Security

CloudTrail - audit
CloudTrail is a service that enables customers to audit API calls in their AWS accounts.
CloudTrail logs are stored in an S3 bucket and can be analyzed using tools such as Amazon Athena, Amazon EMR, and AWS Glue, to identify trends and troubleshoot issues.

Cloudwatch - monitor for cloud instance

CloudWatch Logs Insights enables you to interactively search and analyze your log data in Amazon CloudWatch Logs. You can perform queries to help you more efficiently and effectively respond to operational issues. If an issue occurs, you can use CloudWatch Logs Insights to identify potential causes and validate deployed fixes
Amazon CloudWatch provides monitoring and observability services for AWS resources, including EC2 instances. It allows you to set up alarms on various metrics, such as CPU utilization, network traffic, or disk usage. When a specific threshold is breached, an alarm is triggered.

Amazon CloudWatch alarms can be created on the Auto Scaling group as a whole, such as Average CPU Utilization. This is because alarms are used to tell Auto Scaling when to add/remove instances and such decisions would be based upon the group as a whole.

Inspector - vulnerability management
Inspector is an automated security assessment service provided by AWS. It helps you identify security vulnerabilities and potential issues in your applications and infrastructure. In the given scenario, Amazon Inspector can be used to generate an automated security assessment report that includes the identification of unintended network access to Amazon EC2 instances and operating system vulnerabilities on those instances.
"Vulnerability" which is Inspector.
Inspector is an automated vulnerability management service that continually scans Amazon Elastic Compute Cloud (EC2), AWS Lambda functions, and container workloads for software vulnerabilities and unintended network exposure

X-Ray - **tracing**
X-Ray is a service for analyzing and debugging distributed applications.

X-Ray is a service that helps developers analyze and debug distributed applications, such as those running on microservices architectures. It provides end-to-end visibility into requests as they travel across various components and services, allowing you to identify performance bottlenecks, troubleshoot issues, and optimize application performance.
X-Ray provides a complete view of requests as they travel through your application and filters visual data across payloads, functions, traces, services, APIs, and more with no-code and low-code motions

Trusted Advisor publishes metrics about your check results to CloudWatch.
Trusted Advisor checks and status changes for resources, and service quota usage

---

Trusted Advisor provides recommendations to help you follow AWS best practices for security, cost optimization, performance improvement, and fault tolerance.

AWS Business Support is the LEAST expensive AWS Support plan that contains a **full set of AWS Trusted Advisor** best practice checks

---

GuardDuty：continuously monitors for malicious activity and unauthorized behavior in AWS accounts

GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation

GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads.

GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.

GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation. Continuously monitor your AWS accounts, instances, serverless and container workloads, users, databases, and storage for potential threats

---

总结：

Inspector 偏向 EC2 的安全漏洞和配置错误

X-ray 用来分析和调试分布式应用，查看性能，瓶颈，错误异常等

GuardDuty 则是全 aws 的防护，是持续监控服务

Network ACL is a feature of Amazon Virtual Private Cloud (VPC) that acts as a firewall at the subnet level. It is an optional layer of security that controls inbound and outbound
By default, a Network ACL allows all inbound and outbound traffic.

Security Group：安全组是应用在 EC2 实例级别的一种防火墙。它控制进出 EC2 实例的流量。

Network ACL：网络 ACL 则是应用在子网级别的一种防火墙。它控制进出子网的流量。

Security Group：安全组更适合用于 EC2 实例级别的安全控制，如允许特定端口的流量、允许特定 IP 地址的访问等。

Network ACL：网络 ACL 更适合用于对整个子网中的流量进行更细粒度的控制，如阻止特定 IP 段的流量、控制特定协议的流量等。

Systems Manager Session Manager

AWS Systems Manager **Session Manager** is a new interactive shell and CLI that helps to provide secure, access-controlled, and audited Windows and Linux EC2 instance management. Session Manager removes the need to open inbound ports, manage SSH keys, or use bastion hosts.

A company wants to improve its security and audit posture by limiting Amazon EC2 inbound access.

What should the company use to access instances remotely instead of opening inbound SSH ports and managing SSH keys?

AWS Direct Connect

AWS Direct Connect is a cloud service that links your network directly to AWS to deliver consistent, low-latency performance.

Amazon **AppStream** VS Amazon **WorkSpaces**

Amazon AppStream 2.0 is focused on hosting individual applications on AWS,

Amazon WorkSpaces creates virtual desktops that can be used to create entire working environments for you and your team

Directconnect 是专用网络，用来本地和 aws 建立私有链接，System session manager 则是用来远程管理 ec2 及其他资源。

WAF

WAF can be deployed on Amazon CloudFront, the Application Load Balancer (ALB), Amazon API Gateway, and AWS AppSync. As part of Amazon CloudFront it can be part of your Content Distribution Network (CDN) protecting your resources and content at the Edge locations. As part of the Application Load Balancer it can protect your origin web servers running behind the ALBs. As part of Amazon API Gateway, it can help secure and protect your REST APIs. As part of AWS AppSync, it can help secure and protect your GraphQL APIs.

WAF -- httlps

Which AWS services can use AWS **WAF** to protect against common web exploitations? (Choose two.)
Amazon CloudFront
Amazon API Gateway

Security group (For EC2)

Security groups control the inbound and outbound traffic at the instance level, **ACLs** control traffic at the subnet level (base on IP). So in this case, the correct answer is network ACLs.

---

security group acts as a virtual firewall for your EC2 instances to control incoming and outgoing traffic. Inbound rules control the incoming traffic to your instance, and outbound rules control the outgoing traffic from your instance. When you launch an instance, you can specify one or more security groups If you don't specify a security group, Amazon EC2 uses the default security group for the VPC.

Amazon Detective

Amazon Detective makes it easy to analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities.

Shield -- DDoS
WAF -- httlps
Security group --EC2
Network ACLs --subnet

Storage

Redshift petadata wareshouse

S3
A company wants to use Amazon S3 to store its legacy data. The data is rarely accessed. However, the data is critical and cannot be recreated. The data needs to be available for retrieval within seconds.

Which S3 storage class meets these requirements MOST cost-effectively?

C. S3 Standard-Infrequent Access (S3 Standard-IA)

S3 = Secure, durable, and scalable object storage infrastructure. S3 can be **used to host static websites to deliver HTML**, JavaScript, images, and video for sites that do not contain server-side scripting.

EBS

Amazon Elastic Block Store (Amazon EBS) 是一种易于使用且可扩展的高性能数据块存储

服务，适合用于 Amazon Elastic Compute Cloud (Amazon EC2)。

EFS

Amazon Elastic File System (EFS) 可随着您添加和删除文件自动增大或收缩，无需管理或

预置。

Which AWS services provide high availability across multiple Availability Zones by default? (Choose two.)
Amazon Elastic File System (Amazon EFS)
Amazon S3
DynomaDB

Which Amazon S3 feature or storage class uses the AWS backbone network and edge locations to reduce latencies from the end user to Amazon S3?
S3 Transfer Acceleration

What is the security best practice concerning **sensitive** data stored in Amazon **S3**?
Enable S3 server-side encryption on the S3 bucket

Amazon Redshift is a fully managed data warehouse service that uses cloud-native storage with automatic replication across multiple Availability Zones，其他关键词：

"Petabytes" scale of data，semi-structure

Amazon Redshift 使用 SQL 在数据仓库、运营数据库和数据湖间分析结构化和半结构化数据，使用 AWS 设计的硬件和机器学习在任意规模提供最佳性价比。

借助 **Amazon Redshift**，您可以更轻松地运行和扩展分析，而无需管理您的数据仓库。可以通过对运营数据库、数据湖、数据仓库以及数以千计的第三方数据集中的所有数据运行实时的预测性分析，获取深入见解。

Amazon Redshift 和 Amazon Athena 是两种不同的 AWS 数据分析服务，适用于不同的使用情况和需求。Redshift 适用于大规模数据仓库和持久性数据分析，而 Athena 适用于临时性的数据分析和探索性查询。

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

Amazon Simple Notification Service (Amazon SNS)

Which AWS service or feature is used to send both text and email messages from distributed applications?

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. Using API Gateway, you can create RESTful APIs and WebSocket APIs that enable real-time two-way communication applications. API Gateway supports containerized and serverless workloads, as well as web applications.

Which AWS services can use AWS WAF to protect against common web exploitations?
Amazon API Gateway

Amazon Simple Queue Service (Amazon SQS)

Which AWS service helps developers use loose coupling and reliable messaging between microservices?

Amazon Simple Queue Service (Amazon SQS) lets you send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available.

Cognito

借助 Amazon Cognito，您可将用户注册和登录功能以及控制访问添加到您的 Web 和移动应用程序中。Amazon Cognito 提供可扩展到数百万用户的身份存储，支持社会和企业进行身份联合验证，并提供高级安全功能以保护您的消费者和企业。Amazon Cognito 基于开放身份标准构建，其支持各种合规性法规，并与前短和后端开发资源集成。

Amazon **Cognito** is a service that provides user authentication and authorization services, including the ability to log in through social identity providers such as Google, Facebook, and Amazon. It's commonly used for building applications with user registration, login, and account management functionality.

Instance

Spot Instances. 竞价实例，便宜，但是会随时终止

Amazon EC2 **Dedicated** Hosts allow you to use your existing **per**-socket, **per**-core, or **per**-VM software licenses that are bound to VMs, sockets, or physical cores, subject to your license terms.

Auto scaling it is used to increase/ decrease the number of EC2 instances

Macie

Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS.

Macie automatically detects a large and growing list of sensitive data types, including personally identifiable information (PII) such as names, addresses, and credit card numbers. It also gives you constant visibility of the data security and data privacy of your data stored in Amazon S3.

Amazon Macie 是一项数据安全和数据隐私服务，它利用机器学习（ML）和模式匹配来发现和保护敏感数据。

Glue

stick 3 things together: Extract, transform, load (ETL)
Glue is a fully managed extract, transform, and load (ETL) service that makes it easy to prepare and load data for analytics. It provides capabilities for discovering, cataloging, cleaning, and transforming data, making it ready for analysis. With AWS Glue, you can create and manage data transformation workflows, and it integrates well with other AWS services for data storage, such as Amazon S3 and Amazon Redshift.

AWS Glue is another offering from AWS and is a serverless ETL (Extract, Transform, and Load) service on the cloud. It is fully managed, cost-effective service to categorize your data, clean and enrich it and finally move it from source systems to target systems.

AWS VPN

A company is moving its office and must establish an encrypted connection to AWS.

Database

Amazon **DynamoDB** is a key-value and document database that delivers single-digit millisecond performance at any scale. It's a fully managed, multi-Region database with built-in security, backup and restore, and in-memory caching for internet-scale applications.

Which task does AWS perform automatically?
Encrypt data that is stored in Amazon DynamoDB

Amazon Neptune is a fully managed graph database service that provides high availability and durability through automatic replication of data across multiple Availability Zones.

Code management

CodeGuru

将 Amazon CodeGuru Security 与您的开发管道集成，以提高代码质量并优化应用程序性能。 CodeGuru Security 基于数十年的知识和经验进行训练，使用机器学习和自动推理来**精确识别代码漏洞**。CodeGuru Security 还借鉴了 AWS 安全最佳实践以及有关 Amazon 内部数百万个代码漏洞评测的训练。然后，CodeGuru Security 能以极低的误报率识别代码漏洞。要开始审查代码，您可以在 CodeGuru 控制台中关联 GitHub、GitHub Enterprise、Bitbucket 或 AWS CodeCommit 上现有的代码存储库。

AWS **CodeStar** is a fully managed service that enables you to quickly develop, build, and deploy applications on AWS. It provides a pre-configured continuous delivery toolchain with integrations for various AWS services like AWS CodeCommit for source code repositories, AWS CodeBuild for building code, AWS CodePipeline for continuous delivery, and AWS CodeDeploy for automated deployments. With AWS CodeStar, you can set up an entire development and continuous delivery toolchain for coding, building, testing, and deploying code with ease.

AWS CodeCommit

AWS CodeCommit is a secure, highly scalable, managed source control service that hosts private Git repositories. It makes it easy for teams to securely collaborate on code with contributions encrypted in transit and at rest.

AWS CodeCommit is a managed source control system that hosts Git repositories and works with all Git-based tools.

AWS **Cloud9** is a cloud-based integrated development environment (IDE) that allows a company to write, run, and debug code on a browser-based interface. It provides a collaborative, browser-based environment that includes a code editor, a terminal, and a debugger. The service also integrates with AWS services such as Lambda, Elastic Beanstalk, and EC2 to provide a seamless experience for developers. The company can use it to migrate all of its development teams to a cloud-based IDE

Serverless

A key benefit of using AWS **serverless** computing, specifically with services like AWS Lambda, is that the management of the underlying infrastructure is abstracted away from the developers. AWS takes care of the server provisioning, scaling, and maintenance, allowing developers to focus solely on writing code for their applications. This eliminates the need for manual server management, patching, and monitoring, which reduces operational overhead and allows developers to be more productive and focus on building and deploying applications.
AWS Step Functions is a visual workflow service that helps developers use AWS services to build distributed applications, automate processes, orchestrate microservices, and create data and machine learning (ML) pipelines. It is serverless

Include: dynamoDB,S3, Fargate,Lambda,step function(state machine service)workflow,aurora
Pay for value. Can be scale-to-zero.

AWS CONFIG

AWS CONFIG : its fully managed service , its giving information of our resources configuration , so if any configuration of resources are changed means its send a notifications to users and resolved that issues .
AWS Config is a service that helps you assess, audit, and evaluate the configurations of your AWS resources. It continuously monitors and records changes to your AWS resource configurations and provides a detailed view of the configuration history. With AWS Config, you can capture configuration details and changes, and use the recorded information for compliance auditing, security analysis, resource change tracking, and troubleshooting. It can help you ensure that your resources are configured and used according to your organization's policies and best practices.

发布与部署

AWS Fargate

AWS Fargate 是一种无服务器、随用随付的计算引擎，可让您专注于构建应用程序，而无需管理服务器。将服务器管理、资源分配和扩展等任务转移到 AWS 不仅可以改善您的运营状况，还可以加快云端从构思到生产的过程，并降低总拥有成本。

AWS Fargate 与 Amazon Elastic Container Service（Amazon ECS）和 Amazon Elastic Kubernetes Service（Amazon EKS）兼容。选择任何符合 OCI 标准的容器映像，定义内存和计算资源，然后使用无服务器计算运行容器。由于该服务支持多种 CPU 架构和操作系统，因此您可以在各种应用程序中享受这些好处。

选择 AWS Fargate 还是 Amazon ECS 取决于您更需要哪些抽象级别和控制权，以及您需要满足哪些要求。如果您认为可创建一个 Docker 镜像并想快速轻松地利用 Amazon ECS 运行容器，则 AWS Fargate 是一个很好的选择。如果您希望对您的计算资源和操作系统进行更详细控制并使用更多可用的优惠活动，则 Amazon ECS 可能更适合您的情况。

Beanstalk

AWS Elastic **Beanstalk** 可部署 Web 应用程序，因此您可以专注于您的业务。

Elastic **Beanstalk** 和 AWS **CodeDeploy** 区别：最大的区别是： CodeDeploy 是将应用程序部署到现有 EC2 实例的服务。它不考虑 LoadBalancing 或缩放等因素。ElasticBeanstalk 是更多的 PaaS 服务，它为您提供了扩展应用程序所需的所有包装，因此您不需要担心 DevOps 方面（The developers want to deploy their applications without having to provision the infrastructure themselves）。

Fargate 是一种 serverless 的容器托管服务，适用于容器化的工作负载，提供了高度自动化和弹性伸缩的部署模式。

Elastic Beanstalk 则是一种应用程序托管平台，适用于传统的应用程序和 Web 服务，提供了简化的部署、管理和扩展功能。

Lambda

A company wants to migrate a critical application to AWS. The application has a short runtime. The application is invoked by changes in data or by shifts in system state. The company needs a compute solution that maximizes operational efficiency and minimizes the cost of running the application.

A company needs to perform data processing once a week that typically takes about 5 hours to complete.

Which AWS service should the company use for this workload?

Amazon EC2，不能是 Lambda，因为 Lambda 只能运行 15 分钟

Compliance

AWS Compliance program VS AWS Artifact
AWS Compliance program is described as “helping customers to understand the robust controls in place at AWS to maintain security and compliance in the cloud.”, so the understanding if they meet the requirements before doing anything in AWS:
https://aws.amazon.com/compliance/programs/
AWS Artifact is used to manage and accept all required agreements for IAM roles for members of the organization, as well as monitor for new future agreements, but that is after acknowledging which services are already running:
https://www.youtube.com/watch?v=rss0CJ0bw40

Others

Amazon **Kinesis** is a fully managed service that allows you to collect, process, and analyze streaming data in real-time. This service can be used to process clickstream data from an ecommerce website in real-time.

Amazon Connect, you can set up a contact center in minutes that can scale to support millions of customers.

Edge locations are used by Amazon CloudFront for content delivery and do not directly impact the location of EC2 instances.

Which of the following does Amazon CloudFront use to distribute content to users around the world?
Edge locations

Amazon CloudFront uses a network of edge locations to distribute content to users around the world. These edge locations are geographically distributed points of presence that cache and deliver content to users with low latency.

Service Health Dashboard displays the general status of Amazon Web Services services,
Personal Health Dashboard gives you a personalized (your company)view into the performance and availability of the Amazon Web Services services underlying your Amazon Web Services resources.

"**VPC Flow Logs** is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to the following locations: Amazon CloudWatch Logs, Amazon S3, or Amazon Kinesis Data Firehose. After you create a flow log, you can retrieve and view the flow log records in the log group, bucket, or delivery stream that you configured."

Which AWS services offer gateway VPC endpoints that can be used to avoid sending traffic over the internet?
* Amazon S3
* Amazon DynamoDB
* Kinesis
* SNS

An ecommerce company has deployed a new web application on Amazon EC2 instances. The company wants to distribute incoming HTTP traffic evenly across all running instances.
Which AWS service or resource will meet this requirement?

Application Load Balancer （ALB）

A company recently created its first AWS account.
Which AWS services will require the use of a VPC? (Choose two.)
Amazon Elastic File System (Amazon EFS)
Amazon EC2
RDS
ECS
Lambda
Elastic Beanstalk
Fargate
RedShift

说明：**Amazon EFS** is a file storage service that provides a persistent file system for your

EC2 instances. It requires a VPC to isolate your EFS file system from other resources in the AWS Cloud.

Amazon EC2 is a service that provides virtual machines that you can use to run your applications. It requires a VPC to isolate your EC2 instances from other resources in the

AWS Cloud.

Architecture optimization focuses on the need to continually refine workloads to be more cost-conscious to create better architected systems.

CloudFormation

AWS CloudFormation 允许您通过将基础设施视为代码来建模、预置和管理 AWS 和第三方资源。 Iac(infrastructure as Code)

Global tables build on the global Amazon DynamoDB footprint to provide you with a fully managed, multi-Region, and multi-active database that delivers fast, local, read and write performance for massively scaled, global applications. Global tables replicate your DynamoDB tables automatically across your choice of AWS Regions.

AWS **Batch** is a service that makes it easy to run batch computing workloads on the AWS Cloud. It enables developers, scientists, and engineers to easily and efficiently run hundreds of thousands of batch computing jobs on a managed cluster of Amazon EC2 instances.

Ground station， 和卫星相关 satellite， used for weather forecasting, surface imaging, conmunications,video boradcasts

Elastic load blance 和 alb 区别，elb 用来分发流量的，可以支持多个 zone 分发，但是不支持跨 region；alb 基于第七层，如可以根据 url 分发

AWS OpsWorks CM 是一项运行和管理配置管理服务器的服务。您可以使用 AWS OpsWorks CM 创建和管理 AWS OpsWorks for Chef Automate 和 OpsWorks for Puppet Enterprise 服务器，并添加或删除要管理的服务器的节点。

AWS OpsWorks CM is a service that runs and manages configuration management servers. You can use AWS OpsWorks CM to create and manage AWS OpsWorks for Chef Automate and OpsWorks for Puppet Enterprise servers, and add or remove nodes for the servers to manage.

Devops

Storage class	Expedited	Standard	Bulk
S3 Glacier Instant Retrieval	Not applicable	Not applicable	Not applicable
S3 Glacier Flexible Retrieval	1–5 minutes	3–5 hours	5–12 hours
S3 Glacier Deep Archive	Not available	Within 12 hours	Within 48 hours