**AWS CCP PRACTICE QUESTIONS**

**(Security and Compliance)**

**SECURITY AND COMPLIANCE**

Question 1:

Which of the following AWS services support VPC Endpoint Gateway for a private connection from a VPC? (Select two)

1. Amazon SQS
2. Amazon EC2
3. S3 (Correct)
4. Amazon SNS
5. DynamoDB (Correct)

#### **Explanation**

Correct option:

**S3**

**DynamoDB**

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

There are two types of VPC endpoints: interface endpoints and gateway endpoints.

An interface endpoint is an elastic network interface with a private IP address from the IP address range of your subnet that serves as an entry point for traffic destined to a supported service. Interface endpoints are powered by AWS PrivateLink, a technology that enables you to privately access services by using private IP addresses.

A gateway endpoint is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service. The following AWS services are supported:

Amazon S3

DynamoDB

Exam Alert:

You may see a question around this concept in the exam. Just remember that only S3 and DynamoDB support VPC Endpoint Gateway. All other services that support VPC Endpoints use a VPC Endpoint Interface.

Incorrect options:

**Amazon EC2**

**Amazon SQS**

**Amazon SNS**

As explained earlier, these services support VPC Endpoint Interfaces.

Reference:

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

Question 2:

AWS Shield Advanced provides expanded DDoS attack protection for web applications running on which of the following resources? (Select two)

1. Amazon Route 53 (Correct)
2. Amazon API Gateway
3. AWS CloudFormation
4. AWS Global Accelerator (Correct)
5. AWS Elastic Beanstalk

#### **Explanation**

Correct options:

**Amazon Route 53**

**AWS Global Accelerator**

AWS Shield Standard is activated for all AWS customers, by default. For higher levels of protection against attacks, you can subscribe to AWS Shield Advanced. With Shield Advanced, you also have exclusive access to advanced, real-time metrics and reports for extensive visibility into attacks on your AWS resources. With the assistance of the DRT (DDoS response team), AWS Shield Advanced includes intelligent DDoS attack detection and mitigation for not only for network layer (layer 3) and transport layer (layer 4) attacks but also for application layer (layer 7) attacks.

AWS Shield Advanced provides expanded DDoS attack protection for web applications running on the following resources: Amazon Elastic Compute Cloud, Elastic Load Balancing (ELB), Amazon CloudFront, Amazon Route 53, AWS Global Accelerator.

Incorrect options:

**Amazon API Gateway** - Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. APIs act as the "front door" for applications to access data, business logic, or functionality from your backend services. Amazon Web Application Firewall is used to monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API. It is not covered under AWS Shield Advanced.

**AWS CloudFormation** - AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts. CloudFormation is not covered under AWS Shield Advanced.

**AWS Elastic Beanstalk** - AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with various programming languages. You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. Elastic Beanstalk is covered under AWS Shield Standard. Advanced coverage is not offered for this service.

Reference: <https://docs.aws.amazon.com/waf/latest/developerguide/ddos-overview.html>

Question 3:

Which of the following AWS services has encryption enabled by default?

1. Amazon S3
2. Elastic Block Storage (EBS)
3. Elastic File Storage (EFS)
4. CloudTrail Logs (Correct)

#### **Explanation**

Correct option:

**CloudTrail Logs**

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. CloudTrail can be used to record AWS API calls and other activity for your AWS account and save the recorded information to log files in an Amazon Simple Storage Service (Amazon S3) bucket that you choose. By default, the log files delivered by CloudTrail to your S3 bucket are encrypted using server-side encryption with Amazon S3–managed encryption keys (SSE-S3).

Incorrect options:

**Elastic File Storage (EFS)** - Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. Amazon EFS supports two forms of encryption for file systems, encryption of data in transit and encryption at rest. This is an optional feature and has to be enabled by user if needed.

**Elastic Block Storage (EBS)** - Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) instances for both throughput and transaction-intensive workloads at any scale. Encryption (at rest and during transit) is an optional feature for EBS and has to be enabled by the user.

**Amazon S3** - Amazon Simple Storage Service is storage for the Internet. To upload data into S3 you need to create an S3 bucket in one of the AWS Regions. Amazon S3 default encryption provides a way to set the default encryption behavior for an S3 bucket. Encryption for an S3 bucket is an additional feature and the user needs to enable it.

Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/encrypting-cloudtrail-log-files-with-aws-kms.html

Question 4:

According to the AWS Shared Responsibility Model, which of the following are responsibilities of AWS? (Select two)

1. Creating IAM role for accessing Amazon EC2 instances
2. Replacing faulty hardware of Amazon EC2 instances (Correct)
3. Enabling Multi Factor Authentication on AWS accounts in your organization
4. Creating S3 bucket policies for appropriate user access
5. Maintaining Amazon S3 data in different availability zone to keep it durable (Correct)

#### **Explanation**

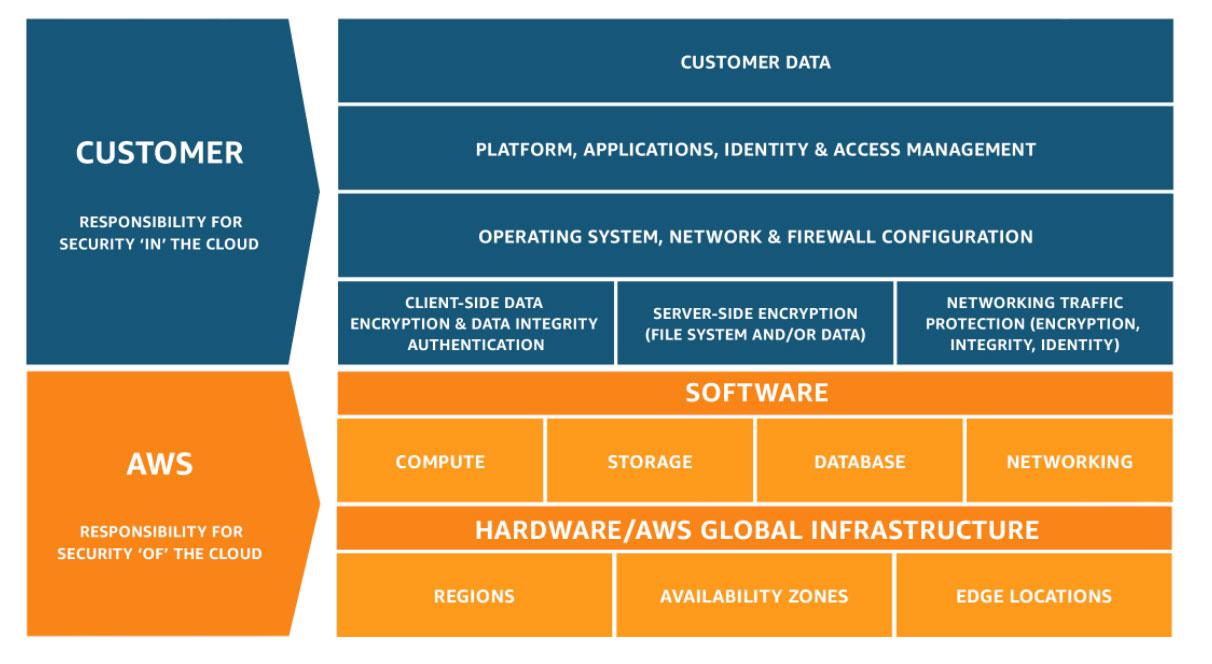
Correct option:

According to the AWS Shared Responsibility Model, AWS is responsible for "Security of the Cloud". This includes protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

**Replacing faulty hardware of Amazon EC2 instances** - Replacing faulty hardware of Amazon EC2 instances comes under the infrastructure maintenance "of" the cloud. This is the responsibility of AWS.

**Maintaining Amazon S3 data in different availability zones to keep it durable** - AWS is responsible for keeping data on AWS Cloud Secure, Durable, Available and Reliable. Keeping data infrastructure safe from failures is the responsibility of AWS.

Shared Responsibility Model Overview:



Incorrect options:

**Enabling Multi Factor Authentication on AWS accounts in your organization** - Enabling Multi Factor Authentication for AWS accounts in your organization is your responsibility. On the other hand, AWS is responsible for making sure that the user data created and their relationships and policies are stored on fail-proof infrastructure.

**Creating IAM role for accessing Amazon EC2 instances** - Creating user roles, policies is the responsibility of the customer. Customers will decide "which" resources get "what" access.

**Creating S3 bucket policies for appropriate user access** - Creating bucket policies for Amazon S3 data access is the responsibility of the customer. The customer decides who gets access to the data he stores on S3 and will use AWS tools to implement these requirements. AWS on the other hand is responsible for keeping the data safe from hardware and software failure.

Reference:

<https://aws.amazon.com/compliance/shared-responsibility-model/>

Question 5:

Which security service of AWS is enabled for all AWS customers, by default, at no additional cost?

1. AWS Web Application Firewall (AWS WAF)
2. AWS Secret Manager
3. AWS Shield Standard (Correct)
4. AWS Shield Advanced

#### **Explanation**

Correct option:

**AWS Shield Standard**

AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your website or applications. While AWS Shield Standard helps protect all AWS customers, you get better protection if you are using Amazon CloudFront and Amazon Route 53. All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge.

Incorrect options:

**AWS Web Application Firewall (AWS WAF)** - AWS WAF is a web application firewall that lets you monitor the HTTP(S) requests that are forwarded to an Amazon CloudFront distribution, an Amazon API Gateway API, or an Application Load Balancer. AWS WAF charges based on the number of web access control lists (web ACLs) that you create, the number of rules that you add per web ACL, and the number of web requests that you receive (it is not a free service).

**AWS Secrets Manager** - AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. With Secrets Manager, you pay based on the number of secrets stored and API calls made.

**AWS Shield Advanced** - AWS Shield Advanced includes intelligent DDoS attack detection and mitigation for not only for network layer (layer 3) and transport layer (layer 4) attacks but also for application layer (layer 7) attacks. AWS Shield Advanced is a paid service that provides additional protections for internet-facing applications.

Reference: https://docs.aws.amazon.com/waf/latest/developerguide/shield-chapter.html

Question 6:

AWS Web Application Firewall (WAF) offers protection from common web exploits at which layer?

1. Layer 7 (Correct)
2. Layer 4
3. Layer 4 and Layer 7
4. Layer 3

#### **Explanation**

Correct option:

**Layer 7**

AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API, Amazon CloudFront or an Application Load Balancer. HTTP and HTTPS requests are part of the Application layer, which is layer 7.

Incorrect options:

**Layer 3** - Layer 3 is the Network layer and this layer decides which physical path data will take when it moves on the network. AWS Shield offers protection at this layer. WAF does not offer protection at this layer.

**Layer 4** - Layer 4 is the Transport layer and this layer data transmission occurs using TCP or UDP protocols. AWS Shield offers protection at this layer. WAF does not offer protection at this layer.

**Layer 4 and 7** - This option has been added as a distractor.

Reference: <https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html>

Question 6:

Which of the following is a hybrid storage service that allows on-premises applications to access data on AWS Cloud?

1. AWS Storage Gateway (Correct)
2. AWS Snowball
3. Amazon EBS
4. AWS Direct Connect

#### **Explanation**

Correct option:

**AWS Storage Gateway**

AWS Storage Gateway is a hybrid cloud storage service that connects your existing on-premises environments with the AWS Cloud. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases. These include moving tape backups to the cloud, reducing on-premises storage with cloud-backed file shares, providing low latency access to data in AWS for on-premises applications, as well as various migration, archiving, processing, and disaster recovery use cases.

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

Incorrect options:

"AWS Direct Connect" - AWS Direct Connect creates a dedicated private connection from a remote network to your VPC. This is a private connection and does not use the public internet. Takes at least a month to establish this connection. Direct Connect is a connectivity service and you cannot use it to provide AWS Cloud based storage access to on-premises applications.

"AWS Snowball" - AWS Snowball is a data transport solution that accelerates moving terabytes to petabytes of data into and out of AWS services using storage devices designed to be secure for physical transport. You cannot use Snowball to provide AWS Cloud based storage access to on-premises applications.

"Amazon EBS" - Amazon Elastic Block Store (EBS) is an easy to use, high-performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) instances for both throughput and transaction-intensive workloads at any scale. You cannot use EBS to provide AWS Cloud based storage access to on-premises applications.

Reference:

<https://aws.amazon.com/storagegateway/features/>

Question 7:

Which of the following is a recommended way to provide programmatic access to AWS resources?

1. Use IAM groups to access AWS resources programmatically
2. Create a new IAM user and share the username and password
3. Use Multi Factor Authentication to access AWS resources programmatically
4. Use Access Key ID and Secret Access Key to access AWS resources programmatically. (Correct)

#### **Explanation**

Correct option:

**Use Access Key ID and Secret Access Key to access AWS resources programmatically**

Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK). Access keys consist of two parts: an access key ID and a secret access key. As a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. When you create an access key pair, save the access key ID and secret access key in a secure location. The secret access key is available only at the time you create it. If you lose your secret access key, you must delete the access key and create a new one.

Incorrect options:

**Create a new IAM user and share the username and password** - This is not a viable option, IAM user credentials are not needed to access resources programmatically.

**Use Multi Factor Authentication to access AWS resources programmatically** - For increased security, AWS recommends that you configure multi-factor authentication (MFA) to help protect your AWS resources. You can enable MFA for IAM users or the AWS account root user. MFA adds extra security because it requires users to provide unique authentication from an AWS supported MFA mechanism in addition to their regular sign-in credentials when they access AWS websites or services. MFA cannot be used for programmatic access to AWS resources.

**Use IAM Groups to access AWS resources programmatically** - An IAM Group is a collection of IAM users. Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users. IAM Group is for managing users and not for programmatic access to AWS resources.

Reference:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html>

Question 8:

A company uses reserved EC2 instances across multiple units with each unit having its own AWS account. However, some of the units under-utilize their reserved instances while other units need more reserved instances. As a Cloud Practitioner, which of the following would you recommend as the most cost-optimal solution?

1. Use AWS System Manager to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units
2. Use AWS organizations to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units. (Correct)
3. Use AWS Cost Explorer to manage AWS accounts of all units and share the reserved EC2 instances amongst all units
4. Use AWS Trusted Advisor to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units

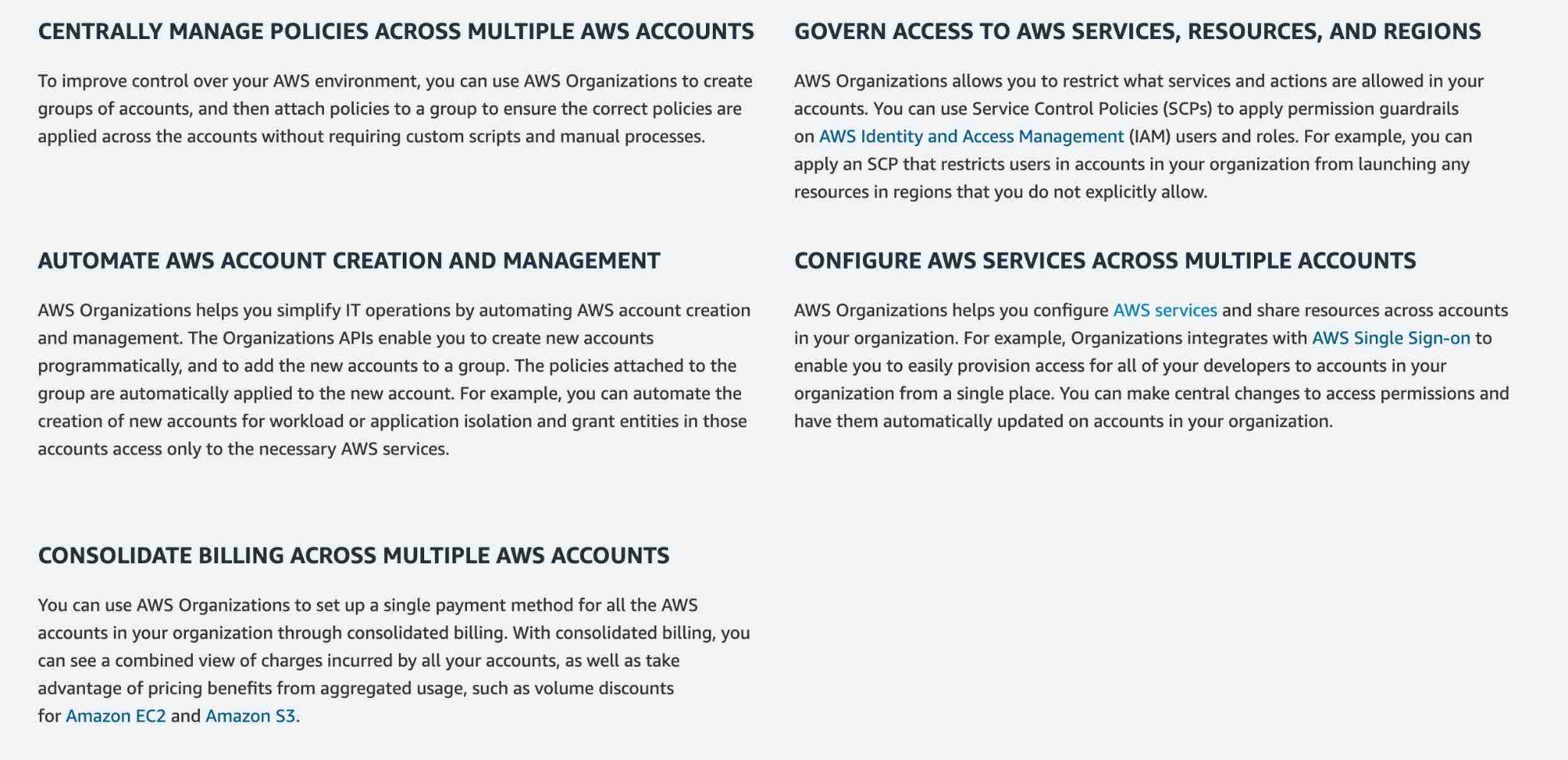
#### **Explanation**

Correct option:

**Use AWS Organizations to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units**

AWS Organizations helps you to centrally manage billing; control access, compliance, and security; and share resources across your AWS accounts. Using AWS Organizations, you can automate account creation, create groups of accounts to reflect your business needs, and apply policies for these groups for governance. You can also simplify billing by setting up a single payment method for all of your AWS accounts. AWS Organizations is available to all AWS customers at no additional charge.

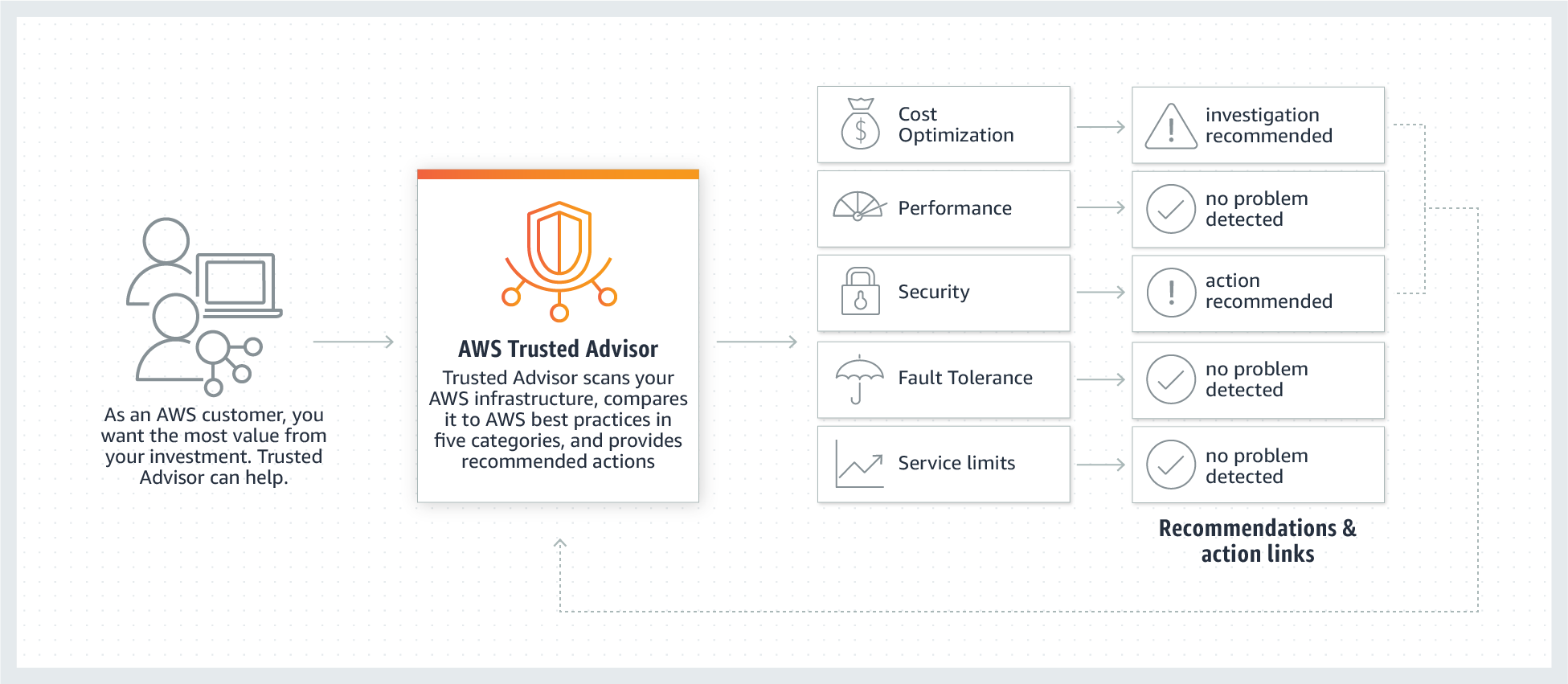
Key Features of AWS Organizations:



Incorrect options:

**Use AWS Trusted Advisor to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units** - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices on cost optimization, security, fault tolerance, service limits, and performance improvement. You cannot use Trusted Advisor to share the reserved EC2 instances amongst multiple AWS accounts.

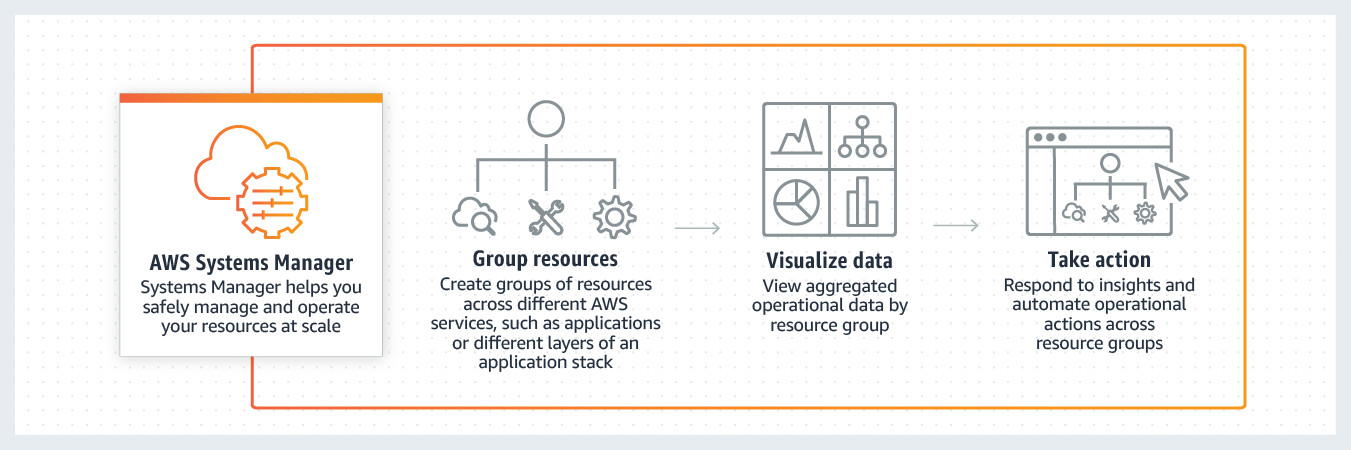
How Trusted Advisor Works:



**Use AWS Cost Explorer to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units** - AWS Cost Explorer lets you explore your AWS costs and usage at both a high level and at a detailed level of analysis, and empowering you to dive deeper using several filtering dimensions (e.g., AWS Service, Region, Linked Account). You cannot use Cost Explorer to share the reserved EC2 instances amongst multiple AWS accounts.

**Use AWS Systems Manager to manage AWS accounts of all units and then share the reserved EC2 instances amongst all units** - Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. With Systems Manager, you can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view operational data for monitoring and troubleshooting, and take action on your groups of resources. You cannot use Systems Manager to share the reserved EC2 instances amongst multiple AWS accounts.

How Systems Manager Works:



References:

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

<https://aws.amazon.com/premiumsupport/technology/trusted-advisor/>

<https://aws.amazon.com/systems-manager/>

Question 9:

Which of the following AWS services manages account privileges?

1. AWS Web Application Firewall (WAF)
2. AWS Identity and Access management (IAM) (Correct)
3. AWS Secret Manager
4. AWS CloudTrail

#### **Explanation**

Correct option:

**AWS Identity and Access Management (IAM)**

In AWS, privilege management is primarily supported by the AWS Identity and Access Management (IAM) service, which allows you to control user and programmatic access to AWS services and resources. You should apply granular policies, which assign permissions to a user, group, role, or resource. You also can require strong password practices, such as complexity level, avoiding re-use, and enforcing multi-factor authentication (MFA). You can use federation with your existing directory service. For workloads that require systems to have access to AWS, IAM enables secure access through roles, instance profiles, identity federation, and temporary credentials.

Incorrect options:

**AWS CloudTrail** - AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides an event history of your AWS account activity, including actions taken through the AWS Management. CloudTrail cannot be used to manage account privileges.

**AWS Web Application Firewall (WAF)** - AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources. It is not an access management system. CloudTrail cannot be used to manage account privileges.

**AWS Secrets Manager** - AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. You cannot use Secrets Manager for creating and using your own keys for encryption on AWS services.

Reference: <https://aws.amazon.com/iam/>

Question 9:

A company wants to have control over creating and using its own keys for encryption on AWS services. Which of the following can be used for this use-case?

1. AWS Managed CMK
2. AWS Owned CMK
3. Secret Manager
4. Customer Manager CMK (Correct)

#### **Explanation**

Correct option:

**Customer Managed CMK**

A customer master key (CMK) is a logical representation of a master key. The CMK includes metadata, such as the key ID, creation date, description, and key state. The CMK also contains the key material used to encrypt and decrypt data. These are created and managed by the AWS customer. Access to these can be controlled using the AWS IAM service.

Incorrect options:

**Secrets Manager** - AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. You cannot use Secrets Manager for creating and using your own keys for encryption on AWS services.

**AWS Managed CMK** - AWS managed CMKs are CMKs in your account that are created, managed, and used on your behalf by an AWS service that is integrated with AWS KMS.

**AWS Owned CMK** - AWS owned CMKs are a collection of CMKs that an AWS service owns and manages for use in multiple AWS accounts. AWS owned CMKs are not in your AWS account. You cannot view or manage these CMKs.

Reference:

<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys>

Question 10:

Under the AWS Shared Responsibility Model, which of the following is a shared responsibility of both AWS and the customer?

1. Infrastructure maintenance of Amazon S3 storage servers
2. Configuration Management (Correct)
3. Guarantee data separation among various AWS customers
4. Availability Zone infrastructure maintenance

#### **Explanation**

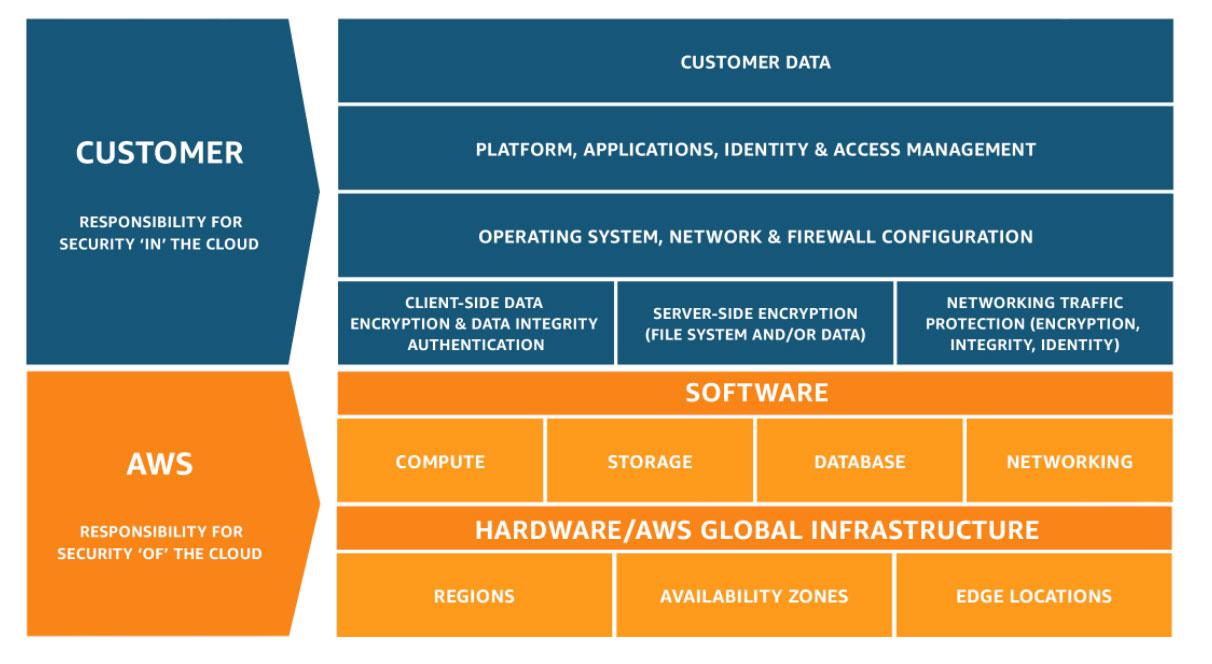
Correct option:

**Configuration Management**

Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer’s operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

Controls that apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives are called shared controls. In a shared control, AWS provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of AWS services. Configuration Management forms a part of shared controls - AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.

Shared Responsibility Model Overview:



Incorrect options:

**Infrastructure maintenance of Amazon S3 storage servers** - AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud.

**Guarantee data separation among various AWS customers** - AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

**Availability Zone infrastructure maintenance** - AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud.

Reference:

[https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master\_keys](https://aws.amazon.com/compliance/shared-responsibility-model/)

Question 11:

A cyber forensics team has detected that AWS owned IP-addresses are being used to carry out malicious attacks. As this constitutes prohibited use of AWS services, which of the following is the correct solution to address this issue?

1. Contact AWS Developer Forum moderators
2. Write an email to Jeff Bezos, the CEO of Amazon, with the details of the incident.
3. Contact AWS Support
4. Contact AWS Abuse Team (Correct)

#### **Explanation**

Correct option:

**Contact AWS Abuse Team**

The AWS Abuse team can assist you when AWS resources are used to engage in abusive behavior.

Please see details of the various scenarios that the AWS Abuse team can address:



Incorrect options:

**Contact AWS Support** - You need to contact the AWS Abuse team for prohibited use of AWS services.

**Contact AWS Developer Forum moderators** - You need to contact the AWS Abuse team for prohibited use of AWS services.

**Write an email to Jeff Bezos, the CEO of Amazon, with the details of the incident** - This has been added as a distractor. For the record, please let us know if you do get a reply from Mr. Bezos.

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/report-aws-abuse/>

Question 12:

A company runs an application on a fleet of EC2 instances. The company wants to automate the traditional maintenance job of running timely assessments and checking for OS vulnerabilities. As a Cloud Practitioner, which service will you suggest for this use case?

1. Amazon GuardDuty
2. Amazon Macie
3. AWS Shield
4. Amazon Inspector (Correct)

#### **Explanation**

Correct option:

**Amazon Inspector**

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on your Amazon EC2 instances. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.

Incorrect options:

**Amazon GuardDuty** - Amazon GuardDuty is a threat detection service that monitors malicious activity and unauthorized behavior to protect your AWS account. GuardDuty analyzes billions of events across your AWS accounts from AWS CloudTrail (AWS user and API activity in your accounts), Amazon VPC Flow Logs (network traffic data), and DNS Logs (name query patterns). This service is for AWS account level access, not for instance-level management like an EC2. GuardDuty cannot be used to check OS vulnerabilities.

**Amazon Macie** - Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS. Macie helps identify and alert you to sensitive data, such as personally identifiable information (PII). This service is for securing data and has nothing to do with an EC2 security assessment. Macie cannot be used to check OS vulnerabilities.

**AWS Shield** - AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. Shield is general protection against DDos attacks for all resources in the AWS network, and not an instance-level security assessment service. Shield cannot be used to check OS vulnerabilities.

Reference:

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

Question 13:

Which AWS Service can be used to mitigate a Distributed Denial of Service (DDoS) attack?

1. Amazon CloudWatch
2. AWS Shield (Correct)
3. AWS KMS
4. AWS System Manager

#### **Explanation**

Correct option:

**AWS Shield**

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. There are two tiers of AWS Shield - Standard and Advanced.

All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your web site or applications. When you use AWS Shield Standard with Amazon CloudFront and Amazon Route 53, you receive comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks.

For higher levels of protection against attacks targeting your applications running on Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator and Amazon Route 53 resources, you can subscribe to AWS Shield Advanced. In addition to the network and transport layer protections that come with Standard, AWS Shield Advanced provides additional detection and mitigation against large and sophisticated DDoS attacks, near real-time visibility into attacks, and integration with AWS WAF, a web application firewall.

Incorrect options:

**Amazon CloudWatch** - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. This is an excellent service for building Resilient systems.

**AWS Systems Manager** - AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. With Systems Manager, you can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view operational data for monitoring and troubleshooting, and take action on your groups of resources.

**AWS KMS** - AWS Key Management Service (KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys.

Reference:

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

Question 14:

A medical research startup wants to understand the compliance of AWS services concerning HIPAA guidelines. Which AWS service can be used to review the HIPAA compliance and governance-related documents on AWS?

1. AWS Trusted Advisor
2. AWS Secret Manager
3. AWS Artifact (Correct)
4. AWS Systems Manager

#### **Explanation**

Correct option:

**AWS Artifact**

AWS Artifact is your go-to, central resource for compliance-related information that matters to your organization. It provides on-demand access to AWS’ security and compliance reports and select online agreements. Reports available in AWS Artifact include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls. Different types of agreements are available in AWS Artifact Agreements to address the needs of customers subject to specific regulations. For example, the Business Associate Addendum (BAA) is available for customers that need to comply with the Health Insurance Portability and Accountability Act (HIPAA). It is not a service, it's a no-cost, self-service portal for on-demand access to AWS’ compliance reports.

Incorrect options:

**AWS Trusted Advisor** - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally.

**AWS Secrets Manager** - AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text.

**AWS Systems Manager** - AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. With Systems Manager, you can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view operational data for monitoring and troubleshooting, and take action on your groups of resources.

Reference:

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