1. A solutions architect is designing an architecture that can provide HTML pages to customers. They want a serverless solution that can host content over the internet and serve a static website with minimal effort. Which AWS service should the solutions architect choose to meet these requirements? **1 / 1 point**

- (●) Amazon Simple Storage Service (Amazon S3)
- ( ) Amazon Elastic Compute Cloud (Amazon EC2)
- ( ) Amazon DynamoDB
- ( ) Amazon Kinesis

Correct

You can use Amazon S3 to host a static website. On a static website, individual webpages include static content. They might also contain client-side scripts. By contrast, a dynamic website relies on server-side processing, which can include server-side scripts that are written in PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting, but AWS has other resources for hosting dynamic websites. To learn more about website hosting on AWS, see Web Hosting (https://aws.amazon.com/websites/).

2. Which of the following options includes true statements for both Amazon Simple Storage Service (Amazon S3) cross-Region replication and AWS Key Management Service (AWS KMS)? **1 / 1 point**

- ( ) To configure S3 cross-Region replication, both the source and destination buckets must belong to the same AWS account. Server-side encryption (SSE) is possible for replicated objects.
- ( ) To configure Amazon S3 cross-Region replication, both the source and destination buckets must belong to the same AWS account. Server-side encryption (SSE) is not possible for replicated objects.
- (●) To configure Amazon S3 cross-Region replication, the source and destination buckets can belong to different AWS accounts. Server-side encryption (SSE) is possible for replicated objects.
- ( ) To configure Amazon S3 cross-Region replication, the source and destination buckets can belong to different AWS accounts. Server-side encryption is not possible for replicated objects.

Correct

Both statements are true. Buckets can belong to different accounts. SSE (powered by Amazon KMS) can be enabled for the replicated objects. For more information, see Replicating objects.

3. True or False: Amazon Relational Database Service (Amazon RDS) is more suitable for databases that handle structured or relational data, where users can count with features like auto-increment and table joins. Amazon DynamoDB is more suitable for NoSQL database workloads, where tables are collection of items that have their own attributes. **1 / 1 point**

- (●) True
- ( ) False

Correct

DynamoDB is a database service for NoSQL data. It is fully managed by AWS. DynamoDB is swift, reliable, and scalable, which makes working with NoSQL data much easier. Amazon RDS is used for relational databases. It is mostly used to handle structured and relational data through Structured Query Language (SQL).

4. Amazon DynamoDB is designed for scale and performance. In most cases, the DynamoDB response times can be measured in single-digit milliseconds. However, there are certain use cases that require response times in microseconds. For these use cases, DynamoDB Accelerator (DAX) delivers fast response times for accessing eventually consistent data. Which statements about DAX are correct? (Choose THREE.) **1 / 1 point**

- [x] DAX reduces operational and application complexity by providing a managed service that is compatible with the DynamoDB API.

Correct

DAX is a managed caching service for Amazon DynamoDB that is compatible with the DynamoDB API.

- [x] Although using DAX has a cost, it can reduce the consumption of DynamoDB table capacity. If the data is read intensive (that is, millions of requests per second), DAX can result in cost savings by caching the data while also providing better read latency, being beneficial for scenarios in need of repeated reads for individual keys.

Correct
Through the use of a cache like DAX, you can offload some read requests to the cache, which would save on read capacity for the table itself.

- [ ] DAX does not support server-side encryption (SSE).
- [x] DAX is not designed for applications that are write-intensive. It can also add cost to applications that do not perform much read activity.

Correct
DAX is beneficial for reads because it is a caching service. However, it is not very beneficial for write-heavy workloads.

- [ ] DAX does not support encrypting data in transit, which means that communication between an application and DAX cannot be encrypted.

5. True or False: AWS Lambda is a compute service that runs code without the need to provision or manage servers. Lambda runs code on a high-availability compute infrastructure. It also performs all the administration of compute resources, including server and operating system maintenance, capacity provisioning and automatic scaling, and logging. Lambda can run code for virtually any type of application or backend service. **1 / 1 point**

- (•) True
- ( ) False

Correct
AWS Lambda is a managed compute service that you can use to run serverless compute functions in a highly available and scalable manner.

6. A solutions architect is designing a solution that needs real-time data ingestion. They are considering either Amazon Kinesis Data Firehose or Amazon Kinesis Data Streams for this solution. Which service should the solutions architect choose to meet the requirement for real-time data ingestion, and why? (Remember that lower data latency means a lower roundtrip time from when data is ingested and available.) **1 / 1 point**

- ○ Amazon Kinesis Data Firehose, because it has lower latency when compared to Amazon Kinesis Data Streams
- ○ Amazon Kinesis Data Firehose, because it has higher latency when compared to Amazon Kinesis Data Streams
- ◉ Amazon Kinesis Data Streams, because it has lower latency when compared to Amazon Kinesis Data Firehose
- ○ Amazon Kinesis Data Streams, because it has higher latency when compared to Amazon Kinesis Data Firehose

✓ **Correct**
Amazon Kinesis Data Streams is suitable for low-latency data streaming, which makes it more suitable for real-time analytics instead of a service like Amazon Kinesis Data Firehose.

7. Which set of AWS services is the BEST fit for the “Object, file, and block storage” category (which means that the services are dedicated to storing data in a durable way)? **1 / 1 point**

- ○ AWS DataSync, AWS Snow Family
- ◉ Amazon Simple Storage Service (Amazon S3), Amazon Elastic File System (Amazon EFS), Amazon Elastic Block Store (Amazon EBS), Amazon FSx
- ○ AWS Storage Gateway, AWS Snow Family
- ○ AWS Elastic Disaster Recovery, AWS Backup

✓ **Correct**
According to the Cloud Storage on AWS page, Amazon S3, Amazon EFS, Amazon EBS, and Amazon FSx belong to the “Object, file, and block storage” category. Amazon S3 is designed to store virtually any amount of data from virtually anywhere. Amazon EFS automatically grows and shrinks as you add and remove files, and it reduces the need for management or provisioning. Amazon EBS is an easy-to-use,

scalable, high-performance block-storage service that is designed for Amazon Elastic Compute Cloud (Amazon EC2). Amazon FSx makes it easier to provide broadly-accessible and highly-performant file storage for a wide variety of use cases. For more information, see Cloud Storage on AWS.

8. True or False: When architecting a solution that can handle high demand and usage spikes, Amazon CloudFront should be used in front of an Amazon Simple Storage Service (Amazon S3) bucket. CloudFront can cache data that gets delivered to customers, and it lets customers use custom domain names. In addition, CloudFront can serve custom SSL certificates that are issued by Amazon Certificate Manager (at no additional cost) and it can provide distributed denial of service (DDoS) protection that is powered by AWS WAF and AWS Shield. **1 / 1 point**

- (●) True
- ( ) False

Correct

CloudFront is a web service that speeds up the distribution of static and dynamic web content (such as .html, .css, .js, and image files) to users. CloudFront delivers content through a worldwide network of data centers that are called edge locations. CloudFront is designed to use edge locations to deliver content with the best possible performance. When a user requests content that is served through CloudFront, the request is routed to the edge location that provides the lowest latency (time delay).

9. Which statements about AWS Storage Gateway are correct? (Choose THREE.) **1 / 1 point**

- [x] AWS Storage Gateway is a set of hybrid cloud storage services that provide on-premises access to virtually unlimited cloud storage.

Correct

You can use Storage Gateway in on-premises environments so that on-premises networks can access cloud storage resources. Storage Gateway works well in hybrid scenarios, such as the one that Morgan designed for this week's architecture.

- [ ] AWS Storage Gateway offers virtually unlimited cloud storage to users and applications, at the cost of new storage hardware.
- [x] AWS Storage Gateway delivers data access to on-premises applications while taking advantage of the agility, economics, and security capabilities of the AWS Cloud.

Correct
You can use Storage Gateway during only the times that you need it, which means that you can take advantage of the economics and security capabilities of the cloud.

- [ ] AWS Storage Gateway is limited to only on-premises applications, which means that it cannot be used from cloud to cloud.
- [x] AWS Storage Gateway helps support compliance requirements through integration with AWS Backup to manage the backup and recovery of Volume Gateway volumes, which simplifies backup management.

Correct
Integration with AWS Backup is supported by Storage Gateway, more information here

- [ ] AWS Storage Gateway can only work as an Amazon S3 File Gateway.

10. What are some benefits of using multiple AWS accounts with AWS Organizations? (Choose THREE.) **1 / 1 point**

- [x] Grouping workloads based on business purpose and ownership

Correct
One of the patterns for organizing AWS account usage is to group workloads based on business purpose or ownership.

- [ ] Using different payment methods per account
- [x] Limiting the scope of impact from adverse events

Correct
Using multiple AWS accounts through AWS Organizations can limit the scope of impact for adverse events by helping resources achieve independence and isolation, and reducing the blast radius of potential incidents.

- [x] Distributing AWS service quotas and API request rate limits

Correct
A benefit of using multiple AWS accounts is the ability to distribute AWS service quotas and API request rate limits across accounts, instead of everything applying to only one account.

- [ ] Having multiple account root users with unrestricted access on each account

11. True or False: A service control policy (SCP) statement with an explicit deny prevents even the account root user from performing API calls. **1 / 1 point**

- (•) True
- ( ) False

Correct
SCPs govern policies on the account level. After permissions have been explicitly denied in an SCP, the action cannot be allowed. Even the root user will not be able to perform the denied action.

12. A solutions architect is designing a solution that provides single sign-on (SSO) to authenticate into AWS accounts that are in AWS Organizations. Which AWS service can the solutions architect use to implement identity federation with existing identity providers, such as Microsoft Active Directory? **1 / 1 point**

- ( ) AWS Identity and Access Management (IAM) users
- ( ) Amazon CloudWatch
- (•) AWS IAM Identity Center (successor to AWS Single Sign-On)
- ( ) AWS CloudTrail

Correct
IAM Identity Center is the best candidate for this task because it offers integration with third-party identity providers (IdPs). Supported identity sources include Microsoft Active Directory Domain Services and external identity providers, such as Okta Universal Directory or Microsoft Azure Active Directory (Azure AD).

13. Which statements are best practices for multi-account environments? (Choose THREE.) **1 / 1 point**

- [x] Enable Amazon CloudWatch billing alarms per account and configure tagging policies in AWS Organizations.

Correct
These actions are good practices because they give the architect visibility into the cost per account. Additionally, a feature called Cost Anomaly Detection can be enabled in the AWS Cost Management portal. You can provide monitoring for linked accounts in AWS Organizations, having automated cost anomaly detection and root cause analysis if something goes wrong.

- [ ] Give AdministratorAccess policies to developers in their development AWS accounts.
- [x] Prevent CloudTrail configuration from being disabled in the shared services account.

Correct
Preventing CloudTrail from being disabled in the shared services account is a best practice because it helps ensure that actions in the AWS accounts are logged. This action can be achieved with a service control policy (SCP) and a policy that explicitly denies CloudTrail configurations from being disabled. For example, see the following policy, which applies an explicit deny to any resource to prevent issuing either the StopLogging and DeleteTrail actions CloudTrail: { "Version": "2012-10-17", "Statement": [{ "Action": ["cloudtrail:StopLogging", "cloudtrail:DeleteTrail"], "Resource": "*", "Effect": "Deny"

- [x] Use multi-factor authentication (MFA) for users in centralized credentialing, such as using AWS IAM Identity Center (successor to AWS Single Sign-On).

Correct
Using MFA for users in centralized credentialing is a best practice because it helps ensure that users have multiple forms of authentication before they are granted access to AWS resources.

- [ ] Reuse passwords for simplicity and ease of access.

- [ ] Provide powerful users and broad roles for Cloud Center of Excellence (CCoE) members, such as granting AdministratorAccess permissions to them.

14. A solutions architect must create well-defined governance standards for a company that has multiple AWS accounts. The company needs centralized infrastructure logging for all AWS accounts. In addition, the company's chief information security officer (CISO) would like to have a measurement that applies a circuit breaker to stop Amazon Elastic Compute Cloud (Amazon EC2) API activities if the billing alarms indicate suspicious activity. The company intends to use AWS Organizations. Which architectural scenario should the solutions architect propose to meet the company's needs in the MOST effective way? **1 / 1 point**

- (●) Enable AWS CloudTrail for all accounts in AWS Organizations. Use Organizations to centralize all logs into one Amazon Simple Storage Service (Amazon S3) bucket. As the circuit breaker, use service control policies (SCPs) that have an explicit deny for Amazon EC2 API activity. These SCPs can then be applied to the root organizational unit (OU) as needed.
- ( ) Enable AWS CloudTrail for all accounts in AWS Organizations. Use Organizations to centralize all logs into one Amazon Simple Storage Service (Amazon S3) bucket. Use multi-factor authentication (MFA) devices for every user in AWS IAM Identity Center (successor to AWS Single Sign-On).
- ( ) Enable AWS CloudTrail for only the production accounts in AWS Organizations. Use Organizations to centralize logs into one Amazon Simple Storage Service (Amazon S3 bucket). For single sign-on, use AWS IAM Identity Center (successor to AWS Single Sign-ON).
- ( ) Enable AWS CloudTrail for all accounts in AWS Organizations. Use Organizations to centralize logs in one Amazon Simple Storage Service (Amazon S3) bucket. As the circuit breaker, use AWS Identity and Access Management (IAM) policies on each account that have an explicit deny for Amazon EC2 API activity. The IAM policies can then be applied to the root organizational unit (OU) as needed.

Correct

You can use AWS Organizations can consolidate all AWS CloudTrail logging into one account. For the circuit breaker, you can create an SCP that explicitly denies Amazon EC2 API calls. The SCP can then

be applied at any level in the organizational structure by using AWS Organizations.