jekobokidou for AWS Community Builders
Posted on Mar 17

The 190 things you need to know to be an AWS Certified Solutions Architect – Associate

#aws #saa03 #certification

I passed the AWS Certified Solutions Architect – Associate certification and I want to share with you the 190 things you need to know for this exam.

001

Design High-Performing Architectures

On termination of an EC2 instance, the default behavior is to also terminate the attached EBS root volume.

002

Design Cost-Optimized Architectures

Amazon ECS with EC2 launch type is charged based on EC2 instances and EBS volumes used.

Amazon ECS with Fargate launch type is charged based on vCPU and memory resources that the containerized application requests.

003

Design Cost-Optimized Architectures

The minimum storage duration is 30 days before you can transition objects from Amazon S3 Standard to Amazon S3 One Zone-IA or Amazon S3 Standard-IA.

004

Design Secure Architectures

Using VPC sharing, an account that owns the VPC (owner) shares one or more subnets with other accounts (participants) that belong to the same organization from AWS Organizations. The owner account cannot share the VPC itself.

005

Design Resilient Architectures

With AWS Global Accelerator, you can shift traffic gradually or all at once between the blue and the green environment and vice-versa without being subject to DNS caching on client devices and internet resolvers, traffic dials and endpoint weights changes are effective within seconds. AWS Global Accelerator does not rely on DNS. Using Anycast IP addresses that dynamically direct traffic to new Backend instances.

006

Design High-Performing Architectures

To establish a private connection between your virtual private cloud (VPC) and the Amazon EFS API, you can create an interface VPC endpoint.

007

Design High-Performing Architectures

You can send data over a Direct Connect connection to an AWS PrivateLink interface VPC endpoint for Amazon EFS by using a private VIF.

008

Design High-Performing Architectures

Using task scheduling in AWS DataSync, you can periodically execute a transfer task from an on-premises storage system to Amazon EFS over Direct Connect.

009

Design High-Performing Architectures

AWS Direct Connect provides three types of virtual interfaces: public, private, and transit.

- **Public virtual interface** : To connect to AWS resources that are reachable by a public IP address such as an Amazon Simple Storage Service (Amazon S3) bucket or AWS public endpoints, use a public virtual interface.
- **Private virtual interface** : To connect to your resources hosted in an Amazon Virtual Private Cloud (Amazon VPC) using their private IP addresses, use a private virtual interface.
- **Transit virtual interface** : To connect to your resources hosted in an Amazon VPC (using their private IP addresses) through a transit gateway, use a transit virtual interface.

010

Design Resilient Architectures

With Amazon RDS Custom for Oracle, you can access and customize your database server host and operating system, for example by applying special patches and changing the database software settings to support third-party applications that require privileged access.

011

Design Cost-Optimized Architectures

You can only use a launch template to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost.

012

Design High-Performing Architectures

All the dependencies of a Lambda function are also packaged into the single Lambda deployment package.

013

Design High-Performing Architectures

By default, AWS Lambda functions always operate from an AWS-owned VPC and hence have access to any public internet address or public AWS APIs. Once an AWS Lambda function is VPC-enabled, it will need a route through a Network Address Translation gateway (NAT gateway) in a public subnet to access public resources.

014

Design High-Performing Architectures

If you intend to reuse code in more than one AWS Lambda function, you should consider creating an AWS Lambda Layer for the reusable code.

015

Design Cost-Optimized Architectures

Dedicated Hosts enable you to use your existing server-bound software licenses like Windows Server and address corporate compliance and regulatory requirements.

016

Design Cost-Optimized Architectures

Use multipart uploads for faster file uploads into the destination Amazon S3 bucket.

017

Design Cost-Optimized Architectures

Use Amazon S3 Transfer Acceleration (Amazon S3TA) to enable faster file uploads into the destination S3 bucket.

Amazon S3 Transfer Acceleration (S3TA) can speed up content transfers to and from Amazon S3 by as much as 50-500% for long-distance transfer of larger objects.

018

Design Resilient Architectures

Amazon S3 delivers strong read-after-write consistency automatically, without changes to performance or availability, without sacrificing regional isolation for applications, and at no additional cost.

After a successful write of a new object or an overwrite of an existing object, any subsequent read request immediately receives the latest version of the object.

019

Design High-Performing Architectures

Leverage AWS Database Migration Service (AWS DMS) as a bridge between Amazon S3 and Amazon Kinesis Data Streams, so that data stored in an S3 bucket is streamed to Kinesis.

020

Design Secure Architectures

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 establishes

federal standards protecting sensitive health information from disclosure without patient's consent. Both Amazon ElastiCache for Redis and Amazon ElastiCache for Memcached are HIPAA Eligible.

021

Design Resilient Architectures

Any database engine level upgrade for an Amazon RDS database instance with Multi-AZ deployment triggers both the primary and standby database instances to be upgraded at the same time. This causes downtime until the upgrade is complete

022

Design Cost-Optimized Architectures

AWS Snowball Edge Storage Optimized is the optimal choice if you need to securely and quickly transfer dozens of terabytes to petabytes of data to AWS.
Effective November 12, 2024, AWS has discontinued end-of-life AWS Snow devices, specifically the Snowcone HDD, Snowcone SSD, Snowball Edge Storage optimized 80TB, Snowball Edge Compute optimized with 52 vCPUs, and the Snowball Edge Compute optimized with GPU.

023

Design Cost-Optimized Architectures

The data stored on AWS Snowball Edge device can be copied into Amazon S3 bucket and later transitioned into Amazon S3 Glacier via a lifecycle policy. You can't directly copy data from AWS Snowball Edge devices into Amazon S3 Glacier.

024

Design Secure Architectures

Use Amazon GuardDuty to monitor any malicious activity on data stored in Amazon S3.
Use Amazon Macie to identify any sensitive data stored on Amazon S3.

025

Design Secure Architectures

With bucket policies, you can grant users within your AWS Account or other AWS Accounts access to your Amazon S3 resources.

026

Design Secure Architectures

You can leverage an AWS Config managed rule to check if any ACM certificates in your account are marked for expiration within the specified number of days.

027

Design Secure Architectures

You can configure AWS Config to stream configuration changes and notifications to an Amazon SNS topic.

028

Design High-Performing Architectures

Amazon FSx for Lustre makes it easy and cost-effective to launch and run the world's most popular high-performance file system. It is used for workloads such as machine learning, high-performance computing (HPC), video processing, and financial modeling.

029

Design High-Performing Architectures

FSx for Lustre integrates with Amazon S3, making it easy to process data sets with the Lustre file system. When linked to an S3 bucket, an FSx for Lustre file system transparently presents S3 objects as files and allows you to write changed data back to S3.

030

Design Secure Architectures

When you create an encrypted Amazon EBS volume and attach it to a supported instance type, data stored at rest on the volume, data moving between the volume and the instance, snapshots created from the volume and volumes created from those snapshots are all encrypted.

031

Design Cost-Optimized Architectures

AWS Cost Explorer helps you identify under-utilized Amazon EC2 instances that may be downsized on an instance by instance basis within the same instance family, and also understand the potential impact on your AWS bill by taking into account your Reserved Instances and Savings Plans.

032

Design Cost-Optimized Architectures

AWS Compute Optimizer recommends optimal AWS Compute resources for your

workloads to reduce costs and improve performance by using machine learning to analyze historical utilization metrics.

033

Design Resilient Architectures

Amazon SQS offers two types of message queues. Standard queues offer maximum throughput, best-effort ordering, and at-least-once delivery. SQS FIFO queues are designed to guarantee that messages are processed exactly once, in the exact order that they are sent.

034

Design Resilient Architectures

By default, FIFO queues support up to 3,000 messages per second with batching, or up to 300 messages per second (300 send, receive, or delete operations per second) without batching.

035

Design Resilient Architectures

The name of a FIFO queue must end with the .fifo suffix. The suffix counts towards the 80-character queue name limit.

You can't convert an existing standard queue into a FIFO queue.

036

Design High-Performing Architectures

AWS Global Accelerator is designed to optimize traffic latency and utilize the AWS global network. AWS Global Accelerator works at the network couch (Layer 3 – TCP/UDP), which is an excellent choice for applications that use UDP.

Without AWS Global Accelerator: It can take many networks to reach the application. Paths to and from the application may differ. Each hop impacts performance and can introduce risks.

With AWS Global Accelerator: Adding AWS Global Accelerator removes these inefficiencies. It leverages the Global AWS Network, resulting in improved performance.

037

Design Resilient Architectures

A Golden AMI is an AMI that you standardize through configuration, consistent security patching, and hardening. It also contains agents you approve for logging, security, performance monitoring, etc.

038

Design Resilient Architectures

Amazon EC2 instance user data is the data that you specified in the form of a configuration script while launching your instance. You can use Amazon EC2 user data to customize the dynamic installation parts at boot time, rather than installing the application itself at boot time.

039

Design Resilient Architectures

The aws S3 sync command uses the CopyObject APIs to copy objects between Amazon S3 buckets. The sync command lists the source and target buckets to identify objects that are in the source bucket but that aren't in the target bucket. If the operation fails, you can run the sync command again without duplicating previously copied objects.

040

Design Resilient Architectures

Amazon S3 Batch Replication provides you a way to replicate objects that existed before a replication configuration was in place, objects that have previously been replicated, and objects that have failed replication.

041

Design Resilient Architectures

With AWS Database Migration Service, you can continuously replicate your data with high availability and consolidate databases into a petabyte-scale data warehouse by streaming data to Amazon Redshift and Amazon S3.

042

Design Resilient Architectures

It is not possible to modify a launch configuration once it is created. The correct option is to create a new launch configuration to use the correct instance type.

043

Design High-Performing Architectures

Amazon Aurora Global Database is designed for globally distributed applications, allowing a single Amazon Aurora database to span multiple AWS regions. It replicates your data with no impact on database performance, enables fast local reads with low latency in each region, and provides disaster recovery from region-wide outages.

044

Design Secure Architectures

When you launch an Amazon EC2 instance, you specify an IAM role to associate with the instance. Applications that run on the instance can then use the role-supplied temporary credentials to sign API requests.

045

Design Cost-Optimized Architectures

Distributing the static content through Amazon S3 allows us to offload most of the network usage to Amazon S3 and free up our applications running on Amazon ECS.

046

Design Resilient Architectures

Each Aurora DB cluster can have up to 15 Aurora Replicas in addition to the primary DB instance.

047

Design Resilient Architectures

You use the reader endpoint for read-only connections for your Aurora cluster. This endpoint uses a load-balancing mechanism to help your cluster handle a query-intensive workload. The reader endpoint is the endpoint that you supply to applications that do reporting or other read-only operations on the cluster.

048

Design Secure Architectures

An AWS transit gateway is a network transit hub that you can use to interconnect your virtual private clouds (VPC) and on-premises networks.

049

Design High-Performing Architectures

A NAT instance or a NAT Gateway can be used in a public subnet in your VPC to enable instances in the private subnet to initiate outbound IPv4 traffic to the Internet.

050

Design High-Performing Architectures

NAT instance can be used as a bastion server. Security Groups can be associated with a NAT instance. NAT instance supports port forwarding.

051

Design Cost-Optimized Architectures

Amazon DynamoDB Accelerator (DAX) is used to natively cache Amazon DynamoDB reads.

052

Design Cost-Optimized Architectures

You can use Amazon CloudFront to improve application performance to serve static content from Amazon S3.

053

Design Resilient Architectures

You can use Amazon CloudWatch Alarms to send an email via Amazon SNS whenever any of the Amazon EC2 instances breaches a certain threshold.

054

Design Secure Architectures

AWS customers can access Amazon Simpl Queue Service (Amazon SQS) from their Amazon Virtual Private Cloud (Amazon VPC) using VPC endpoints, without using public IPs, and without needing to traverse the public internet. VPC endpoints for Amazon SQS are powered by AWS PrivateLink, a highly available, scalable technology that enables you to privately connect your VPC to supported AWS services.

055

Design High-Performing Architectures

If you specify targets using an instance ID, traffic is routed to instances using the primary private IP address specified in the primary network interface for the instance. The load balancer rewrites the destination IP address from the data packet before forwarding it to the target instance.

056

Design Resilient Architectures

Versioning-enabled buckets enable you to recover objects from accidental deletion or overwrite.

057

Design Resilient Architectures

MFA delete requires secondary authentication to take place before objects can be permanently deleted from an Amazon S3 bucket.

058

Design Cost-Optimized Architectures

For heterogeneous database migrations, first use the AWS Schema Conversion Tool to convert the source schema and code to match that of the target database, and then use the AWS Database Migration Service to migrate data from the source database to the target database.

059

Design Secure Architectures

Create a virtual private gateway (VGW) on the AWS side of the VPN and a Customer Gateway on the on-premises side of the VPN.

060

Design Cost-Optimized Architectures

The main pricing parameter while using the AWS Direct Connect connection is the Data Transfer Out (DTO) from AWS to the on-premises data center. DTO refers to the cumulative network traffic that is sent through AWS Direct Connect to destinations outside of AWS. This is charged per gigabyte (GB), and unlike capacity measurements, DTO refers to the amount of data transferred, not the speed.

061

Design Resilient Architectures

A spread placement group can span multiple Availability Zones in the same Region. You can have a maximum of seven running instances per Availability Zone per group. Therefore, to deploy 15 Amazon EC2 instances in a single Spread placement group, the company needs to use 3 Availability Zones.

062

Design Resilient Architectures

AWS Lambda can be combined with DynamoDB to run code for virtually any type of application or backend service.

063

Design Secure Architectures

If you have multiple AWS Site-to-Site VPN connections, you can provide secure

communication between sites using the AWS VPN CloudHub. This enables your remote sites to communicate with each other, and not just with the VPC.

064

Design Secure Architectures

Using IAM roles, it is possible to access cross-account resources.

065

Design Cost-Optimized Architectures

A user pool is a user directory in Amazon Cognito. You can leverage Amazon Cognito User Pools to either provide built-in user management or integrate with external identity providers, such as Facebook, Twitter, Google+, and Amazon.

066

Design Secure Architectures

You can use Secure Socket Layer / Transport Layer Security (SSL/TLS) connections to encrypt data in transit. Amazon RDS creates an SSL certificate and installs the certificate on the DB instance when the instance is provisioned. For MySQL, you launch the MySQL client using the --ssl_ca parameter to reference the public key to encrypt connections. Using SSL, you can encrypt a PostgreSQL connection between your applications and your PostgreSQL DB instances. You can also force all connections to your PostgreSQL DB instance to use SSL.

067

Design Secure Architectures

A permissions boundary can be used to control the maximum permissions employees can grant to the IAM principals (that is, users and roles) that they create and manage.

068

Design High-Performing Architectures

Using Amazon Redshift Spectrum, you can efficiently query and retrieve structured and semistructured data from files in Amazon S3 without having to load the data into Amazon Redshift tables.

069

Design Secure Architectures

Amazon GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail events, Amazon VPC Flow Logs, and DNS logs.

070

Design Cost-Optimized Architectures

If your organization has multiple AWS accounts, then you can subscribe multiple AWS Accounts to AWS Shield Advanced by individually enabling it on each account using the AWS Management Console or API. You will pay the monthly fee once as long as the AWS accounts are all under a single consolidated billing, and you own all the AWS accounts and resources in those accounts.

071

Design Resilient Architectures

Kinesis data streams can continuously capture gigabytes of data per second from hundreds of thousands of sources such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events.

072

Design High-Performing Architectures

By default, scripts entered as user data are executed with root user privileges. By default, user data runs only during the boot cycle when you first launch an instance.

073

Design Cost-Optimized Architectures

You can create an Amazon CloudWatch alarm that monitors an Amazon EC2 instance and automatically reboots the instance. The reboot alarm action is recommended for Instance Health Check failures (as opposed to the recover alarm action, which is suited for System Health Check failures)

074

Design High-Performing Architectures

For example, if you are building a social feed into your application, you can use Neptune to provide results that prioritize showing your users the latest updates from their family, from friends whose updates they 'Like,' and from friends who live close to them.

075

Design Secure Architecturesv

There are two types of VPC endpoints: Interface Endpoints and Gateway Endpoints.

- An **Interface Endpoint** is an Elastic Network Interface with a private IP address from the IP address range of your subnet that serves as an entry point for traffic destined

to a supported service.

- A **Gateway Endpoint** is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service. The following AWS services are supported: Amazon S3 and Amazon DynamoDB.

076

Design High-Performing Architectures

Amazon Kinesis Data Streams Enhanced fan-out allows developers to scale up the number of stream consumers (applications reading data from a stream in real-time) by offering each stream consumer its own 2MB/second pipe of read throughput per shard.

077

Design Resilient Architectures

AWS recommends that you use AWS CloudTrail for logging bucket and object-level actions for your Amazon S3 resources.

078

Design Resilient Architectures

Amazon Simple Notification Service (SNS) is a fully managed messaging service for both application-to-application (A2A) and application-to-person (A2P) communication. It facilitates the delivery of messages or notifications to subscribing endpoints or clients, including mobile devices, email addresses, and SQS queues. A connection between Amazon Kinesis Data Streams (KDS) and SNS can be established using EventBridge Pipes.

079

Design Secure Architectures

If a target group contains only unhealthy registered targets, the load balancer nodes route requests across its unhealthy targets.

080

Design Secure Architectures

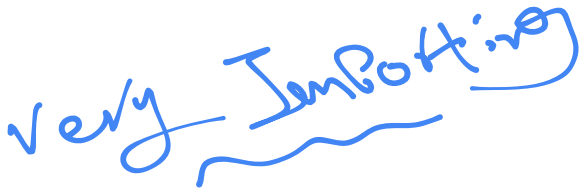
For a Lambda function to be able to access an S3 bucket, create an IAM role for the AWS Lambda function that grants access to the Amazon S3 bucket. Set the IAM role as the AWS Lambda function's execution role. Make sure that the bucket policy also grants access to the AWS Lambda function's execution role.

081

Design High-Performing Architectures

You can use placement groups to influence the placement of a group of interdependent EC2 instances to meet the needs of your workload.

- **Cluster** – packs instances close together inside an Availability Zone (AZ). This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications.
- **Partition** – spreads your instances across logical partitions such that groups of instances in one partition do not share the underlying hardware with groups of instances in different partitions. This strategy is typically used by large distributed and replicated workloads, such as Hadoop, Cassandra, and Kafka.
- **Spread** – strictly places a small group of instances across distinct underlying hardware to reduce correlated failures.



082

Design Resilient Architectures

Throttling is the process of limiting the number of requests an authorized program can submit to a given operation in a given amount of time.

- **Amazon API Gateway** - To prevent your API from being overwhelmed by too many requests, Amazon API Gateway throttles requests to your API using the token bucket algorithm, where a token counts for a request. Specifically, API Gateway sets a limit on a steady-state rate and a burst of request submissions against all APIs in your account. In the token bucket algorithm, the burst is the maximum bucket size.
- **Amazon Simple Queue Service (SQS)** is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. Amazon SQS offers buffer capabilities to smooth out temporary volume spikes without losing messages or increasing latency.
- **Amazon Kinesis** - Amazon Kinesis is a fully managed, scalable service that can ingest, buffer, and process streaming data in real-time.

083

Design High-Performing Architectures

Kinesis Agent cannot write to Amazon Kinesis Firehose for which the delivery stream source is already set as Amazon Kinesis Data Streams. When an Amazon Kinesis Data

Stream is configured as the source of a Kinesis Firehose delivery stream, Firehose's PutRecord and PutRecordBatch operations are disabled and Kinesis Agent cannot write to Kinesis Firehose Delivery Stream directly.

084

Design Secure Architectures

By default, the root volume for an AMI backed by Amazon EBS is deleted when the instance terminates. The default behavior can be changed to ensure that the volume persists after the instance terminates. To change the default behavior, set the DeleteOnTermination attribute to false using a block device mapping.

085

Design Secure Architectures

You can only enable encryption for an Amazon RDS DB instance when you create it, not after the DB instance is created. However, because you can encrypt a copy of an unencrypted DB snapshot, you can effectively add encryption to an unencrypted DB instance. That is, you can create a snapshot of your DB instance, and then create an encrypted copy of that snapshot. So this is the correct option.

086

Design High-Performing Architectures

Amazon FSx for Windows File Server provides fully managed, highly reliable file storage that is accessible over the industry-standard Service Message Block (SMB) protocol. It is built on Windows Server, delivering a wide range of administrative features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration. The Distributed File System Replication (DFSR) service is a new multi-master replication engine that is used to keep folders synchronized on multiple servers. Amazon FSx supports the use of Microsoft's Distributed File System (DFS) to organize shares into a single folder structure up to hundreds of PB in size.

087

Design Secure Architectures

you cannot convert an existing KMS single-Region key to a KMS multi-Region key.

088

Design High-Performing Architectures

EFS Max I/O performance mode is used to scale to higher levels of aggregate

throughput and operations per second. This scaling is done with a tradeoff of slightly higher latencies for file metadata operations

089

Design High-Performing Architectures

EFS General Purpose performance mode is ideal for latency-sensitive use cases, like web serving environments, content management systems, home directories, and general file serving. If you don't choose a performance mode when you create your file system, Amazon EFS selects the General Purpose mode for you by default.

090

Design Cost-Optimized Architectures

With Amazon RDS Read Replicas there are data transfer charges for replicating data across AWS Regions. You are not charged for the data transfer incurred in replicating data between your source DB instance and read replica within the same AWS Region.

091

Design High-Performing Architectures

Amazon Kinesis Data Firehose is the easiest way to reliably load streaming data into data lakes, data stores, and analytics tools. It can capture, transform, and load streaming data into Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk, enabling near real-time analytics with existing business intelligence tools and dashboards you're already using today. It is a fully managed service that automatically scales to match the throughput of your data and requires no ongoing administration.

092

Design Cost-Optimized Architectures

AWS Resource Access Manager (RAM) is a service that enables you to easily and securely share AWS resources with any AWS account or within your AWS Organization. You can share AWS Transit Gateways, Subnets, AWS License Manager configurations, and Amazon Route 53 Resolver rules resources with RAM. RAM eliminates the need to create duplicate resources in multiple accounts, reducing the operational overhead of managing those resources in every single account you own.

093

Design Resilient Architectures

Amazon EC2 Auto Scaling does not immediately terminate instances with an Impaired status. Instead, Amazon EC2 Auto Scaling waits a few minutes for the instance to

recover. Amazon EC2 Auto Scaling might also delay or not terminate instances that fail to report data for status checks. This usually happens when there is insufficient data for the status check metrics in Amazon CloudWatch.

094

Design Secure Architectures

By default, an Amazon S3 object is owned by the AWS account that uploaded it. This is true even when the bucket is owned by another account.

095

Design Cost-Optimized Architectures

Termination priority of EC2 instances in an AutoScaling group - Per the default termination policy, the first priority is given to any allocation strategy for On-Demand vs Spot instances. The next priority is to consider any instance with the oldest launch template unless there is an instance that uses a launch configuration.

Exam

096

Design Secure Architectures

Bucket policies in Amazon S3 can be used to add or deny permissions across some or all of the objects within a single bucket. Policies can be attached to users, groups, or Amazon S3 buckets, enabling centralized management of permissions. With bucket policies, you can grant users within your AWS Account or other AWS Accounts access to your Amazon S3 resources.

097

Design High-Performing Architectures

On a database instance running with Amazon RDS encryption, data stored at rest in the underlying storage is encrypted, as are its automated backups, read replicas, and snapshots.

098

Design Secure Architectures

AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.

099

Design Resilient Architectures

To migrate accounts from one organization to another, you must have root or IAM access to both the member and master accounts. Here are the steps to follow:

1. Remove the member account from the old organization
2. Send an invite to the member account from the new Organization
3. Accept the invite to the new organization from the member account

100

Design Secure Architectures

s3:ListBucket is applied to buckets, so the ARN is in the form "Resource":"arn:aws:s3:::mybucket", without a trailing / s3:GetObject is applied to objects within the bucket, so the ARN is in the form "Resource":"arn:aws:s3:::mybucket/", *with a trailing /* to indicate all objects within the bucket mybucket

101

Design Secure Architectures

IAM permission boundary can only be applied to roles or users, not IAM groups.

102

Design High-Performing Architectures

To allow for multiple consumers to read data from and SQS FIFO queue we should use the message groups FIFO feature by setting the "Group ID" attribute.

103

Design Secure Architectures

When you enable automatic key rotation for a KMS key, AWS KMS generates new cryptographic material for the KMS key every year.

104

Design Secure Architectures

Dedicated Instances are Amazon EC2 instances that run in a virtual private cloud (VPC) on hardware that's dedicated to a single customer. Dedicated Instances that belong to different AWS accounts are physically isolated at a hardware level, even if those accounts are linked to a single-payer account. However, Dedicated Instances may share hardware with other instances from the same AWS account that are not Dedicated Instances.

105

Design Resilient Architectures

Partition placement group – spreads your instances across logical partitions such that groups of instances in one partition do not share the underlying hardware with groups of instances in different partitions. This strategy is typically used by large distributed and replicated workloads, such as Hadoop, Cassandra, and Kafka.

106

Design Secure Architectures

You can share the AWS Key Management Service (AWS KMS) key that was used to encrypt the snapshot with any accounts that you want to be able to access the snapshot. You can share AWS KMS Key with another AWS account by adding the other account to the AWS KMS key policy.

107

Design Secure Architectures

A centralized Shared Services VPC hosts common services like databases, authentication servers (AD), monitoring, and proxies. All other VPCs can access it through AWS Transit Gateway, simplifying connectivity and network management.

108

Design Secure Architectures

To create a NAT gateway, you must specify the public subnet in which the NAT gateway should reside. You must also specify an Elastic IP address to associate with the NAT gateway when you create it. The Elastic IP address cannot be changed after you associate it with the NAT Gateway. After you've created a NAT gateway, you must update the route table associated with one or more of your private subnets to point internet-bound traffic to the NAT gateway. This enables instances in your private subnets to communicate with the internet.

109

Design High-Performing Architectures

Amazon ElastiCache can be used to significantly improve latency and throughput for many read-heavy application workloads (such as social networking, gaming, media sharing, leaderboard, and Q&A portals) or compute-intensive workloads (such as a recommendation engine) by allowing you to store the objects that are often read in the cache.

110

Design Resilient Architectures

An Internet Gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.

111

Design High-Performing Architectures

Provisioned IOPS SSD (io1) is backed by solid-state drives (SSDs) and is a high-performance Amazon EBS storage option designed for critical, I/O intensive database and application workloads, as well as throughput-intensive database workloads. io1 is designed to deliver a consistent baseline performance of up to 50 IOPS/GB to a maximum of 64,000 IOPS and provide up to 1,000 MB/s of throughput per volume.

112

Design Secure Architectures

When you use Amazon CloudFront with an Amazon S3 bucket as the origin, configure an origin access identity (OAI) and associate it with the Amazon CloudFront distribution. Set up the permissions in the Amazon S3 bucket policy so that only the OAI can read the objects.

113

Design Secure Architectures

Amazon CloudFront provides two ways to send authenticated requests to an Amazon S3 origin: origin access control (OAC) and origin access identity (OAI).
AWS recommends using OAC because it supports:

- All Amazon S3 buckets in all AWS Regions, including opt-in Regions launched after December 2022
- Amazon S3 server-side encryption with AWS KMS (SSE-KMS)
- Dynamic requests (PUT and DELETE) to Amazon S3

114

Design Resilient Architectures

Amazon Kinesis Data Streams enables real-time processing of streaming big data. It provides ordering of records, as well as the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications. The Amazon Kinesis Client Library (KCL) delivers all records for a given partition key to the same record processor, making

it easier to build multiple applications reading from the same Amazon Kinesis data stream (for example, to perform counting, aggregation, and filtering). Amazon Kinesis Data Streams is recommended when you need the ability to consume records in the same order a few hours later.

For example, you have a billing application and an audit application that runs a few hours behind the billing application. Because Amazon Kinesis Data Streams stores data for a maximum of 365 days, you can easily run the audit application up to 7 days behind the billing application.

KDS provides the ability to consume records in the same order a few hours later.

115

Design Cost-Optimized Architectures

A CNAME record maps DNS queries for the name of the current record, such as acme.example.com, to another domain (example.com or example.net) or subdomain (acme.example.com or zenith.example.org).

- **CNAME** records can be used to map one domain name to another. Although you should keep in mind that the DNS protocol does not allow you to create a CNAME record for the top node of a DNS namespace, also known as the zone apex. For example, if you register the DNS name example.com, the zone apex is example.com. You cannot create a CNAME record for example.com, but you can create CNAME records for www.example.com, newproduct.example.com, and so on.
- **Alias** records let you route traffic to selected AWS resources, such as Amazon CloudFront distributions and Amazon S3 buckets. They also let you route traffic from one record in a hosted zone to another record. 3rd party websites do not qualify for these as we have no control over those. 'Alias record' cannot be used to map one domain name to another.

116

Design Secure Architectures

If a user or role has an IAM permission policy that grants access to an action that is either not allowed or explicitly denied by the applicable service control policy (SCP), the user or role can't perform that action.

Service control policy (SCP) affects all users and roles in the member accounts, including root user of the member accounts.

Service control policy (SCP) does not affect service-linked role.

117

Design Cost-Optimized Architectures

You can change the tenancy of an instance from dedicated to host.
You can change the tenancy of an instance from host to dedicated.

Each Amazon EC2 instance that you launch into a VPC has a tenancy attribute.

118

Design Resilient Architectures

The nodes for your load balancer distribute requests from clients to registered targets.

- **When cross-zone load balancing is enabled**, each load balancer node distributes traffic across the registered targets in all enabled Availability Zones.
- **When cross-zone load balancing is disabled**, each load balancer node distributes traffic only across the registered targets in its Availability Zone.

119

Design Cost-Optimized Architectures

Amazon SQS provides short polling and long polling to receive messages from a queue. By default, queues use short polling. With short polling, Amazon SQS sends the response right away, even if the query found no messages. With long polling, Amazon SQS sends a response after it collects at least one available message, up to the maximum number of messages specified in the request. Amazon SQS sends an empty response only if the polling wait time expires.

120

Design High-Performing Architectures

AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. The service provides three different types of gateways – Tape Gateway, File Gateway, and Volume Gateway – that seamlessly connect on-premises applications to cloud storage, caching data locally for low-latency access.

- With **cached volumes**, the AWS Volume Gateway stores the full volume in its Amazon S3 service bucket, and just the recently accessed data is retained in the gateway's local cache for low-latency access.
- With **stored volumes**, your entire data volume is available locally in the gateway, for fast read access. Volume Gateway also maintains an asynchronous copy of your stored volume in the service's Amazon S3 bucket.

121

Design Secure Architectures

You can copy an Amazon Machine Image (AMI) across AWS Regions
You can share an Amazon Machine Image (AMI) with another AWS account
Copying an Amazon Machine Image (AMI) backed by an encrypted snapshot cannot result in an unencrypted target snapshot.

122

Design Resilient Architectures

If your instance fails a system status check, you can use Amazon CloudWatch alarm actions to automatically recover it. The recover option is available for over 90% of deployed customer Amazon EC2 instances. The Amazon CloudWatch recovery option works only for system check failures, not for instance status check failures. Also, if you terminate your instance, then it can't be recovered.

123

Design Secure Architectures

To ensure that Elastic Load Balancing stops sending requests to instances that are de-registering or unhealthy while keeping the existing connections open, use connection draining. This enables the load balancer to complete in-flight requests made to instances that are de-registering or unhealthy. The maximum timeout value can be set between 1 and 3,600 seconds (the default is 300 seconds). When the maximum time limit is reached, the load balancer forcibly closes connections to the de-registering instance.

124

Design High-Performing Architectures

When you create a Launch Template, the default value for the instance tenancy is shared and the instance tenancy is controlled by the tenancy attribute of the VPC. If you set the Launch Template Tenancy to shared (default) and the VPC Tenancy is set to dedicated, then the instances have dedicated tenancy. If you set the Launch Template Tenancy to dedicated and the VPC Tenancy is set to default, then again the instances have dedicated tenancy.

125

Design High-Performing Architectures

An Elastic Fabric Adapter (EFA) is a network device that you can attach to your Amazon

EC2 instance to accelerate High Performance Computing (HPC) and machine learning applications. It enhances the performance of inter-instance communication that is critical for scaling HPC and machine learning applications.

126

Design Resilient Architectures

Amazon DynamoDB enables you to back up your table data continuously by using point-in-time recovery (PITR). When you enable PITR, DynamoDB backs up your table data automatically with per-second granularity so that you can restore to any given second in the preceding 35 days.

PITR helps protect you against accidental writes and deletes. For example, if a test script writes accidentally to a production DynamoDB table or someone mistakenly issues a "DeleteItem" call, PITR has you covered.

127

Design High-Performing Architectures

AWS DataSync is an online data transfer service that simplifies, automates, and accelerates copying large amounts of data to and from AWS storage services over the internet or AWS Direct Connect.

AWS DataSync fully automates and accelerates moving large active datasets to AWS, up to 10 times faster than command-line tools. It is natively integrated with Amazon S3, Amazon EFS, Amazon FSx for Windows File Server, Amazon CloudWatch, and AWS CloudTrail, which provides seamless and secure access to your storage services, as well as detailed monitoring of the transfer.

128

Design High-Performing Architectures

AWS CloudFormation StackSet extends the functionality of stacks by enabling you to create, update, or delete stacks across multiple accounts and regions with a single operation.

129

Design Resilient Architectures

Amazon Simple Queue Service (Amazon SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. Amazon SQS eliminates the complexity and overhead associated

with managing and operating message-oriented middleware and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available.

130

Design Secure Architectures

To resolve DNS queries for any resources in the on-premises network from the AWS VPC, you can create an outbound endpoint on Amazon Route 53 Resolver and then Amazon Route 53 Resolver can conditionally forward queries to resolvers on the on-premises network via this endpoint.
To resolve any DNS queries for resources in the AWS VPC from the on-premises network, you can create an inbound endpoint on Amazon Route 53 Resolver and then DNS resolvers on the on-premises network can forward DNS queries to Amazon Route 53 Resolver via this endpoint.

131

Design Cost-Optimized Architectures

If your Spot Instance request is active and has an associated running Spot Instance, or your Spot Instance request is disabled and has an associated stopped Spot Instance, canceling the request does not terminate the instance; you must terminate the running Spot Instance manually.

132

Design Resilient Architectures

A recovered instance is identical to the original instance, including the instance ID, private IP addresses, Elastic IP addresses, and all instance metadata
If your instance has a public IPv4 address, it retains the public IPv4 address after recovery.

133

Design Secure Architectures

You can use a Network Address Translation gateway (NAT gateway) to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances. To create a NAT gateway, you must specify the public subnet in which the NAT gateway should reside.
You must also specify an Elastic IP address to associate with the NAT gateway when you

create it. The Elastic IP address cannot be changed after you associate it with the NAT Gateway.

134

Design High-Performing Architectures

AWS Directory Service for Microsoft Active Directory (aka AWS Managed Microsoft AD) is powered by an actual Microsoft Windows Server Active Directory (AD), managed by AWS. With AWS Managed Microsoft AD, you can run directory-aware workloads in the AWS Cloud such as SQL Server-based applications. You can also configure a trust relationship between AWS Managed Microsoft AD in the AWS Cloud and your existing on-premises Microsoft Active Directory, providing users and groups with access to resources in either domain, using single sign-on (SSO).

135

Design Resilient Architectures

Amazon Simple Queue Service (SQS) delay queues let you postpone the delivery of new messages to a queue for several seconds, for example, when your consumer application needs additional time to process messages. If you create a delay queue, any messages that you send to the queue remain invisible to consumers for the duration of the delay period. The default (minimum) delay for a queue is 0 seconds. The maximum is 15 minutes.

136

Design Resilient Architectures

Amazon Aurora Serverless is an on-demand, auto-scaling configuration for Amazon Aurora (MySQL-compatible and PostgreSQL-compatible editions), where the database will automatically start-up, shut down, and scale capacity up or down based on your application's needs. It enables you to run your database in the cloud without managing any database instances.

137

Design High-Performing Architectures

Amazon DynamoDB stream is an ordered flow of information about changes to items in Amazon DynamoDB table. When you enable a stream on a table, DynamoDB captures information about every modification to data items in the table. Whenever an application creates, updates, or deletes items in the table, DynamoDB Streams writes a stream record with the primary key attributes of the items that were modified. A stream

record contains information about a data modification to a single item in a DynamoDB table.

138

Design Resilient Architectures

Network Load Balancers expose a fixed IP to the public web, therefore allowing your application to be predictably reached using this IP, while allowing you to scale your application behind the Network Load Balancer using an ASG.

139

Design Resilient Architectures

Amazon CloudFront can route to multiple origins based on the content type.

140

Design Cost-Optimized Architectures

Amazon ElastiCache is an ideal front-end for data stores such as Amazon RDS, providing a high-performance middle tier for applications with extremely high request rates and/or low latency requirements.

141

Design High-Performing Architectures

Amazon DynamoDB has two read/write capacity modes for processing reads and writes on your tables: On-demand and Provisioned (default, free-tier eligible)
Amazon DynamoDB on-demand is a flexible billing option capable of serving thousands of requests per second without capacity planning. DynamoDB on-demand offers pay-per-request pricing for read and write requests so that you pay only for what you use.

142

Design Resilient Architectures

With Auto Scaling group, you can control when it adds instances (referred to as scaling out) or removes instances (referred to as scaling in) from your network architecture.

143

Design Secure Architectures

You can authenticate to your database instance using AWS Identity and Access Management (IAM) database authentication. IAM database authentication works with MySQL and PostgreSQL. With this authentication method, you don't need to use a

password when you connect to a database instance. Instead, you use an authentication token.

144

Design Secure Architectures

Amazon S3 Object Lock is an Amazon S3 feature that allows you to store objects using a write once, read many (WORM) model. You can use WORM protection for scenarios where it is imperative that data is not changed or deleted after it has been written.

145

Design Cost-Optimized Architectures

You can enable Amazon API caching in Amazon API Gateway to cache your endpoint's responses. With caching, you can reduce the number of calls made to your endpoint and also improve the latency of requests to your API. When you enable caching for a stage, API Gateway caches responses from your endpoint for a specified time-to-live (TTL) period, in seconds. Amazon API Gateway then responds to the request by looking up the endpoint response from the cache instead of requesting your endpoint. The default TTL value for API caching is 300 seconds. The maximum TTL value is 3600 seconds. TTL=0 means caching is disabled.

146

Design High-Performing Architectures

VPN connection is a secure connection between your on-premises equipment and your VPCs. Each VPN connection has two VPN tunnels which you can use for high availability. A VPN tunnel is an encrypted link where data can pass from the customer network to or from AWS.

147

Design High-Performing Architectures

With AWS Transit Gateway, you can simplify the connectivity between multiple VPCs and also connect to any VPC attached to AWS Transit Gateway with a single VPN connection. AWS Transit Gateway also enables you to scale the IPsec VPN throughput with equal cost multi-path (ECMP) routing support over multiple VPN tunnels. A single VPN tunnel still has a maximum throughput of 1.25 Gbps. If you establish multiple VPN tunnels to an ECMP-enabled transit gateway, it can scale beyond the default maximum limit of 1.25 Gbps. You also must enable the dynamic routing option on your transit gateway to be able to take advantage of ECMP for scalability.

148

Design Resilient Architectures

- **Backup and Restore** - In most traditional environments, data is backed up to tape and sent off-site regularly. If you use this method, it can take a long time to restore your system in the event of a disruption or disaster.
- **Pilot Light** - The term pilot light is often used to describe a DR scenario in which a minimal version of an environment is always running in the cloud.
- **Warm Standby** - The term warm standby is used to describe a DR scenario in which a scaled-down version of a fully functional environment is always running in the cloud.
- **Multi Site** - A multi-site solution runs in AWS as well as on your existing on-site infrastructure, in an active-active configuration.

149

Design Secure Architectures

You can host multiple TLS secured applications, each with its own TLS certificate, behind a single load balancer. To use SNI, all you need to do is bind multiple certificates to the same secure listener on your load balancer. ALB will automatically choose the optimal TLS certificate for each client.

150

Design High-Performing Architectures

- **Geoproximity routing** - (route based on users location) (This routing directs users based on the geographic proximity of their location to AWS resources or defined locations.) Geoproximity routing lets Amazon Route 53 route traffic to your resources based on the geographic location of your users and your resources. For example, Redirect users to the nearest data center or AWS region.
- **Geolocation routing** (choosing the content based on users location) - Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from. For example, you might want all queries from Europe to be routed to an Elastic Load Balancing (ELB) load balancer in the Frankfurt region.

151

Design Resilient Architectures

Amazon EventBridge is recommended when you want to build an application that reacts

to events from SaaS applications and/or AWS services. Amazon EventBridge is the only event-based service that integrates directly with third-party SaaS partners.

152

Design Secure Architectures

Trust policy - Trust policies define which principal entities (accounts, users, roles, and federated users) can assume the role. An IAM role is both an identity and a resource that supports resource-based policies. For this reason, you must attach both a trust policy and an identity-based policy to an IAM role. The IAM service supports only one type of resource-based policy called a role trust policy, which is attached to an IAM role.

153

Design Resilient Architectures

In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance, and help protect your databases against DB instance failure and Availability Zone disruption.

Failover is automatically handled by Amazon RDS so that you can resume database operations as quickly as possible without administrative intervention. When failing over, Amazon RDS simply flips the canonical name record (CNAME) for your DB instance to point at the standby, which is in turn promoted to become the new primary. Multi-AZ means the URL is the same, the failover is automated, and the CNAME will automatically be updated to point to the standby database.

154

Design Resilient Architectures

Only Standard Amazon SQS queue is allowed as an Amazon S3 event notification destination, whereas FIFO SQS queue is not allowed.

155

Design High-Performing Architectures

Redis has purpose-built commands for working with real-time geospatial data at scale. You can perform operations like finding the distance between two elements (for example people or places) and finding all elements within a given distance of a point.

156

Design Resilient Architectures

If the Auto Scaling group (ASG) is using EC2 as the health check type and the Application Load Balancer (ALB) is using its in-built health check, there may be a situation where the ALB health check fails because the health check pings fail to receive a response from the instance. At the same time, ASG health check can come back as successful because it is based on EC2 based health check. Therefore, in this scenario, the ALB will remove the instance from its inventory, however, the Auto Scaling Group will fail to provide the replacement instance.

157

Design Resilient Architectures

By default, cross-zone load balancing is enabled for Application Load Balancer and disabled for Network Load Balancer.

158

Design Resilient Architectures

Using Amazon Route 53 DNS Failover, you can run your primary application simultaneously in multiple AWS regions around the world and failover across regions.

159

Design Resilient Architectures

Set up Amazon Route 53 active-passive type of failover routing policy when you want a primary resource or group of resources to be available the majority of the time and you want a secondary resource or group of resources to be on standby in case all the primary resources become unavailable.

160

Design High-Performing Architectures

If your application endpoint has a failure or availability issue, AWS Global Accelerator will automatically redirect your new connections to a healthy endpoint within seconds.

161

Design Resilient Architectures

Depending on your Region, your Amazon S3 website endpoints follow one of these two formats.

s3-website dot (.) Region - *http://bucket-name.s3-website.Region.amazonaws.com*

s3-website dash (-) Region - *http://bucket-name.s3-website-Region.amazonaws.com*

162

Design Secure Architectures

Amazon S3 object metadata, which can be included with the object, is not encrypted while being stored on Amazon S3. Therefore, AWS recommends that customers not place sensitive information in Amazon S3 metadata.

163

Design Secure Architectures

An IAM user with full administrator access can perform almost all AWS tasks except a few tasks designated only for the root account user. Some of the AWS tasks that only a root account user can do are as follows: change account name or root password or root email address, change AWS support plan, close AWS account, enable AWS Multi-Factor Authentication (AWS MFA) on S3 bucket delete, create Cloudfront key pair, register for GovCloud.

164

Design Resilient Architectures

Auto Scaling group scheduled action - The scheduled action tells Amazon EC2 Auto Scaling to perform a scaling action at specified times. To create a scheduled scaling action, you specify the start time when the scaling action should take effect, and the new minimum, maximum, and desired sizes for the scaling action.

165

Design High-Performing Architectures

When a host needs to send many records per second (RPS) to Amazon Kinesis, simply calling the basic PutRecord API action in a loop is inadequate. To reduce overhead and increase throughput, the application must batch records and implement parallel HTTP requests. This will increase the efficiency overall and ensure you are optimally using the shards.

166

Design High-Performing Architectures

Amazon Simple Queue Service (Amazon SQS) temporary queues help you save development time and deployment costs when using common message patterns such as request-response. You can use the Temporary Queue Client to create high-throughput, cost-effective, application-managed temporary queues.

167

Design Resilient Architectures

Amazon RDS applies operating system updates by performing maintenance on the standby, then promoting the standby to primary and finally performing maintenance on the old primary, which becomes the new standby.

168

Design High-Performing Architectures

AWS Lambda functions time out after 15 minutes, and are not usually meant for long-running jobs.

169

Design Resilient Architectures

Amazon EBS Multi-Attach is supported exclusively on Provisioned IOPS SSD volumes (io1 or io2).

170

Design Cost-Optimized Architectures

AWS recommends using Snowmobile to migrate large datasets of 10PB or more in a single location. For datasets less than 10PB or distributed in multiple locations, you should use Snowball.

171

Design Secure Architectures

If the instance is already running, you can set DeleteOnTermination to False using the command line.

172

Design High-Performing Architectures

IOPS cannot be directly increased on a gp2 volume without increasing its size, which is not possible due to the question's constraints.
An io1 volume allows you to specify a consistent IOPS rate when you create the volume, and Amazon EBS delivers the provisioned performance 99.9 percent of the time.

173

Design Resilient Architectures

Use Amazon CloudFront signed cookies - Amazon CloudFront signed cookies allow you to control who can access your content when you don't want to change your current

URLs or when you want to provide access to multiple restricted files, for example, all of the files in the subscribers' area of a website.

174

Design Secure Architectures

Amazon FSx for NetApp ONTAP is a storage service that allows customers to launch and run fully managed ONTAP file systems in the cloud. ONTAP is NetApp's file system technology that provides a widely adopted set of data access and data management capabilities. Amongst the Amazon FSx family, FSx for ONTAP is the only file system that supports access by Windows, Mac, and Linux-based Amazon EC2 instances within the same AWS region using both SMB and NFS protocols.

175

Design Cost-Optimized Architectures

A Spot fleet is a collection, or fleet, of Spot Instances, and optionally On-Demand Instances. The Spot fleet attempts to launch the number of Spot Instances and On-Demand Instances to meet the target capacity that you specified in the Spot fleet request.

176

Design Secure Architectures

Using AWS Firewall Manager, you can centrally configure AWS WAF rules, AWS Shield Advanced protection, Amazon Virtual Private Cloud (VPC) security groups, AWS Network Firewalls, and Amazon Route 53 Resolver DNS Firewall rules across accounts and resources in your organization. It does not support Network ACLs as of today.

177

Design Resilient Architectures

If you have resources in multiple Availability Zones and they share one NAT gateway, and if the NAT gateway's Availability Zone is down, resources in the other Availability Zones lose internet access. To create a highly available or an Availability Zone independent architecture, create a NAT gateway in each Availability Zone and configure your routing to ensure that resources use the NAT gateway in the same Availability Zone.

178

Design Resilient Architectures

Amazon ElastiCache for Memcached supports multithreading.

179

Design High-Performing Architectures

Create a public Network Load Balancer that links to Amazon EC2 instances that are bastion hosts managed by an Auto Scaling Group. use a Network Load Balancer, which supports TCP traffic, and will automatically allow you to connect to the Amazon EC2 instance bastion.

180

Design High-Performing Architectures

When rebalancing, Amazon EC2 Auto Scaling launches new instances before terminating the old ones, so that rebalancing does not compromise the performance or availability of your application.

181

Design Secure Architectures

Amazon GuardDuty continuously monitors for malicious or unauthorized behavior to help protect your AWS resources, including your AWS accounts and access keys. Amazon GuardDuty identifies any unusual or unauthorized activity, like cryptocurrency mining or infrastructure deployments in a region that has never been used. Powered by threat intelligence and machine learning, GuardDuty is continuously evolving to help you protect your AWS environment.

182

Design Secure Architectures

Amazon FSx file storage is accessible from Windows, Linux, and macOS compute instances and devices running on AWS or on-premises. Thousands of compute instances and devices can access a file system concurrently. Amazon FSx for Windows File Server supports Microsoft Active Directory (AD) integration so the same user permissions and access credentials can be used to access the files on FSx Windows File Server.

183

Design Secure Architectures

You control which Amazon EC2 instances can access your Amazon EFS file system by using VPC security group rules and AWS Identity and Access Management (IAM) policies. Use VPC security groups to control the network traffic to and from your file system. Attach an IAM policy to your file system to control which clients can mount your file system and with what permissions, and you may use Amazon EFS Access Points to

manage application access. Control access to files and directories with POSIX-compliant user and group-level permissions.

184

Design Cost-Optimized Architectures

Storage class analysis only provides recommendations for Standard to Standard IA classes.

185

Design Secure Architectures

When you use server-side encryption with Amazon S3 managed keys (SSE-S3), each object is encrypted with a unique key. As an additional safeguard, it encrypts the key itself with a root key that it regularly rotates.

186

Design Cost-Optimized Architectures

Spot Instance - The request type (one-time or persistent) determines whether the request is opened again when Amazon EC2 interrupts a Spot Instance or if you stop a Spot Instance.

187

Design Resilient Architectures

In Amazon ECS, an Application Load Balancer uses dynamic port mapping, you can run multiple tasks from a single service on the same container instance.

188

Design Resilient Architectures

If an organization is using messaging with existing applications and wants to move the messaging service to the cloud quickly and easily, AWS recommends Amazon MQ for such a use case.

189

Design High-Performing Architectures

Using the Range HTTP header in a GET Object request, you can fetch a byte-range from an object, transferring only the specified portion. You can use concurrent connections to Amazon S3 to fetch different byte ranges from within the same object. This helps you achieve higher aggregate throughput versus a single whole-object request. Fetching

smaller ranges of a large object also allows your application to improve retry times when requests are interrupted.

190

Design Secure Architectures

To encrypt an object at the time of upload, you need to add a header called x-amz-server-side-encryption to the request to tell S3 to encrypt the object using SSE-C, SSE-S3, or SSE-KMS.

Top comments (5)

leob • Mar 18

Okay - after ample consideration I've decided not to pursue this career path, lol ... but thanks for this heroic write-up!

jekobokidou • Mar 18

Hope you are joking 😂

leob • Mar 19

For myself personally, yes I am - but I will immediately believe that for others this is serious!

Brian Clarke • Mar 18

Very heavy for after lunch digestion dude, but much appreciated!

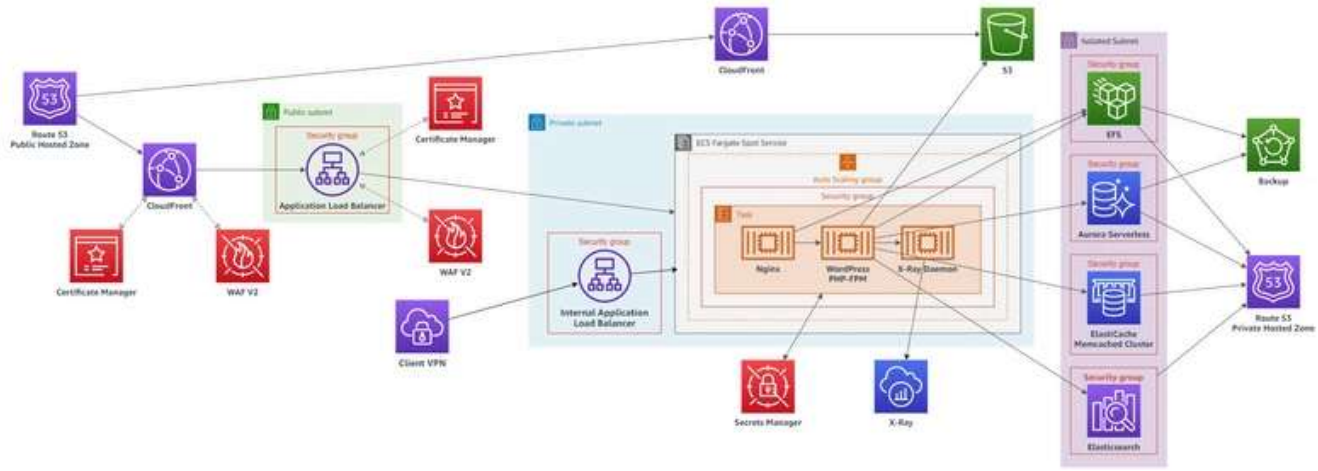
Irene Vifah • Jun 16

Thank you Jeko, in question 36, you say AWS Global Accelerator works at the network couch (Layer 3 – TCP/UDP), which is an excellent choice for applications that use UDP. but isn't it level 4 instead? Kindly clarify and correct. Overall great work

Some comments may only be visible to logged-in visitors. Sign in to view all comments.

Code of Conduct • Report abuse

AWS Community Builders



Best Practices for Running Container WordPress on AWS (ECS, EFS, RDS, ELB) using CDK

This post discusses the process of migrating a growing WordPress eShop business to AWS using AWS CDK for an easily scalable, high availability architecture. The detailed structure encompasses several pillars: Compute, Storage, Database, Cache, CDN, DNS, Security, and Backup.

Read full post

AWS Community Builders

Build On!

Would you like to become an AWS Community Builder? Learn more about the program and apply to join when applications are open next.

Learn more

More from AWS Community Builders

Solving cold start in AWS Lambda with intelligent distributed Cache

#serverless #aws #machinelearning #lambda

AWS Security: KMS Keys

#aws #security #devsecops #cloud

Use OpenAI Codex CLI with Amazon Bedrock Models - Pay As You Go

#vibecoding #genai #aws

AWS Community Builders

How I obtained all AWS associate level certificates in two weeks.

The author shares their personal journey and tips for passing all AWS associate level exams in 2 weeks, highlighting courses, hands-on experience, research, and practice exams as essential success factors.

Read full post