

Exam Session - Cert Prep: Certified Solutions Architect

 cloudacademy.com/quiz/exam/3795309/results

#1

You are designing the compute resources for a cloud-native application that you will host on AWS. You want to configure auto scaling groups, to increase the compute layer's resilience and responsiveness. However, your IT management team has one concern. They want the ability to optimize the Amazon EC2 instances within an auto scaling group as easily and with as little downtime as possible after it has been launched. What is the best way to meet this requirement?



Associate the auto scaling group with a launch template. When you need to update the instances within the autoscaling group, create a new version of the launch template and assign it to the autoscaling group.



Associate the auto scaling group with a launch template. When you need to update the instances within the autoscaling group, stop the instances, modify them, and restart them.



Associate the Auto Scaling Group with a launch configuration. When you need to update the instances within the autoscaling group, create and attach a new launch configuration to the Auto Scaling Group.



Associate the auto scaling group with a launch template. When you need to update the instances within the autoscaling group, delete the existing template and create and attach a new launch template.

Explanation

A launch configuration is a template that the Auto Scaling group uses to launch Amazon EC2 instances. You create the launch configuration by including information such as the Amazon Machine Image ID to use for launching the EC2 instance, the instance type, key pairs, security groups, and block device mappings, among other configuration settings. When you create your Auto Scaling group, you must associate it with a launch configuration. You can attach only one launch configuration to an Auto Scaling group at a time.

Launch configurations cannot be modified. They are immutable.

If you want to change the launch configuration of your Auto Scaling group, you have to first create a new launch configuration and then update your Auto Scaling group by attaching the new launch configuration.

When you attach a new launch configuration to your Auto Scaling group, any new instances are launched using the new configuration parameters. Existing instances are not affected.

Launch templates work very differently. You can have multiple versions of a launch template saved, and disassociate one version from an auto scaling group and replace it with another without deleting any existing templates or stop and restarting your auto scaling group.

 <https://docs.aws.amazon.com/autoscaling/ec2/userguide/LaunchTemplates.html>

Covered in this lecture

Components of EC2 Auto Scaling

Course: Using Elastic Load Balancing & EC2 Auto Scaling to Support AWS Workloads



14m



#2

To optimize the cost associated with your application's compute layer, your development team decided to integrate spot instances to support spikes in your workload. However, your auto scaling group should always contain eight (8) on-demand or reserved instances to process the normal amount of requests, and deploy a combination of spot and on-demand instances to manage spikes of activity requiring more than eight (8) instances. How can you ensure there are always eight (8) on-demand instances to support your compute layers' typical workload?



Within your launch template, set the auto scaling group's minimum capacity to eight (8) instances.



Within your launch template, set the auto scaling group's optional on-demand base to eight (8) instances.




Within your launch template, set the auto scaling group's desired capacity to eight (8) instances.



Within your launch template, set the instance weighting for on-demand instances to eight (8) instances.

Explanation

When you want to include instances with multiple purchase types in the same auto scaling group, you have the ability to maintain a set number of on-demand instances will be deployed at all times, and then split the remaining instances between multiple purchase types as you see fit. To configure this, set a number of instances as your "optional on-demand base" within your launch template. This is not possible using a launch configuration.

 <https://docs.aws.amazon.com/autoscaling/ec2/userguide/asg-purchase-options.html>
#3

An advertising company is running all of its websites, databases, and file storage in the AWS cloud. They are hiring hundreds of new employees to manage regional advertising campaigns to be launched on multiple continents. The permissions for each employee will vary based on the employee's location and job title within the company, and management is concerned about consistently applying access to resources as new users are rapidly added to existing AWS accounts. What is the most efficient way to maintain consistency with a minimal amount of reorganizing the existing corporate access and policy structure in AWS?



Attach IAM policies to each IAM user based on their location and job title.



Create IAM groups based on location and job title and attach an IAM role to each group. Assign IAM users to their corresponding group.



Create IAM groups based on location and job title and attach IAM policies to each group. Assign IAM users to their corresponding group.



Create Organizational Units (OU) for each location and apply Service Control Policies for each Organizational Unit.


Explanation

The best choice here is to create IAM groups based on location and title, attach policies to each group, and then assign IAM users to each IAM group.

Assigning policies to each user would be inefficient and likely inconsistent.

Creating IAM groups and then assigning IAM roles to each group is not possible, as IAM roles can be assigned to IAM users who have a federated identity via an Identity Provider (IdP).

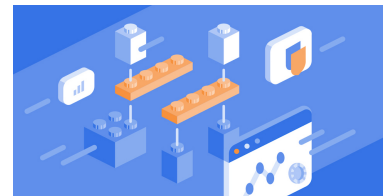
Creating Organizational Units and Service Control Policies would help manage permission boundaries across accounts, but would require additional set up and potential changes to the larger corporate security infrastructure, in addition to IAM identities and permissions. It also would not solve the issue because IAM policies for each user would still need to be put in place.

 <https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#use-groups-for-permissions>

Covered in this lecture

Conclusion

Course: Getting Started with an Amazon Web Services Solution: Real World Practices



3m



#4

As a member of the data management team, you are reviewing which Amazon EFS storage classes for the company's various data types. Approved scripts for app installation and troubleshooting are critical files for to day-to-day management, and are accessed frequently throughout the lifespan of each application. Which EFS storage class would be most effective for storing these approved scripts?



EFS Standard



EFS Standard-Infrequent Access (IA)



EFS One Zone



EFS One Zone-Infrequent Access (IA)

Explanation

EFS Standard and Standard-IA storage classes are regional storage classes that are designed to provide continuous availability to data, even when one or more Availability Zones in an AWS Region are unavailable. They offer the highest levels of availability and durability by storing file system data and metadata redundantly across multiple geographically separated Availability Zones within a Region.

The EFS Standard storage class is used for frequently accessed files. It is the storage class to which customer data is initially written for Standard storage classes.

 <https://docs.aws.amazon.com/efs/latest/ug/storage-classes.html>

#5

You're building a greenfield application hosted with the following configurations: Webserver: On a fleet of public-facing EC2 instances Microsoft SQL DB: on a secure Amazon EC2 instance You need to develop a solution for the database server that will ensure that this server is not accessible directly from the internet but can get accessibility when needed for patching and upgrades. Which of the following infrastructure security solutions would ensure these requirements are fulfilled?



Launch the database server in a private VPC, use AWS Outposts to provide secure internet access to the database when needed.



Launch the database server in a private subnet, use a NAT gateway for secure internet access to the database when needed.



Launch the database server behind an AWS CloudFront distribution, use a CloudFront signed url to expose the database for internet access securely when needed.



Launch the database server behind an Application Load Balancer, Create an ALB Listener to expose the database for internet access securely when needed.

Explanation

When you launch an instance, you launch it into a subnet in your VPC. You can use subnets to isolate the tiers of your application like web, application, and database servers within a single VPC. You can use private subnets for your instances if they should not be accessed directly from the internet. You can also use a NAT gateway for internet access from an instance in a private subnet as needed.

The remaining choices are incorrect for the following reasons:

- AWS Outposts is used to build and run applications on premises using the same programming interfaces as in AWS Regions, not for DB security.
- You can use the AWS CloudFront service to set up a distribution that will allow you to use edge servers to cache content down to globally distributed end users to allow for better performance of static data. AWS CloudFront does not provide protection for database servers.
- Application Load Balancers automatically distribute your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in one or more Availability Zones. It does not deal with security.

 <https://docs.aws.amazon.com/vpc/latest/userguide/infrastructure-security.html>

#6

A user is running a critical batch process which runs for 1 hour and 50 mins every day at a fixed time. Which option is the right instance type and purchase option in this case, assuming the user performs the same task for the next twelve months?



An EBS-backed scheduled reserved instance with partial instance pricing



An EBS-backed instance with standard reserved upfront instance pricing.



An Instance-store backed instance with spot instance pricing



An EBS-backed instance with on-demand instance pricing.

Explanation

For Amazon Web Services, the reserved instance (standard or convertible) helps the user save money if the user is going to run the same instance for a longer period. Generally if the user uses the instances around 30-40% of the year annually it is recommended to use RI. Here as the instance runs only for 1 hour 50 minutes daily, or less than 8 percent of the year, it is not recommended to have RI as it will be costlier.

At its highest potential savings, you are still paying 25 percent of an annual cost for a reserved instance you are using less than 2 hours a day, (or less than 8 percent of each year) you are not saving money.

Spot Instances are not ideal because the process is critical, and must run for a fixed length of time at a fixed time of day. Spot instances would stop and start based on fluctuations in instance pricing, leaving this process potentially unfinished.

The user should use on-demand with EBS in this case. While it has the highest cost, it also has the greatest flexibility to ensure that a critical process like this is always completed.

 <http://aws.amazon.com/ec2/purchasing-options/reserved-instances/>

#7

The average traffic to your online business has quadrupled in the last quarter and you are closely monitoring your database tier consisting of multiple Amazon RDS databases. You have configured CloudWatch alarms to monitor custom RDS metrics for read request latency and write throughput, but want to ensure these alarms are as responsive as possible. However, you have noticed a lag between when the alarm is triggered and when you receive an SNS notification about RDS performance. How can you increase the responsiveness of CloudWatch alarms for these existing RDS metrics? (Choose 2 answers)



Create CloudWatch Log metric filters for default metrics



Configure Route 53 CloudWatch Alarm Health Checks



Enable RDS Enhanced Monitoring



Enable Detailed Monitoring on CloudWatch

Explanation

Most of these choices improve the responsiveness of CloudWatch in some way, but the aspect of this question is **improving the responsiveness of CloudWatch alarms you have already implemented**. This means you are not interested in additional metric information outside of the custom metrics you've already created in CloudWatch, and any features that increase responsiveness to metrics other than what you want will not be beneficial.

So, creating CloudWatch Log metric filters for default RDS metrics will not help, even though this can provide 1-second granularity, it is unlikely the logs will indicate overall latency and throughput of reads and writes, as these performance metrics are not related to specific API calls, but rather general database performance.

Performance Insights allow you to review and analyze your RDS database performance overall, but is not ideal for identifying a performance issue in real-time.


Enabling Enhanced monitoring does provide increased insight into RDS database performance, and with the increased granularity of 5 seconds instead of 60 seconds, or potentially even 1-second granularity through CloudWatch Log Streams. However, Enhanced Monitoring provides specific operating system metrics and other performance metrics, and would not apply to the custom metric you have created using CloudWatch.

Enabling Detailed Monitoring will increase the delivery of average metrics from every 5 minutes to every minute, and this will apply to your custom metrics as well.

In addition, creating a Route 53 CloudWatch Alarm Health Check will monitor the transmission of data to CloudWatch, and can effectively alert you before the CloudWatch alarm is even triggered.

How does this alarm health check work? According to AWS:

When you create a health check that is based on a CloudWatch alarm, Route 53 monitors the data stream for the corresponding alarm instead of monitoring the alarm state. If the data stream indicates that the state of the alarm is OK, the health check is considered healthy. If the data stream indicates that the state is Alarm, the health check is considered unhealthy. If the data stream doesn't provide enough information to determine the state of the alarm, the health check status depends on the setting for Health check status: healthy, unhealthy, or last known status.

 <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-determining-health-of-endpoints.html#dns-failover-determining-health-of-endpoints-cloudwatch>

#8

The IT department at a pharmaceutical company plans to reduce the size of one of its data centers and needs to migrate some of the data stored on a network file system to the Amazon cloud. After the team migrates the files to the cloud, scientists and on-premises applications still need access to these resources as if they were still on site. The team is looking for an automated service that they can use to transfer the assets to the cloud and then continue accessing the files from on-premises after migration. Which combination of AWS services is the appropriate choice to migrate data from an on-premises network file system and continue to access these files in the cloud seamlessly from on-premises?



Use **AWS DataSync** to migrate the data and **AWS Storage Gateway (File Gateway)** to enable on-premises access to files in the AWS cloud.



Use **AWS Storage Gateway** to migrate the data and **AWS Direct Connect** to enable on-premises access to files in the AWS cloud.



Use **AWS Batch** to migrate the data and **AWS Direct Connect** to enable on-premises access to files in the AWS cloud.



Use **AWS Backup** to migrate the data and **AWS Storage Gateway (File Gateway)** to enable on-premises access to files in the AWS cloud.

Explanation

For this question, you need to identify which Amazon services you would use to: (1) Migrate on-premises data to Amazon cloud storage, and (2) enable seamless access to these resources from on-premises once migrated. Let's take a quick look at the services referenced in each of the choices and then determine which set of services is the best choice.

- AWS Direct Connect: AWS Direct Connect is a network service that allows organizations to connect their on-premises resources with AWS resources using a dedicated network connection that does not use the public internet. The team could decide to use Direct Connect as part of a solution to migrate its data; however, Direct Connect could not enable on-premises access to files in the AWS cloud as described in this scenario.
- AWS Storage Gateway: AWS Storage Gateway is a service that allows customers to connect their on-premises applications and resources to AWS cloud storage. There are three Storage Gateway services available: File Gateway, Volume Gateway, and Tape Gateway. The File Gateway in this scenario is the right choice to enable on-premises access to the files once you move the data to AWS.
- AWS Backup: AWS Backup is a service that allows you to automate and manage data backups for various Amazon services. For example, you can use AWS Backup to protect your data stored on EBS volumes, EFS, or Amazon RDS databases. To see a complete list of services that AWS Backup supports, take a look at the Developers Guide for more information. For the scenario presented in this question, AWS Backup is not the appropriate service because it cannot migrate data from on-premises to Amazon storage as described in the problem scenario. AWS Backup is used to back up data that is already in the AWS Cloud.

- AWS DataSync: AWS DataSync allows you to automatically transfer data from one storage location to another. A common use case is to use AWS DataSync to migrate data from on-premises to an AWS storage service, and this is precisely the scenario posed in this question. DataSync is not just for migrating on-premises data; You can also use AWS DataSync to move data from one AWS storage service to another from within AWS.
- AWS Batch: AWS Batch is a compute service that allows developers to package code and run batch jobs. This service is not the appropriate choice to migrate data from on-premises to an AWS storage service.

Of the services described above, DataSync is the best choice to migrate the data, and AWS File Gateway is the right choice to enable seamless access after you move data to AWS.

For more information, see this DataSync FAQ: "How does AWS DataSync convert files and folders to or from objects in Amazon S3?"

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

Covered in this lecture

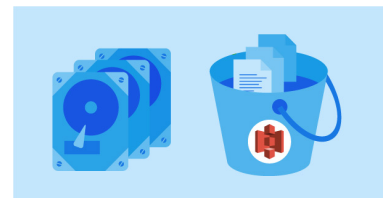
AWS Storage Services

Course:Storage Fundamentals for AWS

4m



#9



Your CFO is extremely concerned with your company's growing AWS bill and overloaded resources. Because your development and DevOps teams have both recently stood up new infrastructure, you are having a hard time finding which workflows can be modified to reduce costs. Which of the following resources would help identify ways to reduce costs and improve workload performance?



AWS Compute Optimizer



AWS Inspector



AWS Trusted Advisor



AWS Cost Explorer

Explanation

AWS Compute Optimizer recommends optimal AWS resources for your workloads to reduce costs and improve performance by using machine learning to analyze historical utilization metrics. Overprovisioning resources can lead to unnecessary infrastructure costs, and underprovisioning resources can lead to poor application performance. Compute Optimizer helps you choose optimal configurations for three types of AWS resources—e.g., Amazon Elastic Compute Cloud (EC2) instance types, Amazon Elastic Block Store (EBS) volumes, and AWS Lambda functions—based on your utilization data.

 <https://aws.amazon.com/compute-optimizer/>

#10

A DevOps team manages an EBS-backed Amazon EC2 instance that hosts a staging environment for a web-based application. The group does not have a backup for the staging environment and would like to set up a process to automatically back it up. If needed, the team should be able to launch a new instance to restore the staging environment from a backup, with each associated EBS volume automatically attached to the instance. The system should be backed up each day and retain the last five backups. Which of the following solutions could the DevOps team use to automate their EC2 backups and allow system recovery as described?



Use Amazon Data Lifecycle Manager to automate Amazon Machine Image (AMI) lifecycles.



Use AWS Backup to automate Amazon Machine Image (AMI) lifecycles.



Use AWS File Gateway to create and manage snapshots for EBS boot device volumes and data volumes.



Use the EBS snapshot service to automate Amazon Machine Image (AMI) lifecycles.


Explanation

In this problem scenario, we have an instance that uses EBS for its root device volume with one or more EBS data volumes. The problem states that we are looking for a way to automatically back up the system so that we can restore it completely from a recent snapshot.

The primary approach to backup EBS storage is using EBS snapshots. EBS snapshots allow you to back up EBS data and store the snapshots in S3. Each snapshot saves only the incremental changes that have occurred since the last snapshot. This approach helps reduce storage costs by not duplicating data with each backup. However, the snapshot service does not alone have a way to build policies to create, retain, and delete snapshots automatically. Also, these snapshots are not in the form of an Amazon Machine Image (AMI) snapshot as is needed in this case.

Luckily, there is a service that you can use to build policies to help create and manage EBS snapshots and AMIs automatically; the service is called Amazon Data Lifecycle Manager (DLM). In this case, you can use DLM to automate AMI lifecycles. For example, you can use DLM to create an EBS-backed AMI and then make additional snapshots regularly. Additionally, you can reduce storage needs by setting a policy to keep only a certain number of snapshots. EBS-backed AMIs automatically include a snapshot for each associated EBS volume.

The other services that appear in the remaining choices are not services that administrators would use to backup EBS volumes or automate AMI lifecycles.

 <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-ami-policy.html>

Covered in this lecture

Overview of EBS

Course: Introduction to Amazon Elastic Block Store (EBS)

10m



#11



You host two separate applications that utilize the same DynamoDB tables containing environmental data. The first application, which focuses on data analysis, is hosted on compute-optimized EC2 instances in a private subnet. It retrieves raw data, processes the data, and uploads the results to a second DynamoDB table. The second application is a public website hosted on general-purpose EC2 instances within a public subnet and allows researchers to view the raw and processed data online. For security reasons, you want both applications to access the relevant DynamoDB tables within your VPC rather than sending requests over the internet. You also want to ensure that while your data analysis application can retrieve and upload data to DynamoDB, outside researchers will not be able to upload data or modify any data through the public website. How can you ensure each application is granted the correct level of authorization? (Choose 2 answers)



Deploy a DynamoDB VPC endpoint in the data analysis application's private subnet, and a DynamoDB VPC endpoint in the public website's public subnet.



Deploy one DynamoDB VPC endpoint in its own subnet. Update the route tables for each application's subnet with routes to the DynamoDB VPC endpoint.



Configure and implement a single VPC endpoint policy to grant access to both applications.



Configure and implement separate VPC endpoint policies for each application.

Explanation

DynamoDB VPC endpoints are Gateway endpoints. You can configure multiple gateway endpoints in a single VPC for the same AWS service, and route different resources to different gateways with different policies based on the specific permissions granted to those resources.



<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html>

#12

A company uses Amazon DynamoDB for a serverless application with Amazon DynamoDB Accelerator (DAX) for caching. The company will be doubling its customer base and wants to ensure the database solution can scale and handle the increased read traffic. The development team has been monitoring the cache hit rates using Amazon Cloud watch and noticed that hit rates are high when the ratio of read to write traffic is high. Which action should the solutions architect recommend in this case to ensure the application can perform well with increased traffic?



Use larger DAX cluster nodes



Enable autoscaling on the DynamoDB table




Add read replicas to the DAX cluster



Create global secondary indexes on the DynamoDB table

Explanation

Adding read replicas to the DAX cluster can help improve the throughput.

 <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DAX.cluster-management.html#DAX.cluster-management.scaling.node-types>

#13

You've been assigned a new client that hosts a stateless proprietary application on four EC2 reserved instances in an existing AWS cloud environment. Additionally, they have two reserved instances reading from a queue. Examining historical performance data, you determine that a large traffic spike occurs during their fiscal year processing in late June. What changes can you make to your EC2 instances to maintain the application's resiliency, improve performance, and reduce cost? (Choose 2 answers)

✗

Register the Reserved instances with a Load Balancer for the queuing.

✓

Assign Spot Instances to interact with the queue for cost savings.

✓

Configure an Amazon EC2 Auto Scaling group of on-demand instances to address the June spike.

✗

Add Spot instances for the expected traffic spike in June.

Explanation

Reserved instances are the best value for steady traffic over an extended period. Licensing agreements for reserved instances can be 1 or 3 years. On-demand instances are perfect for handling short-term traffic spikes. Spot instances are the best value for non-critical applications that can afford to be stopped. Trusted Advisor can provide valuable information on your instance utilization relative to cost savings.

 <https://aws.amazon.com/ec2/pricing/reserved-instances/pricing/>

#14

A library has several 19th-century materials in its collections. It wants to digitize the resources so they can be used by international researchers interested in textual analysis. Which of the following services can the library use for optical character recognition?



Amazon Textract



Amazon Transcribe



Amazon Comprehend



Amazon Rekognition

Explanation

Amazon Textract is a machine learning service that applies optical character recognition (OCR) to extract text from a variety of documents including printed text as well as handwriting.

The remaining choices are incorrect for the following reasons:

Amazon Transcribe is a service that uses deep learning, specifically automatic speech recognition (ASR), for quick and accurate speech-to-text conversions.

Amazon Comprehend uses natural language processing (NLP) to derive insights from text including meaning, relationships, and sentiment.

Amazon Rekognition provides image and video analysis capabilities including object identification and labeling.



<https://aws.amazon.com/textract/>

#15

Your client is a legal firm with offices in New York and Boston. You have gathered all of the requirements and have started designing their AWS cloud environment. The design calls for a VPC for the New York office and a VPC for the Boston office. The client wants this separation for billing purposes and other considerations. But they have a need for interoperability between the two VPCs. How can you best meet this requirement?



Set up Direct Connect between the two VPCs.



Set up a VPC Peering connection.



Set up a VPN between the two VPCs.



Place an Internet Gateway between the two VPCs.

Explanation

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account.



<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html>

#16

A company is using EC2 instances to run their website behind an Application Load Balancer (ALB). The engineering team wants to terminate encrypted connections at the Load Balancer, using Secure Sockets Layer (SSL) protocol, without having the need to manage SSL connections at the EC2 instances. The company does not have an SSL certificate available yet. What should you use to meet this requirement and follow AWS security best practices? (Choose 2 answers)



Buy a third-party SSL certificate and assign it to the load balancer.



Use an HTTPS listener in the Application Load Balancer.



Deploy another EC2 instance in front of the existing EC2 instances. Install and run HAProxy software on the instance.



Assign an SSL certificate issued by AWS Certificate Manager (ACM) to the load balancer.

Explanation

AWS Certificate Manager (ACM) handles the complexity of creating, storing, and renewing public and private SSL/TLS X.509 certificates and keys that protect your AWS websites and applications. You can provide certificates for your integrated AWS services either by issuing them directly with ACM or by importing third-party certificates into the ACM management system. ACM certificates can secure singular domain names, multiple specific domain names, wildcard domains, or combinations of these. These certificates are used to terminate the encrypted connection received from remote clients. The request is then decrypted and redirected to the resources in the Application Load Balancer target group.

IAM certificates should be used only when you must support an SSL connection in an AWS Region that does not support AWS Certificate Manager (ACM) certificates.

As the company didn't already have a certificate, using ACM simplifies the configuration process of implementing a new certificate.

 <https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html>

#17

Your company needs a solution to graph process data from industrial IoT devices and various supporting systems for customers operating in seafood processing. The requirements for the graphing solution are: It must provide graphs and visualization There cannot be any complex IT integrations You should be able to track metrics from both AWS and external sources and It must support multi-source, multi-account and multi-region dashboards Which of the following AWS services would best fulfill these requirements?



AWS Managed Grafana



AWS Managed Prometheus




Amazon Quicksight



AWS CloudWatch

Explanation

Amazon Managed Grafana is a fully managed service for open-source Grafana developed in collaboration with Grafana Labs. Grafana is a popular open-source analytics platform that enables you to query, visualize, alert, and understand your metrics no matter where they are stored.

 <https://docs.aws.amazon.com/prescriptive-guidance/latest/implementing-logging-monitoring-cloudwatch/amg-dashboarding-visualization.html>

#18

A company manages DynamoDB databases to store online transaction-related data such as sales, returns, and inventory changes. After suffering a critical failure in a single region, the company wants to restore backups from snapshots in a primary region to multiple secondary regions as the first step toward a responsive disaster recovery plan. The company wants to move quickly with the least administrative effort and the lowest cost to implement database restores in multiple regions. How can a solutions architect effectively address the company's requirements?



Enable On-Demand backup and restore using DynamoDB backups



Enable On-Demand backup and restore using AWS Backup



Enable continuous backups with point-in-time recovery



Deploy a DynamoDB Accelerator (DAX) cluster

Explanation

You can restore the table to the same AWS Region or to a different Region from where the backup resides. You can also exclude secondary indexes from being created on the new restored table. In addition, you can specify a different encryption mode.

The other restore options, besides deploying DAX, could also restore across regions but not with the same efficiency or cost.



<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/RestoreTutorial.ht>

ml

#19

You are deploying a two-tiered web application with web servers hosted on Amazon EC2 in a public subnet of your VPC and your database tier hosted on RDS instances isolated in a private subnet. Your requirements call for the web tier to be highly available. Which services listed will be needed to make the web-tier highly available? (Choose 3 answers)



Elastic Load Balancer



Route 53



EC2 Auto Scaling



RDS Read replicas

Explanation

The key is that the requirement is for high availability at the web-tier. While multi-AZ deployments and cross-region replication can contribute to high availability, they are each at the storage tier. Route 53 with Health Checks and Failover, Elastic Load Balancer (with health checks and various forms of load balancing, and auto scaling groups create high availability at the web tier.



</course/design-multi-tier-architectures/saa-d1-designing-solutions/>

#20

A genomics company stores petabytes of data for scientists in its R&D department to run various scientific computations. The company is planning to move this data from an on-premises data center to AWS, and they need to select an AWS storage service that will allow them to access this shared data from multiple EC2 instances. The EC2 instances will run a suite of existing scientific tools that expect the data to be in POSIX files and need random read/write access to each file's data. Which storage solution is the appropriate choice to store this data?



Elastic File System (EFS)



Elastic Block Storage (EBS)



Simple Storage Service (S3)



ElastiCache

Explanation

Let's take a look at Amazon's storage solutions and see which would be the right choice for shared access between multiple EC2 instances:

- Elastic Block Storage (EBS): EBS provides block-level storage for your EC2 instances for persistent and durable data storage. EBS is an appropriate choice for storing frequently changing data or if you have specific IOPS requirements. You can attach one or more EBS volumes to an EC2 instance; however, multiple EC2 instances cannot share EBS storage.
- Simple Storage Service (S3): Amazon S3 is a highly available, highly durable object-based storage service that is cost-effective and accessible. Multiple EC2 instances can access this storage, but it might not be the best choice if applications running on the EC2 instance need access to a mounted file system. You cannot mount S3 storage to an EC2 instance. Also, since the applications accessing the files are expecting POSIX files, S3 would not be the right choice.
- ElastiCache: Amazon ElastiCache is a database service, not a storage service like the other options. ElastiCache provides an in-memory cache used by distributed applications to share data. ElastiCache is not associated with EC2 instances for shared storage as required in this scenario.
- Elastic File System (EFS): Amazon EFS is file-level storage optimized for low latency access that appears to users like a file manager interface. EFS uses standard file system semantics such as locking files, renaming files, updating files, and uses a hierarchy structure. You can mount EFS storage to multiple EC2 instances to enable concurrent access to the file system. Also, EFS would support POSIX files as required by the scientific tools the team is using.

From these storage solutions, only EFS will provide the shared storage we are looking for in this scenario.



<https://docs.aws.amazon.com/efs/latest/ug/whatisefs.html>

Covered in this lecture

AWS Storage and Database

9m



#21



A team of solutions architects designed an eCommerce website. The team is concerned about API calls from malicious IP addresses or anomalous behaviors. They would like an intelligent service to continuously monitor their AWS accounts and workloads and then deploy AWS Lambda functions for remediations. How would the solutions architects protect this web presence against the threats that they are concerned about?



Deploy Amazon GuardDuty on their AWS account and workloads.



Monitor their AWS account and workloads with Amazon Cognito



Enable Amazon Inspector on their AWS account and workloads.



Monitor their AWS account and workloads with Amazon CloudWatch

Explanation

Amazon GuardDuty is a threat detection service that continuously monitors AWS accounts and workloads for malicious activity and anomalous behavior. Amazon GuardDuty utilizes machine learning to identify the threats and classify them. The team can leverage AWS CloudWatch events and AWS Lambda functions to trigger automated remediation or prevention. Amazon GuardDuty is the service that this team needs.

The remaining choices are incorrect for the following reasons:

Amazon Cognito is a service for user sign-up/sign-in and access management to web and mobile applications. Amazon Cognito does not monitor AWS accounts and workloads for threats.

Amazon Inspector is a vulnerability management service; it scans AWS workloads for software vulnerabilities and unintended network exposure. Amazon Inspector is a security assessment service that does not use machine learning to detect malicious activities or anomalous behaviors.

Amazon CloudWatch enables monitoring and observability of the resources through data collection, assessment, and correlation. Although CloudWatch collects logs on API calls anomalies, it does not intelligently detect API calls from malicious IP addresses or warn of anomalous behaviors.

Amazon CodeGuru automates code reviews and optimizes application performance with machine learning powered recommendations. CodeGuru provides machine learning capabilities and is not a security or compliance service.

 <https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html>

#22

An IT department currently manages Windows-based file storage for user directories and department file shares. Due to increased costs and resources required to maintain this file storage, the company plans to migrate its files to the cloud and use Amazon FSx for Windows Server. The team is looking for the appropriate configuration options that will minimize their costs for this storage service. Which of the following FSx for Windows configuration options are cost-effective choices the team can make in this scenario? (Choose 2 answers)



Choose the HDD storage type when creating the file system.



Enable data deduplication for the file system.



Choose the SSD storage type when creating the file system.



Select a large custom throughput capacity relative to the storage capacity.

Explanation

When you create an Amazon FSx for Windows file system, several configuration selections impact your costs:

- Storage Capacity, Storage Type (HDD or SSD)
- Throughput Capacity
- Deployment type (single-AZ or multi-AZ)
- Enabling backups

In addition to managing costs by making the appropriate configuration choices, you can also choose to enable data deduplication for the file system. This step can reduce your storage costs by 30 - 80% by reducing the amount of data you store in your file system.

In this problem scenario, the IT team needs storage to support user directories and department file shares. The primary choice that will drive the cost here is the type of storage for the file system. The HDD storage type is the lowest cost and most appropriate for the workload needed to support home directories; SSD is more expensive and provides more performance than is required for this workload. Finally, the team can enable data deduplication to reduce costs for the configuration further.

The problem and choice list do not mention the need for a Multi-AZ deployment or backups. However, both of these options would increase costs.

 <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/optimize-fsx-costs.html>

#23

A law firm uses Amazon DynamoDB as the data store for an application that requires reads and writes. There is also a long-running, read-intensive data analysis job scheduled every week. While the analysis is running, customers often report issues accessing data elements within the application. Which of the following solutions can the solutions architect implement to resolve this?



Create a DAX cluster and a corresponding IAM Service Role for DynamoDB Access. Run reports against the cached data.



Create a DAX table and a corresponding IAM User for DynamoDB Access. Run reports against the cached data.



Use a DynamoDB Stream to capture data changes. Run the application using the DynamoDB stream.



Use the DynamoDB on-demand backup feature to write snapshots of the table to S3. Run reports against the S3 data.

Explanation

Applications that perform repeated reads on a large data set, such as the data analysis, can impact performance by consuming all of the read capacity available for a table. By creating a DAX cluster and running the reports against the cached data, other applications accessing the same data source are not compromised.

Using an IAM role for access to DynamoDB access is considered a best practice compared to using an IAM user. Using an IAM role is best practice because the application can assume the appropriate role (and gain the associated permissions) without maintaining security credentials required to use an IAM user in this scenario.

Additional Resources

- [IAM Identities](#)
- [Common Scenarios for Roles](#)

 <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DAX.html>

#24

A company's container applications are managed with Kubernetes and hosted on Windows virtual servers. The company wants to migrate these applications to the AWS cloud, and needs a solution that supports Kubernetes pods hosted on Windows servers. It is essential that the solution manages the Kubernetes API servers and the etcd cluster. The company's development team would prefer that AWS manage the host instances and containers as much as possible, but is willing to manage them both if necessary. Which AWS service offers the best options for the developer's preferences and the company's essential requirement for their container application? (Choose 2 answers)



Amazon Elastic Compute Cloud (EC2)



Amazon Elastic Kubernetes Service (EKS) with EKS-managed node groups



Amazon Elastic Kubernetes Service (EKS) with self-managed node groups



Amazon Elastic Kubernetes Service (EKS) on AWS Fargate

Explanation

The key requirement in this question is Windows nodes and being sure which service option supports them and which does not.

In this question, the company wants AWS to manage as much as possible.

- AWS Fargate, which manages the highest level of management, does not support Windows. Amazon ECS supports Windows, but the Fargate EKS option does not.
- Amazon EKS with EKS-managed nodes does not support Windows nodes.
- Amazon EKS with self-managed nodes DOES support Windows nodes
- Amazon EC2 supports Windows, but is an IaaS service.

Therefore the best option is EKS with self-managed nodes.

 <https://docs.aws.amazon.com/eks/latest/userguide/eks-compute.html>

#25

Your company has recently discovered a massive security leak in which several users' access credentials were compromised. As a response, the Senior IT Security Manager has requested you to prevent all high-risk data from being modified or deleted by any users, including the root user. What is the most efficient way to implement this security measure?

✗

Migrate the high-risk data to new S3 buckets and enable object versioning. Enable MFA Delete for all buckets.

✓

Migrate the high-risk data to new S3 buckets and enable object locks. Configure a retention mode of compliance mode.

✗

Enable object versioning for all existing buckets with high-risk data. Enable a default legal hold for the bucket

✗

Enable object locks for all existing buckets with high-risk data. Configure a retention mode of governance mode.

Explanation

There are a few key points to this question:

1. Object locks can prevent objects from modification or deletion; objection versioning does not - it only maintains versions of an object until those versions are deleted.
2. Users can only enable Object locks can on new S3 buckets.

3. Object locks have two retention modes - governance mode and compliance mode. Compliance mode prevents objects from being deleted or updated by users, including the root user. Governance mode allows objects to be modified, but prevents objects from being deleted.

 <https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lock-overview.html#object-lock-retention-modes>

#26

You are the AWS account owner for a small IT company, with a team of developers assigned to your account as IAM users within existing IAM groups. New associate-level developers manage resources in the Dev/Test environments, and these resources are quickly launched, used, and then deleted to save on resource costs. The new developers have read-only permissions in the production environment. There is a complex existing set of buckets intended to separate Development and Test resources from Production resources, but you know this policy of separation between environments is not followed at all times. Your company needs to prevent new developers from accessing production environment files placed in an incorrect S3 bucket because these production-level objects are accidentally deleted along with other Dev/Test S3 objects. The ideal solution will prevent existing objects from being accidentally deleted and automatically minimize the problem in the future. What steps are the most efficient to continuously enforce the tagging best practices and apply the principle of least privilege within Amazon S3? (Choose 2 answers)



Assign IAM policies to the Dev/Test IAM group that authorize S3 object operation based on object tags.



Implement an object tagging policy using AWS Config's Auto Remediation feature.



Update all existing object tags to correctly reflect their environment using Amazon S3 batch operations.



Create an AWS Lambda function to check object tags for each new Amazon S3 object. An incorrect tag would trigger an additional Lambda function to fix the tag.

Explanation

One of the key benefits of object tagging is that it "enables fine-grained control of permissions." You also have the Auto Remediation feature within AWS Config to help not only alert you to non-compliant resources but automatically bring the resources into compliance based on permissions and actions you configure.

The other choices are not ideal. Batch operations are designed for updating millions to billions of objects at a time, and setting up a batch operation requires several steps. Going through these manual steps to ensure that very temporary resources are properly tagged is not efficient. Each batch operation is a one-time fix as well that would only address the issue for existing resources, and continue to allow non-compliant resources to be created.

The Lambda functions are not an efficient option because checking the tags for each S3 object would result in a large number of functions, and require manually configuring the lambda functions and ensuring that they work as designed. It would essentially be a manual, managed version of the service already available through AWS Config Auto Remediation.

 <https://docs.aws.amazon.com/AmazonS3/latest/dev/object-tagging.html>

#27

You are responsible for setting up a new Amazon EFS file system. The organization's security policies mandate that the file system store all data in an encrypted form. The organization does not need to control key rotation or policies regarding access to the KMS key. What steps should you take to ensure the data is encrypted at rest in this scenario?



When creating the EFS filesystem enable encryption using the default AWS-managed KMS key for Amazon EFS.



When creating the EFS filesystem enable encryption using a customer-managed KMS key.



When mounting the EFS filesystem to an EC2 instance, use the default AWS-managed KMS key to encrypt the data.



When mounting the EFS filesystem to an EC2 instance, use a customer-managed KMS key to encrypt the data.

Explanation

First, let's eliminate the choices suggesting mounting the EFS filesystem using either the AWS-managed KMS key or a customer-managed KMS key. These answers are incorrect because EFS encryption is not related to mounting the filesystem to an EC2 instance.

You enable encryption for an EFS filesystem when you create the filesystem. When setting up EFS encryption you have the choice to use an AWS-managed key or a customer-managed key. In this scenario, the customer does not need to manage the cryptographic key rotation or any policies associated with managing the key. Therefore the best choice would be to use the AWS-managed key. If the customer did have specific key rotation policies or update the policies associated with key management, then a customer-managed key would be a better choice.

 <https://docs.aws.amazon.com/efs/latest/ug/encryption-at-rest.html>

Covered in this lecture

Amazon Elastic File System

Course:Storage Fundamentals of AWS for Cloud Practitioner

8m



#28



A user is using an EC2 key pair to connect to an EC2 Linux instance backed by an Elastic Block Storage (EBS) volume. The same EC2 key pair that was created and downloaded at the moment the EC2 instance was deployed. The user has lost the EC2 key pair private key and is not able to connect to the EC2 instance via SSH anymore. What steps should the user follow to regain access to the EC2 instance? (Choose 2 answers)



Create a new EC2 key pair and assign it to the EC2 instance using the AWS Management Console.



Stop the instance, detach the root volume and attach it to another EC2 instance as a data volume.



Stop the instance, detach the root volume and attach it to another EC2 instance as the root volume.



Modify the `authorized_keys` file with a new public key, move the volume back to the original instance, and restart the instance.

Explanation

A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance. Amazon EC2 stores the public key, and you store the private key. You use the private key, instead of a password, to securely access your instances. When you launch an instance, you are prompted for a key pair. If you plan to connect to the instance using SSH, you must specify a key pair. You can choose an existing key pair or create a new one.

If you lose the private key for an EBS-backed instance, you can regain access to your instance. You must stop the instance, detach its root volume and attach it to another instance as a data volume, modify the `authorized_keys` file with a new public key, move the volume back to the original instance, and restart the instance. This procedure is not supported for instances with instance store-backed root volumes.

 <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/replacing-lost-key-pair.html>
#29

A new, small hotel chain has hired you to optimize an existing small, single-AZ RDS DB instance to manage reservations for their original location. They recently expanded to new locations and need to optimize their online reservation service. Incoming requests for reservations could double or triple their existing database size in a matter of hours, depending on how well their advertising works. With how much capital they invested in new locations, they value the availability of the database far above any cost concerns. During this peak period, the RDS database will need to manage an equal number of reads and writes. With a limited amount of time to prepare for a potential spike, what is the best single step to ensure the database remains available to schedule reservations with no loss of service?



Enable read replicas.



Enable multi-AZ configuration.



Enable Amazon RDS Storage Auto Scaling.



Manually modify the DB instance to a larger instance class.

Explanation

First, let's review the key pieces of information in this question:


1. They currently use a **small RDS instance** to manage reservations...
2. Incoming requests for reservations could **double or triple their existing database size in a matter of hours...**
3. the RDS database will need to manage **an equal number of reads and writes.**

To handle a large number of reads and writes will require scaling vertically. Read replicas are ideal for handling spikes in read requests, but will not effectively manage writes as well.

Multi-AZ configurations are a feature to enable high availability but are not designed to handle increased read or write workloads.

Storage auto scaling could handle storage limitations, but an influx of writes would overwhelm the small instances compute and memory limitations. It is also feasible that auto scaling would not scale fast enough, given how quickly the hotel business expects its database to double in size. Auto scaling increases database size gradually, and once the storage scales once, it cannot scale again for approximately six hours. (See [this link](https://aws.amazon.com/blogs/database/scaling-your-amazon-rds-instance-vertically-and-horizontally/) for more information.)

This is why the best choice is to manually modify the instance to a database DB class.

 <https://aws.amazon.com/blogs/database/scaling-your-amazon-rds-instance-vertically-and-horizontally/>

#30

Your company has recently acquired several small start-up tech companies within the last year. In an effort to consolidate your resources, you are gradually migrating all digital files to your parent company's AWS accounts, and storing a large number of files within an S3 bucket. You are uploading millions of files, to save costs, but have not had the opportunity to review many of the files and documents to understand which files will be accessed frequently or infrequently. What would be the best way to quickly upload the objects to S3 and ensure the best storage class from a cost perspective?



Upload all the files to the Amazon S3 Standard-IA storage class and review costs for access frequency over time.



Upload all files to the Amazon S3 Intelligent Tiering storage class and review costs related to the frequency of access over time.



Upload all files to the Amazon S3 Standard-IA storage class and immediately set up all objects to be processed with Storage Class Analysis.



Upload all the files to the Amazon S3 Standard storage class and review costs for access frequency over time.

Explanation

There are essentially three types of answers here - choices that use no automation, choices that use the incorrect type of automation given the situation, and a choice that uses the correct type of automation.

First, the choices that use little to no automation in this case would be the least recommended decision. Uploading millions of files to either Standard or Standard-IA and then waiting to review costs and access patterns could be very costly.

Second, the choice to use storage class analysis could work eventually, if you have the time to wait for analytics to be gathered (which could still be as costly as the choice above) and the time to then review the analytics, and then sift through the files to migrate them to the correct storage class. This is a better choice, but not the best choice.

Finally, the correct answer would be to use Intelligent_Tiering, which continuously monitors the access frequency and shifts the objects between a standard and infrequent-access tier depending on how access patterns may change. This happens automatically, and starts immediately, so it is the best choice of the options provided.



<https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html#sc-compare>

#31

The customer support team for an application that helps automotive service departments locate parts has seen an increase in support tickets reporting that end users are getting an HTTP 500-level error when they access the application. An AWS application load balancer sits in front of the application and appears healthy. After some investigation, the DevOps team determines that the errors result from connectivity issues between the load balancer and one or more targets in a target group. The team fixed the problem quickly but would like immediate notification if this situation arises again in the future. Which steps could the team take to enable monitoring and receive notifications if the load balancer responds to user requests with a 500-level error due to connection issues with one or more targets?



Set a CloudWatch Alarm to send an email notification if the number of 500-level response codes returned to the client from the load balancer exceeds some threshold.



Set up a CloudTrail event to send an email notification if the load balancer returns any 500-level response code to the client.



Create a Route 53 health check for each instance in the target group. The health check should use the HTTP protocol with the appropriate resource path and send an email notification if any target returns a 500-level error.



Update the health check settings associated with the target group. The health check should use the HTTP protocol with the appropriate resource path and enable email notification if any target returns a 500-level error.

Explanation

The Amazon CloudWatch service allows you to monitor your AWS resources with a wide range of metrics, including metrics you can use to monitor both your application load balancer and targets. CloudWatch is the solution we are looking for in this question.

In this scenario, we are concerned with being notified when the **load balancer** responds to user requests with a 500-level error. You can do this using the HTTPCode_ELB_5XX_Count metric in the AWS/ApplicationELB namespace for load balancers. Also, you can tell CloudWatch to notify you by email if this metric exceeds a particular threshold.

Let's also take a look at the incorrect choices:

- AWS CloudTrail is a service used to record and track AWS API requests. These API calls can be programmatic requests initiated utilizing the SDK, the command-line interface, from within the AWS management console, or even from a request made by another AWS service. CloudTrail does not track metrics like counting the number of 500-level errors returned by a load balancer.
- The choice that suggests using a Route 53 health check to monitor targets is incorrect for several reasons. Most importantly, the Route 53 health check's primary purpose is not to send notifications as a CloudWatch alarm would; Route 53 health checks exist to support DNS failover. Also, Route 53 health checks do not track metrics like counting the number of 500-level errors as a health check independently. A CloudWatch alarm would be necessary for that.

- You can not configure target group health checks to send email notifications.

 <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-cloudwatch-metrics.html>

#32

You're a web developer looking to write a quick function to allow your site users to upload their photos to a public S3 bucket. Where's the first place you should look before writing your own code to do this?



Amazon Elastic Container Registry



AWS Serverless Application Repository



GitHub



GitLab

Explanation

This quick upload function would be well-suited for AWS Lambda. To find commonly used lambda functions, you can look in the Serverless Application Repository on AWS. ECR is only used for Containers, which would be more overhead than necessary in this case. You could find functions on GitHub, but the import is faster when you go through SAR.

 <https://aws.amazon.com/serverless/serverlessrepo/>

#33

Your team manager requires all EBS volumes and snapshots to be encrypted, so the solutions architect enables EBS encryption by default for the team's AWS accounts. Now a team member is using an unencrypted EBS snapshot provided by another team to create a new EBS volume. What does the solutions architect need to do to ensure that the new EBS volume is encrypted?



No additional action is necessary. The volume from the unencrypted snapshot will automatically be encrypted. Create a new EBS volume from a copy of the unencrypted snapshot.



Manually enable encryption during when creating the volume. Otherwise the volume will not be encrypted.



Encrypt the unencrypted snapshot with the default AWS KMS, and then create a new EBS volume from the encrypted snapshot.



Use Amazon Data Lifecycle Manager to create a new encrypted EBS volume from the unencrypted snapshot.

Explanation

The best way to ensure that your EBS volumes are encrypted is to enable EBS **encryption by default** for the AWS Account. In this case, since encryption by default is enabled, there is no action you need to take to encrypt the volume at creation time; the system will automatically take care of it even if the snapshot is unencrypted. Though you can explicitly enable encryption during the creation process, it is not required.

Though Amazon Data Lifecycle Manager is a valuable service you can use to automate management tasks for EBS volumes and snapshots, you would not use it in this case to create a new encrypted EBS volume from an unencrypted snapshot.

Also, you would not directly encrypt the snapshot with the cryptographic key yourself.

Additional Resources

[Encryption by default](#)



<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#encryption-examples>

#34

Your company is concerned with potential poor architectural practices used by your core internal application. After recently migrating to AWS, you hope to take advantage of an AWS service that recommends best practices for specific workloads. As a Solutions Architect, which of the following services would you recommend for this use case?



AWS Well-Architected Tool



AWS Well-Architected Framework



AWS Trusted Advisor



AWS Inspector

Explanation

The AWS Well-Architected Tool is designed to help you review the state of your applications and workloads, and it provides a central place for architectural best practices and guidance. The AWS Well-Architected Tool is based on the AWS Well-Architected Framework, which was developed to help cloud architects build secure, high-performing, resilient, and efficient application infrastructures. The Framework has been used in thousands of workload reviews by AWS solutions architects. It provides a consistent approach for evaluating your cloud architecture and implementing designs that will scale with your application needs over time.

The remaining tools help more with vulnerabilities or cost savings rather than best practices, except for the Well-Architected Framework, which is not an AWS service.

 <https://aws.amazon.com/well-architected-tool/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>
#35

A pharmaceutical company is building an application that will use both AWS and on-premises resources. The application must comply with regulatory requirements and ensure the protection of intellectual property. One of the essential requirements is that data transferred between AWS and on-premises resources should not flow through the public internet. The company currently manages a single VPC with two private subnets in two different availability zones. Which solution would enable connectivity between AWS and on-premises resources while maintaining a private connection?



Use AWS Direct Connect with a virtual private gateway and a private virtual interface (private VIF).



Use AWS Transit Gateway to create a private site-to-site VPN connection.



Use a virtual private gateway with a customer gateway and create a site-to-site VPN connection.



Use AWS VPN CloudHub to create a private site-to-site VPN connection.


Explanation

Several AWS services are available to help organizations connect AWS cloud resources with their on-premises infrastructure. Using either AWS Direct Connect and a Virtual Private Gateway with a site-to-site VPN connection are standard solutions to help accomplish this goal. However, the key to this question is that the team is looking for a solution where the data transferred between AWS and on-premises resources **should not flow through the public internet**. Because AWS Direct Connect uses a dedicated network connection and does not use the public internet to connect AWS resources to an on-premises network, this is the correct choice. Using a virtual private gateway with a customer gateway to create a site-to-site VPN connection would work, but it uses existing internet connections.

Now, let's look at the other services mentioned in the remaining choices:

- Though the Transit Gateway service can help connect multiple VPCs together with an on-premises network, it alone will not establish a private connection as described in this scenario. A transit gateway can be used with either AWS Direct Connect or a virtual private gateway to connect VPCs with an on-premises network.
- AWS VPN CloudHub is a service that solutions architects can use with a virtual private gateway to connect multiple customer networks located at different locations. With the virtual private gateway, the remote sites can communicate with each other and the customer's Amazon VPCs.

For more information on options for connecting customer networks to Amazon VPCs, take a look at the Amazon Virtual Private Cloud Connectivity Options whitepaper.

 <https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect.html>

#36

A company stores its application data onsite using iSCSI connections to archival disk storage located at an on-premises data center. Now management wants to identify cloud solutions to back up that data to the AWS cloud and store it at minimal expense. The company needs to back up 200 TB of data to the cloud over the course of a month, and the speed of the backup is not a critical factor. The backups are rarely accessed, but when requested, they should be available in less than 6 hours. What are the most cost-effective steps to archiving the data and meeting additional requirements?

✗

- 1) Copy the data to Amazon S3 using AWS DataSync.
- 2) Store the data in Amazon S3 in the S3 Glacier Deep Archive storage class.

✓

- 1) Backup the data using AWS Storage Gateway volume gateways.
- 2) Store the data in Amazon S3 in the S3 Glacier Flexible Retrieval storage class.

✗

- 1) Copy the data to AWS Storage Gateway file gateways.
- 2) Store the data in Amazon S3 in the S3 Glacier Flexible Retrieval storage class.

✗

- 1) Migrate the data to AWS using an AWS Snowball Edge device.
- 2) Store the data in Amazon S3 in the S3 Glacier Deep Archive storage class.

Explanation

Review the questions and consider the key points in bold:

*A company stores its application data onsite using **iSCSI connections** to archival disk storage located at an on-premises data center. Now management wants to identify cloud solutions to backup that data to the cloud and store it at minimal expense.*

*The company needs to back up **200 TB** of data to the cloud over the course of a month, and the speed of the backup is not a critical factor. The backups are rarely accessed, but when requested, they should be available in less than 6 hours.*

What are the most cost-effective steps to archiving the data and meeting additional requirements? (Choose 2 answers)

So why is Storage Gateway the better option?

- It is cheaper - compare uploading 200 TB per month on each service using the [AWS Pricing Calculator](#). DataSync costs more than double what it does on Storage Gateway.
- Speed is not an issue - the main advantage of DataSync is that it is faster, so if speed is not an issue, you do not need DataSync.

- While the amount of data may be ideal for Snowball devices, this option is not as cost-effective. If this were a one-time data upload, or perhaps more sensitive data that should be migrated as securely as possible, then a Snowball device would be a better choice.

Why use S3 Glacier and not S3 Glacier Deep Archive?

You need to retrieve data from the tape gateway in less than 6 hours. This is possible with S3 Glacier storage, but not possible with S3 Glacier Deep Archive. See more information on storage classes [here](#).

 <https://aws.amazon.com/storagegateway/faqs/?nc=sn&loc=6>

#37

You are working on a 2 tier application hosted on a cluster of EC2 instances behind an application load balancer. During peak times, the webserver's auto-scaling group is configured to add additional servers when CPU utilization reaches 70% for the existing servers. Due to compliance requirements, only approved Amazon machine images can be utilized in the creation of servers for the application and all existing AMIs need to be compliant. You need to determine a way to monitor the EC2 instances for non-compliant amazon machine images and be alerted when a non-compliant image is in use. Which of the following monitoring solutions would provide the necessary visibility and alerting whenever a non-compliant AMI is in use?

✗

Enable AWS Inspector for the EC2 instances in the auto-scaling group. Utilize the AWS-managed rule 'Approved CIS hardened AMIs' to trigger an alert whenever a non-compliant AMI is in use.

✓

Enable AWS Config in the region the application is hosted in. Utilize the AWS-managed rule 'approved-amis-by-id' to trigger an alert whenever a non-compliant AMI is in use.

✗

Enable AWS Shield in the region the application is hosted in. Create a rule to trigger an alert whenever a non-compliant AMI is in use.

✗

Create a CloudWatch Event type 'EC2 Instance State-change Notification' in the region the application is hosted in. Create an event rule to trigger an alert whenever a non-compliant AMI is in use.

Explanation

AWS Config can assist with security monitoring by alerting you to when resources such as security groups and IAM credentials have had changes to the baseline configurations. AWS Config has a managed rules set and the AWS managed rule 'approved-amis-by-id' can check that running instances are using approved Amazon Machine Images, or AMIs. You can specify a list of approved AMIs by ID or provide a tag to specify the list of AMI IDs.

The remaining choices are incorrect for the following reasons:

- AWS Inspector is a tool used primarily for the purpose of checking the network accessibility and security vulnerabilities of your EC2 instances and the security state of the applications running on those instances as opposed to alerting on non-compliant Amazon machine images.
- AWS Shield is a managed DDoS service enabled by Amazon to protect applications running on AWS. The rules on AWS Shield are not designed to track and alert for non-compliant Amazon machine images.
- Amazon CloudWatch Events delivers a near real-time stream of system events that describe changes in AWS resources. The CloudWatch Event type 'EC2 Instance State-change Notification' will log state changes of Amazon EC2 Instances, not non-compliant Amazon machine images.

 <https://aws.amazon.com/blogs/devops/aws-config-checking-for-compliance-with-new-managed-rule-options/>
#38

An IT department is using Amazon EFS to share files between a fleet of EC2 instances. The organization's security policy requires encrypted data for this file system both at rest and in-transit. You enabled encryption at rest when the file system was created, but need a way to enforce encryption in-transit whenever mounting the filesystem. What action is the most effective solution to enforce encryption in-transit whenever a user mounts this EFS file system to an EC2 instance?

✗

Create a script that administrators use when mounting the EFS filesystem to an EC2 instance that always uses Transport Layer Security (TLS).

✗

Update the EFS filesystem configuration to specify that you must use Transport Layer Security (TLS) whenever mounting the filesystem.



Update the Amazon Machine Image used for the EC2 instance to only use Transport Layer Security to mount to EFS filesystems.



Use IAM (Identity and Access Management) to control file system data access with an EFS file system policy that includes the condition `aws:SecureTransport` set to true.

Explanation

The key to setting up encryption in-transit with an EFS filesystem is to mount the filesystem using Transport Layer Security (TLS). There is no setting for an EFS filesystem configuration that will let you enforce TLS for a mount operation, nor is there a way to do this with an AMI.

Of the two remaining choices, you could create a script that administrators use to always mount the filesystem using TLS; however, a better choice is to use IAM to establish an EFS filesystem policy that includes the condition `aws:SecureTransport` set to true. Using a filesystem policy is the best choice because this will cause AWS to raise an error if a user tries to mount the filesystem without specifying TLS.



<https://docs.aws.amazon.com/efs/latest/ug/encryption-in-transit.html>

Covered in this lecture

Managing EFS Security

Course: Using Amazon EFS to Create Elastic File Systems for Linux-Based Workloads

5m



#39



You are placed in charge of your company's cloud storage and need to deploy empty EBS volumes. You are concerned about an initial performance hit when the new volumes are first accessed. What steps should you take to ensure peak performance when the empty EBS volumes are first accessed?



Do nothing - empty EBS volumes do not require initialization



Force the immediate initialization of the entire volume



Enable fast snapshot restore



Creating a RAID 0 array

Explanation

Initializing volumes (formerly known as pre-warming) has changed from its prior functionality. Formerly, you would have to initialize (pre-warm) a newly created volume from scratch. This is no longer necessary. Newly created volumes created from snapshots still need to be pre-warmed by reading from the blocks that contain data.



<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-initialize.html>

#40

Multiple AWS accounts within a company's AWS Organization are managing separate websites in EC2 instances behind Application Load Balancers with static content and user-generated content stored in S3 buckets behind CloudFront web distributions. The engineering team wants to protect these vulnerable resources from common web attacks, such as SQL injection, cross-site scripting, and DDoS attacks. Currently, each AWS account allows different types of traffic using AWS Web Application Firewall (WAF). At the same time, they want to use an approach that will allow them to protect new EC2 instances and CloudFront distributions that will be added in the future. What would be an effective and efficient approach to meet this requirement?



Create a set of AWS Web Application Firewall (WAF) rules for account managers for each relevant AWS account to deploy and associate a web ACL to every EC2 instance and S3 bucket.



Tag web application resources such as EC2 instances and CloudFront distributions with resource tags based on their security requirements. Using Firewall Manager, add appropriate AWS WAF rules for each resource tag.



Create a service control policy (SCP) to deny all IAM users' organizational units (OUs) access to AWS WAF. Allow only AWS account root users to modify or create firewall rules with AWS WAF.



Associate AWS Shield Advanced with every Application Load Balancer and CloudFront distribution.

Explanation

AWS Firewall Manager simplifies your administration and maintenance tasks across multiple accounts and resources for AWS WAF, AWS Shield Advanced, Amazon VPC security groups, and AWS Network Firewall. With Firewall Manager, you set up your AWS WAF firewall rules, Shield Advanced protections, Amazon VPC security groups, and Network Firewall firewalls just once. The service automatically applies the rules and protections across your accounts and resources, even as you add new resources. A prerequisite to using AWS Firewall Manager is to use AWS Organization, with all features enabled.

Using Firewall Manager you define the WAF rules in a single place and assign those rules to resources containing a specific tag or resources of a specific type, like CloudFront distributions. Firewall Manager is particularly useful when you want to protect your entire organization rather than a small number of specific accounts and resources, or if you frequently add new resources that you want to protect. Firewall Manager also provides centralized monitoring of DDoS attacks across your organization.

AWS Firewall Manager simplifies your administration and maintenance tasks across multiple accounts and resources for AWS WAF, AWS Shield Advanced, Amazon VPC security groups, and AWS Network Firewall. With Firewall Manager, you set up your AWS WAF firewall rules, Shield Advanced protections, Amazon VPC security groups, and Network Firewall firewalls just once. The service automatically applies the rules and protections across your accounts and resources, even as you add new resources. A prerequisite to using AWS Firewall Manager is to use AWS Organization, with all features enabled.

Using Firewall Manager you define the WAF rules in a single place and assign those rules to resources containing a specific tag or resources of a specific type, like CloudFront distributions. Firewall Manager is particularly useful when you want to protect your entire organization rather than a small number of specific accounts and resources, or if you frequently add new resources that you want to protect. Firewall Manager also provides centralized monitoring of DDoS attacks across your organization.



<https://docs.aws.amazon.com/waf/latest/developerguide/fms-chapter.html>

#41

You are working on a project that involves several AWS resources that will be protected by cryptographic keys. You decided to create these keys using AWS Key Management Services (KMS) and you will need to evaluate the security cost across resources and projects. How will you easily categorize the security keys' cost?



To each key, add a tag and specify the tag key and tag value. Aggregate the costs by tags.



Create symmetric keys and you will be able to aggregate the costs by resources and projects.



After creating the keys, use AWS Organizations to obtain costs across resources and projects.



To each key, add a description and specify the reason for creating this key. Aggregate the costs by descriptions.

Explanation

When you add tags to your AWS resources, AWS can generate a cost allocation report with reports and costs aggregated by tag. To each key created with AWS KMS, you add a tag to it; then, you can evaluate the security cost across resources and projects using the attached tags.

The remaining choices are incorrect for the following reasons:

Creating symmetric or asymmetric keys does not automatically generate reports or cost aggregated by resources or projects.

Although one of the features of AWS Organizations is consolidated billing, this does not provide you with a report on security cost across projects or resources.

Unlike tagging, you cannot use resource descriptions to aggregate security cost across resources or projects.



https://docs.amazonaws.cn/en_us/kms/latest/developerguide/tags-about.html

#42

A customer is using a NAT Gateway to allow a cluster of EC2 instances on a private subnet in their VPC to access an S3 bucket in the same region. After a recent uptick in usage, the customer noticed that data transfer charges rose beyond what they expected. The customer has requested that you find a solution that minimizes data transfer costs without exposing the EC2 instances to the Internet directly. Which option best meets the requirements?



Use a NAT Instance instead of the NAT Gateway and update the routing table for the private subnet to route traffic to the S3 bucket to the NAT Instance



Use CloudFront to cache frequently accessed data



Create a VPC Endpoint for the S3 bucket and update the routing table for the private subnet to route traffic to the S3 bucket to the VPC Endpoint



Create a DX connection between the S3 bucket and the private subnet

Explanation

A VPC endpoint enables you to establish a private connection between a VPC and other AWS resources. Transfers between S3 and AWS resources in the same region are free. Therefore, in this scenario using a VPC Endpoint would save on data transfer costs when compared to a NAT Gateway. A NAT instance would have similar transfer costs to a NAT Gateway. Caching data using CloudFront would not reduce the transfer costs as dramatically as using a VPC Endpoint, and depending on the type of data being transfer may have no or limited impact on costs. A Direct Connect (DX) connection would not be useful in connecting a private VPC subnet to an S3 bucket.



<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html>

Covered in this lecture

Applying Our Knowledge - Sample Questions

Course: Designing Multi-Tier Architectures

6m



#43



You plan to develop an efficient auto scaling process for EC2 instances. A key to this will be bootstrapping for newly created instances. You want to configure new instances as quickly as possible to get them into service efficiently upon startup. What tasks can bootstrapping perform? (Choose 3 answers)



Bid on spot instances



Apply patches and OS updates



Enroll an instance into a directory service



Install application software

Explanation

When you launch an instance in Amazon EC2, you have the option of passing user data to the instance that can be used to perform common automated configuration tasks and even run scripts after the instance starts. You can pass two types of user data to Amazon EC2: shell scripts and cloud-init directives.



<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html>

#44

You are in charge of a web application which is running on EC2 instances. Your site occasionally experiences spikes in traffic that cause your EC2 instances' resources to become overwhelmed. During these spikes, the application may freeze up and lose recently-submitted requests from users. You have implemented Auto Scaling to deploy additional EC2 instances to handle spikes, but the new instances are not deploying fast enough to prevent the existing application servers from freezing. Which of the following is likely to provide the cheapest solution to avoid losing recently submitted requests, assuming that you cannot find a pattern to when these spikes are occurring?



Deploy additional EC2 spot instances when needed.



Set up another Availability Zone with the same resources and use that when the spikes occur.



Use Amazon SQS to delete acknowledged messages and redeliver failed messages.



Implement caching to store recent requests in-memory and remove workload from the EC2 instances.

Explanation

The use of an SQS queue allows submitted requests to be retained as messages in the SQS queue until the application resumes normal operation and can process the requests. Using Amazon SQS to delete acknowledged messages and redeliver failed messages is decoupling the application components.

Using EC2 resources, whether you use reserved or spot instances, is not cost-effective owing to the infrequency of the spikes in traffic.

SQS queues are preferable to in-memory caches because in-memory storage will operate at all times and can be fairly expensive to address an issue that only comes up during spikes.



<http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/Welcome.html>

#45

A company has on-premises Microsoft Active Directory. It is expanding its infrastructure to AWS and other custom SAML-enabled applications. Which service will enable the employees to access the AWS consoles and SAML-based applications while using their corporate login?



AWS SSO



AWS Organizations



Amazon Cognito



AWS Config

Explanation

In this scenario, users with access to corporate on-premises Microsoft AD accounts need to access resources in AWS accounts and SAML-based applications. AWS Single Sign-On (SSO) is a service that allows you to centrally manage access to multiple AWS accounts and business cloud applications. This is the solution that will allow the employees the access they need.

The remaining choices are incorrect for the following reasons:

AWS Security Token Service (STS) enables IAM and federated users to request temporary, limited-privilege credentials. It does not enable corporate users to have direct access to AWS accounts or other business cloud applications.

AWS Organizations is an account management service that enables you to consolidate your web presence across multiple AWS accounts into one organization that you create and manage centrally. It does not enable you to use your company credentials to access AWS accounts or other SAML-based applications.

Amazon Cognito is a service for user sign-up/sign-in and access management to web and mobile applications. Amazon Cognito enables you to authenticate users with external identity providers such as Amazon, Apple, Google or Meta.

AWS Config provides a detailed view of the different configurations on the AWS resources across your account. It is not suitable for corporate users' access to AWS accounts or external business cloud applications.

 <https://docs.aws.amazon.com/singlesignon/latest/userguide/what-is.html>

#46

A secured web application running on an EC2 instance needs to perform PUT and GET operations on objects within an S3 bucket. The EC2 instance and S3 bucket are owned by the same AWS account. Of the policies listed below, which two grant the necessary permissions for this web application? (Choose 2 answers)



An S3 Bucket policy that allows the application (as a principal) to perform PUT/GET operations on approved S3 resources within the bucket



An IAM role assigned to the application hosted on the EC2 instance which allows the application (as a service) to perform PUT/GET operations in Amazon S3.



An S3 Bucket Trust policy that allows the application (as a principal) to assume S3Admin role to PUT/GET objects to this bucket



A service-linked policy applied to the S3 bucket allowing access to the web application.

Explanation

For internal communication between S3 and an application running on EC2 instance, you need two policies:

1. An IAM trust policy that allows the EC2 instance to assume a role
2. An IAM policy or S3 bucket policy that allows the role to get/put objects to the specific bucket

So, the kind of policies that control access to S3 bucket are either an IAM Policy or S3 Bucket Policy. The IAM trust policy is required, but it doesn't control access to S3.

 <http://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html>

#47

An IT department manages a content management system (CMS) running on an Amazon EC2 instance mounted to an Elastic File System (EFS). The CMS throughput demands are high compared to the amount of data stored on the file system. What is the appropriate EFS configuration in this case?



Choose **Provisioned Throughput** mode for the file system.



Choose **Bursting Throughput** mode for the file system.



Start with the **General Purpose** performance mode and update the file system to **Max I/O** if it reaches its I/O limit.



Start with **Bursting Throughput** mode and update the file system to **Max I/O** if it reaches its I/O limit.

Explanation

When we discuss EFS performance, there are two types of EFS configuration settings we need to look at:

- **Performance mode:** There are two performance modes: *General Purpose (default)* and *Max I/O*. You choose the performance mode when creating the file system, and once the file system is created, you cannot modify the performance mode. There are no additional costs associated with either performance mode. Max I/O is a good choice for workloads when there is a lot of parallel file system work needed.

- **Throughput mode:** There are two throughput modes: Bursting Throughput (default) and Provisioned Throughput. Unlike performance modes, there is a cost difference between these throughput modes, and you can change the throughput for the file system after creation.

This question scenario is addressing **throughput**, so let's focus on the two throughput modes:

- **Bursting Throughput:** With bursting throughput mode, the amount of throughput scales as your file system grows; the more data you store, the more throughput is available to you. The default throughput available is capable of bursting to 100 MiB/s. However, this can burst to 100 mebibytes per second per TiB of storage used within the file system with the standard storage class.
- **Provisioned Throughput:** Provisioned throughput mode allows you to specify the throughput irrespective of the amount of storage the file system uses. In some cases, you may need more throughput than you would receive based on the file system's size. For example, applications like web serving or content management systems often required throughput that is high relative to the amount of storage needed for the file system.

The correct answer, in this case, is to choose Provisioned Throughput mode for the file system. Provisioned throughput is the best choice because the problem states that the CMS throughput demands are high compared to the amount of data stored on the file system.

 <https://docs.aws.amazon.com/efs/latest/ug/performance.html>

Covered in this lecture

Storage Classes and Performance Options

Course: Using Amazon EFS to Create Elastic File Systems for Linux-Based Workloads



7m



#48

An audit of your company's IT practices has identified several security breaches involving AWS and specifically, your IAM policies. You are asked to evaluate your IAM policies and institute best practices immediately. As a first measure, what guidelines should you follow for the AWS account root access key? (Choose 3 answers)



If you don't have an access key for your AWS account, do not create one unless essential.



Enable AWS multi-factor authentication (MFA) on your AWS root account.



If you do have an access key for your AWS root account, delete it.



Use the root access key for all administrative actions to ensure maximum security.

Explanation

The access key for your AWS account gives full access to all your AWS services and resources, including your billing information. You cannot restrict the permissions associated with your AWS account access key. If you do not already have an access key for your AWS account, do not create one unless you absolutely need to. You can use your account email address and password to sign in to the management console. Multifactor authentication can add an extra layer of security to all of your accounts.



<http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#lock-away-credentials>

#49

A corporate tax firm stores prepared tax documents in Amazon S3 for each of its customers, and wants to make sure documents will only be accessed by the intended customer using a static CloudFront page that retrieves data from S3. To do so, the tax firm limits document access to a specific, secure IP address provided by each customer. Which access control method should a solutions architect use to meet this security requirement?



S3 pre-signed URLs



CloudFront Signed URLs




CloudFront Origin Access Identities (OAI)



S3 Object Access Control Lists (ACLs)

Explanation

CloudFront Signed URLs, specifically custom signed URLs, allow AWS users to limit access to specific content stored on Amazon CloudFront. No other option provides this type of control.

 https://docs.amazonaws.cn/en_us/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html#private-content-choosing-canned-custom-policy

#50

You are designing an AWS cloud environment for a client. There are applications that will not be migrated to the cloud environment so it will be a hybrid solution. You also need to create an EFS file system that both the cloud and hybrid environments need to access. You will use Direct Connect to facilitate the communication between the on-premises servers and the EFS File System. Which statement characterizes how Amazon will charge you for this configuration?

✗

You will be charged for AWS Direct Connect and for the data transmitted between the on-premises servers and EFS.

✗

There is no charge for Direct Connect and a flat fee for EFS.

✗

This is all covered under the VPC charge so there is no additional charge.

✓

You will be charged for AWS Direct Connect there is no additional cost for on-premises access to your Amazon EFS file systems.

Explanation

By using an Amazon EFS file system mounted on an on-premises server, you can migrate on-premises data into the AWS Cloud hosted in an Amazon EFS file system. You can also take advantage of bursting, meaning that you can move data from your on-premises servers into Amazon EFS, analyze it on a fleet of Amazon EC2 instances in your Amazon VPC, and then store the results permanently in your file system or move the results back to your on-premises server. There is no additional cost for on-premises access to your Amazon EFS file systems. Note that you'll be charged for the AWS Direct Connect connection to your Amazon VPC.

 <http://docs.aws.amazon.com/efs/latest/ug/how-it-works.html>

Covered in this lecture

Amazon Elastic File System (EFS).

Course: Understanding and Optimizing Costs with AWS Storage Services



6m



#51

A company's web service processes user-provided images and text to generate custom web ads. Once an ad has been produced, the company stores the photos temporarily and can reproduce them easily from the ad itself. The company retains a copy of each video ad indefinitely as its intellectual property. Recent storage costs have increased significantly, and the company is looking for a more cost-effective storage solution using Amazon S3. Once the company migrates its files to Amazon S3, how can it most effectively optimize storage to reduce storage costs? (Choose two answers.)



Create a lifecycle rule to move all objects from S3 Standard storage to the S3 Intelligent-Tiering storage class after 15 days.



Upload videos to the S3 Intelligent Tiering storage class instead of the S3 Standard Storage



Create a lifecycle rule to move thumbnail objects from S3 Standard storage to the S3 One Zone-Infrequent Access storage class after 30 days.



Create a lifecycle rule to move thumbnail objects to the S3 Standard-Infrequent Access storage class after 30 days.

Explanation

The S3 Intelligent tiering is the best choice for uploading videos but not images because the cost savings to videos is tangible given the video's size, even though there are added object management costs with this choice.

Uploading the files directly to Intelligent Tiering makes more sense than uploading them to the Standard Storage class first and then transitioning them to Intelligent Tiering — any videos that are not frequently accessed during the first 30 days will be transitioned to the Infrequent Access tier and eventually to archival.

The images can easily be recreated, so they are ideal for the S3 One Zone-IA storage class.

Related Links:

- S3 Storage classes: <https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html>
- Object Lifecycle: <https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

 <https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html>

Covered in this lecture

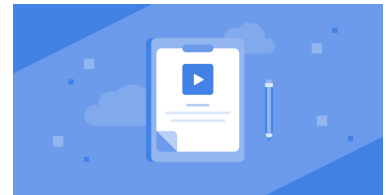
Designing cost optimized storage solutions

Course: Designing Cost-Optimized Architectures in AWS

17m



#52



A company is running a web application in c5.large EC2 instances behind an Application Load Balancer. All of the website content is stored on EBS volumes. Users have complained about the slow website page loads, especially static content like icons, styles, and images uploaded by users. What of the following steps would be the most effective solutions to improve content loading speed?



Increase the EC2 instances' size to c5.2xlarge and replace existing general-purpose EBS volumes with Provisioned IOPS volumes.



Redesign the site to store user-provided content in Amazon S3. Deploy a CloudFront distribution and set designated S3 buckets as Origins.



Add more EC2 instances behind the Application Load Balancer and attach them to an Auto Scaling Group.



Redesign the site to store user-provided content from Amazon EBS instances to Elastic File System (EFS).

Explanation

Amazon CloudFront is a web service that speeds up the distribution of your static and dynamic web content, such as images and static content, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with CloudFront, the request is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

Moving user-provided content to S3 and putting a CloudFront distribution in front of the bucket will also help to reduce the latency and loading time of the images, bringing them closer to users' locations. It would also resolve the content availability problems because the content would be centrally stored and replicated. Moving it to Amazon EFS would increase availability, but it is not as effective a solution for this use case because the user-provided content is ideal for object storage rather than file storage.

Scaling the number of instances either vertically or horizontally would not address the key issue of latency as effectively as CloudFront and S3 combined, and as failure is going to occur, it would not address the availability issue either as long as the content is stored in EBS volumes.



<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

#53

An environmental agency is concluding a 10-year study of mining sites and needs to transfer over 200 terabytes of data to the AWS cloud for storage and analysis. Data will be gradually collected over a period of weeks in an area with no existing network bandwidth. Given the remote location, the agency wants a transfer solution that is cost-effective while requiring minimal device shipments back and forth. Which AWS solution will best address the agency's data storage and migration requirements?



AWS Snowmobile



AWS Snowball Storage Optimized



AWS Snowball Compute Optimized



AWS Snowball Compute Optimized with GPU

Explanation

Consider Snowball Edge if you need to run computing in rugged, austere, mobile, or disconnected (or intermittently connected) environments. Also consider it for large-scale data transfers and migrations when bandwidth is not available for use of a high-speed online transfer service, such as AWS DataSync.

Snowball Edge Storage Optimized is the optimal data transfer choice if you need to securely and quickly transfer terabytes to petabytes of data to AWS. You can use Snowball Edge Storage Optimized if you have a large backlog of data to transfer or if you frequently collect data that needs to be transferred to AWS and your storage is in an area where high-bandwidth internet connections are not available or cost-prohibitive.

A Snowcone is far too small while a Snowmobile is far too large. Storage-optimized Snowball devices offer more than twice the storage capacity of compute-optimized.

 <https://aws.amazon.com/snowball/faqs/>

#54

A web application requires 8 Amazon EC2 instances to meet its service level agreement (SLA) to respond to 99% of the application requests in less than 2 ms. The application load is relatively consistent and does not experience large fluctuations in traffic. The application development team is looking for the right combination of AWS services to help manage this set of servers and maximize resiliency. For example, the team would like to monitor and replace unhealthy instances automatically to maintain eight servers at all times. What services should a solutions architect recommend to maximize resiliency and automatically maintain a fixed number of servers?



Deploy 4 servers to 2 availability zones with an application load balancer distributing requests across the 8 servers. Set up an auto-scaling group that uses the load balancer health checks and set the same minimum, maximum, and desired capacity.



Deploy 8 servers to a single availability zone with an application load balancer distributing requests across the 8 servers. Set up an auto-scaling group that uses the load balancer health checks with a simple scaling policy.



Deploy 4 servers to 2 availability zones with an application load balancer distributing requests across the 8 servers. Set up load balancer health checks to replace unhealthy instances.



Deploy 8 servers to a single availability zone with an application load balancer distributing requests across the 8 servers. Set up a CloudWatch alarm to automatically replace unhealthy instances.

Explanation

The critical point in this question is that you need to identify a solution that will **automatically maintain a fixed number of servers**. Added to this, you need to decide whether to use 1 or 2 availability zones.

Let's start with the number of availability zones. If you want your application to be highly available and resilient, distributing your resource across multiple availability zones is the best choice. If one availability zone becomes unavailable, the servers in the remaining availability zone can support your application load. We can disregard any solution that includes using a single availability zone and only consider those that use two availability zones.

The last thing we need to do is determine how to set up an AWS service to maintain a fixed number of servers. It turns out you can use AWS auto-scaling for more than scaling-out your compute resources. You can also use auto-scaling to build resilient systems by configuring it to maintain a fixed number of resources. When used in this way, the auto-scaling service can monitor your resources and replace unhealthy instances. The choice that suggests using the load balancer to replace unhealthy instances is incorrect because a load balancer cannot replace unhealthy instances.

Additional Resources:

Maintaining Fixed Number of Instances



<https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-benefits.html>

#55

You are assigned to lead your company's migration to an AWS cloud environment. Your company has a large software development division and you are gathering requirements for their instances as well as EBS volumes. This department will often have multiple projects going on at one time, which calls for multiple dev, test, and production environments. They want dev and test to simulate production loads so they will be moderately IO intensive. What type of EBS volume is best suited for dev and test environments?



General Purpose SSD (gp3)



Provisioned IOPS SSD (io2)



Throughput Optimized HDD (st1)



Cold HDD (sc1)

Explanation

General-purpose (SSD) volumes are ideal for the following use cases:

- Transactional workloads
- Virtual desktops
- Medium-sized, single-instance databases
- Low-latency interactive applications
- Boot volumes
- Development and test environments



<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html>

#56

A team is deploying AWS resources, including EC2 and RDS database instances, into a VPC's public subnet after recovering from a system failure. The team attempts to establish connections using HTTPS protocol to these new instances from other subnets within the VPC, and from other peered VPCs within the same region, but receives numerous 500 error messages. The team needs to quickly identify the cause or causes of the connection problem that prevents connecting to the new subnet. What AWS solution should they use to identify the cause of the network problem?



Amazon Route 53 Resolver



VPC Reachability Analyzer



VPC Network Access Analyzer



Amazon Route 53 Application Recovery Controller (ARC)


Explanation

The correct solution, in this case, is the VPC Reachability Analyzer.

VPC Reachability Analyzer is a configuration analysis tool that enables you to perform connectivity testing between a source resource and a destination resource in your virtual private clouds (VPCs). When the destination is reachable, Reachability Analyzer produces hop-by-hop details of the virtual network path between the source and the destination.

The other choices are useful in other situations:

- Route 53 ARC provides continual readiness checks to help make sure, on an ongoing basis, that your applications are scaled to handle failover traffic and configured so you can route around failures. Route 53 ARC helps you centrally coordinate failovers within an AWS Region or across multiple Regions. It provides extremely reliable routing control so you can recover applications by rerouting traffic, for example, across Availability Zones or Regions. To do this, you partition your applications into redundant failure-containment units, or replicas, called cells. The boundary of a cell can be an Availability Zone or a Region, or even a smaller unit within an Availability Zone.
- The Route 53 Resolver can contain endpoints that you configure to answer DNS queries to and from your on-premises environment. You also can integrate DNS resolution between Resolver and DNS resolvers on your network by configuring forwarding rules. Your network can include any network that is reachable from your VPC.
- Network Access Analyzer is a feature that identifies unintended network access to your resources on AWS. You can use Network Access Analyzer to specify your network access requirements and to identify potential network paths that do not meet your specified requirements.

 <https://docs.aws.amazon.com/vpc/latest/reachability/what-is-reachability-analyzer.html>

#57

A company is configuring its new AWS Organization and has implemented an allow list strategy. Now the company needs to grant special permissions to a single AWS account in the Development organizational unit (OU). All AWS users within this single AWS account need to be granted full access to Amazon EC2. Other AWS accounts within the Development OU will not have full access to Amazon EC2. Certain accounts within the Development OU will have partial access to EC2 as needed. The IT Security department has applied a service

control policy (SCP) to the organization's root account that allows AmazonEC2FullAccess. What choice below includes all the necessary steps to grant full EC2 access only to AWS users in this single AWS account?



Apply an SCP granting AmazonEC2FullAccess to the Development OU and the specific AWS account. Apply the AmazonEC2FullAccess IAM policy to all IAM users in the account.



Apply an SCP granting AmazonEC2FullAccess to the Development OU and the specific AWS account.



Apply the AmazonEC2FullAccess IAM policy to all IAM users in the account.



Apply an SCP granting AmazonEC2FullAccess to the Development OU and the specific AWS account. Apply a separate SCP denying EC2 access to all other AWS accounts within the Development OU.

Explanation

Inheritance for service control policies behaves like a filter through which permissions flow to all parts of the tree below. To allow an AWS service API at the member account level, you must allow that API at every level between the member account and the root of your organization. You must attach SCPs to every level from your organization's root to the member account that allows the given AWS service API (such as EC2 Full Access or S3 Full Access). An allow list strategy has you remove the FullAWSAccess SCP that is attached by default to every OU and account. This means that no APIs are permitted anywhere unless you explicitly allow them. To allow a service API to operate in an AWS account, you must create your own SCPs and attach them to the account and every OU above it, up to and including the root. Every SCP in the hierarchy, starting at the root, must explicitly allow the APIs that you want to be usable in the OUs and accounts below it.

Users and roles in accounts must still be granted permissions using AWS Identity and Access Management (IAM) permission policies attached to them or to groups. The SCPs only determine what permissions are available to be granted by such policies. The user can't perform any actions that the applicable SCPs don't allow.



https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_inheritance_auth.html

#58

Your company adopted an open-source based monitoring strategy using Prometheus for container monitoring. The company is undertaking a large initiative to migrate fully to AWS by the end of the fiscal year. Which of the following AWS services may best help manage the operational complexity of scaling the ingestion, storage, alerting, and querying of metrics while being compatible with an open-source cloud-native project?



AWS CloudWatch



AWS EKS with CloudWatch for metrics



Amazon Managed Service for Prometheus



Amazon Managed Service for Grafana

Explanation

Amazon Managed Service for Prometheus is a serverless monitoring service for metrics compatible with open-source Prometheus, making it easier for you to securely monitor and alert on container environments. You should use Amazon Managed Service for Prometheus if you have adopted an open source-based monitoring strategy, have already deployed or plan to adopt Prometheus for container monitoring, and prefer a fully managed experience where AWS provides enhanced security, scalability, and availability.

The remaining choices are not the most effective solution for this problem.

 <https://aws.amazon.com/prometheus/faqs/>

#59

A company manages DynamoDB databases to store online transaction-related data such as sales, returns, and inventory changes. As sales continue to grow, the company is more concerned with backing up database tables across multiple regions as well as across multiple AWS accounts. By replicating backups across business locations and employee accounts, the company believes responses to any issues will be solved faster and easier. How can a solutions architect effectively address the company's requirements?



Enable On-Demand backup and restore using DynamoDB backups



Enable On-Demand backup and restore using AWS Backup



Enable continuous backups with point-in-time recovery



Deploy a DynamoDB Accelerator (DAX) cluster

Explanation

Amazon DynamoDB can help you meet regulatory compliance and business continuity requirements through enhanced backup features in AWS Backup. AWS Backup is a fully managed data protection service that makes it easy to centralize and automate backups across AWS services, in the cloud and on-premises.

Enhanced backup features available through AWS Backup include:

Scheduled backups - You can set up regularly scheduled backups of your DynamoDB tables using backup plans.

Cross-account and cross-Region copying - You can automatically copy your backups to another backup vault in a different AWS Region or account, which allows you to support your data protection requirements.



https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/backuprestore_HowItWorksAWS.html

#60

A gaming company hosts a multiplayer online game on fleets of Amazon EC2 instances deployed into multiple regions around the globe. Each deployment is attached to an auto scaling group behind an Application Load Balancer. Despite the fact that instances are deployed globally, customer support receives frequent complaints about delays between players within the same game and lags in loading new stages as the game progresses. The developers believe this issue is due to network latency between players and EC2 servers hosting the game. Which of the following changes should a Solutions Architect implement to most effectively reduce network latency within the multiplayer game?



Configure your Application Load Balancers as endpoints for AWS Global Accelerator.



Reconfigure your application's EC2 instances into cluster placement groups.



Create CloudFront distributions with your EC2 instances as the origins.



Scale out more EC2 instances by updating the maximum capacity parameter for your auto scaling group's launch templates.

Explanation

AWS Global Accelerator is a service in which you create accelerators to improve the performance of your applications for local and global users. By using a standard accelerator, you can improve availability of your internet applications that are used by a global audience. With a standard accelerator, Global Accelerator directs traffic over the AWS global network to endpoints in the nearest Region to the client, which reduces internet latency and jitter.

Amazon CloudFront speeds up the distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users, but is not capable of routing user requests to your services.

Scaling out more instances would be helpful if the issue were related to a lack of CPU or memory to support customers, but in this case because it is a network issue it would only have a marginally positive effect at best on the actual problem.

Cluster placement groups are ideal for HPC workloads that require faster communication between instances. This scenario involves communication between the gamers and the service, so cluster placement groups would not solve the problem.



<https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html>

#61

An application hosted on EC2 instances has no usage (almost zero load) for the majority of the day. The application workload lasts for roughly five hours a day, at the same time each day. The day-to-day workload is consistent, and will be required for the foreseeable future. Which solution below is the most efficient and cost-effective in this scenario?



Use on-demand capacity reservations to save costs for running the instance all day.



Use on-demand T2 burstable instance configured for unlimited mode



Set instance start and stop times using the AWS Instance Scheduler



Use on-demand T2 burstable instance configured for standard mode

Explanation

The Instance Scheduler on AWS solution automates the starting and stopping of Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Relational Database Service (Amazon RDS) instances.

This solution helps reduce operational costs by stopping resources that are not in use and starting resources when their capacity is needed. For example, a company can use Instance Scheduler on AWS in a production environment to automatically stop instances outside of business hours every day. If you leave all of your instances running at full utilization, this solution can result in up to 70% cost savings for those instances that are only necessary during regular business hours (weekly utilization reduced from 168 hours to 50 hours).

Instance Scheduler on AWS leverages AWS resource tags and AWS Lambda to automatically stop and restart instances across multiple AWS Regions and accounts on a customer-defined schedule. This solution also allows you to use hibernation for stopped Amazon EC2 instances.

Amazon offers burstable instances that perform in standard and unlimited mode, as well as on-demand capacity reservations and scheduled reserved instances. Burstable instances in standard mode are ideal for consistent workloads that have small, limited peaks from time to time. Burstable instances in unlimited mode are ideal for workloads that have prolonged high-CPU performance.

On-demand capacity reservations save capacity for on-demand EC2 instances in a particular availability zone. Scheduled reserved instances allow you to save the capacity in a specific availability zone for at least one year, and save 5-10 percent of the cost.



<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html>

#62

Your latest client contacted you a week before an audit on its AWS cloud infrastructure. Your client is concerned about its lack of automated policy enforcement for data protection and the difficulties they encounter when reporting for audit and compliance. Which service should you enable to assist this client?



AWS DataSync



Amazon FSx



AWS Macie



AWS Backup

Explanation

The client is in search of a solution that automates policy enforcement for data protection and compliance. With AWS Backup the client can enable automated data protection policies and schedules that will meet the regulatory compliance requirements for its upcoming audit. Also, AWS Backup allows you to centrally manage and automate the backup of data across AWS services such as Ec2, S3, EBS, RDS, EFS,FSx, and more.

The remaining choices are incorrect for the following reasons:

AWS DataSync is a data transfer service that enables you to optimize network bandwidth and accelerate data transfer between on-premises storage and AWS storage. DataSync does not provide policy enforcement for data protection.

Amazon GuardDuty is a threat detection service that continuously monitors AWS accounts and workloads for malicious activity and anomalous behavior.

Amazon FSx provides a cost-effective file storage service that makes it easy to launch, run, and scale high-performance file systems in the cloud. It does not offer the data protection needed in this scenario.

Although AWS Macie protects your data through discovery and protection of your sensitive data at scale, Macie does not provide automated data protection, compliance, and governance for your applications running in the cloud.

 <https://docs.aws.amazon.com/aws-backup/latest/devguide/whatisbackup.html>

#63

Your business is slowly migrating to the AWS cloud, but must continue to support its on-premises servers and networks while extending to the cloud. As a result, you are looking for every possible way to optimize costs while ensuring resources remain secure. In order to provide an extra layer of security, you would like for your servers hosted within your VPCs to communicate with other AWS services without leaving your VPC network. You would also like your on-premises servers to be able to connect to these same AWS services through your VPC as an extension of your existing DX connection instead of sending and receiving requests over the public internet. Which AWS networking service or component would satisfy these requirements?

✗

VPC Virtual Private Gateways

✗

VPC Peering Connections

✓


VPC Interface Endpoints

✗

VPC Gateway Endpoints

Explanation

With VPC Interface Endpoints, it is possible to connect to a number of AWS services both from resources within your Amazon VPC and from resources in your on-premises environment. This is not possible with VPC Gateway Endpoints.

 <https://docs.aws.amazon.com/vpc/latest/userguide/vpce-interface.html>

#64

You are rapidly configuring a VPC for a new insurance application that needs to go live imminently to meet an upcoming compliance deadline. The insurance company must migrate a new application to this new VPC and connect it as quickly as possible to an on-premises, company-owned application that cannot migrate to the cloud. Your immediate goal is to connect your on-premises app as quickly as possible but speed and reliability are critical long-term requirements. The medical insurance company suggests implementing the

quickest connection method now, and if necessary, switching over to a faster, more reliable connection service within the next six months if necessary. Which strategy would work best to satisfy their short and long-term networking requirements?



AWS VPN is the best short-term solution, and AWS Direct Connect is the best long-term solution.



AWS VPN is the best short-term and long-term solution.



VPC Endpoints are the best short-term and long-term solutions.



AWS Direct Connect is the best short-term solution, and AWS VPN is the best long-term solution.

Explanation

A VPN connection is the fastest way to complete the connection between on-premises computing and your VPC. However, VPN is not as reliable or as fast as Direct Connect. VPN would satisfy the requirement to establish the connection as quickly as possible. You can subsequently request a Direct Connect connection that is not subject to inconsistencies of the internet and will be faster and more reliable than AWS VPN. Direct Connect can ultimately replace the VPN connection and all requirements will be satisfied.

 <https://aws.amazon.com/directconnect/faqs/>

Covered in this lecture

The Common Patterns with VPC Design

Course: Managing Cloud Networking at Scale - Chalk Talk with Aviatrrix

13m



#65



A cloud engineer is tasked with building a custom data identifier that will discover sensitive data in Amazon S3 bucket and classify these objects according to the type of data discovered. The engineer is searching for a service that will help the team complete this task with little configuration. How can the engineer discover the sensitive data and classify them as quickly as possible?



Enable Amazon Detective on the AWS account containing these buckets, define detection criteria and define finding severity settings



Enable Amazon Macie on the AWS account containing these buckets, define detection criteria and define finding severity settings



Enable Amazon Cognito on the AWS account containing these buckets, define detection criteria, and define finding severity settings.



Enable Amazon Inspector on the AWS account containing these buckets, define detection criteria and define finding severity settings.

Explanation

Amazon Macie is a data security and data privacy service that leverages machine learning and pattern recognition to discover sensitive data and protect them. In this scenario, Amazon Macie will continuously evaluate Amazon S3 buckets on the account, discover data containing PII, and take remediation actions to protect them according to HIPAA compliance.

The remaining choices are incorrect for the following reasons:

Amazon Detective makes it easy to analyze, investigate and determine the root cause of security assessment findings or suspicious activities. Analysis and investigation data are also presented in forms of graphs, continuously refreshed. Amazon Detective does not locate or discover sensitive data in Amazon S3 buckets.

Amazon Cognito is a service for user sign-up/sign-in and access management to web and mobile applications. Amazon Cognito also enables you to authenticate users with external identity providers such as Amazon, Apple, Google or Meta. It does not use machine learning to sensitive information such as PII.

Amazon Inspector is a vulnerability management service; it scans AWS workloads for software vulnerabilities and unintended network exposure. Amazon Inspector is a security assessment service. It does not use machine learning to detect PII in Amazon S3 or take actions to protect sensitive information.

Amazon GuardDuty is a threat detection service that continuously monitors AWS accounts for malicious activities and anomalous behaviors. Amazon GuardDuty leverages machine learning to identify the threats and classify them. It does not apply machine learning to buckets that you select and alert you when sensitive information is discovered.

 <https://docs.aws.amazon.com/macie/latest/user/getting-started.html>