Systems Manager Parameter Store • Uso e gerenciamento de chaves simétricas e assimétricas (por exemplo, AWS KMS)

Habilidades em: • Projetar o gerenciamento e a troca de segredos para cargas de trabalho (por exemplo, credenciais de acesso ao banco de dados, chaves de API, chaves de acesso do IAM, chaves gerenciadas pelo cliente do AWS KMS) • Projetar políticas de chave do KMS para limitar o uso da chave a usuários autorizados • Estabelecer mecanismos para importar e remover material de chave fornecido pelo cliente

Domínio 6: Gerenciamento e governança de segurança

Declaração de tarefa 6.1: Desenvolver uma estratégia para implantar e gerenciar de maneira centralizada as contas da AWS.

Conhecimento sobre: • Estratégias de várias contas • Serviços gerenciados que permitem a administração delegada •Proteções definidas por políticas • Práticas recomendadas da conta-raiz • Perfis entre contas

Habilidades em: • Implantar e configurar o AWS Organizations • Determinar quando e como implantar o AWS Control Tower (por exemplo, quais serviços devem ser desativados para uma implantação bem-sucedida) • Implementar SCPs como uma solução técnica para aplicar uma política (por exemplo, limitações no uso de uma conta raiz, implementação de controles no AWS Control Tower) • Gerenciar de forma centralizada os serviços de segurança e agregar descobertas (por exemplo, usando administração delegada e agregadores do AWS Config) • Proteger as credenciais do usuário-raiz da conta da AWS

Declaração de tarefa 6.2: Implementar uma estratégia de implantação segura e consistente para recursos de nuvem.

Conhecimento sobre: • Práticas recomendadas de implantação com infraestrutura como código (IaC) (por exemplo, fortalecimento de modelos do AWS CloudFormation e detecção de desvios) • Práticas recomendadas para marcação • Gerenciamento, implantação e versionamento centralizados dos serviços da AWS • Visibilidade e controle sobre a infraestrutura da AWS

Habilidades em: • Usar o CloudFormation para implantar recursos de nuvem de forma consistente e segura • Implementar e aplicar estratégias de marcação de várias contas • Configurar e implantar portfólios de serviços aprovados da AWS (por exemplo, usando o AWS Service Catalog) • Organizar os recursos da AWS em diferentes grupos para gerenciamento • Implantar o Firewall Manager para aplicar políticas Compartilhar com segurança recursos entre contas da AWS (por exemplo, usando o AWS Resource Access Manager [AWS RAM]) Declaração de tarefa 6.3: Avaliar a conformidade dos recursos da AWS. Conhecimento sobre: • Classificação de dados usando os serviços da AWS •Como analisar, auditar e avaliar as configurações dos recursos da AWS (por

exemplo, usando o AWS Config)
Habilidades em: • Identificar dados sigilosos usando o Macie • Criar regras do AWS Config para detecção de recursos da AWS que não estão em conformidade • Coletar e organizar evidências usando o Security Hub e o AWS Audit
Manager
Declaração de tarefa 6.4: Identificar as falhas de segurança por meio de avaliações de arquitetura e análise de custos.
Conhecimento sobre: • Custo e uso da AWS para identificação de anomalias • Estratégias para reduzir as superfícies de ataque • AWS Well-Architected Framework
Habilidades em: • Identificar anomalias com base na utilização de recursos e tendências • Identificar recursos não utilizados usando serviços e ferramentas da AWS
(por exemplo, AWS Trusted Advisor, AWS Cost Explorer) • Usar a ferramenta do AWS Well-Architected para identificar falhas de
segurança

1) A gaming company is planning to launch a globally available game that is hosted in one AWS Region. The game backend is hosted on Amazon EC2 instances that are part of an Auto Scaling group. The game uses the gRPC protocol for bidirectional streaming between game clients and the backend. The company needs to filter incoming traffic based on the source IP address to protect the game.

Which solution will meet these requirements?

A) Configure an AWS Global Accelerator accelerator with an Application Load Balancer (ALB) endpoint. Attach the ALB to the Auto Scaling group. Configure an AWS WAF web ACL for the ALB to filter traffic based on the source IP address.
B) Configure an AWS Global Accelerator accelerator with a Network Load Balancer (NLB) endpoint. Attach the NLB to the Auto Scaling group. Configure security groups for the EC2 instances to filter traffic based on the source IP address.
C) Configure an Amazon CloudFront distribution with an Application Load Balancer (ALB) endpoint. Attach the ALB to the Auto Scaling group. Configure an AWS WAF web ACL for the ALB to filter traffic based on the source IP address.
D) Configure an Amazon CloudFront distribution with a Network Load Balancer (NLB) endpoint. Attach the NLB to the Auto Scaling group. Configure security groups for the EC2 instances to filter traffic based on the source IP address.

2) A company has multiple VPCs in the us-east-1 Region. The company has deployed a website in one of the VPCs. The company wants to implement split-view DNS so that the website is accessible internally from the VPCs and externally over the internet with the same domain name, example.com.

Which solution will meet these requirements?

A) Change the DHCP options for each VPC to use the IP address of an on-premises DNS server. Create a private hosted zone and a public hosted zone for example.com. Map the private hosted zone to the website's internal IP address. Map the public hosted zone to the website's external IP address.
B) Create Amazon Route 53 private hosted zones and public hosted zones that have the same name, example.com. Associate the VPCs with the private hosted zone. Create records in each hosted zone that determine how traffic is routed.
C) Create an Amazon Route 53 Resolver inbound endpoint for resolving example.com internally. Create a Route 53 public hosted zone for routing external DNS queries.
D) Create an Amazon Route 53 Resolver outbound endpoint for resolving example.com externally. Create a Route 53 private hosted zone for routing internal DNS queries.

3) A company has developed a new web application that processes confidential data that is hosted on Amazon EC2 instances. The application needs to scale and must use certificates to authenticate clients. The application is configured to request a client's certificate and will validate the certificate as part of the initial handshake.

Which Elastic Load Balancing (ELB) solution will meet these requirements?

A) Configure an Application Load Balancer (ALB) that includes an HTTPS listener on port 443. Create an Auto Scaling group for the EC2 instances. Configure the Auto Scaling group as the target group of the ALB. Configure HTTPS as the protocol for the target group.
B) Configure a Network Load Balancer (NLB) that includes a TLS listener on port 443. Create an Auto Scaling group for the EC2 instances. Configure the Auto Scaling group as the target group of the NLB. Configure the NLB to terminate TLS. Configure TLS as the protocol for the target group.
C) Configure a Network Load Balancer (NLB) that includes a TCP listener on port 443. Create an Auto Scaling group for the EC2 instances. Configure the Auto Scaling group as the target group of the NLB. Configure TCP as the protocol for the target group.
D) Configure an Application Load Balancer (ALB) that includes a TLS listener on port 443. Create an Auto Scaling group for the EC2 instances. Configure the Auto Scaling group as the target group of the ALB. Configure TLS as the protocol for the target group.

4) A company collects a high volume of shipping data and stores the data in an on-premises data center. A network engineer wants to use Amazon S3 to store the data during the first phase of a migration to AWS. During this phase, an application that resides in the data center will need to access the data privately in an S3 bucket that the company created.

The company has set up an AWS Direct Connect connection with a private VIF to connect the on-premises data center to a VPC. The network engineer plans to use this Direct Connect connection for the hybrid cloud setup. The solution must be highly available.

What should the network engineer do next to implement this architecture?

A) Configure an S3 gateway endpoint in the VPC. Update VPC route tables to route traffic to the S3 gateway endpoint. Configure the S3 gateway endpoint DNS name in the on-premises application.
B) Configure an S3 interface endpoint in the VPC. Configure the S3 interface endpoint DNS name in the on-premises application.
C) Configure an S3 gateway endpoint in the VPC. Update VPC route tables to route traffic to the S3 gateway endpoint. Configure an HTTP proxy on an Amazon EC2 instance in the VPC to route traffic to the S3 gateway endpoint. Configure the HTTP proxy DNS name in the on-premises application.
D) Configure an S3 interface endpoint in the VPC. Update VPC route tables to route traffic to the S3 interface endpoint. Configure an HTTP proxy on an Amazon EC2 instance in the VPC to route traffic to the S3 interface endpoint. Configure the HTTP proxy DNS name in the on-premises application.

5) A company is designing infrastructure on AWS with three VPCs connected to a transit gateway. The three VPCs are an application VPC, a backend VPC, and an inspection VPC. The application VPC and the backend VPC have compute instances deployed in Availability Zone A and Availability Zone B. Stateful firewalls are deployed in the same Availability Zones in the inspection VPC, which is a shared services VPC.

All traffic is routed through the inspection VPC through the stateful layer 7 virtual firewall appliances to comply with a security policy that mandates traffic inspection. There are no overlapping IP addresses across the three VPCs. A network engineer must ensure that traffic between the application VPC and the backend VPC can route through the inspection VPC's stateful firewalls.

Which solution will meet these requirements?

A) Create IPsec VPN connections between the transit gateway and the virtual firewall appliances.
B) Configure Virtual Router Redundancy Protocol (VRRP) on the virtual firewall appliances.
C) Set up BGP between the transit gateway and the virtual firewall appliances.
D) Enable transit gateway appliance mode for the VPC attachment to the inspection VPC.

6) A company hosts a public hosted zone in Amazon Route 53. The company wants to configure DNS Security Extensions (DNSSEC) signing for the public hosted zone. All the company's business-critical applications are running in the us-west-2 Region.

The company has created a symmetric, customer managed, single-Region key in us-west-2 by using AWS Key Management Service (AWS KMS). A network engineer finds that the existing AWS KMS key cannot be used to create a key-signing key (KSK).

How can the network engineer resolve this issue?

A) Recreate a symmetric, customer managed, multi-Region key in the us-east-1 Region. Use this key to create a KSK.
B) Recreate a symmetric, customer managed, single-Region key in us-west-2. Use this key to create a KSK.
C) Recreate an asymmetric, customer managed key with an ECC_NIST_P256 key spec in the us-east-1 Region. Use this key to create a KSK.
D) Recreate an asymmetric, customer managed key with an ECC_NIST_P256 key spec in us-west-2. Use this key to create a KSK.

7) A company is migrating many applications from two on-premises data centers to AWS. The company's network team is setting up connectivity to the AWS environment. The migration will involve spreading the applications across two AWS Regions: us-east-1 and us-west-2. The company has set up AWS Direct Connect connections at two different locations. Direct Connect connection 1 is to the first data center and is at a location in us-east-1. Direct Connect connection 2 is to the second data center and is at a location in us-west-2.

The company has connected both Direct Connect connections to a single Direct Connect gateway by using transit VIFs. The Direct Connect gateway is associated with transit gateways that are deployed in each Region. All traffic to and from AWS must travel through the first data center. In the event of failure, the second data center must take over the traffic.

How should the network team configure BGP to meet these requirements?

A) Configure the local preference BGP community tag 7224:7300 for the transit VIF connected to Direct Connect connection 1.
B) Configure the local preference BGP community tag 7224:9300 for the transit VIF connected to Direct Connect connection 2.
C) Use the AS_PATH attribute to prepend the additional hop for the transit VIF connected to Direct Connect connection 2.
D) Use the AS_PATH attribute to prepend the additional hop for the transit VIF connected to Direct Connect connection 1.

8) An ecommerce company has a business-critical application that runs on Amazon EC2 instances in a VPC. The company's development team has been testing a new version of the application on test EC2 instances. The development team wants to test the new application version against production traffic to address any problems that might occur before the company releases the new version across all servers.

Which solution will meet this requirement with no impact on the end user's experience?

A) Configure Amazon Route 53 weighted routing policies by configuring records that have the same name and type as each of the instances. Assign relative weights to the production instances and the test instances.
B) Create an Application Load Balancer with weighted target groups. Add more than one target group to the forward action of a listener rule. Specify a weight for each target group.
C) Implement Traffic Mirroring to replay the production requests to the test instances. Configure the source as the production instances. Configure the target as the test instances.
D) Configure an NGINX proxy in front of the production servers. Use the NGINX mirroring capability.

9) A company hosts its ecommerce application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances are in a private subnet with the default DHCP options set. Internet connectivity is through a NAT gateway that is configured in the public subnet.

A third-party audit of the security infrastructure identifies a DNS exfiltration vulnerability. The company must implement a highly available solution that protects against this vulnerability.

Which solution will meet these requirements MOST cost-effectively?

A) Configure a BIND server with DNS filtering. Modify the DNS servers in the DHCP options set.
B) Use Amazon Route 53 Resolver DNS Firewall. Configure a domain list with a rule group.
C) Use AWS Network Firewall with domain name filtering.
D) Configure an Amazon Route 53 Resolver outbound endpoint with rules to filter and block suspicious traffic.

10) A company is using Amazon Route 53 Resolver for its hybrid DNS infrastructure. The company is using Route 53 Resolver forwarding rules for authoritative domains that are hosted on on-premises DNS servers. The company achieves hybrid network connectivity by using an AWS Site-to-Site VPN connection.

A new governance policy requires logging for DNS traffic that originates in the AWS Cloud. The policy also requires the company to query DNS traffic to identify the source IP address of the resources that the query originated from, along with the DNS name that was requested.

Which solution will meet these requirements?

A) Create VPC flow logs for all VPCs. Send the logs to Amazon CloudWatch Logs. Use CloudWatch Logs Insights to query the IP address and DNS name.
B) Configure Route 53 Resolver query logging for all VPCs. Send the logs to Amazon CloudWatch Logs. Use CloudWatch Logs Insights to query the IP address and DNS name.
C) Configure DNS logging for the Site-to-Site VPN connection. Send the logs to an Amazon S3 bucket. Use Amazon Athena to query the IP address and DNS name.
D) Modify the existing Route 53 Resolver rules to configure logging. Send the logs to an Amazon S3 bucket. Use Amazon Athena to query the IP address and DNS name.

Answers

1) A **–** The accelerator in AWS Global Accelerator will project low-latency endpoints to the global users of the game. The accelerator also will route the traffic over the AWS network backbone to the AWS Region that is hosting the game. The Application Load Balancer (ALB) will support the use of the gRPC protocol and client IP address preservation. The ALB will distribute traffic to the Amazon EC2 instances in the Auto Scaling group to support the game's load and will provide an endpoint that will support the accelerator. The association of an AWS WAF web ACL with the ALB will provide the required IP filtering.

The other answer options do not meet the requirements. A Network Load Balancer does not support client IP address preservation, and Amazon CloudFront does not support the gRPC protocol.

2) B **–** The solution requires split-view DNS, which is directly supported by Amazon Route 53. You can configure split-view DNS by creating public hosted zones and private hosted zones in Route 53 with the same name. If the private hosted zones are associated with VPCs, Route 53 Resolver will use the private hosted zones to answer queries from those VPCs and will use the public hosted zones to answer public queries.

The other answer options will not work. An on-premises DNS server will not be able to replace Route 53 Resolver for operations within the VPC. A Resolver inbound endpoint will allow on-premises queries from on-premises networks to be resolved. A Resolver outbound endpoint is used to resolve queries from the VPC for on-premises addresses. Neither of those Resolver endpoints will provide the necessary public and internal resolution.

3) C **–** The application must scale to handle load and must use client certificates to authenticate directly with a web server. The solution requires the TLS sessions to be connected to the underlying web server or web servers. The need to scale requires the use of an Auto Scaling group with a load balancer. The load balancer must pass the TLS sessions to the Amazon EC2 instances. This architecture is supported by a Network Load Balancer (NLB) with a TCP listener on port 443. The NLB operates at the transport layer of the stack to pass the connection through to the web servers.

The other answer options will end the TLS connection from the client at the load balancer. These options will not allow the client certificate to be visible to the web servers. The NLB with a TCP listener on port 443 is the only option that will maintain the session all the way from the client to the web servers in the Auto Scaling group.

4) B **–** The question requires a solution that will provide a connection to Amazon S3 from workloads on AWS and from an on-premises data center. An S3 interface endpoint will provide the needed access from workloads on AWS and can support connections from the on-premises environment over AWS Direct Connect. The use of the S3 interface endpoint will require the on-premises client applications to use the endpoint DNS records.

Option A includes the use of a gateway endpoint. Routing to the gateway endpoint depends on the route tables of the VPC, and route tables do not support the use of DNS endpoints for the on-premises application. While option C could route the traffic, this option contains a single point of failure in the HTTP proxy server and does not offer the high availability that the question requires. Option D also contains an HTTP proxy, which is unneeded and creates a single point of failure. This option also includes the use of an interface endpoint name in a route table, which is incorrect.

5) D **–** The correct answer is to enable transit gateway appliance mode for the VPC attachment to the inspection VPC. The underlying issue in the question comes from cross-AZ traffic. When appliance mode is not enabled, a transit gateway attempts to keep traffic routed between VPC attachments in the originating Availability Zone until the traffic reaches its destination. This behavior causes return traffic to be routed to the virtual firewall in the firewall's local Availability Zone rather than to the Availability Zone that initiated the traffic. This discrepancy causes the firewall to drop the traffic.

Option A will create unnecessary connections and will not provide the symmetry that is needed for the traffic to flow through the firewalls. Option B includes the use of Virtual Router Redundancy Protocol (VRRP) for instance load sharing. AWS does not directly support this protocol, which depends on multicast. Multicast is not supported within a VPC. Option C is incorrect because virtual firewall appliances cannot use BGP peering with a transit gateway.

6) C – When Amazon Route 53 creates a key-signing key (KSK), Route 53 requires you to provide a customer managed key. The customer managed key must be located in the us-east-1 Region. The key must be an asymmetric customer managed key with an ECC_NIST_P256 key spec.

The other answer options are incorrect for a combination of two reasons. Option A includes a symmetric key, which violates the requirement for an asymmetric key. Option D correctly includes the asymmetric key, but the key is in the wrong Region. Option B has the wrong key and the wrong Region. Only keys that meet all the requirements can be used to create the KSK and support DNSSEC signing in Route 53.

7) A **–** The correct answer is to configure the local BGP community tag 7224:7300 for the transit VIF connected to the first AWS Direct Connect connection. By default, AWS uses the distance from the local AWS Region to the Direct Connect location to determine the VIF or transit VIF for routing. You can modify this behavior by assigning local preference communities to VIFs. This question asks for the VIF in Direct Connect connection 1 to have a higher preference. AWS supports the 7224:7300 local preference tag for high-preference use cases.

Option B includes the 7224:9300 community tag, which is used to control how far a customer-advertised prefix is propagated. This community tag will not help solve this routing priority problem. The remaining answer options propose the use of the AS_PATH attribute to control the traffic between Direct Connect connections in multiple Regions. This strategy would be appropriate for handling multiple VIFs in a single Region, but this strategy is not appropriate for handling multiple VIFs in this question's multi-Region environment.

8) C **–** Traffic Mirroring is the correct answer. Because this mirroring will occur at the transport layer, all the inbound requests can be captured and mirrored into a test environment without affecting the performance of the production environment. This solution will eliminate any possibility of a user encountering an error that is caused by a test of the new version. The existing production environment will serve all user requests.

The other answer options will either expose some of the users to the new version of the application or will add overhead and a potential failure point. The question requires the solution to have no impact on an end user's experience. By exposing the users to potential errors or performance problems, these options will produce a negative impact.

9) B **–** With Amazon Route 53 Resolver DNS Firewall, you can monitor and control the domains that applications in your VPCs can access. DNS Firewall supports the use of allow lists or deny lists to filter the set of domains that you can use. This solution can effectively prevent the use of DNS queries to exfiltrate data.

In option A, the configuration of a BIND server with DNS filtering could work. However, a single BIND server would be a single point of failure. Additionally, a fleet of BIND servers with load balancers would be more complex and expensive than the correct answer.

In option C, AWS Network Firewall provides filtering of application layer traffic and network layer traffic. However, Network Firewall does not have visibility into queries from Route 53 Resolver. Option D includes the configuration of a Route 53 Resolver outbound endpoint, which is used to forward queries for specific domains to an on-premises DNS server. However, this endpoint does not filter or block traffic.

10) B **–** The correct answer is to configure Amazon Route 53 Resolver query logging for all the VPCs. The query logs can be stored in Amazon CloudWatch Logs and can be analyzed with CloudWatch Logs Insights.

The other answer options will fail to capture the needed DNS queries. In option A, flow logs will fail to capture traffic from the Amazon EC2 instances to the Amazon provided DNS servers. In option C, AWS Site-to-Site VPN connections do not offer an option for DNS logging. In option D, Route 53 Resolver rules do not allow the configuration of logging.

1) **A company hosts a web application on an Amazon EC2 instance. Users report that the web application is occasionally unresponsive. Amazon CloudWatch metrics indicate that the CPU utilization is 100% during these times. A SysOps administrator must implement a solution to monitor for this issue.**

   Which solution will meet this requirement?

   A. Create a CloudWatch alarm that monitors AWS CloudTrail events for the EC2 instance.
   B. Create a CloudWatch alarm that monitors CloudWatch metrics for EC2 instance CPU utilization.
   C. Create an Amazon Simple Notification Service (Amazon SNS) topic to monitor CloudWatch metrics for EC2 instance CPU utilization.
   D. Create a recurring assessment check on the EC2 instance by using Amazon Inspector to detect deviations in CPU utilization.

2) **A company has an application that uses Amazon ElastiCache for Memcached to cache query responses to improve latency. However, the application's users are reporting slow response times. A SysOps administrator notices that the Amazon CloudWatch metrics for Memcached evictions are high.**

   Which actions should the SysOps administrator take to fix this issue? (Select TWO.)

   A. Flush the contents of ElastiCache for Memcached.
   B. Increase the ConnectionOverhead parameter value.
   C. Increase the number of nodes in the cluster.
   D. Increase the size of the nodes in the cluster.
   E. Decrease the number of nodes in the cluster.

3) **A company needs to ensure that an AWS Lambda function can access resources in a VPC in the company's account. The Lambda function requires access to third-party APIs that can be accessed only over the internet.**

   Which action should a SysOps administrator take to meet these requirements?

   A. Attach an Elastic IP address to the Lambda function and configure a route to the internet gateway of the VPC.
   B. Connect the Lambda function to a private subnet that has a route to the virtual private gateway of the VPC.
   C. Connect the Lambda function to a public subnet that has a route to the internet gateway of the VPC.
   D. Connect the Lambda function to a private subnet that has a route to a NAT gateway deployed in a public subnet of the VPC.

4) A company runs an application on a large fleet of Amazon EC2 instances to process financial transactions. The EC2 instances share data by using an Amazon Elastic File System (Amazon EFS) file system.

The company wants to deploy the application to a new Availability Zone and has created new subnets and a mount target in the new Availability Zone. When a SysOps administrator launches new EC2 instances in the new subnets, the EC2 instances are unable to mount the file system.

What is a reason for this issue?

A. The EFS mount target has been created in a private subnet.
B. The IAM role that is associated with the EC2 instances does not allow the efs:MountFileSystem action.
C. The route tables have not been configured to route traffic to a VPC endpoint for Amazon EFS in the new Availability Zone.
D. The security group for the mount target does not allow inbound NFS connections from the security group used by the EC2 instances.

5) A company uses AWS Organizations to create and manage many AWS accounts. The company wants to deploy new IAM roles in each account.

Which action should the SysOps administrator take to deploy the new roles in each of the organization's accounts?

A. Create a service control policy (SCP) in the organization to add the new IAM roles to each account.
B. Deploy an AWS CloudFormation change set to the organization with a template to create the new IAM roles.
C. Use AWS CloudFormation StackSets to deploy a template to each account to create the new IAM roles.
D. Use AWS Config to create an organization rule to add the new IAM roles to each account.

6) **A company runs several production workloads on Amazon EC2 instances. A SysOps administrator discovered that a production EC2 instance failed a system health check. The SysOps administrator recovered the instance manually.**

The SysOps administrator wants to automate the recovery task of EC2 instances and receive notifications whenever a system health check fails. Detailed monitoring is activated for all of the company's production EC2 instances.

Which of the following is the MOST operationally efficient solution that meets these requirements?

A. For each production EC2 instance, create an Amazon CloudWatch alarm for Status Check Failed: System. Set the alarm action to recover the EC2 instance. Configure the alarm notification to be published to an Amazon Simple Notification Service (Amazon SNS) topic.
B. On each production EC2 instance, create a script that monitors the system health by sending a heartbeat notification every minute to a central monitoring server. If an EC2 instance fails to send a heartbeat, run a script on the monitoring server to stop and start the EC2 instance and to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic.
C. On each production EC2 instance, create a script that sends network pings to a highly available endpoint by way of a cron job. If the script detects a network response timeout, invoke a command to reboot the EC2 instance.
D. On each production EC2 instance, configure an Amazon CloudWatch agent to collect and send logs to a log group in Amazon CloudWatch Logs. Create a CloudWatch alarm that is based on a metric filter that tracks errors. Configure the alarm to invoke an AWS Lambda function to reboot the EC2 instance and send a notification email.

7) **The company uses AWS Organizations to manage its accounts. For the production account, a SysOps administrator must ensure that all data is backed up daily for all current and future Amazon EC2 instances and Amazon Elastic File System (Amazon EFS) file systems. Backups must be retained for 30 days.**

Which solution will meet these requirements with the LEAST amount of effort?

A. Create a backup plan in AWS Backup. Assign resources by resource ID, selecting all existing EC2 and EFS resources that are running in the account. Edit the backup plan daily to include any new resources. Schedule the backup plan to run every day with a lifecycle policy to expire backups after 30 days.
B. Create a backup plan in AWS Backup. Assign resources by tags. Ensure that all existing EC2 and EFS resources are tagged correctly. Apply a service control policy (SCP) for the production account OU that prevents instance and file system creation unless the correct tags are applied. Schedule the backup plan to run every day with a lifecycle policy to expire backups after 30 days.
C. Create a lifecycle policy in Amazon Data Lifecycle Manager (Amazon DLM). Assign all resources by resource ID, selecting all existing EC2 and EFS resources that are running in the account. Edit the lifecycle policy daily to include any new resources. Schedule the lifecycle policy to create snapshots every day with a retention period of 30 days.
D. Create a lifecycle policy in Amazon Data Lifecycle Manager (Amazon DLM). Assign all resources by tags. Ensure that all existing EC2 and EFS resources are tagged correctly. Apply a service control policy (SCP) that prevents resource creation unless the correct tags are applied. Schedule the lifecycle policy to create snapshots every day with a retention period of 30 days.

8) A company is using AWS CloudTrail and wants to ensure that SysOps administrators can easily verify that the log files have not been deleted or changed.

Which action should a SysOps administrator take to meet this requirement?

A. Grant administrators access to the AWS Key Management Service (AWS KMS) key used to encrypt the log files.
B. Enable CloudTrail log file integrity validation when the trail is created or updated.
C. Turn on Amazon S3 server access logging for the bucket storing the log files.
D. Configure the S3 bucket to replicate the log files to another bucket.

9) A company is running a custom database on an Amazon EC2 instance. The database stores its data on an Amazon Elastic Block Store (Amazon EBS) volume. A SysOps administrator must set up a backup strategy for the EBS volume.

What should the SysOps administrator do to meet this requirement?

A. Create an Amazon CloudWatch alarm for the VolumeIdleTime metric with an action to take a snapshot of the EBS volume.
B. Create a pipeline in AWS Data Pipeline to take a snapshot of the EBS volume on a recurring schedule.
C. Create an Amazon Data Lifecycle Manager (Amazon DLM) policy to take a snapshot of the EBS volume on a recurring schedule.
D. Create an AWS DataSync task to take a snapshot of the EBS volume on a recurring schedule.

10) A company runs a large number of Amazon EC2 instances for internal departments. The company needs to track the costs of its existing AWS resources by department.

What should a SysOps administrator do to meet this requirement?

A. Activate all of the AWS generated cost allocation tags for the account.
B. Apply user-defined tags to the instances through Tag Editor. Activate these tags for cost allocation.
C. Schedule an AWS Lambda function to run the AWS Pricing Calculator for EC2 usage on a recurring schedule.
D. Use the AWS Trusted Advisor dashboard to export EC2 cost reports.

NOTE: As of March 28, 2023, the AWS Certified SysOps Administrator - Associate exam will not include exam labs until further notice. This removal of exam labs is temporary while we evaluate the exam labs and make improvements to provide an optimal candidate experience. With this change, the exam will consist of 65 multiple-choice questions and multiple-response questions, with an exam time of 130 minutes. All exam prep resources that are available on the exam page remain valid for this changed exam format.

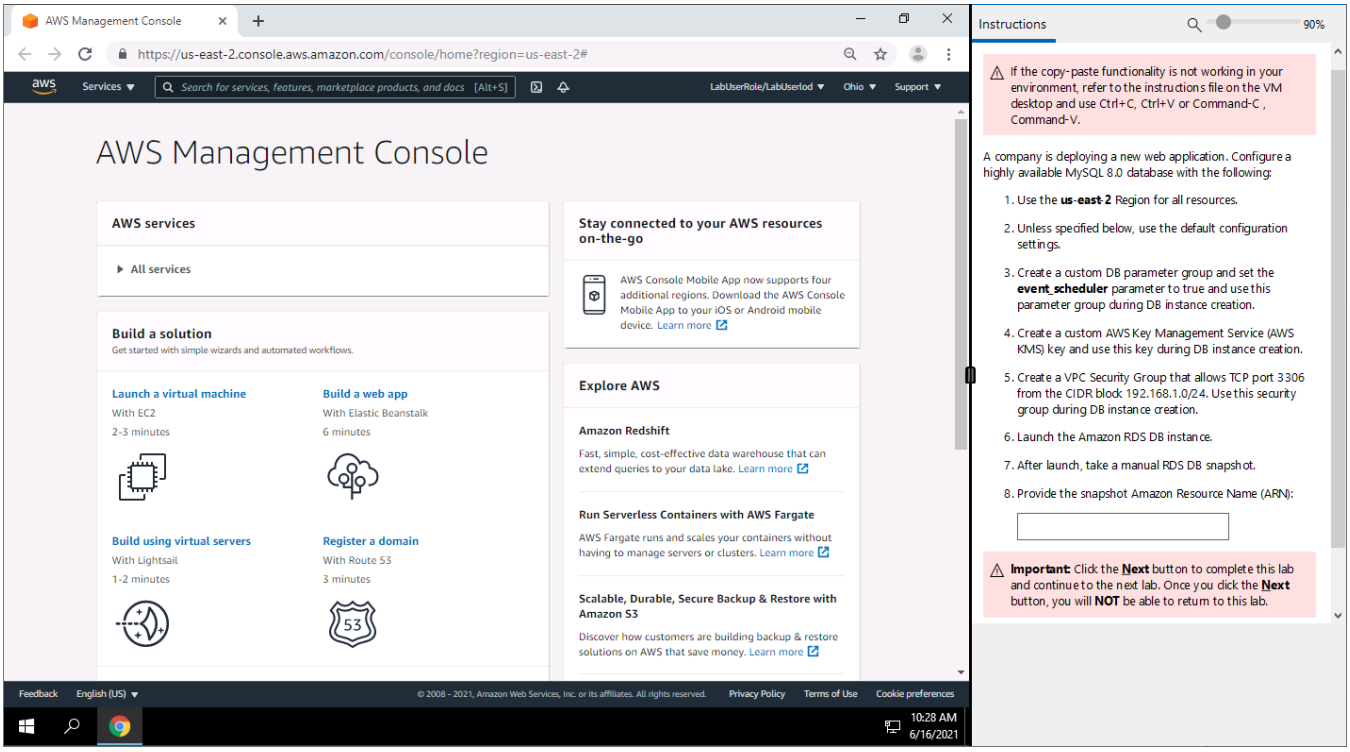
11) Sample Exam Lab

A company is deploying a new web application. Configure a highly available MySQL 8.0 database with the following:

1. Use the **us-east-2** Region for all resources.
2. Unless specified below, use the default configuration settings.
3. Create a custom DB parameter group and set the **event_scheduler** parameter to true and use this parameter group during DB instance creation.
4. Create a custom AWS Key Management Service (AWS KMS) key and use this key during DB instance creation.
5. Create a VPC security group that allows TCP port 3306 from the CIDR block 192.168.1.0/24. Use this security group during DB instance creation.
6. Launch the Amazon RDS DB instance.
7. After launch, take a manual RDS DB snapshot.

Provide the snapshot Amazon Resource Name (ARN): _____

Note: Below is a screenshot of how this sample exam lab would appear during the exam.



Answers

1) B — Amazon CloudWatch provides you with data and actionable insights to monitor your applications. Amazon EC2 sends metrics to CloudWatch. The CPUUtilization metric represents the percentage of allocated EC2 compute units that are currently in use on an instance. You can create a CloudWatch alarm that monitors CPUUtilization for one of your instances. For example, you might want to receive an email notification when the average CPUUtilization over a 5-minute period is greater than 75%.

2) C, D — The Evictions metric for Amazon ElastiCache for Memcached represents the number of non-expired items that the cache evicted to provide space for new items. If you are experiencing evictions with your cluster, it is usually a sign that you need to scale up (use a node that has a larger memory footprint) or scale out (add additional nodes to the cluster) to accommodate the additional data.

3) D — By default, AWS Lambda runs your functions in a secure VPC with access to AWS services and the internet. Lambda owns this VPC, which is not connected to your account's default VPC. When you connect a Lambda function to a VPC in your account to access private resources, the function cannot access the internet unless your VPC provides access. Internet access from a private subnet requires network address translation (NAT). To give your function access to the internet, route outbound traffic to a NAT gateway in a public subnet.

4) D — The security groups that you associate with a mount target must allow inbound access for the TCP protocol on the NFS port from the security group used by the instances.

5) C — With AWS CloudFormation StackSets, you can create, update, or delete stacks across multiple accounts and AWS Regions with a single operation. A user in the AWS Organizations management account can create a stack set with service-managed permissions that deploys stack instances to accounts in the organization or in specific organizational units (OUs). For example, you can use AWS CloudFormation StackSets to deploy your centralized IAM roles to all accounts in your organization.

6) A — You can use Amazon CloudWatch alarm actions to create alarms that automatically stop, terminate, reboot, or recover your Amazon EC2 instances. For example, if an instance becomes impaired due to hardware or software issues on the physical host, loss of network connectivity, or loss of system power, you can automatically initiate a recovery action to migrate the instance to new hardware. You also can configure a message to be published to an Amazon Simple Notification Service (Amazon SNS) topic to receive a notification of the recovery action.

7) B — AWS Backup is a fully managed backup service that makes it easy to centralize and automate the backup of data across AWS services. The use of tags to assign resources is a simple and scalable way to back up multiple resources. Any resources with the tags that you specify are assigned to the backup plan. A tag policy is a type of service control policy (SCP) in AWS Organizations that can help you standardize and enforce tags across resources in your organization's accounts.

8) B — You can validate the integrity of AWS CloudTrail log files and detect whether the log files were unchanged, modified, or deleted since CloudTrail delivered them to your Amazon S3 bucket. With a validated log file, you can assert positively that the log file itself has not changed, or that particular user credentials performed specific API activity. The CloudTrail log file integrity validation process also informs you if a log file has been deleted or changed. You gain the insight to assert positively that log files either were delivered or were not delivered to your account during a given period of time. You can activate log file integrity validation with the CloudTrail console when you create or update a trail.

9) C — You can use Amazon Data Lifecycle Manager (Amazon DLM) to automate the creation, retention, and deletion of Amazon Elastic Block Store (Amazon EBS) snapshots. You can create a lifecycle policy that includes specific tags to back up EBS volumes on a specified schedule and for a specified retention period. For example, you can take a snapshot of an EBS volume every day and keep the snapshots for 30 days.

10) B — User-defined tags are tags that you define, create, and apply to resources manually. You can use Tag Editor to search for all resources and apply tags to them. Use cost allocation tags to track your AWS costs on a detailed level. After you activate cost allocation tags, AWS uses the tags to organize your resource costs to make it easier for you to categorize and track your AWS costs. For example, to track costs by department, you can use a tag that is named "Department" with the value equal to the department name.

11) Exam lab solution:

Create a custom DB parameter group and set the event_scheduler parameter to true and use this parameter during DB instance creation.

i. Open the Amazon RDS console from https://console.amazonaws.com/rds/.
ii. In the **Resources** section, choose **Parameter groups**.
iii. Choose **Create parameter group**.
iv. In the **Parameter group family** list, select **mysql8.0**
v. In the **Group name** box, enter the new DB cluster parameter group name of **mysql80witheventscheduler**.
vi. In the **Description** box, enter a description for the new DB cluster parameter group.
vii. Choose **Create**.
viii. In the list of parameter groups, check the box next to the parameter group that you want to modify, which is **mysql80witheventscheduler**.
ix. Choose **Parameter group actions** and choose **Edit**.
x. In the **Filter parameters** box, enter **event_s**. This should filter just the **event_scheduler** parameter.
xi. Choose the box for the **event_scheduler** parameter. Under **Values**, change the setting to **ON**.
xii. Choose **Save changes**.

Create a custom AWS Key Management Service (AWS KMS) key and use this key during DB instance creation.

i. Open the AWS KMS console from https://console.aws.amazon.com/kms.
ii. In the navigation pane, choose **Customer managed keys**.
iii. Choose **Create key**.
iv. To create a symmetric CMK, for **Key type,** choose **Symmetric**.
v. Choose **Next**.
vi. Type the alias or display name for the CMK. For this walkthrough, use the value **mysqlDbKey**
vii. (Optional) Type a description for the CMK.
viii. Choose **Next**.
ix. (Optional) To add a tag, click **Add tag**. Type a tag key and an optional tag value. To add more than one tag to the CMK, choose **Add tag**.
x. Once completed, choose **Next**.
xi. Select the IAM users and roles that can administer the CMK. For this walkthrough, use your IAM user.
xii. Choose **Next**.
xiii. Select the IAM users and roles that can use the CMK for cryptographic operations. For this walkthrough, none are needed.
xiv. Choose **Next**.
xv. Review the key policy document that was created from your choices. Note that it can also be edited.
xvi. Choose **Finish** to create the CMK.

Create a VPC security group that allows TCP port 3306 from the CIDR block 192.168.1.0/24 and use this security group during DB instance creation.

i. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/home.
ii. In the navigation pane, choose **Security Groups**.
iii. Choose **Create security group**.
iv. Enter a name for the security group (for example, **mysqlAccessGroup**) and then provide a description.
v. From **VPC**, select the ID of your VPC.
vi. Under **Inbound rules**, choose **Add rule**.
vii. Set **Type** to **MYSQL/Aurora.**
viii. Set **Source** to **192.168.1.0/24.**
ix. Scroll down and choose **Create security group**.

Launch the Amazon RDS DB instance.

i. Open the Amazon RDS console from https://console.aws.amazon.com/rds/.
ii. In the navigation pane, choose **Databases**.
iii. Choose **Create database**.
iv. On the **Create database** page, verify that the **Standard create** option is chosen. Then choose **MySQL**.
v. In the **Templates** section, choose **Production.**
vi. In the **DB instance identifier** section, type the name **mysqldemo**
vii. In the **Settings** section, set these values:
    i. **Master password**
    ii. **Confirm password** – Retype the password.
viii. In the **DB instance size** section, set these values:
    iii. **Burstable classes (includes t classes)**
    iv. **db.t3.micro**
ix. In the **Connectivity** section, for **Virtual private cloud (VPC)**, choose an existing VPC.
x. Expand the **Additional connectivity configuration** menu and set these values:
    v. For **Subnet group** select the DB subnet group.
    vi. For **Public access**, select **No**.
    vii. For **Existing VPC security groups** choose **mysqlAccessGroup**.
xi. Remove the other existing security groups, such as the default security group, by choosing the **X** associated with each.
xii. Expand the **Additional configuration** section.
xiii. For the **DB parameter group**, select **mysql80witheventscheduler**
xiv. For **Master key,** select **mysqlDbKey**
xv. Choose **Create database** to create your RDS MySQL DB instance.

After launch, take a manual RDS DB snapshot.

i. Open the Amazon RDS console from https://console.aws.amazon.com/rds/.
ii. In the navigation pane, choose **Databases**.
iii. In the list of DB instances, choose the DB instance for which you want to take a snapshot.
iv. Choose **Actions** and choose **Take snapshot**.
v. The **Take DB snapshot** window appears.
vi. In the **Snapshot name** box, type the name of the snapshot. For this walkthrough, use **mysqlsnapshot**.
vii. Choose **Take snapshot**.

viii. From the RDS console, in the navigation pane, choose **Snapshots**.
ix. Choose the snapshot name **mysqlsnapshot**
x. In the **Details** section, note the ARN field and the ARN.

Provide the DB snapshot ARN: _____

1) A company ingests a large set of clickstream data in nested JSON format from different sources and stores it in Amazon S3. Data analysts need to analyze this data in combination with data stored in an Amazon Redshift cluster. Data analysts want to build a cost-effective and automated solution for this need.

Which solution meets these requirements?

A) Use Apache Spark SQL on Amazon EMR to convert the clickstream data to a tabular format. Use the Amazon Redshift COPY command to load the data into the Amazon Redshift cluster.
B) Use AWS Lambda to convert the data to a tabular format and write it to Amazon S3. Use the Amazon Redshift COPY command to load the data into the Amazon Redshift cluster.
C) Use the Relationalize class in an AWS Glue ETL job to transform the data and write the data back to Amazon S3. Use Amazon Redshift Spectrum to create external tables and join with the internal tables.
D) Use the Amazon Redshift COPY command to move the clickstream data directly into new tables in the Amazon Redshift cluster.

2) A publisher website captures user activity and sends clickstream data to Amazon Kinesis Data Streams. The publisher wants to design a cost-effective solution to process the data to create a timeline of user activity within a session. The solution must be able to scale depending on the number of active sessions.

Which solution meets these requirements?

A) Include a variable in the clickstream data from the publisher website to maintain a counter for the number of active user sessions. Use a timestamp for the partition key for the stream. Configure the consumer application to read the data from the stream and change the number of processor threads based upon the counter. Deploy the consumer application on Amazon EC2 instances in an EC2 Auto Scaling group.
B) Include a variable in the clickstream to maintain a counter for each user action during their session. Use the action type as the partition key for the stream. Use the Kinesis Client Library (KCL) in the consumer application to retrieve the data from the stream and perform the processing. Configure the consumer application to read the data from the stream and change the number of processor threads based upon the counter. Deploy the consumer application on AWS Lambda.
C) Include a session identifier in the clickstream data from the publisher website and use as the partition key for the stream. Use the Kinesis Client Library (KCL) in the consumer application to retrieve the data from the stream and perform the processing. Deploy the consumer application on Amazon EC2 instances in an EC2 Auto Scaling group. Use an AWS Lambda function to reshard the stream based upon Amazon CloudWatch alarms.
D) Include a variable in the clickstream data from the publisher website to maintain a counter for the number of active user sessions. Use a timestamp for the partition key for the stream. Configure the consumer application to read the data from the stream and change the number of processor threads based upon the counter. Deploy the consumer application on AWS Lambda.

3) A company is currently using Amazon DynamoDB as the database for a user support application. The company is developing a new version of the application that will store a PDF file for each support case ranging in size from 1–10 MB. The file should be retrievable whenever the case is accessed in the application.

How can the company store the file in the MOST cost-effective manner?

A) Store the file in Amazon DocumentDB and the document ID as an attribute in the DynamoDB table.
B) Store the file in Amazon S3 and the object key as an attribute in the DynamoDB table.
C) Split the file into smaller parts and store the parts as multiple items in a separate DynamoDB table.
D) Store the file as an attribute in the DynamoDB table using Base64 encoding.

4) A company needs to implement a near-real-time fraud prevention feature for its ecommerce site. User and order details need to be delivered to an Amazon SageMaker endpoint to flag suspected fraud. The amount of input data needed for the inference could be as much as 1.5 MB.

Which solution meets the requirements with the LOWEST overall latency?

A) Create an Amazon Managed Streaming for Kafka cluster and ingest the data for each order into a topic. Use a Kafka consumer running on Amazon EC2 instances to read these messages and invoke the Amazon SageMaker endpoint.
B) Create an Amazon Kinesis Data Streams stream and ingest the data for each order into the stream. Create an AWS Lambda function to read these messages and invoke the Amazon SageMaker endpoint.
C) Create an Amazon Kinesis Data Firehose delivery stream and ingest the data for each order into the stream. Configure Kinesis Data Firehose to deliver the data to an Amazon S3 bucket. Trigger an AWS Lambda function with an S3 event notification to read the data and invoke the Amazon SageMaker endpoint.
D) Create an Amazon SNS topic and publish the data for each order to the topic. Subscribe the Amazon SageMaker endpoint to the SNS topic.

5) A media company is migrating its on-premises legacy Hadoop cluster with its associated data processing scripts and workflow to an Amazon EMR environment running the latest Hadoop release. The developers want to reuse the Java code that was written for data processing jobs for the on-premises cluster.

Which approach meets these requirements?

A) Deploy the existing Oracle Java Archive as a custom bootstrap action and run the job on the EMR cluster.
B) Compile the Java program for the desired Hadoop version and run it using a CUSTOM_JAR step on the EMR cluster.
C) Submit the Java program as an Apache Hive or Apache Spark step for the EMR cluster.
D) Use SSH to connect the master node of the EMR cluster and submit the Java program using the AWS CLI.

6) An online retail company wants to perform analytics on data in large Amazon S3 objects using Amazon EMR. An Apache Spark job repeatedly queries the same data to populate an analytics dashboard. The analytics team wants to minimize the time to load the data and create the dashboard.

Which approaches could improve the performance? (Select TWO.)

A) Copy the source data into Amazon Redshift and rewrite the Apache Spark code to create analytical reports by querying Amazon Redshift.
B) Copy the source data from Amazon S3 into Hadoop Distributed File System (HDFS) using s3distcp.
C) Load the data into Spark DataFrames.
D) Stream the data into Amazon Kinesis and use the Kinesis Connector Library (KCL) in multiple Spark jobs to perform analytical jobs.
E) Use Amazon S3 Select to retrieve the data necessary for the dashboards from the S3 objects.

7) A data engineer needs to create a dashboard to display social media trends during the last hour of a large company event. The dashboard needs to display the associated metrics with a consistent latency of less than 2 minutes.

Which solution meets these requirements?

A) Publish the raw social media data to an Amazon Kinesis Data Firehose delivery stream. Use Kinesis Data Analytics for SQL Applications to perform a sliding window analysis to compute the metrics and output the results to a Kinesis Data Streams data stream. Configure an AWS Lambda function to save the stream data to an Amazon DynamoDB table. Deploy a real-time dashboard hosted in an Amazon S3 bucket to read and display the metrics data stored in the DynamoDB table.
B) Publish the raw social media data to an Amazon Kinesis Data Firehose delivery stream. Configure the stream to deliver the data to an Amazon Elasticsearch Service cluster with a buffer interval of 0 seconds. Use Kibana to perform the analysis and display the results.
C) Publish the raw social media data to an Amazon Kinesis Data Streams data stream. Configure an AWS Lambda function to compute the metrics on the stream data and save the results in an Amazon S3 bucket. Configure a dashboard in Amazon QuickSight to query the data using Amazon Athena and display the results.
D) Publish the raw social media data to an Amazon SNS topic. Subscribe an Amazon SQS queue to the topic. Configure Amazon EC2 instances as workers to poll the queue, compute the metrics, and save the results to an Amazon Aurora MySQL database. Configure a dashboard in Amazon QuickSight to query the data in Aurora and display the results.

8) A real estate company is receiving new property listing data from its agents through .csv files every day and storing these files in Amazon S3. The data analytics team created an Amazon QuickSight visualization report that uses a dataset imported from the S3 files. The data analytics team wants the visualization report to reflect the current data up to the previous day.

How can a data analyst meet these requirements?

A) Schedule an AWS Lambda function to drop and re-create the dataset daily.
B) Configure the visualization to query the data in Amazon S3 directly without loading the data into SPICE.
C) Schedule the dataset to refresh daily.
D) Close and open the Amazon QuickSight visualization.

9) A financial company uses Amazon EMR for its analytics workloads. During the company's annual security audit, the security team determined that none of the EMR clusters' root volumes are encrypted. The security team recommends the company encrypt its EMR clusters' root volume as soon as possible.

Which solution would meet these requirements?

A) Enable at-rest encryption for EMR File System (EMRFS) data in Amazon S3 in a security configuration. Re-create the cluster using the newly created security configuration.
B) Specify local disk encryption in a security configuration. Re-create the cluster using the newly created security configuration.
C) Detach the Amazon EBS volumes from the master node. Encrypt the EBS volume and attach it back to the master node.
D) Re-create the EMR cluster with LZO encryption enabled on all volumes.

10) A company is providing analytics services to its marketing and human resources (HR) departments. The departments can only access the data through their business intelligence (BI) tools, which run Presto queries on an Amazon EMR cluster that uses the EMR File System (EMRFS). The marketing data analyst must be granted access to the advertising table only. The HR data analyst must be granted access to the personnel table only.

Which approach will satisfy these requirements?

A) Create separate IAM roles for the marketing and HR users. Assign the roles with AWS Glue resource-based policies to access their corresponding tables in the AWS Glue Data Catalog. Configure Presto to use the AWS Glue Data Catalog as the Apache Hive metastore.
B) Create the marketing and HR users in Apache Ranger. Create separate policies that allow access to the user's corresponding table only. Configure Presto to use Apache Ranger and an external Apache Hive metastore running in Amazon RDS.
C) Create separate IAM roles for the marketing and HR users. Configure EMR to use IAM roles for EMRFS access. Create a separate bucket for the HR and marketing data. Assign appropriate permissions so the users will only see their corresponding datasets.
D) Create the marketing and HR users in Apache Ranger. Create separate policies that allows access to the user's corresponding table only. Configure Presto to use Apache Ranger and the AWS Glue Data Catalog as the Apache Hive metastore.

Answers

1) C – The Relationalize PySpark transform can be used to flatten the nested data into a structured format. Amazon Redshift Spectrum can join the external tables and query the transformed clickstream data in place rather than needing to scale the cluster to accommodate the large dataset.

2) C – Partitioning by the session ID will allow a single processor to process all the actions for a user session in order. An AWS Lambda function can call the UpdateShardCount API action to change the number of shards in the stream. The KCL will automatically manage the number of processors to match the number of shards. Amazon EC2 Auto Scaling will assure the correct number of instances are running to meet the processing load.

3) B – Use Amazon S3 to store large attribute values that cannot fit in an Amazon DynamoDB item. Store each file as an object in Amazon S3 and then store the object path in the DynamoDB item.

4) A – An Amazon Managed Streaming for Kafka cluster can be used to deliver the messages with very low latency. It has a configurable message size that can handle the 1.5 MB payload.

5) B – A CUSTOM JAR step can be configured to download a JAR file from an Amazon S3 bucket and execute it. Since the Hadoop versions are different, the Java application has to be recompiled.

6) C, E – One of the speed advantages of Apache Spark comes from loading data into immutable dataframes, which can be accessed repeatedly in memory. Spark DataFrames organizes distributed data into columns. This makes summaries and aggregates much quicker to calculate. Also, instead of loading an entire large Amazon S3 object, load only what is needed using Amazon S3 Select. Keeping the data in Amazon S3 avoids loading the large dataset into HDFS.

7) A – Amazon Kinesis Data Analytics can query data in a Kinesis Data Firehose delivery stream in near-real time using SQL. A sliding window analysis is appropriate for determining trends in the stream. Amazon S3 can host a static webpage that includes JavaScript that reads the data in Amazon DynamoDB and refreshes the dashboard.

8) C – Datasets created using Amazon S3 as the data source are automatically imported into SPICE. The Amazon QuickSight console allows for the refresh of SPICE data on a schedule.

9) B – Local disk encryption can be enabled as part of a security configuration to encrypt root and storage volumes.

10) A – AWS Glue resource policies can be used to control access to Data Catalog resources.

1) A media company is running a critical production application that uses Amazon RDS for PostgreSQL with Multi-AZ deployments. The database size is currently 25 TB. The IT director wants to migrate the database to Amazon Aurora PostgreSQL with minimal effort and minimal disruption to the business.

What is the best migration strategy to meet these requirements?

A) Use the AWS Schema Conversion Tool (AWS SCT) to copy the database schema from RDS for PostgreSQL to an Aurora PostgreSQL DB cluster. Create an AWS DMS task to copy the data.
B) Create a script to continuously back up the RDS for PostgreSQL instance using pg_dump, and restore the backup to an Aurora PostgreSQL DB cluster using pg_restore.
C) Create a read replica from the existing production RDS for PostgreSQL instance. Check that the replication lag is zero and then promote the read replica as a standalone Aurora PostgreSQL DB cluster.
D) Create an Aurora Replica from the existing production RDS for PostgreSQL instance. Stop the writes on the master, check that the replication lag is zero, and then promote the Aurora Replica as a standalone Aurora PostgreSQL DB cluster.

2) A medical company is planning to migrate its on-premises PostgreSQL database, along with application and web servers, to AWS. Amazon RDS for PostgreSQL is being considered as the target database engine. Access to the database should be limited to application servers and a bastion host in a VPC.

Which solution meets the security requirements?

A) Launch the RDS for PostgreSQL database in a DB subnet group containing private subnets. Modify the pg_hba.conf file on the DB instance to allow connections from only the application servers and bastion host.
B) Launch the RDS for PostgreSQL database in a DB subnet group containing public subnets. Create a new security group with inbound rules to allow connections from only the security groups of the application servers and bastion host. Attach the new security group to the DB instance.
C) Launch the RDS for PostgreSQL database in a DB subnet group containing private subnets. Create a new security group with inbound rules to allow connections from only the security groups of the application servers and bastion host. Attach the new security group to the DB instance.
D) Launch the RDS for PostgreSQL database in a DB subnet group containing private subnets. Create a NACL attached to the VPC and private subnets. Modify the inbound and outbound rules to allow connections to and from the application servers and bastion host.

3) A database specialist is troubleshooting complaints from an application's users who are experiencing performance issues when saving data in an Amazon ElastiCache for Redis cluster with cluster mode disabled. The database specialist finds that the performance issues are occurring during the cluster's backup window. The cluster runs in a replication group containing three nodes. Memory on the nodes is fully utilized. Organizational policies prohibit the database specialist from changing the backup window time.

How could the database specialist address the performance concern? (Select TWO.)

A) Add an additional node to the cluster in the same Availability Zone as the primary.
B) Configure the backup job to take a snapshot of a read replica.
C) Increase the local instance storage size for the cluster nodes.
D) Increase the reserved-memory-percent parameter value.
E) Configure the backup process to flush the cache before taking the backup.

4) A company's security department has mandated that their existing Amazon RDS for MySQL DB instance be encrypted at rest.

What should a database specialist do to meet this requirement?

A) Modify the database to enable encryption. Apply this setting immediately without waiting for the next scheduled maintenance window.
B) Export the database to an Amazon S3 bucket with encryption enabled. Create a new database and import the export file.
C) Create a snapshot of the database. Create an encrypted copy of the snapshot. Create a new database from the encrypted snapshot.
D) Create a snapshot of the database. Restore the snapshot into a new database with encryption enabled.

5) A company has a highly available production 10 TB SQL Server relational database running on Amazon EC2. Users have recently been reporting performance and connectivity issues. A database specialist has been asked to configure a monitoring and alerting strategy that will provide metrics visibility and notifications to troubleshoot these issues.

Which solution will meet these requirements?

A) Configure AWS CloudTrail logs to monitor and detect signs of potential problems. Create an AWS Lambda function that is triggered when specific API calls are made and send notifications to an Amazon SNS topic.
B) Install an Amazon Inspector agent on the DB instance. Configure the agent to stream server and database activity to Amazon CloudWatch Logs. Configure metric filters and alarms to send notifications to an Amazon SNS topic.
C) Migrate the database to Amazon RDS for SQL Server and use Performance Insights to monitor and detect signs of potential problems. Create a scheduled AWS Lambda function that retrieves metrics from the Performance Insights API and send notifications to an Amazon SNS topic.
D) Configure Amazon CloudWatch Application Insights for .NET and SQL Server to monitor and detect signs of potential problems. Configure CloudWatch Events to send notifications to an Amazon SNS topic.

6) A company's ecommerce application stores order transactions in an Amazon RDS for MySQL database. The database has run out of available storage and the application is currently unable to take orders.

Which action should a database specialist take to resolve the issue in the shortest amount of time?

A) Add more storage space to the DB instance using the ModifyDBInstance action.
B) Create a new DB instance with more storage space from the latest backup.
C) Change the DB instance status from STORAGE_FULL to AVAILABLE.
D) Configure a read replica with more storage space.

7) A company undergoing a security audit has determined that its database administrators are presently sharing an administrative database user account for the company's Amazon Aurora deployment. To support proper traceability, governance, and compliance, each database administration team member must start using individual, named accounts. Furthermore, long-term database user credentials should not be used.

Which solution should a database specialist implement to meet these requirements?

A) Use the AWS CLI to fetch the AWS IAM users and passwords for all team members. For each IAM user, create an Aurora user with the same password as the IAM user.
B) Enable IAM database authentication on the Aurora cluster. Create a database user for each team member without a password. Attach an IAM policy to each administrator's IAM user account that grants the connect privilege using their database user account.
C) Create a database user for each team member. Share the new database user credentials with the team members. Have users change the password on the first login to the same password as their IAM user.
D) Create an IAM role and associate an IAM policy that grants the connect privilege using the shared account. Configure a trust policy that allows the administrator's IAM user account to assume the role.

8) A global company wants to run an application in several AWS Regions to support a global user base. The application will need a database that can support a high volume of low-latency reads and writes that is expected to vary over time. The data must be shared across all of the Regions to support dynamic company-wide reports.

Which database meets these requirements?

A) Use Amazon Aurora Serverless and configure endpoints in each Region.
B) Use Amazon RDS for MySQL and deploy read replicas in an auto scaling group in each Region.
C) Use Amazon DocumentDB (with MongoDB compatibility) and configure read replicas in an auto scaling group in each Region.
D) Use Amazon DynamoDB global tables and configure DynamoDB auto scaling for the tables.

9) A company's customer relationship management application uses an Amazon RDS for PostgreSQL Multi-AZ database. The database size is approximately 100 GB. A database specialist has been tasked with developing a cost-effective disaster recovery plan that will restore the database in a different Region within 2 hours. The restored database should not be missing more than 8 hours of transactions.

What is the MOST cost-effective solution that meets the availability requirements?

A) Create an RDS read replica in the second Region. For disaster recovery, promote the read replica to a standalone instance.
B) Create an RDS read replica in the second Region using a smaller instance size. For disaster recovery, scale the read replica and promote it to a standalone instance.
C) Schedule an AWS Lambda function to create an hourly snapshot of the DB instance and another Lambda function to copy the snapshot to the second Region. For disaster recovery, create a new RDS Multi-AZ DB instance from the last snapshot.
D) Create a new RDS Multi-AZ DB instance in the second Region. Configure an AWS DMS task for ongoing replication.

10) An operations team in a large company wants to centrally manage resource provisioning for its development teams across multiple accounts. When a new AWS account is created, the developers require full privileges for a database environment that uses the same configuration, data schema, and source data as the company's production Amazon RDS for MySQL DB instance.

How can the operations team achieve this?

A) Enable the source DB instance to be shared with the new account so the development team may take a snapshot. Create an AWS CloudFormation template to launch the new DB instance from the snapshot.
B) Create an AWS CLI script to launch the approved DB instance configuration in the new account. Create an AWS DMS task to copy the data from the source DB instance to the new DB instance.
C) Take a manual snapshot of the source DB instance and share the snapshot privately with the new account. Specify the snapshot ARN in an RDS resource in an AWS CloudFormation template and use StackSets to deploy to the new account.
D) Create a DB instance read replica of the source DB instance. Share the read replica with the new AWS account.

Answers

1) D - To migrate from an Amazon RDS for PostgreSQL DB instance to an Amazon Aurora PostgreSQL DB cluster, create an Aurora Replica of your source PostgreSQL DB instance. When the replica lag between the PostgreSQL DB instance and the Aurora PostgreSQL Replica is zero, you can promote the Aurora Replica to be a standalone Aurora PostgreSQL DB cluster.

2) C - Create custom rules in the security group for your DB instances that allow connections from the security group you created for your Amazon EC2 instances. This would allow instances associated with the security group to access the DB instances. Including bastion hosts in your VPC environment enables you to securely connect to your database instances running in private subnets.

3) B,D - Because of the system resources required during a backup, we recommend that you create backups from one of the read replicas. If all of a node's available memory is consumed, then excessive paging to the disk can occur. We recommend setting the reserved-memory-percent parameter to 25% to reserve enough memory for background processes.

4) C - To enable encryption at rest for an existing unencrypted DB instance, you can create a snapshot of your DB instance, and then create an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot so you have an encrypted copy of your original DB instance.

5) D - Amazon CloudWatch Application Insights uses machine learning classification algorithms to analyze metrics and identify signs of problems with your applications. Windows Event Viewer and SQL Server Error logs are included in the analysis. To receive notifications, you can create an Amazon EventBridge (in CloudWatch Events) rule for the Application Insights Problem Detected event.

6) A - If your DB instance runs out of storage space, it might no longer be available. To recover from this scenario, add more storage space to your instance using the ModifyDBInstance action. To prevent storage space issues from happening in the future, enable storage autoscaling.

7) B - You can authenticate to your DB cluster using AWS IAM database authentication. With this authentication method, you don't need to use a password when you connect to a DB cluster. Instead, you use an authentication token that expires 15 minutes after creation.

8) D - Amazon DynamoDB global tables provide a multi-Region, multi-master database in the AWS Regions you specify. DynamoDB performs all of the necessary tasks to create identical tables in these Regions and propagate ongoing data changes to all of them. DynamoDB auto scaling cost effectively adjusts provisioned throughput to actual traffic patterns.

9) C - Backup and restore is the most cost-effective solution to provide a 2-hour RTO and 8-hour RPO. Manual hourly snapshots need to be copied to the second Region to be available for the creation of the new database. Taking the snapshots every hour will keep the incremental snapshot size low, reduce the time to copy the snapshot across Regions, and meet the RPO. Also, taking snapshots frequently does not impact the cost. A pair of AWS Lambda functions can be scheduled to take the snapshot and copy it to the second Region.

10) C - A manual DB snapshot can be shared privately with other AWS accounts. AWS CloudFormation StackSets extends the functionality of stacks by enabling you to create, update, or delete stacks across multiple accounts and Regions with a single operation. Using an administrator account, you define and manage an AWS CloudFormation template, and use the template as the basis for provisioning stacks into selected target accounts across specified Regions.

1) A media company is running a critical production application that uses Amazon RDS for PostgreSQL with Multi-AZ deployments. The database size is currently 25 TB. The IT director wants to migrate the database to Amazon Aurora PostgreSQL with minimal effort and minimal disruption to the business.

What is the best migration strategy to meet these requirements?

A) Use the AWS Schema Conversion Tool (AWS SCT) to copy the database schema from RDS for PostgreSQL to an Aurora PostgreSQL DB cluster. Create an AWS DMS task to copy the data.
B) Create a script to continuously back up the RDS for PostgreSQL instance using pg_dump, and restore the backup to an Aurora PostgreSQL DB cluster using pg_restore.
C) Create a read replica from the existing production RDS for PostgreSQL instance. Check that the replication lag is zero and then promote the read replica as a standalone Aurora PostgreSQL DB cluster.
D) Create an Aurora Replica from the existing production RDS for PostgreSQL instance. Stop the writes on the master, check that the replication lag is zero, and then promote the Aurora Replica as a standalone Aurora PostgreSQL DB cluster.

2) A medical company is planning to migrate its on-premises PostgreSQL database, along with application and web servers, to AWS. Amazon RDS for PostgreSQL is being considered as the target database engine. Access to the database should be limited to application servers and a bastion host in a VPC.

Which solution meets the security requirements?

A) Launch the RDS for PostgreSQL database in a DB subnet group containing private subnets. Modify the pg_hba.conf file on the DB instance to allow connections from only the application servers and bastion host.
B) Launch the RDS for PostgreSQL database in a DB subnet group containing public subnets. Create a new security group with inbound rules to allow connections from only the security groups of the application servers and bastion host. Attach the new security group to the DB instance.
C) Launch the RDS for PostgreSQL database in a DB subnet group containing private subnets. Create a new security group with inbound rules to allow connections from only the security groups of the application servers and bastion host. Attach the new security group to the DB instance.
D) Launch the RDS for PostgreSQL database in a DB subnet group containing private subnets. Create a NACL attached to the VPC and private subnets. Modify the inbound and outbound rules to allow connections to and from the application servers and bastion host.

3) A database specialist is troubleshooting complaints from an application's users who are experiencing performance issues when saving data in an Amazon ElastiCache for Redis cluster with cluster mode disabled. The database specialist finds that the performance issues are occurring during the cluster's backup window. The cluster runs in a replication group containing three nodes. Memory on the nodes is fully utilized. Organizational policies prohibit the database specialist from changing the backup window time.

How could the database specialist address the performance concern? (Select TWO.)

A) Add an additional node to the cluster in the same Availability Zone as the primary.
B) Configure the backup job to take a snapshot of a read replica.
C) Increase the local instance storage size for the cluster nodes.
D) Increase the reserved-memory-percent parameter value.
E) Configure the backup process to flush the cache before taking the backup.

4) A company's security department has mandated that their existing Amazon RDS for MySQL DB instance be encrypted at rest.

What should a database specialist do to meet this requirement?

A) Modify the database to enable encryption. Apply this setting immediately without waiting for the next scheduled maintenance window.
B) Export the database to an Amazon S3 bucket with encryption enabled. Create a new database and import the export file.
C) Create a snapshot of the database. Create an encrypted copy of the snapshot. Create a new database from the encrypted snapshot.
D) Create a snapshot of the database. Restore the snapshot into a new database with encryption enabled.

5) A company has a highly available production 10 TB SQL Server relational database running on Amazon EC2. Users have recently been reporting performance and connectivity issues. A database specialist has been asked to configure a monitoring and alerting strategy that will provide metrics visibility and notifications to troubleshoot these issues.

Which solution will meet these requirements?

A) Configure AWS CloudTrail logs to monitor and detect signs of potential problems. Create an AWS Lambda function that is triggered when specific API calls are made and send notifications to an Amazon SNS topic.
B) Install an Amazon Inspector agent on the DB instance. Configure the agent to stream server and database activity to Amazon CloudWatch Logs. Configure metric filters and alarms to send notifications to an Amazon SNS topic.
C) Migrate the database to Amazon RDS for SQL Server and use Performance Insights to monitor and detect signs of potential problems. Create a scheduled AWS Lambda function that retrieves metrics from the Performance Insights API and send notifications to an Amazon SNS topic.
D) Configure Amazon CloudWatch Application Insights for .NET and SQL Server to monitor and detect signs of potential problems. Configure CloudWatch Events to send notifications to an Amazon SNS topic.

6) A company's ecommerce application stores order transactions in an Amazon RDS for MySQL database. The database has run out of available storage and the application is currently unable to take orders.

Which action should a database specialist take to resolve the issue in the shortest amount of time?

A) Add more storage space to the DB instance using the ModifyDBInstance action.
B) Create a new DB instance with more storage space from the latest backup.
C) Change the DB instance status from STORAGE_FULL to AVAILABLE.
D) Configure a read replica with more storage space.

7) A company undergoing a security audit has determined that its database administrators are presently sharing an administrative database user account for the company's Amazon Aurora deployment. To support proper traceability, governance, and compliance, each database administration team member must start using individual, named accounts. Furthermore, long-term database user credentials should not be used.

Which solution should a database specialist implement to meet these requirements?

A) Use the AWS CLI to fetch the AWS IAM users and passwords for all team members. For each IAM user, create an Aurora user with the same password as the IAM user.
B) Enable IAM database authentication on the Aurora cluster. Create a database user for each team member without a password. Attach an IAM policy to each administrator's IAM user account that grants the connect privilege using their database user account.
C) Create a database user for each team member. Share the new database user credentials with the team members. Have users change the password on the first login to the same password as their IAM user.
D) Create an IAM role and associate an IAM policy that grants the connect privilege using the shared account. Configure a trust policy that allows the administrator's IAM user account to assume the role.

8) A global company wants to run an application in several AWS Regions to support a global user base. The application will need a database that can support a high volume of low-latency reads and writes that is expected to vary over time. The data must be shared across all of the Regions to support dynamic company-wide reports.

Which database meets these requirements?

A) Use Amazon Aurora Serverless and configure endpoints in each Region.
B) Use Amazon RDS for MySQL and deploy read replicas in an auto scaling group in each Region.
C) Use Amazon DocumentDB (with MongoDB compatibility) and configure read replicas in an auto scaling group in each Region.
D) Use Amazon DynamoDB global tables and configure DynamoDB auto scaling for the tables.

9) A company's customer relationship management application uses an Amazon RDS for PostgreSQL Multi-AZ database. The database size is approximately 100 GB. A database specialist has been tasked with developing a cost-effective disaster recovery plan that will restore the database in a different Region within 2 hours. The restored database should not be missing more than 8 hours of transactions.

What is the MOST cost-effective solution that meets the availability requirements?

A) Create an RDS read replica in the second Region. For disaster recovery, promote the read replica to a standalone instance.
B) Create an RDS read replica in the second Region using a smaller instance size. For disaster recovery, scale the read replica and promote it to a standalone instance.
C) Schedule an AWS Lambda function to create an hourly snapshot of the DB instance and another Lambda function to copy the snapshot to the second Region. For disaster recovery, create a new RDS Multi-AZ DB instance from the last snapshot.
D) Create a new RDS Multi-AZ DB instance in the second Region. Configure an AWS DMS task for ongoing replication.

10) An operations team in a large company wants to centrally manage resource provisioning for its development teams across multiple accounts. When a new AWS account is created, the developers require full privileges for a database environment that uses the same configuration, data schema, and source data as the company's production Amazon RDS for MySQL DB instance.

How can the operations team achieve this?

A) Enable the source DB instance to be shared with the new account so the development team may take a snapshot. Create an AWS CloudFormation template to launch the new DB instance from the snapshot.
B) Create an AWS CLI script to launch the approved DB instance configuration in the new account. Create an AWS DMS task to copy the data from the source DB instance to the new DB instance.
C) Take a manual snapshot of the source DB instance and share the snapshot privately with the new account. Specify the snapshot ARN in an RDS resource in an AWS CloudFormation template and use StackSets to deploy to the new account.
D) Create a DB instance read replica of the source DB instance. Share the read replica with the new AWS account.

Answers

1) D - To migrate from an Amazon RDS for PostgreSQL DB instance to an Amazon Aurora PostgreSQL DB cluster, create an Aurora Replica of your source PostgreSQL DB instance. When the replica lag between the PostgreSQL DB instance and the Aurora PostgreSQL Replica is zero, you can promote the Aurora Replica to be a standalone Aurora PostgreSQL DB cluster.

2) C - Create custom rules in the security group for your DB instances that allow connections from the security group you created for your Amazon EC2 instances. This would allow instances associated with the security group to access the DB instances. Including bastion hosts in your VPC environment enables you to securely connect to your database instances running in private subnets.

3) B,D - Because of the system resources required during a backup, we recommend that you create backups from one of the read replicas. If all of a node's available memory is consumed, then excessive paging to the disk can occur. We recommend setting the reserved-memory-percent parameter to 25% to reserve enough memory for background processes.

4) C - To enable encryption at rest for an existing unencrypted DB instance, you can create a snapshot of your DB instance, and then create an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot so you have an encrypted copy of your original DB instance.

5) D - Amazon CloudWatch Application Insights uses machine learning classification algorithms to analyze metrics and identify signs of problems with your applications. Windows Event Viewer and SQL Server Error logs are included in the analysis. To receive notifications, you can create an Amazon EventBridge (in CloudWatch Events) rule for the Application Insights Problem Detected event.

6) A - If your DB instance runs out of storage space, it might no longer be available. To recover from this scenario, add more storage space to your instance using the ModifyDBInstance action. To prevent storage space issues from happening in the future, enable storage autoscaling.

7) B - You can authenticate to your DB cluster using AWS IAM database authentication. With this authentication method, you don't need to use a password when you connect to a DB cluster. Instead, you use an authentication token that expires 15 minutes after creation.

8) D - Amazon DynamoDB global tables provide a multi-Region, multi-master database in the AWS Regions you specify. DynamoDB performs all of the necessary tasks to create identical tables in these Regions and propagate ongoing data changes to all of them. DynamoDB auto scaling cost effectively adjusts provisioned throughput to actual traffic patterns.

9) C - Backup and restore is the most cost-effective solution to provide a 2-hour RTO and 8-hour RPO. Manual hourly snapshots need to be copied to the second Region to be available for the creation of the new database. Taking the snapshots every hour will keep the incremental snapshot size low, reduce the time to copy the snapshot across Regions, and meet the RPO. Also, taking snapshots frequently does not impact the cost. A pair of AWS Lambda functions can be scheduled to take the snapshot and copy it to the second Region.

10) C - A manual DB snapshot can be shared privately with other AWS accounts. AWS CloudFormation StackSets extends the functionality of stacks by enabling you to create, update, or delete stacks across multiple accounts and Regions with a single operation. Using an administrator account, you define and manage an AWS CloudFormation template, and use the template as the basis for provisioning stacks into selected target accounts across specified Regions.

1) A machine learning team has several large CSV datasets in Amazon S3. Historically, models built with the Amazon SageMaker Linear Learner algorithm have taken hours to train on similar-sized datasets. The team's leaders need to accelerate the training process.

What can a machine learning specialist do to address this concern?

A) Use Amazon SageMaker Pipe mode.
B) Use Amazon Machine Learning to train the models.
C) Use Amazon Kinesis to stream the data to Amazon SageMaker.
D) Use AWS Glue to transform the CSV dataset to the JSON format.

2) A term frequency–inverse document frequency (tf–idf) matrix using both unigrams and bigrams is built from a text corpus consisting of the following two sentences:

1. Please call the number below.
2. Please do not call us.

What are the dimensions of the tf–idf matrix?

A) (2, 16)
B) (2, 8)
C) (2, 10)
D) (8, 10)

3) A company is setting up a system to manage all of the datasets it stores in Amazon S3. The company would like to automate running transformation jobs on the data and maintaining a catalog of the metadata concerning the datasets. The solution should require the least amount of setup and maintenance.

Which solution will allow the company to achieve its goals?

A) Create an Amazon EMR cluster with Apache Hive installed. Then, create a Hive metastore and a script to run transformation jobs on a schedule.
B) Create an AWS Glue crawler to populate the AWS Glue Data Catalog. Then, author an AWS Glue ETL job, and set up a schedule for data transformation jobs.
C) Create an Amazon EMR cluster with Apache Spark installed. Then, create an Apache Hive metastore and a script to run transformation jobs on a schedule.
D) Create an Amazon SageMaker Jupyter notebook instance that transforms the data. Then, create an Apache Hive metastore and a script to run transformation jobs on a schedule.

4) A data scientist is working on optimizing a model during the training process by varying multiple parameters. The data scientist observes that, during multiple runs with identical parameters, the loss function converges to different, yet stable, values.

What should the data scientist do to improve the training process?

A) Increase the learning rate. Keep the batch size the same.
B) Decrease the learning rate. Reduce the batch size.
C) Decrease the learning rate. Keep the batch size the same.
D) Do not change the learning rate. Increase the batch size.

5) A data scientist is evaluating different binary classification models. A false positive result is 5 times more expensive (from a business perspective) than a false negative result.

The models should be evaluated based on the following criteria:

1) **Must have a recall rate of at least 80%**
2) **Must have a false positive rate of 10% or less**
3) **Must minimize business costs**

After creating each binary classification model, the data scientist generates the corresponding confusion matrix.

Which confusion matrix represents the model that satisfies the requirements?

A) TN = 91, FP = 9
FN = 22, TP = 78
B) TN = 99, FP = 1
FN = 21, TP = 79
C) TN = 96, FP = 4
FN = 10, TP = 90
D) TN = 98, FP = 2
FN = 18, TP = 82

6) A data scientist uses logistic regression to build a fraud detection model. While the model accuracy is 99%, 90% of the fraud cases are not detected by the model.

What action will definitively help the model detect more than 10% of fraud cases?

A) Using undersampling to balance the dataset
B) Decreasing the class probability threshold
C) Using regularization to reduce overfitting
D) Using oversampling to balance the dataset

7) A company is interested in building a fraud detection model. Currently, the data scientist does not have a sufficient amount of information due to the low number of fraud cases.

Which method is MOST likely to detect the GREATEST number of valid fraud cases?

A) Oversampling using bootstrapping
B) Undersampling
C) Oversampling using SMOTE
D) Class weight adjustment

8) A machine learning engineer is preparing a data frame for a supervised learning task with the Amazon SageMaker Linear Learner algorithm. The ML engineer notices the target label classes are highly imbalanced and multiple feature columns contain missing values. The proportion of missing values across the entire data frame is less than 5%.

What should the ML engineer do to minimize bias due to missing values?

A) Replace each missing value by the mean or median across non-missing values in same row.
B) Delete observations that contain missing values because these represent less than 5% of the data.
C) Replace each missing value by the mean or median across non-missing values in the same column.
D) For each feature, approximate the missing values using supervised learning based on other features.

9) A company has collected customer comments on its products, rating them as safe or unsafe, using decision trees. The training dataset has the following features: id, date, full review, full review summary, and a binary safe/unsafe tag. During training, any data sample with missing features was dropped. In a few instances, the test set was found to be missing the full review text field.

For this use case, which is the most effective course of action to address test data samples with missing features?

A) Drop the test samples with missing full review text fields, and then run through the test set.
B) Copy the summary text fields and use them to fill in the missing full review text fields, and then run through the test set.
C) Use an algorithm that handles missing data better than decision trees.
D) Generate synthetic data to fill in the fields that are missing data, and then run through the test set.

10) An insurance company needs to automate claim compliance reviews because human reviews are expensive and error-prone. The company has a large set of claims and a compliance label for each. Each claim consists of a few sentences in English, many of which contain complex related information. Management would like to use Amazon SageMaker built-in algorithms to design a machine learning supervised model that can be trained to read each claim and predict if the claim is compliant or not.

Which approach should be used to extract features from the claims to be used as inputs for the downstream supervised task?

A) Derive a dictionary of tokens from claims in the entire dataset. Apply one-hot encoding to tokens found in each claim of the training set. Send the derived features space as inputs to an Amazon SageMaker built-in supervised learning algorithm.
B) Apply Amazon SageMaker BlazingText in Word2Vec mode to claims in the training set. Send the derived features space as inputs for the downstream supervised task.
C) Apply Amazon SageMaker BlazingText in classification mode to labeled claims in the training set to derive features for the claims that correspond to the compliant and non-compliant labels, respectively.
D) Apply Amazon SageMaker Object2Vec to claims in the training set. Send the derived features space as inputs for the downstream supervised task.

Answers

1) A – Amazon SageMaker Pipe mode streams the data directly to the container, which improves the performance of training jobs. (Refer to this link for supporting information.) In Pipe mode, your training job streams data directly from Amazon S3. Streaming can provide faster start times for training jobs and better throughput. With Pipe mode, you also reduce the size of the Amazon EBS volumes for your training instances. B would not apply in this scenario. C is a streaming ingestion solution, but is not applicable in this scenario. D transforms the data structure.

2) A – There are 2 sentences, 8 unique unigrams, and 8 unique bigrams, so the result would be (2,16). The phrases are "Please call the number below" and "Please do not call us." Each word individually (unigram) is "Please," "call," "the," "number," "below," "do," "not," and "us." The unique bigrams are "Please call," "call the," "the number," "number below," "Please do," "do not," "not call," and "call us." The tf–idf vectorizer is described at this link.

3) B – AWS Glue is the correct answer because this option requires the least amount of setup and maintenance since it is serverless, and it does not require management of the infrastructure. Refer to this link for supporting information. A, C, and D are all solutions that can solve the problem, but require more steps for configuration, and require higher operational overhead to run and maintain.

4) B – It is most likely that the loss function is very curvy and has multiple local minima where the training is getting stuck. Decreasing the batch size would help the data scientist stochastically get out of the local minima saddles. Decreasing the learning rate would prevent overshooting the global loss function minimum. Refer to the paper at this link for an explanation.

5) D – The following calculations are required:

TP = True Positive
FP = False Positive
FN = False Negative
TN = True Negative
FN = False Negative

Recall = TP / (TP + FN)

False Positive Rate (FPR) = FP / (FP + TN)

Cost = 5 * FP + FN

	A	B	C	D
Recall	78 / (78 + 22) = 0.78	79 / (79 + 21) = 0.79	90 / (90 + 10) = 0.9	82 / (82 + 18) = 0.82
False Positive Rate	9 / (9 + 91) = 0.09	1 / (1 + 99) = 0.01	4 / (4 + 96) = 0.04	2 / (2 + 98) = 0.02
Costs	5 * 9 + 22 = 67	5 * 1 + 21 = 26	5 * 4 + 10 = 30	5 * 2 + 18 = 28

Options C and D have a recall greater than 80% and an FPR less than 10%, but D is the most cost effective. For supporting information, refer to this link.

6) B – Decreasing the class probability threshold makes the model more sensitive and, therefore, marks more cases as the positive class, which is fraud in this case. This will increase the likelihood of fraud detection. However, it comes at the price of lowering precision. This is covered in the Discussion section of the paper at this link.

7) C – With datasets that are not fully populated, the Synthetic Minority Over-sampling Technique (SMOTE) adds new information by adding synthetic data points to the minority class. This technique would be the most effective in this scenario. Refer to Section 4.2 at this link for supporting information.

8) D – Use supervised learning to predict missing values based on the values of other features. Different supervised learning approaches might have different performances, but any properly implemented supervised learning approach should provide the same or better approximation than mean or median approximation, as proposed in responses A and C. Supervised learning applied to the imputation of missing values is an active field of research. Refer to this link for an example.

9) B – In this case, a full review summary usually contains the most descriptive phrases of the entire review and is a valid stand-in for the missing full review text field. For supporting information, refer to page 1627 at this link, and this link and this link.

10) D – Amazon SageMaker Object2Vec generalizes the Word2Vec embedding technique for words to more complex objects, such as sentences and paragraphs. Since the supervised learning task is at the level of whole claims, for which there are labels, and no labels are available at the word level, Object2Vec needs be used instead of Word2Vec. For supporting information, refer to this link and this link.

1) A company has many AWS accounts that individual business groups own. One of the accounts was recently compromised. The attacker launched a large number of instances, resulting in a high bill for that account.

The company addressed the security breach, but a solutions architect needs to develop a solution to prevent excessive spending in all accounts. Each business group wants to retain full control of its AWS account.

Which solution should the solutions architect recommend to meet these requirements?

A) Use AWS Organizations. Add each AWS account to the management account. Create an SCP that uses the ec2:instanceType condition key to prevent the launch of high-cost instance types in each account.
B) Attach a new customer-managed IAM policy to an IAM group in each account. Configure the policy to use the ec2:instanceType condition key to prevent the launch of high-cost instance types. Place all the existing IAM users in each group.
C) Turn on billing alerts for each AWS account. Create Amazon CloudWatch alarms that send an Amazon Simple Notification Service (Amazon SNS) notification to the account administrator whenever the account exceeds a designated spending threshold.
D) Turn on AWS Cost Explorer in each account. Review the Cost Explorer reports for each account on a regular basis to ensure that spending does not exceed the desired amount.

2) A company has multiple AWS accounts in an organization in AWS Organizations. The company has integrated its on-premises Active Directory with AWS Single Sign-On (AWS SSO) to grant Active Directory users least privilege permissions to manage infrastructure across all the accounts.

A solutions architect must integrate a third-party monitoring solution that requires read-only access across all AWS accounts. The monitoring solution will run in its own AWS account.

What should the solutions architect do to provide the monitoring solution with the required permissions?

A) Create a user in an AWS SSO directory. Assign a read-only permissions set to the user. Assign all AWS accounts that need monitoring to the user. Provide the third-party monitoring solution with the user name and password.
B) Create an IAM role in the organization's management account. Allow the AWS account of the third-party monitoring solution to assume the role.
C) Invite the AWS account of the third-party monitoring solution to join the organization. Enable all features.
D) Create an AWS CloudFormation template that defines a new IAM role for the third-party monitoring solution. Specify the AWS account of the third-party monitoring solution in the trust policy. Create the IAM role across all linked AWS accounts by using a stack set.

3) A team is building an HTML form that is hosted in a public Amazon S3 bucket. The form uses JavaScript to post data to an Amazon API Gateway API endpoint. The API endpoint is integrated with AWS Lambda functions. The team has tested each method in the API Gateway console and has received valid responses.

Which combination of steps must the team complete so that the form can successfully post to the API endpoint and receive a valid response? (Select TWO.)

A) Configure the S3 bucket to allow cross-origin resource sharing (CORS).
B) Host the form on Amazon EC2 rather than on Amazon S3.
C) Request a quota increase for API Gateway.
D) Enable cross-origin resource sharing (CORS) in API Gateway.
E) Configure the S3 bucket for web hosting.

4) A company runs a serverless mobile app that uses Amazon API Gateway, AWS Lambda functions, Amazon Cognito, and Amazon DynamoDB. During large surges in traffic, users report intermittent system failures. The API Gateway API endpoint is returning HTTP status code 502 (Bad Gateway) errors to valid requests.

Which solution will resolve this issue?

A) Increase the concurrency quota for the Lambda functions. Configure Amazon CloudWatch to send notification alerts when the ConcurrentExecutions metric approaches the quota.
B) Configure notification alerts for the quota of transactions per second on the API Gateway API endpoint. Create a Lambda function that will increase the quota when the quota is reached.
C) Shard users to Amazon Cognito user pools in multiple AWS Regions to reduce user authentication latency.
D) Use DynamoDB strongly consistent reads to ensure that the client application always receives the most recent data.

5) A company is launching a new web service on an Amazon Elastic Container Service (Amazon ECS) cluster. The cluster consists of 100 Amazon EC2 instances. Company policy requires the security group on the cluster instances to block all inbound traffic except HTTPS (port 443).

Which solution will meet these requirements?

A) Change the SSH port to 2222 on the cluster instances by using a user data script. Log in to each instance by using SSH over port 2222.
B) Change the SSH port to 2222 on the cluster instances by using a user data script. Use AWS Trusted Advisor to remotely manage the cluster instances over port 2222.
C) Launch the cluster instances with no SSH key pairs. Use AWS Systems Manager Run Command to remotely manage the cluster instances.
D) Launch the cluster instances with no SSH key pairs. Use AWS Trusted Advisor to remotely manage the cluster instances.

6) A company has two AWS accounts: one account for production workloads and one account for development workloads. A development team and an operations team create and manage these workloads. The company needs a security strategy that meets the following requirements:

- **Developers need to create and delete development application infrastructure.**
- **Operators need to create and delete development and production application infrastructure.**
- **Developers must have no access to production infrastructure.**
- **All users must have a single set of AWS credentials.**

Which strategy will meet these requirements?

A) In the production account:
- Create an operations IAM group that can create and delete application infrastructure.
- Create an IAM user for each operator. Assign these users to the operations group.

In the development account:
- Create a development IAM group that can create and delete application infrastructure.
- Create an IAM user for each operator and developer. Assign these users to the development group.

B) In the production account:
- Create an operations IAM group that can create and delete application infrastructure.

In the development account:
- Create a development IAM group that can create and delete application infrastructure.
- Create an IAM user for each developer. Assign these users to the development group.
- Create an IAM user for each operator. Assign these users to the development group and to the operations group in the production account.

C) In the development account:
- Create a shared IAM role that can create and delete application infrastructure in the production account.
- Create a development IAM group that can create and delete application infrastructure.
- Create an operations IAM group that can assume the shared role.
- Create an IAM user for each developer. Assign these users to the development group.
- Create an IAM user for each operator. Assign these users to the development group and to the operations group.

D) In the production account:
- Create a shared IAM role that can create and delete application infrastructure.
- Add the development account to the trust policy for the shared role.

In the development account:
- Create a development IAM group that can create and delete application infrastructure.
- Create an operations IAM group that can assume the shared role in the production account.
- Create an IAM user for each developer. Assign these users to the development group.
- Create an IAM user for each operator. Assign these users to the development group and to the operations group.

7) A solutions architect needs to reduce costs for a big data application. The application environment consists of hundreds of devices that send events to Amazon Kinesis Data Streams. The device ID is used as the partition key, so each device gets a separate shard. Each device sends between 50 KB and 450 KB of data each second. An AWS Lambda function polls the shards, processes the data, and stores the result in Amazon S3.

Every hour, another Lambda function runs an Amazon Athena query against the result data to identify outliers. This Lambda function places the outliers in an Amazon Simple Queue Service (Amazon SQS) queue. An Amazon EC2 Auto Scaling group of two EC2 instances monitors the queue and runs a 30-second process to address the outliers. The devices submit an average of 10 outlying values every hour.

Which combination of changes to the application will MOST reduce costs? (Select TWO.)

A) Change the Auto Scaling group launch configuration to use smaller instance types in the same instance family.
B) Replace the Auto Scaling group with a Lambda function that is invoked when messages arrive in the queue.
C) Reconfigure the devices and data stream to set a ratio of 10 devices to 1 data stream shard.
D) Reconfigure the devices and data stream to set a ratio of 2 devices to 1 data stream shard.
E) Change the desired capacity of the Auto Scaling group to a single EC2 instance.

8) A company operates an ecommerce application on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. After an order is successfully processed, the application immediately posts order data to a third-party affiliate's external tracking system that pays sales commissions for order referrals.

During a successful marketing promotion, the number of EC2 instances increased from 2 to 20. The application continued to work correctly during this time. However, the increased request rate overwhelmed the third-party affiliate and resulted in failed requests.

Which combination of architectural changes should a solutions architect make to ensure that the entire process functions correctly under load? (Select TWO.)

A) Move the code that calls the affiliate to a new AWS Lambda function. Modify the application to invoke the Lambda function asynchronously.
B) Move the code that calls the affiliate to a new AWS Lambda function. Modify the application to place the order data in an Amazon Simple Queue Service (Amazon SQS) queue. Invoke the Lambda function from the queue.
C) Increase the timeout of the new AWS Lambda function.
D) Decrease the reserved concurrency of the new AWS Lambda function.
E) Increase the memory of the new AWS Lambda function.

9) A company has built an online ticketing web application on AWS. The application is hosted on AWS App Runner and uses images that are stored in an Amazon Elastic Container Registry (Amazon ECR) repository. The application stores data in an Amazon Aurora MySQL DB cluster. The company has set up a domain name in Amazon Route 53.

The company needs to deploy the application across two AWS Regions in an active-active configuration.

Which combination of steps will meet these requirements with the LEAST change to the architecture? (Select THREE.)

A) Set up Cross-Region Replication to the second Region for the ECR images.
B) Create a VPC endpoint from the ECR repository in the second Region.
C) Edit the App Runner configuration by adding a second deployment target to the second Region.
D) Deploy App Runner to the second Region. Set up Route 53 latency-based routing.
E) Change the database by using Amazon DynamoDB global tables in the two desired Regions.
F) Use an Aurora global database with write forwarding enabled in the second Region.

10) A company has deployed a multi-tier web application in the AWS Cloud. The application consists of the following tiers:

- **A Windows-based web tier that is hosted on Amazon EC2 instances with Elastic IP addresses**
- **A Linux-based application tier that is hosted on EC2 instances that run behind an Application Load Balancer (ALB) that uses path-based routing**
- **A MySQL database that runs on a Linux EC2 instance**

All the EC2 instances are using Intel-based x86 CPUs. A solutions architect needs to modernize the infrastructure to achieve better performance. The solution must minimize the operational overhead of the application.

Which combination of actions should the solutions architect take to meet these requirements? (Select TWO.)

A) Run the MySQL database on multiple EC2 instances.
B) Place the web tier instances behind an ALB.
C) Migrate the MySQL database to Amazon Aurora Serverless.
D) Migrate all EC2 instance types to Graviton2.
E) Replace the ALB for the application tier instances with a company-managed load balancer.

Answers

1) C – Billing alarms will provide the company with alerts about excessive spending without taking away control from any of the business groups. Options A and B are incorrect because each business group wants to retain control of its account. These options would not prevent the launch of a large number of instances. Option D is a manual process that would not provide immediate alerts about excessive spending.

2) D – AWS CloudFormation StackSets can deploy the IAM role across multiple accounts with a single operation. Option A is incorrect because credentials that are supplied by AWS Single Sign-On (AWS SSO) are temporary. The application would lose permissions and would have to log in again. Option B would grant access to the management account only. Option C is incorrect because when an account joins an organization, the account does not receive permissions to access the other accounts in the organization.

3) D, E – Cross-origin resource sharing (CORS) is a browser security feature that restricts HTTP requests that initiate from scripts that run in the browser. CORS is typically required to build web applications that access APIs that are hosted on a different domain or origin. You can enable CORS to allow requests to your API from a web application that is hosted on a different domain. For example, if your API is hosted on https://[api_id].execute-api.[region].amazonaws.com/ and you want to call your API from a web application that is hosted on [bucketname].s3.website-[region], your API must support CORS. Option E is required for the HTML form to be served through a website endpoint.

Option A is incorrect because the CORS header must be configured to be returned by the dynamic response from the API endpoint. The configuration of CORS for the S3 bucket does not help. Option B is incorrect because there is no advantage to serving a static webpage from a web server that runs on Amazon EC2 instead of from an S3 bucket. Option C is incorrect because API Gateway has a default quota of 10,000 requests per second for each AWS Region. If necessary, you can increase this quota.

4) A – Amazon API Gateway will intermittently return HTTP status code 502 (Bad Gateway) errors if the AWS Lambda function exceeds its concurrency quota. Option B is incorrect because, in this case, API Gateway would return a status code 429 error for too many requests. Option C is incorrect because the errors occur during calls to the API Gateway API endpoint, not during the authentication process. Option D is incorrect because stale data would not cause a Bad Gateway error.

5) C – AWS Systems Manager Run Command requires no inbound ports to be open. Run Command operates entirely over outbound HTTPS, which is open by default for security groups. Options A and B are incorrect because the requirements state that the only inbound port that should be open is 443. Option D is incorrect because AWS Trusted Advisor does not perform this management function.

6) D – The correct answer follows the standard guidelines for granting cross-account access between two accounts that you control. Option A does not meet the requirements because it requires two sets of credentials for operators. Option B is incorrect because you cannot add an IAM user to an IAM group in a different account. Option C is incorrect because a role cannot grant access to resources in another account. The shared role must be in the same account with resources that the shared role manages.

7) B, D – The average amount of compute to address the outliers each hour is 300 seconds (10 events for 30 seconds each). Option B is correct because with AWS Lambda, you pay only for the small amount of compute time that is required to process the outlying values. While options A and E would reduce costs, they both involve paying for one or more Amazon EC2 instances that would sit unused for 3,300 seconds each hour. Options C and D reduce the shard hour costs of the Kinesis data stream. However, option C is incorrect because the amount of data would exceed the 1 MB/s quota of a single shard.

8) B, D – In option B, the use of an Amazon Simple Queue Service (Amazon SQS) queue will decouple the main application from calls to the affiliate. This change will protect the main application from the reduced capacity of the affiliate. Additionally, failed requests can automatically return to the queue. In option D, a decreased number of concurrent invocations will prevent the affiliate application from getting overwhelmed.

Although option A will reduce the load on the Amazon EC2 instances, this solution will not reduce the number of requests to the affiliate application. Although option C will allow the AWS Lambda function to wait longer for the external call to return, this solution will not reduce the load on the overwhelmed affiliate application. Option E is incorrect because an increase in memory will have no effect on the interaction between the Lambda function and the affiliate tracking system.

9) A, D, F – AWS App Runner is a fully managed service that developers can use to quickly deploy containerized web applications with images that are stored in an Amazon Elastic Container Registry (Amazon ECR) repository. Option A is correct because Cross-Region Replication makes a copy of the repository in a second AWS Region. Option D is correct because you can use Route 53 to host the custom domain name and to route traffic to resources in multiple AWS Regions. Option F is correct because Amazon Aurora global databases extend across multiple Regions and are designed for globally distributed applications.

Option B is incorrect because a VPC endpoint will not provide access to an image that is stored in a different Region. In option C, no such configuration exists in App Runner. Although option E would work, the introduction of Amazon DynamoDB would require more change to the architecture than the use of an Aurora global database. The question asks for the least change to the architecture.

10) B, C – In option B, by placing the web tier behind an Application Load Balancer (ALB), you can improve availability and scalability of the web tier. The ALB serves as the single point of contact for clients and distributes incoming application traffic to the Amazon EC2 instances. Option C is correct because Amazon Aurora Serverless provides high performance and high availability with reduced operational complexity.

Option A is incorrect because additional EC2 instances will not minimize operational overhead. A managed service would be a better option. Option D is incorrect because the application includes Windows instances, which are not available for Graviton2. Option E is incorrect because a company-managed load balancer will not minimize operational overhead.