Question #624

A company wants to provide users with access to AWS resources. The company has 1,500 users and manages their access to on-premises resources through Active Directory user groups on the corporate network. However, the company does not want users to have to maintain another identity to access the resources. A solutions architect must manage user access to the AWS resources while preserving access to the on-premises resources.

What should the solutions architect do to meet these requirements?

A. Create an IAM user for each user in the company. Attach the appropriate policies to each user.

B. Use Amazon Cognito with an Active Directory user pool. Create roles with the appropriate policies attached.

C. Define cross-account roles with the appropriate policies attached. Map the roles to the Active Directory groups.

D. Configure Security Assertion Markup Language (SAML) 2 0-based federation. Create roles with the appropriate policies attached Map the roles to the Active Directory groups.

Correct Answer: *D*

Community vote distribution

D (71%) B (29%)

sangavi_vijay 3 days, 4 hours ago

Selected Answer: B

why its not b?

upvoted 1 times

TariqKipkemei 1 month ago

Selected Answer: D

Use Amazon Cognito via SAML integration. (SAML) is an open federation standard that allows an identity provider (for this case on-prem AD) to authenticate users and pass identity and security information about them to a service provider (for this case AWS).

I will settle for D, because this is definitely required for this to work.

upvoted 2 times

NickGordon 1 month, 3 weeks ago

Selected Answer: D

D.

An Amazon Cognito user pool is a user directory for WEB and MOBILE app authentication and authorization. So it is not a best option for corporate users.

upvoted 1 times

potomac 1 month, 3 weeks ago

Selected Answer: D

I think it is D

upvoted 1 times

ahlofan 1 month, 3 weeks ago

Selected Answer: B

Access to Aws resource -> cognito, then use iam role
SAML or AD -> identity pool

upvoted 1 times

dilaaziz 1 month, 4 weeks ago

Selected Answer: D

https://aws.amazon.com/identity/saml/

upvoted 1 times

Question #625

A company is hosting a website behind multiple Application Load Balancers. The company has different distribution rights for its content around the world. A solutions architect needs to ensure that users are served the correct content without violating distribution rights.

Which configuration should the solutions architect choose to meet these requirements?

A. Configure Amazon CloudFront with AWS WAF.

B. Configure Application Load Balancers with AWS WAF

C. Configure Amazon Route 53 with a geolocation policy

D. Configure Amazon Route 53 with a geoproximity routing policy

Correct Answer: *C*

Community vote distribution

C (78%) A (22%)

master9 4 days, 22 hours ago

Selected Answer: A

AWS CloudFront supports geographic restrictions, also known as geo-blocking, which can be used to control the distribution of your content based on the geographic location of your viewers.

You can use the CloudFront geographic restrictions feature to either grant permission to your users to access your content only if they're in one of the approved countries on your allowlist, or prevent your users from accessing your content if they're in one of the banned countries on your denylist.

For example, if a request comes from a country where you are not authorized to distribute your content, you can use CloudFront geographic restrictions to block the request.

upvoted 1 times

Murtadhaceit 2 weeks, 3 days ago

Selected Answer: C

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy-geo.html

upvoted 1 times

ekisako 3 weeks, 6 days ago

Selected Answer: A

https://repost.aws/knowledge-center/cloudfront-geo-restriction

upvoted 1 times

TariqKipkemei 1 month ago

Selected Answer: C

Use Geolocation routing policy to route traffic based on the location of the users.

upvoted 1 times

LemonGremlin 1 month, 2 weeks ago

It is C

upvoted 1 times

shihabnoori 1 month, 3 weeks ago

C. Configure Amazon Route 53 with a geolocation policy

upvoted 2 times

potomac 1 month, 3 weeks ago

Selected Answer: C

Geolocation routing policy — Use when you want to route traffic based on the location of users.

Geo-proximity routing policy — Use when you want to route traffic based on the location of your resources and optionally switch resource traffic at one location to resources elsewhere.

upvoted 4 times

dilaaziz 1 month, 4 weeks ago

Selected Answer: C

https://aws.amazon.com/about-aws/whats-new/2014/07/31/amazon-route-53-announces-domain-name-registration-geo-routing-and-lower-pricing/

upvoted 1 times

Question #626

A company stores its data on premises. The amount of data is growing beyond the company's available capacity.

The company wants to migrate its data from the on-premises location to an Amazon S3 bucket. The company needs a solution that will automatically validate the integrity of the data after the transfer.

Which solution will meet these requirements?

A. Order an AWS Snowball Edge device. Configure the Snowball Edge device to perform the online data transfer to an S3 bucket

B. Deploy an AWS DataSync agent on premises. Configure the DataSync agent to perform the online data transfer to an S3 bucket.

C. Create an Amazon S3 File Gateway on premises Configure the S3 File Gateway to perform the online data transfer to an S3 bucket

D. Configure an accelerator in Amazon S3 Transfer Acceleration on premises. Configure the accelerator to perform the online data transfer to an S3 bucket.

Correct Answer: *B*

Community vote distribution

B (100%)

TariqKipkemei 1 month ago

Selected Answer: B

During a transfer, AWS DataSync always checks the integrity of your data.

https://docs.aws.amazon.com/datasync/latest/userguide/configure-data-verification-options.html

upvoted 2 times

potomac 1 month, 3 weeks ago

Selected Answer: B

During a transfer, AWS DataSync always checks the integrity of your data, but you can specify how and when this verification happens with the following options: Verify only the data transferred (recommended) – DataSync calculates the checksum of transferred files and metadata at the source location.

https://docs.aws.amazon.com/datasync/latest/userguide/configure-data-verification-options.html

upvoted 3 times

dilaaziz 1 month, 4 weeks ago

Selected Answer: B

https://aws.amazon.com/datasync/faqs/

upvoted 1 times

Question #627

A company wants to migrate two DNS servers to AWS. The servers host a total of approximately 200 zones and receive 1 million requests each day on average. The company wants to maximize availability while minimizing the operational overhead that is related to the management of the two servers.

What should a solutions architect recommend to meet these requirements?

A. Create 200 new hosted zones in the Amazon Route 53 console Import zone files.

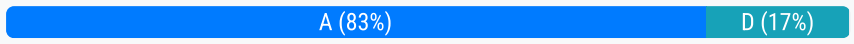
B. Launch a single large Amazon EC2 instance Import zone tiles. Configure Amazon CloudWatch alarms and notifications to alert the company about any downtime.

C. Migrate the servers to AWS by using AWS Server Migration Service (AWS SMS). Configure Amazon CloudWatch alarms and notifications to alert the company about any downtime.

D. Launch an Amazon EC2 instance in an Auto Scaling group across two Availability Zones. Import zone files. Set the desired capacity to 1 and the maximum capacity to 3 for the Auto Scaling group. Configure scaling alarms to scale based on CPU utilization.

Correct Answer: *A*

Community vote distribution



TariqKipkemei 1 month ago

Selected Answer: A

'maximize availability while minimizing the operational overhead' = severless = Amazon Route 53

upvoted 1 times

EdenWang 1 month, 2 weeks ago

Selected Answer: A

Only A makes sense

upvoted 2 times

NickGordon 1 month, 3 weeks ago

Selected Answer: A

Should be A

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/migrate-dns-domain-in-use.html

upvoted 2 times

potomac 1 month, 3 weeks ago

Selected Answer: D

D makes more sense to me

upvoted 1 times

Question #628

A global company runs its applications in multiple AWS accounts in AWS Organizations. The company's applications use multipart uploads to upload data to multiple Amazon S3 buckets across AWS Regions. The company wants to report on incomplete multipart uploads for cost compliance purposes.

Which solution will meet these requirements with the LEAST operational overhead?

A. Configure AWS Config with a rule to report the incomplete multipart upload object count.

B. Create a service control policy (SCP) to report the incomplete multipart upload object count.

C. Configure S3 Storage Lens to report the incomplete multipart upload object count.

D. Create an S3 Multi-Region Access Point to report the incomplete multipart upload object count.

Correct Answer: *C*

Community vote distribution

C (100%)

LocNV 5 days, 19 hours ago

Selected Answer: C

S3 Storage Lens provides four Cost Efficiency metrics for analyzing incomplete multipart uploads in your S3 buckets. These metrics are free of charge and automatically configured for all S3 Storage Lens dashboards.

Incomplete Multipart Upload Storage Bytes – The total bytes in scope with incomplete multipart uploads
% Incomplete MPU Bytes – The percentage of bytes in scope that are results of incomplete multipart uploads
Incomplete Multipart Upload Object Count – The number of objects in scope that are incomplete multipart uploads
% Incomplete MPU Objects – The percentage of objects in scope that are incomplete multipart uploads
https://aws.amazon.com/blogs/aws-cloud-financial-management/discovering-and-deleting-incomplete-multipart-uploads-to-lower-amazon-s3-costs/

upvoted 1 times

TariqKipkemei 1 month ago

Selected Answer: C

Amazon S3 Storage Lens is a cloud storage analytics solution with support for AWS Organizations to give you organization-wide visibility into object storage, with point-in-time metrics and trend lines as well as actionable recommendations.

upvoted 2 times

potomac 1 month, 3 weeks ago

Selected Answer: C

C for sure

upvoted 1 times

warp 1 month, 3 weeks ago

Selected Answer: C

S3 storage lenses can be used to find incomplete multipart uploads: https://aws.amazon.com/blogs/aws-cloud-financial-management/discovering-and-deleting-incomplete-multipart-uploads-to-lower-amazon-s3-costs/

upvoted 4 times

Question #629

A company runs a production database on Amazon RDS for MySQL. The company wants to upgrade the database version for security compliance reasons. Because the database contains critical data, the company wants a quick solution to upgrade and test functionality without losing any data.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create an RDS manual snapshot. Upgrade to the new version of Amazon RDS for MySQL.

B. Use native backup and restore. Restore the data to the upgraded new version of Amazon RDS for MySQL.

C. Use AWS Database Migration Service (AWS DMS) to replicate the data to the upgraded new version of Amazon RDS for MySQL.

D. Use Amazon RDS Blue/Green Deployments to deploy and test production changes.

Correct Answer: *D*

Community vote distribution

D (100%)

TariqKipkemei 1 month ago

Selected Answer: D

A blue/green deployment copies a production database environment to a separate, synchronized staging environment. You can make changes to the database in the staging environment without affecting the production environment. When you are ready, you can promote the staging environment to be the new production database environment, with downtime typically under one minute.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/blue-green-deployments.html

upvoted 1 times

potomac 1 month, 3 weeks ago

Selected Answer: D

D is the answer

upvoted 1 times

warp 1 month, 3 weeks ago

Selected Answer: D

You can make changes to the RDS DB instances in the green environment without affecting production workloads. For example, you can upgrade the major or minor DB engine version, upgrade the underlying file system configuration, or change database parameters in the staging environment. You can thoroughly test changes in the green environment.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/blue-green-deployments-overview.html

upvoted 3 times

Question #630

A solutions architect is creating a data processing job that runs once daily and can take up to 2 hours to complete. If the job is interrupted, it has to restart from the beginning.

How should the solutions architect address this issue in the MOST cost-effective manner?

A. Create a script that runs locally on an Amazon EC2 Reserved Instance that is triggered by a cron job.

B. Create an AWS Lambda function triggered by an Amazon EventBridge scheduled event.

C. Use an Amazon Elastic Container Service (Amazon ECS) Fargate task triggered by an Amazon EventBridge scheduled event.

D. Use an Amazon Elastic Container Service (Amazon ECS) task running on Amazon EC2 triggered by an Amazon EventBridge scheduled event.

Correct Answer: *C*

Community vote distribution

C (75%) B (25%)

TariqKipkemei 1 month ago

Selected Answer: C

AWS Fargate will bill you based on the amount of vCPU, RAM, OS, CPU architecture, and storage that your containerized apps consume while running on EKS or ECS.

upvoted 1 times

cevin93 1 month ago

Selected Answer: C

should be C

upvoted 1 times

Alex1atd 1 month, 1 week ago

Selected Answer: C

Lambda function have a limit timeout about 15 minutes, so cannot be B.
Answer is C

upvoted 1 times

hungta 1 month, 2 weeks ago

Selected Answer: C

Lamda function have a limit timeout about 15 minutes

upvoted 1 times

cciesam 1 month, 3 weeks ago

Selected Answer: B

I think it should be B. Considering the Cost.

upvoted 2 times

Murtadhaceit 2 weeks, 3 days ago

Lambda times out after 15 minutes. This job requires a 2-hour time without interruption block. So, definitely not B.

upvoted 2 times

zhdetn 1 month, 2 weeks ago

Lambda Maximum execution time: 900 seconds (15 minutes)

upvoted 5 times

potomac 1 month, 3 weeks ago

Selected Answer: C

I guess it is C

upvoted 2 times

Question #631

A social media company wants to store its database of user profiles, relationships, and interactions in the AWS Cloud. The company needs an application to monitor any changes in the database. The application needs to analyze the relationships between the data entities and to provide recommendations to users.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use Amazon Neptune to store the information. Use Amazon Kinesis Data Streams to process changes in the database.

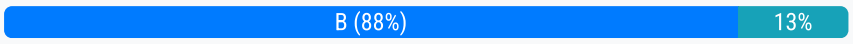
B. Use Amazon Neptune to store the information. Use Neptune Streams to process changes in the database.

C. Use Amazon Quantum Ledger Database (Amazon QLDB) to store the information. Use Amazon Kinesis Data Streams to process changes in the database.

D. Use Amazon Quantum Ledger Database (Amazon QLDB) to store the information. Use Neptune Streams to process changes in the database.

Correct Answer: *B*

Community vote distribution



TariqKipkemei 1 month ago

Selected Answer: B

Amazon Neptune Database is a serverless graph database designed for superior scalability and availability. Neptune Database provides built-in security, continuous backups, and integrations with other AWS services. Suitable for social media. With the Neptune Streams feature, you can generate a complete sequence of change-log entries that record every change made to your graph data as it happens.

upvoted 2 times

NickGordon 1 month, 3 weeks ago

Selected Answer: B

B

Social network -> Graph Structure -> Neptune

upvoted 1 times

ekisako 1 month, 3 weeks ago

Selected Answer: B

Keyword: analyze the relationships
With Amazon Neptune, you can create sophisticated, interactive graph applications that can query billions of relationships in milliseconds.

https://aws.amazon.com/neptune/features/

upvoted 2 times

potomac 1 month, 3 weeks ago

Selected Answer: C

Amazon Neptune is primarily used for managing highly connected graph data, making it well-suited for graph-based applications.

In contrast, Amazon QLDB is designed for applications that require an immutable and auditable transaction history to ensure data integrity.

upvoted 1 times

warp 1 month, 3 weeks ago

Selected Answer: B

Neptune is a graph type database and Neptune streams provides view on changes into the database:
https://docs.aws.amazon.com/neptune/latest/userguide/streams.html

upvoted 2 times

AF_1221 2 months ago

C is the correct answer
provides a well-suited, managed, and scalable solution for storing and monitoring the database with the least operational overhead, meeting the requirements of the social media company.

upvoted 2 times

Question #632

A company is creating a new application that will store a large amount of data. The data will be analyzed hourly and will be modified by several Amazon EC2 Linux instances that are deployed across multiple Availability Zones. The needed amount of storage space will continue to grow for the next 6 months.

Which storage solution should a solutions architect recommend to meet these requirements?

A. Store the data in Amazon S3 Glacier. Update the S3 Glacier vault policy to allow access to the application instances.

B. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on the application instances.

C. Store the data in an Amazon Elastic File System (Amazon EFS) file system. Mount the file system on the application instances.

D. Store the data in an Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS volume shared between the application instances.

Correct Answer: *C*

Community vote distribution

C (100%)

TariqKipkemei 1 month ago

Selected Answer: C

Multiple Linux instances = Amazon Elastic File System (Amazon EFS) with multiple mount targets.

upvoted 2 times

potomac 1 month, 3 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

AF_1221 2 months ago

C is correct
Shared File System: Amazon EFS allows multiple Amazon EC2 instances to mount the same file system simultaneously, making it easy for multiple instances to access and modify the data concurrently.

upvoted 3 times

Question #633

A company manages an application that stores data on an Amazon RDS for PostgreSQL Multi-AZ DB instance. Increases in traffic are causing performance problems. The company determines that database queries are the primary reason for the slow performance.

What should a solutions architect do to improve the application's performance?

A. Serve read traffic from the Multi-AZ standby replica.

B. Configure the DB instance to use Transfer Acceleration.

C. Create a read replica from the source DB instance. Serve read traffic from the read replica.

D. Use Amazon Kinesis Data Firehose between the application and Amazon RDS to increase the concurrency of database requests.

Correct Answer: *C*

Community vote distribution

C (100%)

TariqKipkemei 1 month ago

Selected Answer: C

A Multi-AZ DB instance Creates a primary DB instance with one standby DB instance in a different Availability Zone. Using a Multi-AZ DB instance provides high availability, but the standby DB instance doesn't support connections for read workloads.
Therefore you will need to create a read replica from the source DB instance then serve read traffic from the read replica.

upvoted 2 times

potomac 1 month, 3 weeks ago

Selected Answer: C

you can’t read from the standby DB instance. If applications require more read capacity, you should create or add additional read replicas.

upvoted 1 times

warp 1 month, 3 weeks ago

Selected Answer: C

After you create a read replica from a source DB instance, the source becomes the primary DB instance. When you make updates to the primary DB instance, Amazon RDS copies them asynchronously to the read replica.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

upvoted 1 times

Question #634

A company collects 10 GB of telemetry data daily from various machines. The company stores the data in an Amazon S3 bucket in a source data account.

The company has hired several consulting agencies to use this data for analysis. Each agency needs read access to the data for its analysts. The company must share the data from the source data account by choosing a solution that maximizes security and operational efficiency.

Which solution will meet these requirements?

A. Configure S3 global tables to replicate data for each agency.

B. Make the S3 bucket public for a limited time. Inform only the agencies.

C. Configure cross-account access for the S3 bucket to the accounts that the agencies own.

D. Set up an IAM user for each analyst in the source data account. Grant each user access to the S3 bucket.

Correct Answer: *C*

Community vote distribution

TariqKipkemei 1 month ago

Selected Answer: C

With cross-account bucket permissions Account A—can grant another AWS account, Account B, permission to access its resources such as buckets and objects. Account B can then delegate those permissions to users in its account.

https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-walkthroughs-managing-access-example2.html#:~:text=4%3A%20Clean%20up-,An%20AWS%20account,-%E2%80%94for%20example%2C%20Account

upvoted 2 times

NickGordon 1 month, 3 weeks ago

Selected Answer: C

C is the best answer

upvoted 1 times

cciesam 1 month, 3 weeks ago

Selected Answer: D

C may not correct as it's doesn't say if the analyst are using AWS services

upvoted 1 times

NickGordon 1 month, 3 weeks ago

in that case, an analyst user group should be created and the access should be assigned to the group. So C is better

upvoted 1 times

potomac 1 month, 3 weeks ago

Selected Answer: C

I think it is C

upvoted 1 times

Question #635

A company uses Amazon FSx for NetApp ONTAP in its primary AWS Region for CIFS and NFS file shares. Applications that run on Amazon EC2 instances access the file shares. The company needs a storage disaster recovery (DR) solution in a secondary Region. The data that is replicated in the secondary Region needs to be accessed by using the same protocols as the primary Region.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create an AWS Lambda function to copy the data to an Amazon S3 bucket. Replicate the S3 bucket to the secondary Region.

B. Create a backup of the FSx for ONTAP volumes by using AWS Backup. Copy the volumes to the secondary Region. Create a new FSx for ONTAP instance from the backup.

C. Create an FSx for ONTAP instance in the secondary Region. Use NetApp SnapMirror to replicate data from the primary Region to the secondary Region.

D. Create an Amazon Elastic File System (Amazon EFS) volume. Migrate the current data to the volume. Replicate the volume to the secondary Region.

Correct Answer: *C*

Community vote distribution

C (100%)

SHAAHIBHUSHANAWS 3 weeks, 6 days ago

C
https://aws.amazon.com/blogs/storage/cross-region-disaster-recovery-with-amazon-fsx-for-netapp-ontap/

upvoted 1 times

TariqKipkemei 1 month ago

Selected Answer: C

Amazon FSx for NetApp ONTAP supports NetApp SnapMirror, a replication technology that you can use to replicate data between two ONTAP file systems. You can configure automatic NetApp SnapMirror replication of your data to another Amazon FSx for NetApp ONTAP file system, including a file system in another AWS Region. If needed, you can fail over your applications and users to use the other Amazon FSx for NetApp ONTAP file system. With SnapMirror, you can configure replication with a Recovery Point Objective (RPO) of as low as 5 minutes, and a Recovery Time Objective (RTO) in single-digit minutes. You can configure SnapMirror using the ONTAP CLI or REST API.

upvoted 1 times

Oblako 1 month, 1 week ago

Selected Answer: C

SnapMirror enables you to configure replication with an RPO of as low as five minutes, and an RTO in single digit minutes. It is the recommended solution for DR when using FSx for ONTAP: https://aws.amazon.com/blogs/storage/cross-region-disaster-recovery-with-amazon-fsx-for-netapp-ontap/

upvoted 1 times

potomac 1 month, 3 weeks ago

Selected Answer: C

You can use NetApp SnapMirror to schedule periodic replication of your FSx for ONTAP file system to or from a second file system. This capability is available for both in-Region and cross-Region deployments.

https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/scheduled-replication.html

upvoted 2 times

Question #636

A development team is creating an event-based application that uses AWS Lambda functions. Events will be generated when files are added to an Amazon S3 bucket. The development team currently has Amazon Simple Notification Service (Amazon SNS) configured as the event target from Amazon S3.

What should a solutions architect do to process the events from Amazon S3 in a scalable way?

A. Create an SNS subscription that processes the event in Amazon Elastic Container Service (Amazon ECS) before the event runs in Lambda.

B. Create an SNS subscription that processes the event in Amazon Elastic Kubernetes Service (Amazon EKS) before the event runs in Lambda

C. Create an SNS subscription that sends the event to Amazon Simple Queue Service (Amazon SQS). Configure the SOS queue to trigger a Lambda function.

D. Create an SNS subscription that sends the event to AWS Server Migration Service (AWS SMS). Configure the Lambda function to poll from the SMS event.

Correct Answer: *C*

Community vote distribution

C (100%)

TariqKipkemei 4 weeks ago

Selected Answer: C

scalable service = serverless = Amazon SQS implemented with FAN-OUT.
However SQS is a pull based event distribution service, it does not trigger other services.
C is the closest option.

upvoted 2 times

potomac 1 month, 3 weeks ago

Selected Answer: C

Amazon SQS is designed for event-driven and scalable message processing. It can handle large volumes of messages and automatically scales based on the incoming workload. This allows for better load distribution and scaling as compared to direct Lambda invocation.

upvoted 4 times

Question #637

A solutions architect is designing a new service behind Amazon API Gateway. The request patterns for the service will be unpredictable and can change suddenly from 0 requests to over 500 per second. The total size of the data that needs to be persisted in a backend database is currently less than 1 GB with unpredictable future growth. Data can be queried using simple key-value requests.

Which combination ofAWS services would meet these requirements? (Choose two.)

A. AWS Fargate

B. AWS Lambda

C. Amazon DynamoDB

D. Amazon EC2 Auto Scaling

E. MySQL-compatible Amazon Aurora

Correct Answer: *BC*

Community vote distribution

BC (100%)

potomac Highly Voted 1 month, 3 weeks ago

Selected Answer: BC

B and C

upvoted 8 times

TariqKipkemei Highly Voted 4 weeks ago

Selected Answer: BC

Scalable, unpredictable request patterns = AWS Lambda
Scalable, key-value data = Amazon DynamoDB

upvoted 6 times

Ashhher Most Recent 4 days, 5 hours ago

Selected Answer: BC

why not Fargate?

upvoted 1 times

Question #638

A company collects and shares research data with the company's employees all over the world. The company wants to collect and store the data in an Amazon S3 bucket and process the data in the AWS Cloud. The company will share the data with the company's employees. The company needs a secure solution in the AWS Cloud that minimizes operational overhead.

Which solution will meet these requirements?

A. Use an AWS Lambda function to create an S3 presigned URL. Instruct employees to use the URL.

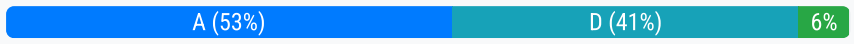
B. Create an IAM user for each employee. Create an IAM policy for each employee to allow S3 access. Instruct employees to use the AWS Management Console.

C. Create an S3 File Gateway. Create a share for uploading and a share for downloading. Allow employees to mount shares on their local computers to use S3 File Gateway.

D. Configure AWS Transfer Family SFTP endpoints. Select the custom identity provider options. Use AWS Secrets Manager to manage the user credentials Instruct employees to use Transfer Family.

Correct Answer: *A*

Community vote distribution



t0nx Highly Voted 1 month, 1 week ago

Selected Answer: D

AWS Transfer Family (Option D)

By configuring AWS Transfer Family SFTP endpoints, you can provide a secure and convenient way for employees to access and transfer data to and from the S3 bucket.
Using custom identity provider options allows you to integrate with existing identity systems, and AWS Secrets Manager can be used to manage user credentials securely.

A suggests using an AWS Lambda function to create an S3 presigned URL. While this can work, it involves manual generation of URLs and sharing them, which may not be as scalable or user-friendly.

B suggests creating an IAM user for each employee with IAM policies for S3 access. This involves more operational overhead, as managing IAM users for each employee can be cumbersome and less scalable.

C suggests using an S3 File Gateway. While this can work, it introduces additional components and may not be as straightforward or as efficient as using AWS Transfer Family for SFTP access.

upvoted 7 times

ale_brd_ Most Recent 3 days, 22 hours ago

Selected Answer: A

i would go with A, storing secret for each employ does not seem to me as minimizing operational overhead...

upvoted 1 times

Cyberkayu 1 week, 4 days ago

Selected Answer: A

questions earlier can generate (lambda) presigned URL/cookies to customers who pay the subscription, or decouple image uploading from social media users. i dont see why Lambda+S3 presigned URL dont work with employees around the world here.

Answer A.

upvoted 1 times

evelynsun 2 weeks, 1 day ago

it's A!
This is the most efficient and secure way to share data with employees. It eliminates the need for employees to create their own AWS accounts or manage their own access credentials. It also provides a centralized way to manage the data, so the company can ensure that the data is always up-to-date and secure.

upvoted 2 times

SHAAHIBHUSHANAWS 3 weeks, 6 days ago

D
Transfer family give secure SFTP way to transfer data.
A is wrong as it needs someone to create presigned urls for both upload and download. Not a workable solution.

upvoted 2 times

Selected Answer: A

a secure solution that minimizes operational overhead = AWS Lambda + S3 presigned URL

upvoted 2 times

AwsZora 1 month, 1 week ago

Selected Answer: A

A is simple

upvoted 1 times

Oblako 1 month, 1 week ago

Selected Answer: B

C and D are incorrect as the data will be processed in AWS, no need to download, transfer.

A, I believe is also incorrect. As it it not operationally efficient to use use a lambda function to generate Presigned URLs when using the data within AWS. Let's say an employee of that company wants to process millions of those files in SageMaker for a study. This would mean they`d have to invoke this lambda function millions of times to generate pre-signed URLs for all of these files. Not really efficient.

Nothing is really wrong with answer B. As it is the employees will process the data in the AWS Cloud, they need an IAM user anyway. It seems a bit odd that the answer states: "Create an IAM policy for each employee to allow S3 access". As this should be done using a group. But Still I am going with B.

upvoted 1 times

potomac 1 month, 3 weeks ago

Selected Answer: A

D is not for minimizing operational overhead

upvoted 4 times

Question #639

A company is building a new furniture inventory application. The company has deployed the application on a fleet ofAmazon EC2 instances across multiple Availability Zones. The EC2 instances run behind an Application Load Balancer (ALB) in their VPC.

A solutions architect has observed that incoming traffic seems to favor one EC2 instance, resulting in latency for some requests.

What should the solutions architect do to resolve this issue?

A. Disable session affinity (sticky sessions) on the ALB

B. Replace the ALB with a Network Load Balancer

C. Increase the number of EC2 instances in each Availability Zone

D. Adjust the frequency of the health checks on the ALB's target group

Correct Answer: *A*

Community vote distribution

A (100%)

MikeSWA 4 days, 15 hours ago

what about c?
it actually helps distribute traffic equally across instances in all enabled AZs.

upvoted 1 times

evelynsun 2 weeks, 1 day ago

it's A!!
Session affinity is a feature of the Application Load Balancer that keeps client requests on the same EC2 instance for the duration of the session. This can cause latency issues if one EC2 instance is overloaded while others are not, as the overloaded instance will handle all subsequent requests until it is taken offline.

To resolve this issue, the solutions architect should disable session affinity on the ALB. This can be done by setting the "Session affinity" parameter to "Off" in the ALB's configuration.

Disabling session affinity will cause the ALB to distribute requests across all EC2 instances in the target group, rather than keeping them on a single instance. This will help to balance the load and reduce latency for all requests.

upvoted 1 times

TariqKipkemei 4 weeks ago

Selected Answer: A

Disable session affinity (sticky sessions) on the ALB

upvoted 1 times

NickGordon 1 month, 3 weeks ago

Selected Answer: A

A

https://repost.aws/knowledge-center/elb-fix-unequal-traffic-routing

upvoted 1 times

potomac 1 month, 3 weeks ago

Selected Answer: A

A makes more sense than others

upvoted 2 times

Question #640

A company has an application workflow that uses an AWS Lambda function to download and decrypt files from Amazon S3. These files are encrypted using AWS Key Management Service (AWS KMS) keys. A solutions architect needs to design a solution that will ensure the required permissions are set correctly.

Which combination of actions accomplish this? (Choose two.)

A. Attach the kms:decrypt permission to the Lambda function's resource policy

B. Grant the decrypt permission for the Lambda IAM role in the KMS key's policy

C. Grant the decrypt permission for the Lambda resource policy in the KMS key's policy.

D. Create a new IAM policy with the kms:decrypt permission and attach the policy to the Lambda function.

E. Create a new IAM role with the kms:decrypt permission and attach the execution role to the Lambda function.

Correct Answer: *BE*

Community vote distribution

BE (75%) 13% 13%

NickGordon Highly Voted 1 month, 3 weeks ago

Selected Answer: BE

BE is right.

The key policy has to be modified to give lambda execution role access. You can't set another resource policy as principle. So C is not right

upvoted 5 times

TariqKipkemei Most Recent 4 weeks ago

Selected Answer: BE

Create a new IAM role with the kms:decrypt permission and attach the execution role to the Lambda function then grant the decrypt permission for the Lambda IAM role in the KMS key's policy

upvoted 1 times

louisaok 1 month, 3 weeks ago

Selected Answer: CE

CE is right

upvoted 1 times

potomac 1 month, 3 weeks ago

Selected Answer: DE

DE?
Create an IAM role for the Lambda function that also grants decryption permission to the S3 bucket.
Configure the IAM role as the Lambda functions execution role.

To use an IAM policy to control access to a KMS key, the key policy for the KMS key must give the account permission to use IAM policies.

https://repost.aws/knowledge-center/lambda-execution-role-s3-bucket
https://docs.aws.amazon.com/kms/latest/developerguide/iam-policies.html

upvoted 1 times

potomac 1 month, 3 weeks ago

change to CE
C. Grant the decrypt permission for the Lambda resource policy in the KMS key's policy.
E. Create a new IAM role with the kms:decrypt permission and attach the execution role to the Lambda function.

https://docs.aws.amazon.com/lambda/latest/dg/access-control-resource-based.html
https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html

upvoted 2 times

Question #641

A company wants to monitor its AWS costs for financial review. The cloud operations team is designing an architecture in the AWS Organizations management account to query AWS Cost and Usage Reports for all member accounts. The team must run this query once a month and provide a detailed analysis of the bill.

Which solution is the MOST scalable and cost-effective way to meet these requirements?

A. Enable Cost and Usage Reports in the management account. Deliver reports to Amazon Kinesis. Use Amazon EMR for analysis.

B. Enable Cost and Usage Reports in the management account. Deliver the reports to Amazon S3 Use Amazon Athena for analysis.

C. Enable Cost and Usage Reports for member accounts. Deliver the reports to Amazon S3 Use Amazon Redshift for analysis.

D. Enable Cost and Usage Reports for member accounts. Deliver the reports to Amazon Kinesis. Use Amazon QuickSight tor analysis.

Correct Answer: *B*

Community vote distribution

B (100%)

TariqKipkemei 4 weeks ago

Selected Answer: B

Scalable and cost-effective way = Enable Cost and Usage Reports in the management account. Deliver the reports to Amazon S3 Use Amazon Athena for analysis

upvoted 1 times

NickGordon 1 month, 3 weeks ago

Selected Answer: B

B

https://aws.amazon.com/blogs/big-data/analyze-amazon-s3-storage-costs-using-aws-cost-and-usage-reports-amazon-s3-inventory-and-amazon-athena/

upvoted 2 times

potomac 1 month, 3 weeks ago

Selected Answer: B

B
once a month

upvoted 2 times

Question #642

A company wants to run a gaming application on Amazon EC2 instances that are part of an Auto Scaling group in the AWS Cloud. The application will transmit data by using UDP packets. The company wants to ensure that the application can scale out and in as traffic increases and decreases.

What should a solutions architect do to meet these requirements?

A. Attach a Network Load Balancer to the Auto Scaling group.

B. Attach an Application Load Balancer to the Auto Scaling group.

C. Deploy an Amazon Route 53 record set with a weighted policy to route traffic appropriately.

D. Deploy a NAT instance that is configured with port forwarding to the EC2 instances in the Auto Scaling group.

Correct Answer: *A*

Community vote distribution

A (100%)

Sugarbear_01 Highly Voted 1 month, 4 weeks ago

Selected Answer: A

https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html

upvoted 7 times

TariqKipkemei Most Recent 4 weeks ago

Selected Answer: A

UDP packets = Network Load Balancer

upvoted 1 times

Question #643

A company runs several websites on AWS for its different brands. Each website generates tens of gigabytes of web traffic logs each day. A solutions architect needs to design a scalable solution to give the company's developers the ability to analyze traffic patterns across all the company's websites. This analysis by the developers will occur on demand once a week over the course of several months. The solution must support queries with standard SQL.

Which solution will meet these requirements MOST cost-effectively?

A. Store the logs in Amazon S3. Use Amazon Athena tor analysis.

B. Store the logs in Amazon RDS. Use a database client for analysis.

C. Store the logs in Amazon OpenSearch Service. Use OpenSearch Service for analysis.

D. Store the logs in an Amazon EMR cluster Use a supported open-source framework for SQL-based analysis.

Correct Answer: *A*

Community vote distribution

pavan2302 1 week, 3 days ago

Selected Answer: C

https://docs.aws.amazon.com/opensearch-service/latest/developerguide/cold-storage.html

upvoted 1 times

TariqKipkemei 4 weeks ago

Selected Answer: A

solution must support queries with standard SQL = Amazon S3 with Athena

upvoted 2 times

NickGordon 1 month, 3 weeks ago

Selected Answer: A

A, most cost effective

upvoted 1 times

potomac 1 month, 3 weeks ago

Selected Answer: A

option D (using Amazon EMR with an open-source framework) may be overkill for the relatively simple SQL-based analysis.

upvoted 1 times

Question #644

An international company has a subdomain for each country that the company operates in. The subdomains are formatted as example.com, country1.example.com, and country2.example.com. The company's workloads are behind an Application Load Balancer. The company wants to encrypt the website data that is in transit.

Which combination of steps will meet these requirements? (Choose two.)

A. Use the AWS Certificate Manager (ACM) console to request a public certificate for the apex top domain example com and a wildcard certificate for *.example.com.

B. Use the AWS Certificate Manager (ACM) console to request a private certificate for the apex top domain example.com and a wildcard certificate for *.example.com.

C. Use the AWS Certificate Manager (ACM) console to request a public and private certificate for the apex top domain example.com.

D. Validate domain ownership by email address. Switch to DNS validation by adding the required DNS records to the DNS provider.

E. Validate domain ownership for the domain by adding the required DNS records to the DNS provider.

Correct Answer: *AE*

Community vote distribution

AE (100%)

TariqKipkemei 4 weeks ago

Selected Answer: AE

Validate domain ownership for the domain by adding the required DNS records to the DNS provider then use the AWS Certificate Manager (ACM) console to request a public certificate for the apex top domain example com and a wildcard certificate for *.example.com

upvoted 2 times

cciesam 1 month, 3 weeks ago

Selected Answer: AE

AE correct

upvoted 1 times

potomac 1 month, 3 weeks ago

Selected Answer: AE

BCD are wrong

upvoted 2 times

t0nx 1 month, 1 week ago

Why E and not D ?

upvoted 1 times

Cyberkayu 1 week, 4 days ago

need to put A-record and CNAME in public DNS record to proof you are the legal owner of the domain name.

upvoted 1 times

Question #645

A company is required to use cryptographic keys in its on-premises key manager. The key manager is outside of the AWS Cloud because of regulatory and compliance requirements. The company wants to manage encryption and decryption by using cryptographic keys that are retained outside of the AWS Cloud and that support a variety of external key managers from different vendors.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use AWS CloudHSM key store backed by a CloudHSM cluster.

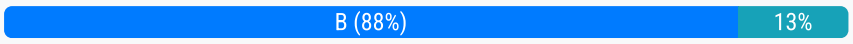
B. Use an AWS Key Management Service (AWS KMS) external key store backed by an external key manager.

C. Use the default AWS Key Management Service (AWS KMS) managed key store.

D. Use a custom key store backed by an AWS CloudHSM cluster.

Correct Answer: *B*

Community vote distribution



evelynsun 2 weeks, 1 day ago

Selected Answer: A

it's A.
This solution is the LEAST operational overhead because it does not require the company to manage any infrastructure or software outside of the AWS Cloud. The AWS CloudHSM key store is managed by AWS, and the company can use it to store and manage its cryptographic keys without having to worry about the underlying infrastructure or software. The CloudHSM cluster is managed by AWS, and the company can use it to create and manage its cryptographic keys without having to worry about the hardware or software.

the AWS CloudHSM key store can also be used for external key managers. The AWS CloudHSM key store is a managed key store that is backed by an AWS CloudHSM cluster. The AWS CloudHSM cluster is a managed service that is provided by AWS.

upvoted 1 times

evelynsun 2 weeks, 1 day ago

it's A.
This solution is the LEAST operational overhead because it does not require the company to manage any infrastructure or software outside of the AWS Cloud. The AWS CloudHSM key store is managed by AWS, and the company can use it to store and manage its cryptographic keys without having to worry about the underlying infrastructure or software. The CloudHSM cluster is managed by AWS, and the company can use it to create and manage its cryptographic keys without having to worry about the hardware or software.

the AWS CloudHSM key store can also be used for external key managers. The AWS CloudHSM key store is a managed key store that is backed by an AWS CloudHSM cluster. The AWS CloudHSM cluster is a managed service that is provided by AWS.

upvoted 1 times

SHAAHIBHUSHANAWS 3 weeks, 6 days ago

B
https://docs.aws.amazon.com/kms/latest/developerguide/keystore-external.html

upvoted 1 times

TariqKipkemei 4 weeks ago

Selected Answer: B

https://docs.aws.amazon.com/kms/latest/developerguide/keystore-external.html#:~:text=Document%20history-,External%20key%20stores,-PDF

upvoted 2 times

1rob 1 month, 1 week ago

Selected Answer: B

Answer A does not comply because aws cloudHSM is within aws
Answer B is the correct answer because the company is required to use its on-premises key manager. Following https://docs.aws.amazon.com/kms/latest/developerguide/custom-key-store-overview.html gives :An external key store is an AWS KMS custom key store backed by an external key manager outside of AWS that you own and control.(...)

Answer C and D are both solutions in the aws cloud so that does not fit.

upvoted 1 times

potomac 1 month, 3 weeks ago

Selected Answer: B

https://docs.aws.amazon.com/kms/latest/developerguide/keystore-external.html

upvoted 4 times

Question #646

A solutions architect needs to host a high performance computing (HPC) workload in the AWS Cloud. The workload will run on hundreds of Amazon EC2 instances and will require parallel access to a shared file system to enable distributed processing of large datasets. Datasets will be accessed across multiple instances simultaneously. The workload requires access latency within 1 ms. After processing has completed, engineers will need access to the dataset for manual postprocessing.

Which solution will meet these requirements?

A. Use Amazon Elastic File System (Amazon EFS) as a shared file system. Access the dataset from Amazon EFS.

B. Mount an Amazon S3 bucket to serve as the shared file system. Perform postprocessing directly from the S3 bucket.

C. Use Amazon FSx for Lustre as a shared file system. Link the file system to an Amazon S3 bucket for postprocessing.

D. Configure AWS Resource Access Manager to share an Amazon S3 bucket so that it can be mounted to all instances for processing and postprocessing.

Correct Answer: *C*

Community vote distribution

C (100%)

potomac Highly Voted 1 month, 3 weeks ago

Selected Answer: C

Amazon FSx for Lustre is a fully managed, high-performance file system optimized for HPC workloads. It is designed to deliver sub-millisecond latencies and high throughput, making it ideal for applications that require parallel access to shared storage, such as simulations and data analytics.

upvoted 5 times

TariqKipkemei Most Recent 3 weeks, 6 days ago

Selected Answer: C

high performance computing (HPC) workloads, shared file system= Amazon FSx for Lustre

upvoted 1 times

Question #647

A gaming company is building an application with Voice over IP capabilities. The application will serve traffic to users across the world. The application needs to be highly available with an automated failover across AWS Regions. The company wants to minimize the latency of users without relying on IP address caching on user devices.

What should a solutions architect do to meet these requirements?

A. Use AWS Global Accelerator with health checks.

B. Use Amazon Route 53 with a geolocation routing policy.

C. Create an Amazon CloudFront distribution that includes multiple origins.

D. Create an Application Load Balancer that uses path-based routing.

Correct Answer: *A*

Community vote distribution

A (93%) 7%

potomac Highly Voted 1 month, 3 weeks ago

Selected Answer: A

Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover.

upvoted 6 times

Murtadhaceit Most Recent 2 weeks, 3 days ago

Selected Answer: A

VoIP ==> UDP ==> Global Accelerator.

upvoted 2 times

kaleemanjum 3 weeks, 1 day ago

Selected Answer: A

AWS Global Accelerator: AWS Global Accelerator is a service that uses static IP addresses (Anycast IPs) to provide a global entry point for your applications. It routes traffic over the AWS global network to the optimal AWS endpoint based on health, geography, and routing policies.

Health Checks: AWS Global Accelerator supports health checks, allowing it to route traffic only to healthy endpoints. This helps in achieving high availability and automated failover across AWS Regions.

upvoted 1 times

SHAAHIBHUSHANAWS 3 weeks, 6 days ago

A
https://aws.amazon.com/global-accelerator/faqs/#:~:text=Global%20Accelerator%20is%20a%20good,AWS%20Shield%20for%20DDoS%20protection.

upvoted 1 times

ekisako 1 month, 3 weeks ago

Selected Answer: A

https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-benefits-of-migrating.html

upvoted 2 times

cciesam 1 month, 3 weeks ago

Selected Answer: A

Global Accelerator is the answer as it can handle both TCP and UDP

upvoted 2 times

Sugarbear_01 1 month, 4 weeks ago

Selected Answer: C

This answer should be C

upvoted 1 times

Question #648

A weather forecasting company needs to process hundreds of gigabytes of data with sub-millisecond latency. The company has a high performance computing (HPC) environment in its data center and wants to expand its forecasting capabilities.

A solutions architect must identify a highly available cloud storage solution that can handle large amounts of sustained throughput. Files that are stored in the solution should be accessible to thousands of compute instances that will simultaneously access and process the entire dataset.

What should the solutions architect do to meet these requirements?

A. Use Amazon FSx for Lustre scratch file systems.

B. Use Amazon FSx for Lustre persistent file systems.

C. Use Amazon Elastic File System (Amazon EFS) with Bursting Throughput mode.

D. Use Amazon Elastic File System (Amazon EFS) with Provisioned Throughput mode.

Correct Answer: *B*

Community vote distribution

B (100%)

potomac Highly Voted 1 month, 3 weeks ago

Selected Answer: B

Option A (Amazon FSx for Lustre scratch file systems) is designed for temporary data storage and does not provide the data persistence required for this scenario.

upvoted 5 times

TariqKipkemei Most Recent 3 weeks, 6 days ago

Selected Answer: B

high performance computing, highly available cloud storage solution = Amazon FSx for Lustre persistent file systems

upvoted 2 times

Question #649

An ecommerce company runs a PostgreSQL database on premises. The database stores data by using high IOPS Amazon Elastic Block Store (Amazon EBS) block storage. The daily peak I/O transactions per second do not exceed 15,000 IOPS. The company wants to migrate the database to Amazon RDS for PostgreSQL and provision disk IOPS performance independent of disk storage capacity.

Which solution will meet these requirements MOST cost-effectively?

A. Configure the General Purpose SSD (gp2) EBS volume storage type and provision 15,000 IOPS.

B. Configure the Provisioned IOPS SSD (io1) EBS volume storage type and provision 15,000 IOPS.

C. Configure the General Purpose SSD (gp3) EBS volume storage type and provision 15,000 IOPS.

D. Configure the EBS magnetic volume type to achieve maximum IOPS.

Correct Answer: *C*

Community vote distribution

C (100%)

TariqKipkemei 3 weeks, 6 days ago

Selected Answer: C

MOST cost-effective =GP3

upvoted 1 times

SHAAHIBHUSHANAWS 3 weeks, 6 days ago

C
https://aws.amazon.com/ebs/general-purpose/

upvoted 1 times

Oblako 1 month, 1 week ago

Selected Answer: C

Both gp2 and gp3 can provision up to 16.000 IOPS. gp3 is cheaper than gp2.

upvoted 2 times

lagorb 1 month, 2 weeks ago

gp2 and gp3 can provision up to 16.000 IOPS, and gp3 is cheaper than gp2

upvoted 2 times

potomac 1 month, 3 weeks ago

Selected Answer: C

GP3 is better and cheaper than GP2

upvoted 2 times

Question #650

A company wants to migrate its on-premises Microsoft SQL Server Enterprise edition database to AWS. The company's online application uses the database to process transactions. The data analysis team uses the same production database to run reports for analytical processing. The company wants to reduce operational overhead by moving to managed services wherever possible.

Which solution will meet these requirements with the LEAST operational overhead?

A. Migrate to Amazon RDS for Microsoft SOL Server. Use read replicas for reporting purposes

B. Migrate to Microsoft SQL Server on Amazon EC2. Use Always On read replicas for reporting purposes

C. Migrate to Amazon DynamoDB. Use DynamoDB on-demand replicas for reporting purposes

D. Migrate to Amazon Aurora MySQL. Use Aurora read replicas for reporting purposes

Correct Answer: *A*

Community vote distribution

A (100%)

superalaga 2 weeks ago

Selected Answer: A

You can migrate with both A&B but option A is LEAST operational overhead/
A: https://aws.amazon.com/tutorials/move-to-managed/migrate-sql-server-to-amazon-rds/
B: https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-a-microsoft-sql-server-database-to-aurora-mysql-by-using-aws-dms-and-aws-sct.html

upvoted 1 times

TariqKipkemei 3 weeks, 6 days ago

Selected Answer: A

Only Amazon RDS allows the creation of readable standby DB instances.

upvoted 1 times

potomac 1 month, 3 weeks ago

Selected Answer: A

A is the only choice

upvoted 3 times

Question #651

A company stores a large volume of image files in an Amazon S3 bucket. The images need to be readily available for the first 180 days. The images are infrequently accessed for the next 180 days. After 360 days, the images need to be archived but must be available instantly upon request. After 5 years, only auditors can access the images. The auditors must be able to retrieve the images within 12 hours. The images cannot be lost during this process.

A developer will use S3 Standard storage for the first 180 days. The developer needs to configure an S3 Lifecycle rule.

Which solution will meet these requirements MOST cost-effectively?

A. Transition the objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 180 days. S3 Glacier Instant Retrieval after 360 days, and S3 Glacier Deep Archive after 5 years.

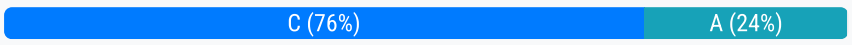
B. Transition the objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 180 days. S3 Glacier Flexible Retrieval after 360 days, and S3 Glacier Deep Archive after 5 years.

C. Transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 180 days, S3 Glacier Instant Retrieval after 360 days, and S3 Glacier Deep Archive after 5 years.

D. Transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 180 days, S3 Glacier Flexible Retrieval after 360 days, and S3 Glacier Deep Archive after 5 years.

Correct Answer: *C*

Community vote distribution



ale_brd_ 3 days, 23 hours ago

Selected Answer: C

Images cannot be lost = high availability. A exposes images to risk

upvoted 1 times

TariqKipkemei 3 weeks, 4 days ago

Selected Answer: C

Images cannot be lost = high availability.
Transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 180 days, S3 Glacier Instant Retrieval after 360 days, and S3 Glacier Deep Archive after 5 years.

upvoted 3 times

Alex1atd 1 month, 1 week ago

Selected Answer: C

The images cannot be lost during this process.

upvoted 3 times

1rob 1 month, 1 week ago

Selected Answer: C

"The images cannot be lost during this process" , imho this rules out S3 One zone infrequent access. S3 Glacier Instant Retrieval gives immediate access. S3 Glacier Flexible Retrieval does not give immediate access. so C.

upvoted 3 times

EdenWang 1 month, 1 week ago

Selected Answer: A

high availability is not mentioned, thus I go for A

upvoted 1 times

cciesam 1 month, 3 weeks ago

Selected Answer: A

I'll go for A as it doesn't talk about High availability. Considering cost. I'll go for A

upvoted 3 times

ekisako 1 month, 3 weeks ago

"The images cannot be lost during this process."

upvoted 2 times

Selected Answer: C

https://aws.amazon.com/s3/storage-classes/glacier/

upvoted 3 times

Question #652

A company has a large data workload that runs for 6 hours each day. The company cannot lose any data while the process is running. A solutions architect is designing an Amazon EMR cluster configuration to support this critical data workload.

Which solution will meet these requirements MOST cost-effectively?

A. Configure a long-running cluster that runs the primary node and core nodes on On-Demand Instances and the task nodes on Spot Instances.

B. Configure a transient cluster that runs the primary node and core nodes on On-Demand Instances and the task nodes on Spot Instances.

C. Configure a transient cluster that runs the primary node on an On-Demand Instance and the core nodes and task nodes on Spot Instances.

D. Configure a long-running cluster that runs the primary node on an On-Demand Instance, the core nodes on Spot Instances, and the task nodes on Spot Instances.

Correct Answer: *B*

Community vote distribution

B (100%)

potomac Highly Voted 1 month, 3 weeks ago

Selected Answer: B

A transient cluster provides cost savings because it runs only during the computation time, and it provides scalability and flexibility in a cloud environment.

Option C (transient cluster with On-Demand primary node and Spot core and task nodes) exposes the core nodes to Spot Instance interruptions, which may not be acceptable for a workload that cannot lose any data.

upvoted 10 times

louisaok Highly Voted 1 month, 3 weeks ago

Relax man. take a break since you have made this far so far.

upvoted 9 times

TariqKipkemei Most Recent 3 weeks, 4 days ago

Selected Answer: B

Cannot loose data = ondemand primary + core nodes
Save on costs = spot task nodes
Runs for 6 hours = transient cluster

upvoted 4 times

SHAAHIBHUSHANAWS 3 weeks, 6 days ago

A
https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-plan-instances-guidelines.html
It's long running and no data loss is needed.

upvoted 1 times

MFKang 1 month, 2 weeks ago

Get up Stand up

upvoted 2 times

Question #653

A company maintains an Amazon RDS database that maps users to cost centers. The company has accounts in an organization in AWS Organizations. The company needs a solution that will tag all resources that are created in a specific AWS account in the organization. The solution must tag each resource with the cost center ID of the user who created the resource.

Which solution will meet these requirements?

A. Move the specific AWS account to a new organizational unit (OU) in Organizations from the management account. Create a service control policy (SCP) that requires all existing resources to have the correct cost center tag before the resources are created. Apply the SCP to the new OU.

B. Create an AWS Lambda function to tag the resources after the Lambda function looks up the appropriate cost center from the RDS database. Configure an Amazon EventBridge rule that reacts to AWS CloudTrail events to invoke the Lambda function.

C. Create an AWS CloudFormation stack to deploy an AWS Lambda function. Configure the Lambda function to look up the appropriate cost center from the RDS database and to tag resources. Create an Amazon EventBridge scheduled rule to invoke the CloudFormation stack.

D. Create an AWS Lambda function to tag the resources with a default value. Configure an Amazon EventBridge rule that reacts to AWS CloudTrail events to invoke the Lambda function when a resource is missing the cost center tag.

Correct Answer: *B*

Community vote distribution

B (64%) A (36%)

fea9bdf 17 hours, 36 minutes ago

Answer is A, SCP handles the assignment, no need for a Lambda function, that's unnecessary t seems like
Service Control Policies (SCPs)

SCPs are a policy type that you can utilize to manage permissions across accounts in your AWS Organization.
Using SCPs lets you ensure that your accounts stay within your organization's access control guidelines.
SCPs can be used along-side tag policies to ensure that the tags are applied at the resource creation time and remain attached to the resource.

upvoted 1 times

ale_brd_ 3 days, 23 hours ago

Selected Answer: B

the company still maintains the RDS, nowhere was asked to drop using it, therefore we shall use a solution that takes advantages of it.

upvoted 1 times

ftaws 1 week, 3 days ago

Selected Answer: A

I also choose A.

upvoted 2 times

Cyberkayu 1 week, 4 days ago

Selected Answer: A

Company have Organization. A specific AWS account need to ensure all resources were tagged.

Move this specific AWS account under the company OU, use SCP to enforce top down policies that every member account to adhere.

Answer A.

upvoted 1 times

evelynsun 2 weeks, 1 day ago

Selected Answer: B

sorry, i would choose B.
because it allows you to tag resources as they are created, without requiring you to move existing resources.

upvoted 1 times

evelynsun 2 weeks, 1 day ago

Selected Answer: A

This solution is the best way to meet the requirements of the company. It ensures that all resources in the specific AWS account are tagged with the cost center ID of the user who created the resource. It also allows the company to easily manage and enforce compliance with its tagging policies.

upvoted 1 times

Selected Answer: B

Create an AWS Lambda function to tag the resources after the Lambda function looks up the appropriate cost center from the RDS database. Configure an Amazon EventBridge rule that reacts to AWS CloudTrail events to invoke the Lambda function.

upvoted 1 times

t0nx 1 month, 1 week ago

Selected Answer: B

This solution utilizes AWS Lambda and Amazon EventBridge to automate the tagging process based on information from the RDS database and CloudTrail events.

AWS Lambda Function: Create a Lambda function that can look up the cost center information from the RDS database and tag resources accordingly.

Amazon EventBridge Rule: Set up an EventBridge rule to react to AWS CloudTrail events. The rule triggers the Lambda function whenever a resource is created, allowing dynamic tagging based on the cost center associated with the user in the RDS database.

This solution provides automation, ensuring that resources are tagged appropriately with the cost center ID of the user who created the resource. It also allows for flexibility in updating cost center information without modifying the infrastructure.

upvoted 4 times

Question #654

A company recently migrated its web application to the AWS Cloud. The company uses an Amazon EC2 instance to run multiple processes to host the application. The processes include an Apache web server that serves static content. The Apache web server makes requests to a PHP application that uses a local Redis server for user sessions.

The company wants to redesign the architecture to be highly available and to use AWS managed solutions.

Which solution will meet these requirements?

A. Use AWS Elastic Beanstalk to host the static content and the PHP application. Configure Elastic Beanstalk to deploy its EC2 instance into a public subnet. Assign a public IP address.

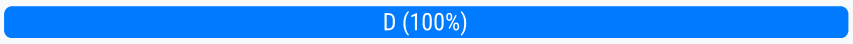
B. Use AWS Lambda to host the static content and the PHP application. Use an Amazon API Gateway REST API to proxy requests to the Lambda function. Set the API Gateway CORS configuration to respond to the domain name. Configure Amazon ElastiCache for Redis to handle session information.

C. Keep the backend code on the EC2 instance. Create an Amazon ElastiCache for Redis cluster that has Multi-AZ enabled. Configure the ElastiCache for Redis cluster in cluster mode. Copy the frontend resources to Amazon S3. Configure the backend code to reference the EC2 instance.

D. Configure an Amazon CloudFront distribution with an Amazon S3 endpoint to an S3 bucket that is configured to host the static content. Configure an Application Load Balancer that targets an Amazon Elastic Container Service (Amazon ECS) service that runs AWS Fargate tasks for the PHP application. Configure the PHP application to use an Amazon ElastiCache for Redis cluster that runs in multiple Availability Zones.

Correct Answer: *D*

Community vote distribution



evelynsun 2 weeks, 1 day ago

Selected Answer: D

This solution meets the requirements because it uses AWS managed solutions for hosting the static content and the PHP application. It also uses Amazon ECS to run the PHP application in a highly available and scalable manner. The solution also uses Amazon ElastiCache for Redis to handle session information, which is highly available and scalable. The solution also uses Amazon CloudFront to provide a secure and reliable way to deliver the static content to users.

upvoted 1 times

TariqKipkemei 3 weeks, 4 days ago

Selected Answer: D

Configure an Amazon CloudFront distribution with an Amazon S3 endpoint to an S3 bucket that is configured to host the static content. Configure an Application Load Balancer that targets an Amazon Elastic Container Service (Amazon ECS) service that runs AWS Fargate tasks for the PHP application. Configure the PHP application to use an Amazon ElastiCache for Redis cluster that runs in multiple Availability Zones.

upvoted 1 times

Question #655

A company runs a web application on Amazon EC2 instances in an Auto Scaling group that has a target group. The company designed the application to work with session affinity (sticky sessions) for a better user experience.

The application must be available publicly over the internet as an endpoint. A WAF must be applied to the endpoint for additional security. Session affinity (sticky sessions) must be configured on the endpoint.

Which combination of steps will meet these requirements? (Choose two.)

A. Create a public Network Load Balancer. Specify the application target group.

B. Create a Gateway Load Balancer. Specify the application target group.

C. Create a public Application Load Balancer. Specify the application target group.

D. Create a second target group. Add Elastic IP addresses to the EC2 instances.

E. Create a web ACL in AWS WAF. Associate the web ACL with the endpoint

Correct Answer: *CE*

Community vote distribution

CE (100%)

Mikado211 1 week, 5 days ago

Selected Answer: CE

- Make it accessible from the web + sticky session == Public ALB
- Additional security == web ACL in WAF (and integrate the web ACL to the ALB)

upvoted 1 times

ZZZ_Sleep 1 week, 6 days ago

Selected Answer: CE

session affinity (sticky sessions) = Application Load Balancer

WAF must be applied to the endpoint for additional security = web ACL in WAF

upvoted 1 times

TariqKipkemei 3 weeks, 4 days ago

Selected Answer: CE

Session Affinity = Application Load Balancer
Create a public Application Load Balancer. Specify the application target group then create a web ACL in AWS WAF. Associate the web ACL with the ALB endpoint.

upvoted 2 times

Question #656

A company runs a website that stores images of historical events. Website users need the ability to search and view images based on the year that the event in the image occurred. On average, users request each image only once or twice a year. The company wants a highly available solution to store and deliver the images to users.

Which solution will meet these requirements MOST cost-effectively?

A. Store images in Amazon Elastic Block Store (Amazon EBS). Use a web server that runs on Amazon EC2.

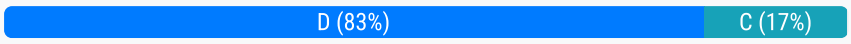
B. Store images in Amazon Elastic File System (Amazon EFS). Use a web server that runs on Amazon EC2.

C. Store images in Amazon S3 Standard. Use S3 Standard to directly deliver images by using a static website.

D. Store images in Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Use S3 Standard-IA to directly deliver images by using a static website.

Correct Answer: *D*

Community vote distribution



chikuwan Highly Voted 1 month, 1 week ago

Selected Answer: D

users request each image only once or twice a year
So the answer is D

upvoted 6 times

Kumar05162 Most Recent 1 week ago

Option D: Store images in Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Use S3 Standard-IA to directly deliver images by using a static website.

S3 Standard-IA is designed specifically for infrequently accessed data, offering lower storage costs compared to S3 Standard while still providing the necessary durability and availability.

upvoted 1 times

ZZZ_Sleep 1 week, 6 days ago

Selected Answer: D

High Availability = excluded A (EBS)
cost-effective = excluded B (EFS)
only once or twice a year = S3 Standard-IA, excluded C (S3 Standard, frequent access)

Left D, answer

upvoted 1 times

LuADS 3 weeks, 3 days ago

Selected Answer: C

Suppose there are thousands or millions of users, each image should be recovered once or twice a year X total users... makes it more expensive than the standard class since the recovery price of Standard-IA is $0.01 per GB + price of the requests which is also more expensive too.

upvoted 2 times

TariqKipkemei 3 weeks, 4 days ago

Selected Answer: D

MOST cost-effectively, request each image only once or twice a year= S3 Standard-Infrequent Access

upvoted 1 times

SHAAHIBHUSHANAWS 3 weeks, 6 days ago

D
https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html
Look at table

upvoted 1 times

achechen 1 month ago

Selected Answer: D

if the images are accessed once or twice a year, then it is cheaper to use infrequent access tier

upvoted 2 times

aragornfsm 1 month ago

I believe the correct answer is option D, but ChatGPT mentioned option C. I didn't understand. I'm curious about the actual correct answer.

Question #657

A company has multiple AWS accounts in an organization in AWS Organizations that different business units use. The company has multiple offices around the world. The company needs to update security group rules to allow new office CIDR ranges or to remove old CIDR ranges across the organization. The company wants to centralize the management of security group rules to minimize the administrative overhead that updating CIDR ranges requires.

Which solution will meet these requirements MOST cost-effectively?

A. Create VPC security groups in the organization's management account. Update the security groups when a CIDR range update is necessary.

B. Create a VPC customer managed prefix list that contains the list of CIDRs. Use AWS Resource Access Manager (AWS RAM) to share the prefix list across the organization. Use the prefix list in the security groups across the organization.

C. Create an AWS managed prefix list. Use an AWS Security Hub policy to enforce the security group update across the organization. Use an AWS Lambda function to update the prefix list automatically when the CIDR ranges change.

D. Create security groups in a central administrative AWS account. Create an AWS Firewall Manager common security group policy for the whole organization. Select the previously created security groups as primary groups in the policy.

Correct Answer: *B*

Community vote distribution

B (100%)

ale_brd_ 4 days ago

Selected Answer: B

Answer is B

upvoted 1 times

TariqKipkemei 3 weeks, 3 days ago

Selected Answer: B

A managed prefix list is a set of one or more CIDR blocks. You can use prefix lists to make it easier to configure and maintain your security groups and route tables. You can create a prefix list from the IP addresses that you frequently use, and reference them as a set in security group rules and routes instead of referencing them individually. If you scale your network and need to allow traffic from another CIDR block, you can update the relevant prefix list and all security groups that use the prefix list are updated. You can also use managed prefix lists with other AWS accounts using Resource Access Manager (RAM).

https://docs.aws.amazon.com/vpc/latest/userguide/managed-prefix-lists.html#:~:text=A-,managed%20prefix,-list%20is%20a

upvoted 3 times

achechen 1 month ago

Selected Answer: B

looks like B is the answer. Reference: https://docs.aws.amazon.com/vpc/latest/userguide/managed-prefix-lists.html

upvoted 2 times

Question #658

A company uses an on-premises network-attached storage (NAS) system to provide file shares to its high performance computing (HPC) workloads. The company wants to migrate its latency-sensitive HPC workloads and its storage to the AWS Cloud. The company must be able to provide NFS and SMB multi-protocol access from the file system.

Which solution will meet these requirements with the LEAST latency? (Choose two.)

A. Deploy compute optimized EC2 instances into a cluster placement group.

B. Deploy compute optimized EC2 instances into a partition placement group.

C. Attach the EC2 instances to an Amazon FSx for Lustre file system.

D. Attach the EC2 instances to an Amazon FSx for OpenZFS file system.

E. Attach the EC2 instances to an Amazon FSx for NetApp ONTAP file system.

Correct Answer: *AE*

Community vote distribution

AE (71%) AC (29%)

ZZZ_Sleep 1 week, 6 days ago

Selected Answer: AE

LEAST latency = cluster placement group

Amazon FSx for Lustre = SMB
Amazon FSx for OpenZFS = NFS
Amazon FSx for NetApp ONTAP = NFS, SMB, iSCSI

So, answer are A and E

upvoted 1 times

Sumith4112 3 weeks, 1 day ago

Selected Answer: AE

A becase cluster placement group means low latency.
E

upvoted 1 times

TariqKipkemei 3 weeks, 3 days ago

Selected Answer: AE

HPC, NFS, SMB = FSx for NetApp ONTAP file system
HPC, latency-sensitive = cluster placement group

upvoted 2 times

SHAAHIBHUSHANAWS 3 weeks, 6 days ago

AE
https://aws.amazon.com/fsx/when-to-choose-fsx/

upvoted 1 times

lucasbg 1 month ago

Selected Answer: AE

You talked avout smb and nfs, you talked fsx netapp ontap

C is wrong because lustre is a POSIX fs

upvoted 2 times

achechen 1 month ago

Selected Answer: AE

I don't think FSx for Lustre supports SMB. At least I could not find anything in the documentation. However, FSx for ONTAP delivers NFS and SMB support.

upvoted 2 times

chikuwan 1 month, 1 week ago

Selected Answer: AE

https://aws.amazon.com/jp/fsx/lustre/features/

upvoted 1 times

reika1914 1 month, 1 week ago

Selected Answer: AC

To meet the requirements of migrating latency-sensitive HPC workloads with multi-protocol access (NFS and SMB) to AWS with minimal latency, the following solutions would be the most appropriate:

A. Deploy compute optimized EC2 instances into a cluster placement group.
C. Attach the EC2 instances to an Amazon FSx for Lustre file system.

upvoted 2 times

Chiquitabandita 1 month, 1 week ago

Selected Answer: AE

https://aws.amazon.com/fsx/netapp-ontap/features/#:~:text=Amazon%20FSx%20for%20NetApp%20ONTAP%20provides%20access%20to%20shared%20file,access)%20to%20the%20same%20data. "Amazon FSx for NetApp ONTAP provides access to shared file storage over all versions of the Network File System (NFS) and Server Message Block (SMB) protocols, and also supports multi-protocol access (i.e. concurrent NFS and SMB access) to the same data."

upvoted 3 times

LemonGremlin 1 month, 1 week ago

Selected Answer: AC

Option A: A cluster placement group provides low-latency and high-bandwidth connectivity between instances. This is particularly beneficial for high-performance computing workloads that are latency-sensitive. Instances within a cluster placement group are placed in close proximity to each other within the same Availability Zone.

Option C: Amazon FSx for Lustre is a high-performance file system optimized for fast access to data. It is well-suited for high-performance computing workloads. It provides low-latency access to data and supports the NFS protocol.

upvoted 3 times

t0nx 1 month, 1 week ago

Thank you

upvoted 1 times

Question #659

A company is relocating its data center and wants to securely transfer 50 TB of data to AWS within 2 weeks. The existing data center has a Site-to-Site VPN connection to AWS that is 90% utilized.

Which AWS service should a solutions architect use to meet these requirements?

A. AWS DataSync with a VPC endpoint

B. AWS Direct Connect

C. AWS Snowball Edge Storage Optimized

D. AWS Storage Gateway

Correct Answer: *C*

Community vote distribution

C (100%)

ftaws 1 week, 3 days ago

Not memtioned network bandwidth. How we know that?

upvoted 1 times

Cyberkayu 1 week, 4 days ago

Selected Answer: C

90% utilization of the bandwidth = they discouraged the use of internet bandwidth for uploading, go seek for offline data seeding to AWS method

upvoted 2 times

TariqKipkemei 3 weeks, 3 days ago

Selected Answer: C

50 TB of data to AWS within 2 weeks = Snowball Edge Storage Optimized

upvoted 3 times

Question #660

A company hosts an application on Amazon EC2 On-Demand Instances in an Auto Scaling group. Application peak hours occur at the same time each day. Application users report slow application performance at the start of peak hours. The application performs normally 2-3 hours after peak hours begin. The company wants to ensure that the application works properly at the start of peak hours.

Which solution will meet these requirements?

A. Configure an Application Load Balancer to distribute traffic properly to the instances.

B. Configure a dynamic scaling policy for the Auto Scaling group to launch new instances based on memory utilization.

C. Configure a dynamic scaling policy for the Auto Scaling group to launch new instances based on CPU utilization.

D. Configure a scheduled scaling policy for the Auto Scaling group to launch new instances before peak hours.

Correct Answer: *D*

Community vote distribution

D (100%)

ZZZ_Sleep 1 week, 6 days ago

Selected Answer: D

occur at the same time each day = predictable

So, scheduled scaling policy, Answer is D.

Dynamic scaling policy work for unpredictable

upvoted 2 times

TariqKipkemei 3 weeks, 3 days ago

Selected Answer: D

Techincally both dynamic and scheduled scaling would work but there is strict requirement for the application to work properly at the start of peak hours and no mention of cost.

So scheduled scaling policy it is.

upvoted 2 times

TOR_0511 4 weeks ago

Selected Answer: D

Application users report slow application performance at the start of peak hours. The company wants to ensure that the application works properly at the start of peak hours

upvoted 1 times

Arnaud92 1 month, 1 week ago

D. The application performs normally 2-3 hours after peak hours begin is a key! (schedule policy)

upvoted 3 times

Question #661

A company runs applications on AWS that connect to the company's Amazon RDS database. The applications scale on weekends and at peak times of the year. The company wants to scale the database more effectively for its applications that connect to the database.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use Amazon DynamoDB with connection pooling with a target group configuration for the database. Change the applications to use the DynamoDB endpoint.

B. Use Amazon RDS Proxy with a target group for the database. Change the applications to use the RDS Proxy endpoint.

C. Use a custom proxy that runs on Amazon EC2 as an intermediary to the database. Change the applications to use the custom proxy endpoint.

D. Use an AWS Lambda function to provide connection pooling with a target group configuration for the database. Change the applications to use the Lambda function.

Correct Answer: *B*

Community vote distribution

B (100%)

TariqKipkemei 3 weeks, 3 days ago

Selected Answer: B

Amazon RDS Proxy is a fully managed, highly available database proxy for Amazon Relational Database Service (RDS) that makes applications more resilient to database failures. Many applications, including those built on modern serverless architectures, can have a large number of open connections to the database server and may open and close database connections at a high rate, exhausting database memory and compute resources. Amazon RDS Proxy allows applications to pool and share connections established with the database, improving database efficiency and application scalability. With RDS Proxy, failover times for Aurora and RDS databases are reduced by up to 66%

upvoted 2 times

TOR_0511 4 weeks ago

Selected Answer: B

A out because DynamoDB is a NoSQL DB
B As the question is referring about DB connections so this option has the LEAST operational overhead

upvoted 2 times

Question #662

A company uses AWS Cost Explorer to monitor its AWS costs. The company notices that Amazon Elastic Block Store (Amazon EBS) storage and snapshot costs increase every month. However, the company does not purchase additional EBS storage every month. The company wants to optimize monthly costs for its current storage usage.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use logs in Amazon CloudWatch Logs to monitor the storage utilization of Amazon EBS. Use Amazon EBS Elastic Volumes to reduce the size of the EBS volumes.

B. Use a custom script to monitor space usage. Use Amazon EBS Elastic Volumes to reduce the size of the EBS volumes.

C. Delete all expired and unused snapshots to reduce snapshot costs.

D. Delete all nonessential snapshots. Use Amazon Data Lifecycle Manager to create and manage the snapshots according to the company's snapshot policy requirements.

Correct Answer: *D*

Community vote distribution

D (100%)

TariqKipkemei 3 weeks, 3 days ago

Selected Answer: D

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html

upvoted 2 times

t0nx 1 month, 1 week ago

Selected Answer: D

This option involves managing snapshots efficiently to optimize costs with minimal operational overhead.

Delete all nonessential snapshots: This reduces costs by eliminating unnecessary snapshot storage.
Use Amazon Data Lifecycle Manager (DLM): DLM can automate the creation and deletion of snapshots based on defined policies. This reduces operational overhead by automating snapshot management according to the company's snapshot policy requirements.

upvoted 3 times

Question #663

A company is developing a new application on AWS. The application consists of an Amazon Elastic Container Service (Amazon ECS) cluster, an Amazon S3 bucket that contains assets for the application, and an Amazon RDS for MySQL database that contains the dataset for the application. The dataset contains sensitive information. The company wants to ensure that only the ECS cluster can access the data in the RDS for MySQL database and the data in the S3 bucket.

Which solution will meet these requirements?

A. Create a new AWS Key Management Service (AWS KMS) customer managed key to encrypt both the S3 bucket and the RDS for MySQL database. Ensure that the KMS key policy includes encrypt and decrypt permissions for the ECS task execution role.

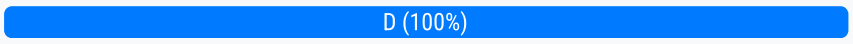
B. Create an AWS Key Management Service (AWS KMS) AWS managed key to encrypt both the S3 bucket and the RDS for MySQL database. Ensure that the S3 bucket policy specifies the ECS task execution role as a user.

C. Create an S3 bucket policy that restricts bucket access to the ECS task execution role. Create a VPC endpoint for Amazon RDS for MySQL. Update the RDS for MySQL security group to allow access from only the subnets that the ECS cluster will generate tasks in.

D. Create a VPC endpoint for Amazon RDS for MySQL. Update the RDS for MySQL security group to allow access from only the subnets that the ECS cluster will generate tasks in. Create a VPC endpoint for Amazon S3. Update the S3 bucket policy to allow access from only the S3 VPC endpoint.

Correct Answer: *D*

Community vote distribution



t0nx Highly Voted 1 month, 1 week ago

Selected Answer: D

Option D is the most comprehensive solution as it leverages VPC endpoints for both Amazon RDS and Amazon S3, along with proper network-level controls to restrict access to only the necessary resources from the ECS cluster.

upvoted 7 times

Min_93 Most Recent 4 days, 7 hours ago

Options A and B involve using AWS Key Management Service (AWS KMS) for encryption but do not directly address the requirement to restrict access to the ECS cluster. Option C is not the most direct approach for restricting access to the RDS database, as it focuses on the S3 bucket.

Therefore, option D is the most appropriate solution for ensuring that only the ECS cluster can access the data in the RDS for MySQL database and the data in the S3 bucket.

upvoted 1 times

TariqKipkemei 3 weeks, 3 days ago

Selected Answer: D

A VPC endpoint enables customers to privately connect to supported AWS services and VPC endpoint services powered by AWS PrivateLink.

upvoted 2 times

SHAAHIBHUSHANAWS 3 weeks, 6 days ago

C

need to restrict access from ECS cluster

upvoted 2 times

LemonGremlin 1 month, 1 week ago

Selected Answer: D

Create a VPC endpoint for Amazon RDS for MySQL: This ensures that the ECS cluster can access the RDS database directly within the same Virtual Private Cloud (VPC), without having to go over the internet. By updating the security group to allow access only from the specific subnets that the ECS cluster will generate tasks in, you limit access to only the authorized entities.

Create a VPC endpoint for Amazon S3: This allows the ECS cluster to access the S3 bucket directly within the same VPC. By updating the S3 bucket policy to allow access only from the S3 VPC endpoint, you restrict access to the designated VPC, ensuring that only authorized resources can access the S3 bucket.

upvoted 2 times

SHAAHIBHUSHANAWS 3 weeks, 6 days ago

I agree this will allow only resources from VPC but will not restrict only ECS cluster. I suggest we use bucket policy to use ECS cluster role on top of network settings.

upvoted 1 times

Question #664

A company has a web application that runs on premises. The application experiences latency issues during peak hours. The latency issues occur twice each month. At the start of a latency issue, the application's CPU utilization immediately increases to 10 times its normal amount.

The company wants to migrate the application to AWS to improve latency. The company also wants to scale the application automatically when application demand increases. The company will use AWS Elastic Beanstalk for application deployment.

Which solution will meet these requirements?

A. Configure an Elastic Beanstalk environment to use burstable performance instances in unlimited mode. Configure the environment to scale based on requests.

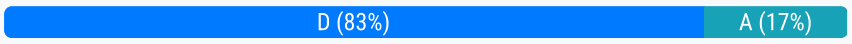
B. Configure an Elastic Beanstalk environment to use compute optimized instances. Configure the environment to scale based on requests.

C. Configure an Elastic Beanstalk environment to use compute optimized instances. Configure the environment to scale on a schedule.

D. Configure an Elastic Beanstalk environment to use burstable performance instances in unlimited mode. Configure the environment to scale on predictive metrics.

Correct Answer: *D*

Community vote distribution



LemonGremlin Highly Voted 1 month, 1 week ago

Selected Answer: D

Burstable Performance Instances (T3 or T3a): These instances are designed for burstable workloads and provide a baseline level of CPU performance with the ability to burst above that baseline when needed. Bursting is particularly beneficial for handling sudden spikes in CPU utilization, such as those described in the scenario.

Unlimited Mode: Enabling "unlimited" mode allows instances to burst beyond their baseline performance without accumulating CPU credits. This is important for handling sudden and sustained increases in CPU utilization during peak hours.

Scale on Predictive Metrics: Configuring the environment to scale on predictive metrics allows AWS Elastic Beanstalk to proactively adjust the number of instances based on anticipated demand. This can help ensure that the environment is scaled up before the latency issues occur, addressing them in advance.

upvoted 5 times

ftaws 1 week, 3 days ago

Traffic is "immediately increases". We can't predict and can not use Predictive Metrics.
And requirement need auto scaling

upvoted 1 times

Min_93 Most Recent 4 days, 7 hours ago

Selected Answer: D

Option A, which suggests using burstable performance instances in unlimited mode, is appropriate. However, option D is more specific to the requirement of scaling based on predictive metrics, which is crucial for handling the latency issues that occur at specific times each month.

Options B and C suggest using compute optimized instances and scaling based on requests or on a schedule. While these options might work for general scalability, they may not address the immediate and intense spikes in CPU utilization that are mentioned in the scenario.

Therefore, option D is the most appropriate solution for improving latency and automatically scaling the application based on predictive metrics using AWS Elastic Beanstalk.

upvoted 1 times

evelynsun 2 weeks, 1 day ago

Selected Answer: A

This solution meets the requirements because it allows the company to automatically scale the application's CPU capacity based on the number of requests it receives. The burstable performance instances provide high CPU performance when needed, which can help to reduce latency during peak hours.

not D: this solution has some drawbacks. First, it can be expensive to use burstable performance instances in unlimited mode, as the instances are charged per hour. Second, it can be difficult to predict the exact CPU requirements of the application, which can lead to over- or under-provisioning of CPU resources.

upvoted 1 times

TariqKipkemei 3 weeks, 3 days ago

Selected Answer: A

The company also wants to scale the application automatically when application demand increases = Scale based on requests

upvoted 1 times

SHAAHIBHUSHANAWS 3 weeks, 6 days ago

B
Question is asking scale based on demand so better scale based on requests. Predictive metrics not defined and may be interpreted differently by many users.

upvoted 2 times

reika1914 1 month, 1 week ago

Selected Answer: D

Given the scenario described, the best solution among the provided options to meet the requirements of migrating the application to AWS, improving latency, and scaling the application automatically during increased demand would be:

D. Configure an Elastic Beanstalk environment to use burstable performance instances in unlimited mode. Configure the environment to scale on predictive metrics.

upvoted 1 times

t0nx 1 month, 1 week ago

Selected Answer: D

In this scenario, the application experiences latency issues during peak hours with a sudden increase in CPU utilization. Using burstable performance instances in unlimited mode allows the application to burst beyond the baseline performance when needed. Configuring the environment to scale on predictive metrics enables proactive scaling based on anticipated increases in demand.

upvoted 3 times

Question #665

A company has customers located across the world. The company wants to use automation to secure its systems and network infrastructure. The company's security team must be able to track and audit all incremental changes to the infrastructure.

Which solution will meet these requirements?

A. Use AWS Organizations to set up the infrastructure. Use AWS Config to track changes.

B. Use AWS CloudFormation to set up the infrastructure. Use AWS Config to track changes.

C. Use AWS Organizations to set up the infrastructure. Use AWS Service Catalog to track changes.

D. Use AWS CloudFormation to set up the infrastructure. Use AWS Service Catalog to track changes.

Correct Answer: *B*

Community vote distribution

B (100%)

TariqKipkemei Highly Voted 3 weeks, 3 days ago

Selected Answer: B

use automation to secure its systems and network infrastructure = AWS CloudFormation
track and audit all incremental changes to the infrastructure = AWS Config

upvoted 5 times

Min_93 Most Recent 4 days, 7 hours ago

Selected Answer: B

Option B is the most suitable because it combines the benefits of infrastructure as code (CloudFormation) with tracking and auditing capabilities (AWS Config). With CloudFormation, the company can define and deploy its infrastructure in a repeatable and automated way, ensuring consistency and adherence to security standards. AWS Config then complements this by providing visibility into changes and configuration details.

upvoted 2 times

Question #666

A startup company is hosting a website for its customers on an Amazon EC2 instance. The website consists of a stateless Python application and a MySQL database. The website serves only a small amount of traffic. The company is concerned about the reliability of the instance and needs to migrate to a highly available architecture. The company cannot modify the application code.

Which combination of actions should a solutions architect take to achieve high availability for the website? (Choose two.)

A. Provision an internet gateway in each Availability Zone in use.

B. Migrate the database to an Amazon RDS for MySQL Multi-AZ DB instance.

C. Migrate the database to Amazon DynamoDB, and enable DynamoDB auto scaling.

D. Use AWS DataSync to synchronize the database data across multiple EC2 instances.

E. Create an Application Load Balancer to distribute traffic to an Auto Scaling group of EC2 instances that are distributed across two Availability Zones.

Correct Answer: *BE*

Community vote distribution

BE (100%)

Cyberkayu 1 week, 4 days ago

A. no failed over mechanism
C. DynamoDB is no SQL, cannot use with MySQL
D. Not HA, just sync/replication tools.

Answer BE.

upvoted 2 times

TariqKipkemei 3 weeks ago

Selected Answer: BE

To achieve high availability for the website, Migrate the database to an Amazon RDS for MySQL Multi-AZ DB instance and Create an Application Load Balancer to distribute traffic to an Auto Scaling group of EC2 instances that are distributed across two Availability Zones.

upvoted 3 times

Question #667

A company is moving its data and applications to AWS during a multiyear migration project. The company wants to securely access data on Amazon S3 from the company's AWS Region and from the company's on-premises location. The data must not traverse the internet. The company has established an AWS Direct Connect connection between its Region and its on-premises location.

Which solution will meet these requirements?

A. Create gateway endpoints for Amazon S3. Use the gateway endpoints to securely access the data from the Region and the on-premises location.

B. Create a gateway in AWS Transit Gateway to access Amazon S3 securely from the Region and the on-premises location.

C. Create interface endpoints for Amazon S3. Use the interface endpoints to securely access the data from the Region and the on-premises location.

D. Use an AWS Key Management Service (AWS KMS) key to access the data securely from the Region and the on-premises location.

Correct Answer: *C*

Community vote distribution

C (75%) | A (17%) | 8%

fea9bdf 18 hours, 15 minutes ago

Answer seems to be C
gateway endpoints do not allow access from on-premises networks, from peered VPCs in other AWS Regions, or through a transit gateway. For those scenarios, you must use an interface endpoint, which is available for an additional cost. For more information, see Types of VPC endpoints for Amazon S3 in the Amazon S3 User Guide.

upvoted 1 times

ale_brd_ 4 days, 1 hour ago

Selected Answer: C

gateway endpoint uses public ip address even if traffic does not directly route thru the internet, also they are no meant to be used from on-premises. Answer is C

upvoted 2 times

Min_93 4 days, 7 hours ago

Selected Answer: C

Options A, B, and D are not the most suitable for the following reasons:

A. Create gateway endpoints for Amazon S3:

Gateway endpoints are used for accessing S3 from within a VPC, but they do not extend connectivity to on-premises locations.
B. Create a gateway in AWS Transit Gateway:

AWS Transit Gateway is designed for routing traffic between VPCs and on-premises networks but is not used as a direct gateway for S3 access.
D. Use an AWS Key Management Service (AWS KMS) key:

AWS KMS is a key management service and does not provide direct access to S3. It's used for managing encryption keys.
Therefore, option C, creating interface endpoints for Amazon S3, is the most appropriate solution for securely accessing S3 from both the AWS Region and the on-premises location.

upvoted 1 times

Min_93 4 days, 7 hours ago

Gateway endpoints for Amazon S3

Interface endpoints for Amazon S3

In both cases, your network traffic remains on the AWS network.

Use Amazon S3 public IP addresses

Use private IP addresses from your VPC to access Amazon S3

Use the same Amazon S3 DNS names

Require endpoint-specific Amazon S3 DNS names

Do not allow access from on premises

Allow access from on premises

Do not allow access from another AWS Region

Allow access from a VPC in another AWS Region by using VPC peering or AWS Transit Gateway

Not billed

Billed

upvoted 1 times

ftaws 1 week, 3 days ago

Selected Answer: B

Transit Gateway support inter region.
interface gateway not use in S3

upvoted 1 times

Min_93 4 days, 7 hours ago

com.amazonaws.ap-southeast-1.s3 amazon Interface

Interface is now available for S3

upvoted 1 times

Ernestokoro 2 weeks, 6 days ago

Ans is C: >>You can access Amazon S3 from your VPC using gateway VPC endpoints. After you create the gateway endpoint, you can add it as a target in your route table for traffic destined from your VPC to Amazon S3.
There is no additional charge for using gateway endpoints. Amazon S3 supports both gateway endpoints and interface endpoints. With a gateway endpoint, you can access Amazon S3 from your VPC, without requiring an internet gateway or NAT device for your VPC, and with no additional cost. However, gateway endpoints do not allow access from on-premises networks, from peered VPCs in other AWS Regions, or through a transit gateway. For those scenarios, you must use an interface endpoint, which is available for an additional cost. For more information, see Types of VPC endpoints for Amazon S3 in the Amazon S3 User Guide.
https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html

upvoted 4 times

Beshowasfy 2 weeks, 6 days ago

Selected Answer: A

GW Endpoint is only for S3 and DynamoDB, interface endpoint for other services so C is wrong

upvoted 2 times

ale_brd_ 4 days, 1 hour ago

you can't access gateway endpoint from on-premises

upvoted 1 times

TariqKipkemei 3 weeks ago

Selected Answer: C

S3 gateway endpoints do not currently support access from resources in a different Region, different VPC, or from an on-premises (non-AWS) environment.
https://aws.amazon.com/blogs/architecture/choosing-your-vpc-endpoint-strategy-for-amazon-s3/#:~:text=associated.%20S3%20gateway-,endpoints,-do%20not%20currently

upvoted 1 times

SHAAHIBHUSHANAWS 3 weeks, 6 days ago

C

. S3 gateway endpoints do not currently support access from resources in a different Region, different VPC, or from an on-premises (non-AWS) environment. However, if you're willing to manage a complex custom architecture, you can use proxies. In all those scenarios, where access is from resources external to VPC, S3 interface endpoints access S3 in a secure way.
https://aws.amazon.com/blogs/architecture/choosing-your-vpc-endpoint-strategy-for-amazon-s3/

upvoted 2 times

VladanO 4 weeks ago

Selected Answer: A
https://docs.aws.amazon.com/vpc/latest/privatelink/gateway-endpoints.html
Gateway VPC endpoints provide reliable connectivity to Amazon S3 and DynamoDB without requiring an internet gateway or a NAT device for your VPC.
There is no additional charge for using gateway endpoints.

upvoted 1 times

t0nx 1 month, 1 week ago

Selected Answer: C

CCCCCC

upvoted 1 times

LemonGremlin 1 month, 1 week ago

Selected Answer: C

Amazon VPC interface endpoints enable you to privately connect your VPC to supported AWS services without requiring an internet gateway, NAT device, VPN, or Direct Connect connection.
By creating interface endpoints for Amazon S3 in both the AWS Region and the on-premises location, you can securely access data without

traversing the internet.
Direct Connect Connection:

With an AWS Direct Connect connection established between the AWS Region and the on-premises location, the data can flow over the dedicated, private connection rather than going over the public internet.

upvoted 4 times

Question #668

A company created a new organization in AWS Organizations. The organization has multiple accounts for the company's development teams. The development team members use AWS IAM Identity Center (AWS Single Sign-On) to access the accounts. For each of the company's applications, the development teams must use a predefined application name to tag resources that are created.

A solutions architect needs to design a solution that gives the development team the ability to create resources only if the application name tag has an approved value.

Which solution will meet these requirements?

A. Create an IAM group that has a conditional Allow policy that requires the application name tag to be specified for resources to be created.

B. Create a cross-account role that has a Deny policy for any resource that has the application name tag.

C. Create a resource group in AWS Resource Groups to validate that the tags are applied to all resources in all accounts.

D. Create a tag policy in Organizations that has a list of allowed application names.

Correct Answer: *D*

Community vote distribution

D (100%)

m_y_s 2 weeks, 5 days ago

Selected Answer: D

A tag policy can also specify that noncompliant tagging operations on specified resource types are enforced. In other words, noncompliant tagging requests on specified resource types are prevented from completing.

upvoted 1 times

Beshowasfy 2 weeks, 6 days ago

Selected Answer: D

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies.html

upvoted 1 times

SHAAHIBHUSHANAWS 3 weeks, 6 days ago

D
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies.html

upvoted 1 times

rcptryk 4 weeks, 1 day ago

Selected Answer: D

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies.html

upvoted 2 times

Question #669

A company runs its databases on Amazon RDS for PostgreSQL. The company wants a secure solution to manage the master user password by rotating the password every 30 days.

Which solution will meet these requirements with the LEAST operational overhead?

A. Use Amazon EventBridge to schedule a custom AWS Lambda function to rotate the password every 30 days.

B. Use the modify-db-instance command in the AWS CLI to change the password.

C. Integrate AWS Secrets Manager with Amazon RDS for PostgreSQL to automate password rotation.

D. Integrate AWS Systems Manager Parameter Store with Amazon RDS for PostgreSQL to automate password rotation.

Correct Answer: *C*

Community vote distribution

C (100%)

TariqKipkemei Highly Voted 3 weeks ago

Selected Answer: C

password rotation = AWS Secrets Manager

upvoted 5 times

rcptryk Most Recent 4 weeks, 1 day ago

Selected Answer: C

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-secrets-manager.html

upvoted 3 times

Question #670

A company performs tests on an application that uses an Amazon DynamoDB table. The tests run for 4 hours once a week. The company knows how many read and write operations the application performs to the table each second during the tests. The company does not currently use DynamoDB for any other use case. A solutions architect needs to optimize the costs for the table.

Which solution will meet these requirements?

A. Choose on-demand mode. Update the read and write capacity units appropriately.

B. Choose provisioned mode. Update the read and write capacity units appropriately.

C. Purchase DynamoDB reserved capacity for a 1-year term.

D. Purchase DynamoDB reserved capacity for a 3-year term.

Correct Answer: *B*

Community vote distribution

B (100%)

meenkaza 2 days, 19 hours ago

Selected Answer: B

Provisioned Mode (Option B): Provisioned mode allows you to specify the desired read and write capacity units. Since the workload occurs once a week for 4 hours, you can provision the read and write capacity units accordingly to handle the expected load during that time. This can be a more cost-effective option than on-demand pricing for predictable workloads.

upvoted 1 times

Question #671

A company runs its applications on Amazon EC2 instances. The company performs periodic financial assessments of its AWS costs. The company recently identified unusual spending.

The company needs a solution to prevent unusual spending. The solution must monitor costs and notify responsible stakeholders in the event of unusual spending.

Which solution will meet these requirements?

A. Use an AWS Budgets template to create a zero spend budget.

B. Create an AWS Cost Anomaly Detection monitor in the AWS Billing and Cost Management console.

C. Create AWS Pricing Calculator estimates for the current running workload pricing details.

D. Use Amazon CloudWatch to monitor costs and to identify unusual spending.

Correct Answer: *B*

Community vote distribution

B (100%)

meenkaza 2 days, 19 hours ago

Selected Answer: B

AWS Cost Anomaly Detection (Option B): AWS Cost Anomaly Detection is designed to automatically detect unusual spending patterns based on machine learning algorithms. It can identify anomalies and send notifications when it detects unexpected changes in spending. This aligns well with the requirement to prevent unusual spending and notify stakeholders.

upvoted 4 times

Question #672

A marketing company receives a large amount of new clickstream data in Amazon S3 from a marketing campaign. The company needs to analyze the clickstream data in Amazon S3 quickly. Then the company needs to determine whether to process the data further in the data pipeline.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create external tables in a Spark catalog. Configure jobs in AWS Glue to query the data.

B. Configure an AWS Glue crawler to crawl the data. Configure Amazon Athena to query the data.

C. Create external tables in a Hive metastore. Configure Spark jobs in Amazon EMR to query the data.

D. Configure an AWS Glue crawler to crawl the data. Configure Amazon Kinesis Data Analytics to use SQL to query the data.

Correct Answer: *B*

Community vote distribution

B (100%)

meenkaza 2 days, 19 hours ago

Selected Answer: B

AWS Glue with Athena (Option B): AWS Glue is a fully managed extract, transform, and load (ETL) service, and Athena is a serverless query service that allows you to analyze data directly in Amazon S3 using SQL queries. By configuring an AWS Glue crawler to crawl the data, you can create a schema for the data, and then use Athena to query the data directly without the need to load it into a separate database. This minimizes operational overhead.

upvoted 3 times

Question #673

A company runs an SMB file server in its data center. The file server stores large files that the company frequently accesses for up to 7 days after the file creation date. After 7 days, the company needs to be able to access the files with a maximum retrieval time of 24 hours.

Which solution will meet these requirements?

A. Use AWS DataSync to copy data that is older than 7 days from the SMB file server to AWS.

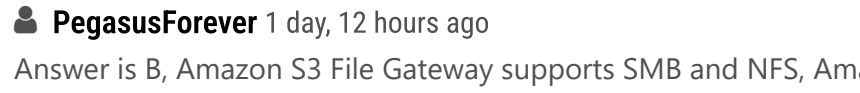
B. Create an Amazon S3 File Gateway to increase the company's storage space. Create an S3 Lifecycle policy to transition the data to S3 Glacier Deep Archive after 7 days.

C. Create an Amazon FSx File Gateway to increase the company's storage space. Create an Amazon S3 Lifecycle policy to transition the data after 7 days.

D. Configure access to Amazon S3 for each user. Create an S3 Lifecycle policy to transition the data to S3 Glacier Flexible Retrieval after 7 days.

Correct Answer: *B*

Community vote distribution



PegasusForever 1 day, 12 hours ago

Answer is B, Amazon S3 File Gateway supports SMB and NFS, Amazon FSx File Gateway SMB for windows workloads.

upvoted 2 times

cciesam 1 day, 17 hours ago

Selected Answer: B

S3 file gateway supports SMB and S3 Glacier Deep Archive can retrieve data within 12 hours.
https://aws.amazon.com/storagegateway/file/s3/

https://docs.aws.amazon.com/prescriptive-guidance/latest/backup-recovery/amazon-s3-glacier.html

upvoted 2 times

Roger_Liu 1 day, 23 hours ago

Selected Answer: B

I prefer to choose Amazon S3 File Gateway.
https://docs.aws.amazon.com/filegateway/latest/files3/file-gateway-concepts.html

upvoted 2 times

meenkaza 2 days, 19 hours ago

Selected Answer: C

Amazon FSx File Gateway with S3 Lifecycle policy (Option C): Amazon FSx is a fully managed file storage service, and with a File Gateway, it allows seamless integration between on-premises file servers and AWS storage. By creating an Amazon FSx File Gateway and implementing an S3 Lifecycle policy to transition data to S3 after 7 days, you can achieve the desired storage and retrieval characteristics.

upvoted 3 times

Question #674

A company runs a web application on Amazon EC2 instances in an Auto Scaling group. The application uses a database that runs on an Amazon RDS for PostgreSQL DB instance. The application performs slowly when traffic increases. The database experiences a heavy read load during periods of high traffic.

Which actions should a solutions architect take to resolve these performance issues? (Choose two.)

A. Turn on auto scaling for the DB instance.

B. Create a read replica for the DB instance. Configure the application to send read traffic to the read replica.

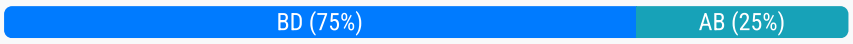
C. Convert the DB instance to a Multi-AZ DB instance deployment. Configure the application to send read traffic to the standby DB instance.

D. Create an Amazon ElastiCache cluster. Configure the application to cache query results in the ElastiCache cluster.

E. Configure the Auto Scaling group subnets to ensure that the EC2 instances are provisioned in the same Availability Zone as the DB instance.

Correct Answer: *BD*

Community vote distribution



Riajul 2 days, 6 hours ago

Selected Answer: AB

A and B should be most correct ans

upvoted 1 times

Riajul 2 days, 17 hours ago

Should be A and B

upvoted 1 times

meenkaza 2 days, 19 hours ago

Selected Answer: BD

B. Create a read replica for the DB instance. Configure the application to send read traffic to the read replica.

By creating a read replica, you offload read traffic from the primary DB instance to the replica, distributing the load and improving overall performance during periods of heavy read traffic.
D. Create an Amazon ElastiCache cluster. Configure the application to cache query results in the ElastiCache cluster.

Amazon ElastiCache can be used to cache frequently accessed data, reducing the load on the database. This is particularly effective for read-heavy workloads, as it allows the application to retrieve data from the cache rather than making repeated database queries.

upvoted 3 times

Question #675

A company uses Amazon EC2 instances and Amazon Elastic Block Store (Amazon EBS) volumes to run an application. The company creates one snapshot of each EBS volume every day to meet compliance requirements. The company wants to implement an architecture that prevents the accidental deletion of EBS volume snapshots. The solution must not change the administrative rights of the storage administrator user.

Which solution will meet these requirements with the LEAST administrative effort?

A. Create an IAM role that has permission to delete snapshots. Attach the role to a new EC2 instance. Use the AWS CLI from the new EC2 instance to delete snapshots.

B. Create an IAM policy that denies snapshot deletion. Attach the policy to the storage administrator user.

C. Add tags to the snapshots. Create retention rules in Recycle Bin for EBS snapshots that have the tags.

D. Lock the EBS snapshots to prevent deletion.

Correct Answer: *D*

Community vote distribution

D (100%)

meenkaza 2 days, 19 hours ago

Selected Answer: D

Locking EBS Snapshots (Option D): The "lock" feature in AWS allows you to prevent accidental deletion of resources, including EBS snapshots. This can be set at the snapshot level, providing a straightforward and effective way to meet the requirements without changing the administrative rights of the storage administrator user.

upvoted 3 times

Question #676

A company's application uses Network Load Balancers, Auto Scaling groups, Amazon EC2 instances, and databases that are deployed in an Amazon VPC. The company wants to capture information about traffic to and from the network interfaces in near real time in its Amazon VPC. The company wants to send the information to Amazon OpenSearch Service for analysis.

Which solution will meet these requirements?

A. Create a log group in Amazon CloudWatch Logs. Configure VPC Flow Logs to send the log data to the log group. Use Amazon Kinesis Data Streams to stream the logs from the log group to OpenSearch Service.

B. Create a log group in Amazon CloudWatch Logs. Configure VPC Flow Logs to send the log data to the log group. Use Amazon Kinesis Data Firehose to stream the logs from the log group to OpenSearch Service.

C. Create a trail in AWS CloudTrail. Configure VPC Flow Logs to send the log data to the trail. Use Amazon Kinesis Data Streams to stream the logs from the trail to OpenSearch Service.

D. Create a trail in AWS CloudTrail. Configure VPC Flow Logs to send the log data to the trail. Use Amazon Kinesis Data Firehose to stream the logs from the trail to OpenSearch Service.

Correct Answer: *B*

Community vote distribution

B (100%)

meenkaza 2 days, 19 hours ago

Selected Answer: B

Amazon CloudWatch Logs and VPC Flow Logs (Option B): VPC Flow Logs capture information about the IP traffic going to and from network interfaces in a VPC. By configuring VPC Flow Logs to send the log data to a log group in Amazon CloudWatch Logs, you can then use Amazon Kinesis Data Firehose to stream the logs from the log group to Amazon OpenSearch Service for analysis. This approach provides near real-time streaming of logs to the analytics service.

upvoted 2 times

Question #677

A company is developing an application that will run on a production Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The EKS cluster has managed node groups that are provisioned with On-Demand Instances.

The company needs a dedicated EKS cluster for development work. The company will use the development cluster infrequently to test the resiliency of the application. The EKS cluster must manage all the nodes.

Which solution will meet these requirements MOST cost-effectively?

A. Create a managed node group that contains only Spot Instances.

B. Create two managed node groups. Provision one node group with On-Demand Instances. Provision the second node group with Spot Instances.

C. Create an Auto Scaling group that has a launch configuration that uses Spot Instances. Configure the user data to add the nodes to the EKS cluster.

D. Create a managed node group that contains only On-Demand Instances.

Correct Answer: *B*

Community vote distribution

B (100%)

cciesam 1 day, 16 hours ago

Selected Answer: B

B is the best ans.

upvoted 1 times

Naijaboy99 2 days, 8 hours ago

Option B

upvoted 2 times

Question #678

A company stores sensitive data in Amazon S3. A solutions architect needs to create an encryption solution. The company needs to fully control the ability of users to create, rotate, and disable encryption keys with minimal effort for any data that must be encrypted.

Which solution will meet these requirements?

A. Use default server-side encryption with Amazon S3 managed encryption keys (SSE-S3) to store the sensitive data.

B. Create a customer managed key by using AWS Key Management Service (AWS KMS). Use the new key to encrypt the S3 objects by using server-side encryption with AWS KMS keys (SSE-KMS).

C. Create an AWS managed key by using AWS Key Management Service (AWS KMS). Use the new key to encrypt the S3 objects by using server-side encryption with AWS KMS keys (SSE-KMS).

D. Download S3 objects to an Amazon EC2 instance. Encrypt the objects by using customer managed keys. Upload the encrypted objects back into Amazon S3.

Correct Answer: B

Community vote distribution

B (100%)

Riajul 2 days, 6 hours ago

Selected Answer: B

Option B should be correct

upvoted 1 times

meenkaza 2 days, 19 hours ago

Selected Answer: B

SSE-KMS with Customer Managed Key (Option B): This option allows you to create a customer managed key using AWS KMS. With a customer managed key, you have full control over key lifecycle management, including the ability to create, rotate, and disable keys with minimal effort. SSE-KMS also integrates with AWS Identity and Access Management (IAM) for fine-grained access control.

upvoted 3 times

Question #679

A company wants to back up its on-premises virtual machines (VMs) to AWS. The company's backup solution exports on-premises backups to an Amazon S3 bucket as objects. The S3 backups must be retained for 30 days and must be automatically deleted after 30 days.

Which combination of steps will meet these requirements? (Choose three.)

A. Create an S3 bucket that has S3 Object Lock enabled.

B. Create an S3 bucket that has object versioning enabled.

C. Configure a default retention period of 30 days for the objects.

D. Configure an S3 Lifecycle policy to protect the objects for 30 days.

E. Configure an S3 Lifecycle policy to expire the objects after 30 days.

F. Configure the backup solution to tag the objects with a 30-day retention period

Correct Answer: *ACE*

Community vote distribution

ACE (50%) | ADE (50%)

PegasusForever 1 day, 11 hours ago

ABE -> https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html
A. Create an S3 bucket that has S3 Object Lock enabled. -> You set a Retention period of 30 days with this feature.
B. Create an S3 bucket that has object versioning enabled -> Object Lock works only in buckets that have S3 Versioning enabled
E. Configure an S3 Lifecycle policy to expire the objects after 30 days. -> It is valid using the lifecicle policy.

upvoted 1 times

cciesam 1 day, 15 hours ago

Selected Answer: ACE

ACE is the correct ans.

upvoted 2 times

Riajul 2 days, 6 hours ago

Selected Answer: ADE

ADE should be correct

upvoted 1 times

Naijaboy99 2 days, 8 hours ago

Correct Answer is A C E

upvoted 1 times

meenkaza 2 days, 19 hours ago

Selected Answer: ADE

A. Create an S3 bucket that has S3 Object Lock enabled.

S3 Object Lock provides the ability to enforce retention periods on objects, preventing deletion or modification for a specified duration.
D. Configure an S3 Lifecycle policy to protect the objects for 30 days.

By configuring a lifecycle policy, you can define a transition action to move objects to the S3 Glacier storage class (or any other storage class) after 30 days.
E. Configure an S3 Lifecycle policy to expire the objects after 30 days.

upvoted 1 times

Question #680

A solutions architect needs to copy files from an Amazon S3 bucket to an Amazon Elastic File System (Amazon EFS) file system and another S3 bucket. The files must be copied continuously. New files are added to the original S3 bucket consistently. The copied files should be overwritten only if the source file changes.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create an AWS DataSync location for both the destination S3 bucket and the EFS file system. Create a task for the destination S3 bucket and the EFS file system. Set the transfer mode to transfer only data that has changed.

B. Create an AWS Lambda function. Mount the file system to the function. Set up an S3 event notification to invoke the function when files are created and changed in Amazon S3. Configure the function to copy files to the file system and the destination S3 bucket.

C. Create an AWS DataSync location for both the destination S3 bucket and the EFS file system. Create a task for the destination S3 bucket and the EFS file system. Set the transfer mode to transfer all data.

D. Launch an Amazon EC2 instance in the same VPC as the file system. Mount the file system. Create a script to routinely synchronize all objects that changed in the origin S3 bucket to the destination S3 bucket and the mounted file system.

Correct Answer: *A*

Community vote distribution

A (100%)

cciesam 1 day, 15 hours ago

Selected Answer: A

ans: A

upvoted 2 times

meenkaza 2 days, 19 hours ago

AWS DataSync (Option A): AWS DataSync is designed for efficient and reliable copying of data between different storage solutions. By setting up an AWS DataSync task with the transfer mode set to transfer only data that has changed, you ensure that only the new or modified files are copied. This minimizes data transfer and operational overhead.

upvoted 4 times

Question #681

A company uses Amazon EC2 instances and stores data on Amazon Elastic Block Store (Amazon EBS) volumes. The company must ensure that all data is encrypted at rest by using AWS Key Management Service (AWS KMS). The company must be able to control rotation of the encryption keys.

Which solution will meet these requirements with the LEAST operational overhead?

A. Create a customer managed key. Use the key to encrypt the EBS volumes.

B. Use an AWS managed key to encrypt the EBS volumes. Use the key to configure automatic key rotation.

C. Create an external KMS key with imported key material. Use the key to encrypt the EBS volumes.

D. Use an AWS owned key to encrypt the EBS volumes.

Correct Answer: *A*

Community vote distribution

A (100%)

fea9bdf 18 hours, 46 minutes ago

Answer is C
Details are on this link below:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/default-bucket-encryption.html
Amazon S3 buckets have bucket encryption enabled by default, and new objects are automatically encrypted by using server-side encryption with Amazon S3 managed keys (SSE-S3). This encryption applies to all new objects in your Amazon S3 buckets, and comes at no cost to you.

If you need more control over your encryption keys, such as managing key rotation and access policy grants, you can elect to use server-side encryption with AWS Key Management Service (AWS KMS) keys (SSE-KMS), or dual-layer server-side encryption with AWS KMS keys (DSSE-KMS). For more information about SSE-KMS, see Specifying server-side encryption with AWS KMS (SSE-KMS). For more information about DSSE-KMS, see Using dual-layer server-side encryption with AWS KMS keys (DSSE-KMS).

upvoted 1 times

Riajul 2 days, 6 hours ago

Should be option A

upvoted 1 times

Naijaboy99 2 days, 8 hours ago

option B is the correct answer with least operational overhead on admins

upvoted 1 times

Naijaboy99 2 days, 8 hours ago

@meenkaza was right the answer is A

upvoted 1 times

meenkaza 2 days, 19 hours ago

Selected Answer: A

option A (Create a customer managed key. Use the key to encrypt the EBS volumes) is the most suitable option with the least operational overhead for the given requirements.

upvoted 3 times

Question #682

A company needs a solution to enforce data encryption at rest on Amazon EC2 instances. The solution must automatically identify noncompliant resources and enforce compliance policies on findings.

Which solution will meet these requirements with the LEAST administrative overhead?

A. Use an IAM policy that allows users to create only encrypted Amazon Elastic Block Store (Amazon EBS) volumes. Use AWS Config and AWS Systems Manager to automate the detection and remediation of unencrypted EBS volumes.

B. Use AWS Key Management Service (AWS KMS) to manage access to encrypted Amazon Elastic Block Store (Amazon EBS) volumes. Use AWS Lambda and Amazon EventBridge to automate the detection and remediation of unencrypted EBS volumes.

C. Use Amazon Macie to detect unencrypted Amazon Elastic Block Store (Amazon EBS) volumes. Use AWS Systems Manager Automation rules to automatically encrypt existing and new EBS volumes.

D. Use Amazon inspector to detect unencrypted Amazon Elastic Block Store (Amazon EBS) volumes. Use AWS Systems Manager Automation rules to automatically encrypt existing and new EBS volumes.

Correct Answer: *A*

Community vote distribution

A (100%)

meenkaza 2 days, 19 hours ago

Selected Answer: A

IAM Policy and AWS Config (Option A): By creating an IAM policy that allows users to create only encrypted EBS volumes, you proactively prevent the creation of unencrypted volumes. Using AWS Config, you can set up rules to detect noncompliant resources, and AWS Systems Manager Automation can be used for automated remediation. This approach provides a proactive and automated solution.

upvoted 4 times

Question #683

A company is migrating its multi-tier on-premises application to AWS. The application consists of a single-node MySQL database and a multi-node web tier. The company must minimize changes to the application during the migration. The company wants to improve application resiliency after the migration.

Which combination of steps will meet these requirements? (Choose two.)

A. Migrate the web tier to Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer.

B. Migrate the database to Amazon EC2 instances in an Auto Scaling group behind a Network Load Balancer.

C. Migrate the database to an Amazon RDS Multi-AZ deployment.

D. Migrate the web tier to an AWS Lambda function.

E. Migrate the database to an Amazon DynamoDB table.

Correct Answer: AC

Community vote distribution

AC (100%)

fea9bdf 18 hours, 56 minutes ago

Also Dynamo DB is noSQL, that can not be an option here

upvoted 1 times

Naijaboy99 2 days, 8 hours ago

option A C

upvoted 1 times

meenkaza 2 days, 19 hours ago

Selected Answer: AC

Web Tier Migration (Option A): Migrating the web tier to Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB) provides horizontal scalability, automatic scaling, and improved resiliency. Auto Scaling helps in managing and maintaining the desired number of EC2 instances based on demand, and the ALB distributes incoming traffic across multiple instances.

Database Migration to Amazon RDS Multi-AZ (Option C): Migrating the database to Amazon RDS in a Multi-AZ deployment provides high availability and automatic failover. In a Multi-AZ deployment, Amazon RDS maintains a standby replica in a different Availability Zone, and in the event of a failure, it automatically promotes the replica to the primary instance. This enhances the resiliency of the database.

upvoted 4 times

Question #684

A company wants to migrate its web applications from on premises to AWS. The company is located close to the eu-central-1 Region. Because of regulations, the company cannot launch some of its applications in eu-central-1. The company wants to achieve single-digit millisecond latency.

Which solution will meet these requirements?

A. Deploy the applications in eu-central-1. Extend the company's VPC from eu-central-1 to an edge location in Amazon CloudFront.

B. Deploy the applications in AWS Local Zones by extending the company's VPC from eu-central-1 to the chosen Local Zone.

C. Deploy the applications in eu-central-1. Extend the company's VPC from eu-central-1 to the regional edge caches in Amazon CloudFront.

D. Deploy the applications in AWS Wavelength Zones by extending the company's VPC from eu-central-1 to the chosen Wavelength Zone.

Correct Answer: *D*

Community vote distribution

D (100%)

Naijaboy99 2 days, 8 hours ago

option B

upvoted 2 times

meenkaza 2 days, 19 hours ago

Selected Answer: D

AWS Wavelength (Option D): AWS Wavelength Zones bring AWS services to the edge of the 5G network, providing ultra-low latency for applications that require single-digit millisecond latencies. Deploying applications in Wavelength Zones allows the company to extend its VPC from the eu-central-1 Region to the chosen Wavelength Zone, providing the required low-latency access.

upvoted 2 times