Exam Cram
Amazon VPC, EC2, and ELB

© Digital Cloud Training | https://digitalcloud.training

Exam Cram: Amazon VPC, EC2, and ELB

- A VPC is a logically isolated portion of the AWS cloud within a Region
- The VPC router takes care of routing within the VPC and outside of the VPC
- The route table is used to configure the VPC router
- An Internet Gateway is attached to a VPC and used to connect to the Internet
- A VPC spans all the Availability Zones (AZs) in the Region
- Each VPC has a different block of IP addresses (CIDR block)
- Subnets are created within AZs
- Each subnet has a block of IP addresses from the CIDR block

Exam Cram: Amazon VPC, EC2, and ELB

- Security Groups apply at the Instance level
- Security Groups can be applied to instances in any subnet
- Security groups support allow rules only
- Separate rules are defined for outbound traffic
- A source can be an IP address or security group ID
- NACLs apply at the subnet level
- NACLs apply only to traffic entering / exiting the subnet
- Rules are processed in order (numbered)
- NACLs have an explicit deny at the end

Exam Cram: Amazon VPC, EC2, and ELB

- An EC2 instance is a virtual server
- EC2 instances run Windows, Linux, or MacOS
- EC2 hosts are managed by AWS
- An AMI defines the configuration of the instance
- You can customize your instance and create a custom AMI
- A snapshot is a point-in-time backup of an instance
- User Data is run when the instance starts for the first time
- Instance metadata is data about your EC2 instance
- Instance metadata is available at: http://169.254.169.254/latest/meta-data

Exam Cram: Amazon VPC, EC2, and ELB

- Access keys are composed of the access key ID and secret access key
- You can use access keys to sign programmatic requests to the AWS CLI or AWS API
- Best practice to use temporary security credentials (IAM roles) instead of access keys
- Also, disable any AWS account root user access keys
- The access key is associated with an IAM account
- The access key will use permissions assigned to the IAM user
- IAM roles should be used instead of access keys where possible

Exam Cram: Amazon VPC, EC2, and ELB

- Elastic Load Balancers (ELBs) provide a single endpoint for your application
- ELBs distribute connections to back-end instances, IPs, containers, and functions
- Target Groups are used for attaching the target applications to the ELB
- The ALB is used for web applications with L7 routing (HTTP/HTTPS) and offers advanced request routing
- The NLB is used for TCP and UDP based applications and offers ultra low latency, static Ips and VPC endpoint services
- The GLB distributes connections to appliances like IDS, IPS, NGFW, and WAF

DigitalCloud TRAINING

Exam Cram: Amazon VPC, EC2, and ELB

- Session state data can be stored in databases such as DynamoDB and ElastiCache
- Can include temporary data, metadata, authentication information etc.
- Sticky sessions can be used on ELBs to bind a session to an EC2 instance
- Sticky sessions uses cookies that are generated at the ELB level
- You can use a combination of duration-based stickiness, application-based stickiness, and no stickiness across your target groups
- Sticky sessions are not supported with TLS listeners and TLS target groups (NLB)

Exam Cram
Amazon S3 and CloudFront

© Digital Cloud Training | https://digitalcloud.training

Exam Cram: Amazon S3 and CloudFront

- You can store any type of file in S3
- Files can be anywhere from 0 bytes to 5 TB
- There is unlimited storage available
- S3 is a universal namespace so bucket names must be unique globally
- However, you create your buckets within a REGION
- It is a best practice to create buckets in regions that are physically closest to your users to reduce latency
- There is no hierarchy for objects within a bucket
- Delivers strong read-after-write consistency
- The object name is the key the data is the value
- A folder is a shared prefix for grouping objects

Exam Cram: Amazon S3 and CloudFront

- Folders can be created within folders
- Buckets cannot be created within other buckets
- Amazon S3 is a public service
- VPC Endpoints can be used to connect using private Ips
- IAM Policies are identity-based policies and can control access to S3
- IAM Policies are attached to IAM users, groups, or roles
- IAM Policies are written in JSON using the AWS access policy language
- Bucket Policies are resource-based policies
- Can only be attached to Amazon S3 buckets
- Also use the AWS access policy language

Exam Cram: Amazon S3 and CloudFront

- ACLs are a legacy access control mechanism that predates IAM
- AWS generally recommends using S3 bucket policies or IAM policies rather than ACLs
- ACLs can be attached to a bucket or directly to an object
- ACLs offer limited options for grantees and permissions
- MFA Delete adds MFA requirement for bucket owners
- Applies to changing versioning state or permanent object deletion
- Versioning can be enabled by bucket owners, AWS account that created the bucket, authorized IAM users
- MFA delete can be enabled by the bucket owner only
- MFA-Protected API Access enforces another authentication factor when accessing AWS resources

Exam Cram: Amazon S3 and CloudFront

- Encryption options:
  - Server-side encryption with S3 managed keys (SSE-S3)
  - Server-side encryption with AWS KMS managed keys (SSE-KMS)
  - Server-side encryption with client provided keys (SSE-C)
  - Client-side encryption
- Amazon S3 default encryption provides a way to set the default encryption behavior for an S3 bucket
- You can set default encryption on a bucket so that all new objects are encrypted when they are stored in the bucket
- The objects are encrypted using server-side encryption
- Amazon S3 encrypts objects before saving them to disk and decrypts them when the objects are downloaded
- There is no change to the encryption of objects that existed in the bucket before default encryption was enabled

Exam Cram: Amazon S3 and CloudFront

- Server Access Logging provides detailed records for the requests that are made to a bucket
- Details include the requester, bucket name, request time, request action, response status, and error code
- CORS allows requests from an origin to another origin
- Origin is defined by DNS name, protocol, and port
- CORS is enabled through setting:
  - Access-Control-Allow-Origin
  - Access-Control-Allow-Methods
  - Access-Control-Allow-Headers

Exam Cram: Amazon S3 and CloudFront

- S3 automatically scales to high request rates with at least:
  - 3,500 PUT/COPY/POST/DELETE or
  - 5,500 GET/HEAD requests per second per partitioned prefix (per prefix)
- Can increase read and write performance by using parallelization across multiple prefixes
- To increase uploads over long distances, use Amazon S3 Transfer Acceleration
- Byte-Range fetches use the Range HTTP header to transfer only specified byte-range from an object
- Combine S3 and EC2 in the same AWS Region
- Use the latest version of the AWS SDKs
- Use caching services to cache the latest content
- Horizontally scale requests across S3 endpoints

Exam Cram: Amazon S3 and CloudFront

- CloudFront can be used for caching content for performance
- A distribution is created in CloudFront
- Each distribution has an origin
- Only web distributions are currently supported
- Signed URLs provide more control over access to content
- Can specify beginning and expiration date and time, IP addresses/ranges of users
- Signed cookies are similar to Signed URLs
- Use signed cookies when you don’t want to change URLs
- Can also be used when you want to provide access to multiple restricted files

Exam Cram
Infrastructure as Code and PaaS

© Digital Cloud Training | https://digitalcloud.training

Exam Cram: Infrastructure as Code and PaaS

- With CloudFormation infrastructure patterns are defined in a template file using code
- CloudFormation builds your infrastructure according to the template (JSON or YAML)
- Infrastructure is provisioned consistently, with fewer mistakes (human error)
- Less time and effort than configuring resources manually
- You can use version control and peer review for your CloudFormation templates
- Free to use (you're only charged for the resources provisioned)
- Can be used to manage updates and dependencies
- Can be used to rollback and delete the entire stack as well

© Digital Cloud Training | https://digitalcloud.training

Exam Cram: Infrastructure as Code and PaaS

- You create, update and delete stacks using templates
- Stacks are deployed through the Management Console, CLI or APIs
- With StackSets you can create, update, or delete stacks across multiple accounts and Regions with a single operation
- An administrator account is the AWS account in which you create StackSets
- A stack set is managed by signing into the AWS administrator account in which it was created
- Nested stacks allow re-use of CloudFormation code for common use cases
- Rewatch the template deep dive session for important exam knowledge

Exam Cram: Infrastructure as Code and PaaS

- AWS Elastic Beanstalk deploys and manages web applications
- Can also deploy the ELB, Auto Scaling, and even a DB
- Web servers are standard applications that listen for and then process HTTP requests, typically over port 80
- Workers use a background processing task to listen for messages on an Amazon SQS queue

Exam Cram: Infrastructure as Code and PaaS

- Elastic Beanstalk deployment options:
  - **All at once** deploys the new version to all instances simultaneously
  - **Rolling** updates a batch of instances, and then move onto the next batch once the first batch is healthy
  - **Rolling with additional batch** is like Rolling but launches new instances in a batch ensuring that there is full availability
  - **Immutable** launches new instances in a new ASG and deploys the version update to these instances before swapping traffic to these instances once healthy
  - **Blue/green** creates a new "stage" environment and deploy updates there

DigitalCloud TRAINING

© Digital Cloud Training | https://digitalcloud.training

Exam Cram: Infrastructure as Code and PaaS

- Elastic Beanstalk configuration files (.ebextensions) can be added to your web application's source code
- Used to customize environment and resources
- Configuration files are YAML or JSON-formatted documents with a .config file extension
- They should be placed in the .ebextensions folder in the application source code bundle
- The option_settings section of a configuration file defines values for configuration options
- The Resources section lets you further customize the resources in your application's environment
- SSL/TLS certificates can be assigned to an environment’s Elastic Load Balancer (can use ACM)
- The connections between clients and the load balancer are secured

Exam Cram
AWS Lambda and AWS SAM

© Digital Cloud Training | https://digitalcloud.training

Exam Cram: AWS Lambda and AWS SAM

- With serverless there are no instances to manage
- You don’t need to provision hardware
- There is no management of operating systems or software
- Capacity provisioning and patching is handled automatically
- Provides automatic scaling and high availability
- Can be very cheap!
- AWS Lambda executes code only when needed and scales automatically
- You pay only for the compute time you consume

Exam Cram: AWS Lambda and AWS SAM

Synchronous invocation:

- CLI, SDK, API Gateway
- Wait for the function to process the event and return a response
- Error handling happens client side (retries, exponential backoff etc.)

Asynchronous invocation:

- S3, SNS, CloudWatch Events etc.
- Event is queued for processing and a response is returned immediately
- Lambda retries up to 3 times
- Processing must be idempotent (due to retries)

Event source mapping:

- SQS, Kinesis Data Streams, DynamoDB Streams
- Lambda does the polling (polls the source)
- Records are processed in order (except for SQS standard)

Exam Cram: AWS Lambda and AWS SAM

- You can use Lambda to process event notifications from Amazon S3
- Amazon S3 can send an event to a Lambda function when an object is created or deleted
- Amazon S3 invokes your function asynchronously with an event that contains details about the object

Exam Cram: AWS Lambda and AWS SAM

- Versioning means you can have multiple versions of your function
- You can use versions to manage the deployment of your AWS Lambda functions
- You work on $LATEST which is the latest version of the code - this is mutable (changeable)
- When you're ready to publish a Lambda function you create a version (these are numbered)
- Each version has its own ARN
- Lambda aliases are pointers to a specific Lambda version
- Using an alias, you can invoke a function without having to know which version of the function is being referenced
- Aliases are mutable (changeable)

Exam Cram: AWS Lambda and AWS SAM

- A deployment package is used to deploy function code to Lambda
- Lambda supports two types of deployment packages:
  - Container images
  - .zip file archives
- A .zip file archive includes your application code and its dependencies
- The deployment package is uploaded from Amazon S3 or your computer
- There are limits to the size of zip archives:
  - 50 MB (zipped, for direct upload)
  - 250 MB (unzipped)
  - 3 MB (console editor)

© Digital Cloud Training | https://digitalcloud.training

Exam Cram: AWS Lambda and AWS SAM

- You can configure your Lambda function to pull in additional code and content in the form of layers
- A layer is a ZIP archive that contains libraries, a custom runtime, or other dependencies
- To add layers to your function, use the update-function-configuration command
- Environment variables can be used to adjust your function's behavior without updating code
- An environment variable is a pair of strings that is stored in a function's version-specific configuration
- Environment variables are defined on the unpublished version of a function
- When you publish a version, the environment variables are locked for that version

Exam Cram: AWS Lambda and AWS SAM

- The default concurrency limit per AWS Region is 1,000 invocations at any given time
- There is no maximum concurrency limit for Lambda functions (depends on use case)
- Reserved concurrency guarantees a set number of concurrent executions will be available for a critical function
- When provisioned concurrency is allocated, the function scales with the same burst behavior as standard concurrency
- Lambda sends metrics to Amazon CloudWatch for performance monitoring
- Execution logs are stored in Amazon CloudWatch Logs
- The Lambda function execution role must have permissions (IAM) to allow writes to CloudWatch Logs
- You can use AWS X-Ray to visualize the components of your application

Exam Cram: AWS Lambda and AWS SAM

- You can connect your functions to an Amazon VPC
- Must connect to a private subnet with a NAT Gateway for Internet access (no public IP)
- Be careful with DNS resolution of public hostnames as it could add to function running time (cost)
- To connect to a VPC, your function's execution role must have the permissions to create the network interface in the VPC
- AWS Signer is a fully managed code-signing service
- Used to ensure the trust and integrity of code
- Code is validated against a digital signature
- With Lambda you can ensure only trusted code runs in Lambda functions

Exam Cram: AWS Lambda and AWS SAM

- Best practices for function code include:
  - Separate the Lambda handler from your core logic
  - Take advantage of execution environment reuse to improve the performance of your function
  - Use a keep-alive directive to maintain persistent connections
  - Use environment variables to pass operational parameters to your function
  - Control the dependencies in your function's deployment package
  - Minimize your deployment package size to its runtime necessities
  - Avoid using recursive code in your function

Exam Cram
Amazon DynamoDB

Exam Cram: Amazon DynamoDB

- Fully managed NoSQL database service
- Key/value store and document store
- It is a non-relational, key-value type of database
- Data is stored in partitions which are replicated across multiple AZs
- DynamoDB provides low latency (milliseconds)
- Microsecond latency can be achieved with DynamoDB Accelerator (DAX)
- All data is stored on SSD storage
- Data is replicated across multiple AZs in a Region
- DynamoDB Global Tables synchronizes tables across Regions

© Digital Cloud Training | https://digitalcloud.training

Exam Cram: Amazon DynamoDB

- DynamoDB table classes are:
  - DynamoDB Standard – default and recommended for most workloads
  - DynamoDB Standard-Infrequent Access (DynamoDB Standard-IA) – lower cost storage for infrequently accessed data
- DynamoDB supports identity-based policies
- DynamoDB doesn't support resource-based policies
- There are two types of Primary key – Partition keys and composite keys
- A composite key is a Partition key + Sort key in combination
- Best practices:
  - Use high-cardinality attributes
  - Use composite attributes
  - Cache popular items (DAX)
  - Use random numbers for write-heavy use cases

Exam Cram: Amazon DynamoDB

- DynamoDB supports eventually consistent and strongly consistent reads
- Eventually consistent reads:
  - When you read data from a DynamoDB table, the response might not reflect the results of a recently completed write operation
- Strongly consistent reads:
  - DynamoDB returns a response with the most up-to-date data, reflecting updates from all prior write operations
- Strongly consistent reads use more throughput capacity than eventually consistent reads
- DynamoDB uses eventually consistent reads by default
- You can configure strongly consistent reads with the GetItem, Query and Scan APIs

Exam Cram: Amazon DynamoDB

- DynamoDB transactions makes coordinated, all-or-nothing changes to multiple items both within and across tables
- Transactions provide atomicity, consistency, isolation, and durability (ACID) in DynamoDB
- Enables reading and writing of multiple items across multiple tables as an all or nothing operation
- There is no additional cost to enable transactions for DynamoDB tables
- You pay only for the reads or writes that are part of your transaction
- DynamoDB performs two underlying reads or writes of every item in the transaction

Exam Cram: Amazon DynamoDB

- Throttling occurs when the configured RCU or WCU are exceeded
- May receive a ProvisionedThroughputExceededException
- The Scan operation returns one or more items and item attributes by accessing every item in a table or a secondary index
- A query operation finds items in your table based on the primary key attribute and a distinct value to search for
- An LSI provides an alternative sort key to use for scans and queries
- Gives you a different view of your data, organized by alternative sort key
- A GSI is used to speed up queries on non-key attributes
- Can specify a different partition key as well as a different sort key

Exam Cram: Amazon DynamoDB

- Optimistic locking is a strategy to ensure that the client-side item that you are updating (or deleting) is the same as the item in Amazon DynamoDB
- Protects database writes from being overwritten by the writes of others, and vice versa
- TTL lets you define when items in a table expire so that they can be automatically deleted from the database
- With TTL enabled on a table, you can set a timestamp for deletion on a per-item basis
- No extra cost and does not use WCU / RCU

Exam Cram: Amazon DynamoDB

- DynamoDB Streams captures a time-ordered sequence of item-level modifications in any DynamoDB table
- The information is stored in a log for up to 24 hours
- DAX is a managed service that provides in-memory acceleration for DynamoDB tables
- Improves performance from milliseconds to microseconds, even at millions of requests per second
- DynamoDB global tables is a fully managed solution for deploying a multi-region, multi-master database
- When you create a global table, you specify the AWS Regions where you want the table to be available

Exam Cram
Application Integration and APIs

Exam Cram: Application Integration and APIs

- Amazon SQS is pull-based, not push-based (like SNS)
- Messages are up to 256KB in size
- Larger messages can be sent using the Amazon SQS Extended Client Library for Java
- Messages can be kept in the queue from 1 minute to 14 days
- Default retention period is 4 days
- Amazon SQS guarantees that your messages will be processed at least once
- Standard queues offer best-effort ordering and at-least-once delivery
- FIFO queues offer first-in-first-out ordering and exactly-once processing

Exam Cram: Application Integration and APIs

- The main task of a dead-letter queue is handling message failure
- A dead-letter queue lets you set aside and isolate messages that can’t be processed correctly
- It is not a queue type, it is a standard or FIFO queue that has been specified
- Messages are moved to the dead-letter queue when the ReceiveCount for a message exceeds the maxReceiveCount for a queue
- Delay queues add a delay to processing of the messages
- The visibility timeout is the amount of time a message is invisible in the queue after a reader picks it up
- If the job is not processed within the visibility timeout, the message will become visible again and another reader will process it

Exam Cram: Application Integration and APIs

- SQS Long polling is a way to retrieve messages from SQS queues – waits for messages to arrive
- SQS Short polling returns immediately (even if the message queue is empty)
- SQS Long polling can lower costs
- SQS Long polling can be enabled at the queue level or at the API level using WaitTimeSeconds
- SQS Long polling is in effect when the Receive Message Wait Time is a value greater than 0 seconds and up to 20 seconds
- You can use Amazon S3 and the Amazon SQS Extended Client Library for Java to manage Amazon SQS messages
- Useful for storing and consuming messages up to 2 GB in size

Exam Cram: Application Integration and APIs

- Amazon SNS is a highly available, durable, secure, fully managed pub/sub messaging service
- Amazon SNS provides topics for high-throughput, push-based, many-to-many messaging
- Multiple recipients can be grouped using Topics
- You can subscribe one or more Amazon SQS queues to an Amazon SNS topic
- AWS Step Functions is used to build distributed applications as a series of steps in a visual workflow
- You can quickly build and run state machines to execute the steps of your application

DigitalCloud TRAINING

Exam Cram: Application Integration and APIs

- EventBridge was formerly Amazon CloudWatch Events
- Amazon EventBridge is a serverless event bus
- Used to build event-driven applications
- Event sources can be AWS services or third-party applications
- Rules are run based on events and routed to targets

Exam Cram: Application Integration and APIs

Amazon API Gateway supports:

- REST APIs - support OIDC and OAuth 2.0 authorization, and come with built-in support for CORS and automatic deployments
- HTTP APIs - designed for low-latency, cost-effective integrations with AWS services, including AWS Lambda, and HTTP endpoints
- WebSocket APIs – deployed as a stateful frontend for an AWS service (such as Lambda or DynamoDB) or for an HTTP endpoint
- REST APIs and HTTP APIs support authorizers for AWS Lambda, IAM, and Amazon Cognito
- WebSocket APIs support IAM authorization and Lambda authorizers

Exam Cram: Application Integration and APIs

- An edge-optimized API endpoint is best for geographically distributed clients
- API requests are routed to the nearest CloudFront Point of Presence (POP)
- A regional API endpoint is intended for clients in the same region
- Reduces connection overhead for connections from the same Region
- Private REST APIs can only be accessed from within a VPC using an interface VPC endpoint
- A resource represents a path in your API
- Methods are created within resources
- A Method resource is integrated with an Integration resource

© Digital Cloud Training | https://digitalcloud.training

Exam Cram: Application Integration and APIs

- Deployments are a snapshot of the APIs resources and methods
- Deployments must be created and associated with a stage for anyone to access the API
- A stage is a logical reference to a lifecycle state of your REST or WebSocket API (e.g. ‘dev’, ‘prod’, ‘beta’, ‘v2’)
- You can add caching to API calls by provisioning an Amazon API Gateway cache and specifying its size in gigabytes
- Caches are defined per stage
- API Gateway sets a limit on a steady-state rate and a burst of request submissions against all APIs in your account
- API Gateway can apply server-side throttling limits and per-client throttling limits (when using API keys associated with a usage policy)

Exam Cram
Containers on Amazon ECS/EKS

© Digital Cloud Training | https://digitalcloud.training

Exam Cram: Containers on Amazon ECS/EKS

- Amazon ECS is used for managing and deploying Docker containers
- Serverless with AWS Fargate – managed for you and fully scalable
- Fully managed container orchestration – control plane is managed for you
- Docker support – run and manage Docker containers with integration into the Docker Compose CLI
- Windows container support – ECS supports management of Windows containers
- Elastic Load Balancing integration – distribute traffic across containers using ALB or NLB
- Amazon ECS Anywhere (NEW) – enables the use of Amazon ECS control plane to manage on-premises implementations
- ECS Clusters are a logical grouping of container instances that you can place tasks on
- Clusters can contain tasks using the Fargate and EC2 launch type

Exam Cram: Containers on Amazon ECS/EKS

- You can use any AMI that meets the Amazon ECS AMI specification
- The EC2 instances used as container hosts must run an ECS agent
- The ECS container agent allows container instances to connect to the cluster
- The container agent runs on each infrastructure resource on an ECS cluster
- Containers are created from a read-only template called an image which has the instructions for creating a Docker container
- Images are built from a Dockerfile
- Only Docker containers are supported on ECS
- Images are stored in a registry such as DockerHub or Amazon Elastic Container Registry (ECR)
- A task definition is required to run Docker containers in Amazon ECS
- A task definition is a text file in JSON format that describes one or more containers

Exam Cram: Containers on Amazon ECS/EKS

- The ECS task IAM role provides permissions to the container
- The container instance IAM role provides permissions to the host
- Tasks have access to all of the permissions that are supplied to the container instance role through instance metadata
- Amazon ECS supports the following task placement strategies:
  - binpack - place tasks based on the least available amount of CPU or memory
  - random - place tasks randomly
  - spread - place tasks evenly based on the specified value

© Digital Cloud Training | https://digitalcloud.training

Exam Cram: Containers on Amazon ECS/EKS

- A task placement constraint is a rule that is considered during task placement
- ECS supports the following types of task placement constraints:
  - distinctInstance - Place each task on a different container instance
  - memberOf - Place tasks on container instances that satisfy an expression
- Cluster queries are expressions that enable you to group objects
- For example, you can group container instances by attributes such as Availability Zone, instance type, or custom metadata
- Service auto scaling automatically adjusts the desired task count up or down using the Application Auto Scaling service
- Cluster auto scaling uses a Capacity Provider to scale the number of EC2 cluster instances using EC2 Auto Scaling

Exam Cram: Containers on Amazon ECS/EKS

- Amazon ECR is a fully-managed container registry
- Integrated with Amazon ECS and Amazon EKS
- Supports Open Container Initiative (OCI) and Docker Registry HTTP API V2 standards
- You can use Docker tools and Docker CLI commands such as push, pull, list, and tag
- Can be accessed from any Docker environment – in the cloud, on-premises, or on you machine
- You can use namespaces to organize repositories
- ECR supports lifecycle policies, image scanning, cross-Region/account replication and pull through cache rules

Exam Cram: Containers on Amazon ECS/EKS

- Amazon Elastic Kubernetes Service (Amazon EKS) is a managed service
- Use when you need to standardize container orchestration across multiple environments using a managed Kubernetes implementation
- Cluster Auto Scaling:
  - Vertical Pod Autoscaler - automatically adjusts the CPU and memory reservations for your pods to help "right size" your applications
  - Horizontal Pod Autoscaler - automatically scales the number of pods in a deployment, replication controller, or replica set based on that resource's CPU utilization
- Workload Auto Scaling:
- Amazon EKS supports two autoscaling products:
  - Kubernetes Cluster Autoscaler
  - Karpenter open source autoscaling project
- Amazon EKS supports native VPC networking with the Amazon VPC Container Network Interface (CNI) plugin for Kubernetes

Exam Cram
AWS Developer Tools (CI/CD)

© Digital Cloud Training | https://digitalcloud.training

Exam Cram: AWS Developer Tools (CI/CD)

- GitHub is a cloud-based platform that hosts Git repositories for collaboration and CI/CD integration:
  - Centralized repository for all of your code, binaries, images, and libraries
  - Tracks and manages code changes
  - Maintains version history
  - Manages updates from multiple sources
- Other examples exist and integrate into AWS code pipelines including BitBucket and GitLab
- Git works with GitHub by sending local code changes to a shared online repository and retrieving the latest updates from others

© Digital Cloud Training | https://digitalcloud.training

Exam Cram: AWS Developer Tools (CI/CD)

- AWS CodePipeline is a managed continuous delivery service that helps you automate your release pipelines
- Automates the build, test, and deploy phases of your release process every time there is a code change
- CodePipeline provides tooling integrations for many AWS and third-party software
- CodeGuru provides intelligent recommendations for improving application performance, efficiency, and code quality

Exam Cram: AWS Developer Tools (CI/CD)

- CodeGuru reviews Java and Python code and offers suggestions for improvement
- Suggestions are best on best practices
- Finds complex issues such as resource leak and security analysis
- Made up of two services:
  - Amazon CodeGuru Reviewer
  - Amazon CodeGuru Profiler

Exam Cram: AWS Developer Tools (CI/CD)

- AWS CodeBuild is a fully managed continuous integration (CI) service
- Compiles source code, runs tests, and produces software packages that are ready to deploy
- CodeBuild takes source code from GitHub, Bitbucket, CodePipeline, S3 etc.
- Build instructions can be defined in the code (buildspec.yml)
- Output logs can be sent to Amazon S3 & Amazon CloudWatch Log

Exam Cram: AWS Developer Tools (CI/CD)

- CodeDeploy is a deployment service that automates application deployments
- Deploys to Amazon EC2 instances, on-premises instances, serverless Lambda functions, and Amazon ECS
- You can deploy a nearly unlimited variety of application content
- An AWS CodeDeploy application contains information about what to deploy and how to deploy it
- Need to choose the compute platform:
  - EC2/On-premises
  - AWS Lambda
  - Amazon ECS

Exam Cram: AWS Developer Tools (CI/CD)

- For EC2/On-Premises traffic is directed using an in-place or blue/green deployment type (to a replacement set of instances)
- For AWS Lambda traffic is shifted using a canary, linear, or all-at-once configuration (to a new version of the function)
- For Amazon ECS, CodeDeploy performs a blue/green deployment by installing an updated version of the application as a new replacement task set
- For Amazon ECS traffic is shifted using a canary, linear, or all-at-once configuration (to a replacement task set)
- **Note:** All AWS Lambda and Amazon ECS deployments are blue/green. An EC2/On-Premises deployment can be in-place or blue/green

Exam Cram
Databases and Analytics

© Digital Cloud Training | https://digitalcloud.training

Exam Cram: Databases and Analytics

- RDS uses EC2 instances, so you must choose an instance family/type
- Relational databases are known as Structured Query Language (SQL) databases
- RDS is an Online Transaction Processing (OLTP) type of database
- Easy to setup, highly available, fault tolerant, and scalable
- Common use cases include online stores and banking systems
- You can encrypt your Amazon RDS instances and snapshots at rest by enabling the encryption option for your Amazon RDS DB instance (during creation)
- Encryption uses AWS Key Management Service (KMS)
- Scales up by increasing instance size (compute and storage)
- Read replicas option for read heavy workloads (scales out for reads/queries only)
- Disaster recovery with Multi-AZ option

Exam Cram: Databases and Analytics

- Encryption at rest can be enabled – includes DB storage, backups, read replicas and snapshots
- You can only enable encryption for an Amazon RDS DB instance when you create it, not after the DB instance is created
- DB instances that are encrypted can't be modified to disable encryption
- RDS for Oracle and SQL Server is also supported using TDE (may have performance impact)
- AWS KMS is used for managing encryption keys

Exam Cram: Databases and Analytics

- You can't have:
  - An encrypted read replica of an unencrypted DB instance
  - An unencrypted read replica of an encrypted DB instance
- Read replicas of encrypted primary instances are encrypted
- The same KMS key is used if in the same Region as the primary
- If the read replica is in a different Region, a different KMS key is used
- You can't restore an unencrypted backup or snapshot to an encrypted DB instance

Exam Cram: Databases and Analytics

- ElastiCache is a fully managed implementation of either Redis or Memcached
- ElastiCache is a key/value store
- In-memory database offering high performance and low latency
- Can be put in front of databases such as RDS and DynamoDB
- ElastiCache nodes run on Amazon EC2 instances, so you must choose an instance family/type
- Data is not persistent with Memcached but can be with Redis
- Encryption can only be enabled with Redis
- Memcached is the only option for multithreaded applications
- Caching options include:
  - Lazy loading – loads data only when necessary (if a cache miss occurs), results in higher latency for reads
  - Write-through - cache is updated whenever a new write or update is made to the underlying database, results in higher latency for writes

Exam Cram: Databases and Analytics

- With Kinesis Data Streams producers send data to Kinesis, data is stored in Shards for 24 hours (by default, up to 7 days)
- Consumers then take the data and process it - data can then be saved into another AWS service
- Real time with latency of ~200ms
- The Kinesis Client Library (KCL) helps you consume and process data from a Kinesis data stream
- Each shard is processed by exactly one KCL worker and has exactly one corresponding record processor
- One worker can process any number of shards, so it's fine if the number of shards exceeds the number of instances

Exam Cram: Databases and Analytics

- Producers send data to Firehose
- There are no Shards, completely automated (scalability is elastic)
- Firehose data is sent to another AWS service for storing, data can be optionally processed/transformed using AWS Lambda
- Near real-time delivery (~60 seconds latency)
- Kinesis Data Analytics provides real-time SQL processing for streaming data
- KDA provides analytics for data coming in from Kinesis Data Streams and Kinesis Data Firehose
- KDA destinations can be Kinesis Data Streams, Kinesis Data Firehose, or AWS Lambda

© Digital Cloud Training | https://digitalcloud.training

Exam Cram: Databases and Analytics

- Amazon OpenSearch is a distributed search and analytics suite
- OpenSearch is based on the popular open source Elasticsearch
- OpenSearch supports queries using SQL syntax
- OpenSearch integrates with open-source tools
- OpenSearch scales by adding or removing instances
- OpenSearch is available in up to three Availability Zones
- You can backup OpenSearch using snapshots
- Offers encryption at-rest and in-transit
- Clusters are created (Management Console, API, or CLI)
- Clusters are also known as OpenSearch Service domains

Exam Cram: Databases and Analytics

- OpenSearch best practices:
  - Use three dedicated master nodes
  - Configure at least one replica for each index
  - Apply restrictive resource-based access policies to the domain (or use fine-grained access control)
  - Create the domain within an Amazon VPC
  - For sensitive data enable node-to-node encryption and encryption at rest

Exam Cram
Management and Security

© Digital Cloud Training | https://digitalcloud.training

Exam Cram: Management and Security

- CloudWatch is used for performance monitoring, alarms, log collection and automated actions
- CloudWatch Core Features:
  - CloudWatch Metrics – services send time-ordered data points to CloudWatch
  - CloudWatch Alarms – monitor metrics and initiate actions
  - CloudWatch Logs – centralized collection of system and application logs
  - CloudWatch Events – stream of system events describing changes to AWS resources and can trigger actions
- Metrics are sent to CloudWatch for many AWS services
- EC2 metrics are sent every 5 minutes by default (free)
- Detailed EC2 monitoring sends every 1 minute (chargeable)
- Unified CloudWatch Agent sends system-level metrics for EC2 and on-premises servers
- System-level metrics include memory and disk usage

Exam Cram: Management and Security

- The unified CloudWatch agent enables you to do the following:
  - Collect internal system-level metrics from Amazon EC2 instances across operating systems
  - Collect system-level metrics from on-premises servers
  - Retrieve custom metrics from your applications or services using the StatsD and collectd protocols
  - Collect logs from Amazon EC2 instances and on-premises servers (Windows / Linux)
- Agent must be installed on the server
- Can be installed on:
  - Amazon EC2 instances
  - On-premises servers
  - Linux, Windows Server, or macOS

Exam Cram: Management and Security

- CloudTrail logs API activity for auditing
- By default, management events are logged and retained for 90 days
- A CloudTrail Trail logs any events to S3 for indefinite retention
- Trail can be within Region or all Regions
- CloudWatch Events can triggered based on API calls in CloudTrail
- Events can be streamed to CloudWatch Logs
- Management events provide information about management operations that are performed on resources in your AWS account
- Data events provide information about the resource operations performed on or in a resource
- Insights events identify and respond to unusual activity associated with write API calls by continuously analyzing CloudTrail management events

Exam Cram: Management and Security

- KMS keys are the primary resources in AWS KMS
- Used to be known as “customer master keys” or CMKs
- The KMS key also contains the key material used to encrypt and decrypt data
- By default, AWS KMS creates the key material for a KMS key
- You can also import your own key material
- A KMS key can encrypt data up to 4KB in size
- A KMS key can generate, encrypt and decrypt Data Encryption Keys (DEKs)
- Automatic rotation generates new key material every year (optional for customer managed keys)
- Supported for symmetric keys with key material AWS KMS creates

Exam Cram: Management and Security

- To share snapshots with another account you must specify Decrypt and CreateGrant permissions
- The kms:ViaService condition key can be used to limit key usage to specific AWS services
- Cryptographic erasure means removing the ability to decrypt data and can be achieved when using imported key material and deleting that key material
- You must use the DeleteImportedKeyMaterial API to remove the key material
- An InvalidKeyId exception when using SSM Parameter Store indicates the KMS key is not enabled
- Make sure you know the differences between AWS managed and customer managed KMS keys and automatic vs manual rotation

Exam Cram: Management and Security

- Parameter Store provides secure, hierarchical storage for configuration data and secrets
- Highly scalable, available, and durable
- Store data such as passwords, database strings, and license codes as parameter values
- Store values as plaintext (unencrypted data) or ciphertext (encrypted data)
- Stores and rotate secrets safely without the need for code deployments
- Secrets Manager offers automatic rotation of credentials (built-in) for:
  - Amazon RDS (MySQL, PostgreSQL, and Amazon Aurora)
  - Amazon Redshift
  - Amazon DocumentDB
  - For other services you can write your own AWS Lambda function for automatic rotation

Exam Cram: Management and Security

- An Amazon Cognito User Pool is a directory for managing sign-in and sign-up for mobile applications
- Users can also sign in using social IdPs
- Cognito acts as an Identity Broker between the IdP and AWS
- Identity pools are used to obtain temporary, limited-privilege credentials for AWS services
- Identities can come from a Cognito user pool
- Identities can also come from social IdPs
- Identity pools use AWS STS to obtain the credentials
- An IAM role is assumed providing access to the AWS services

© Digital Cloud Training | https://digitalcloud.training