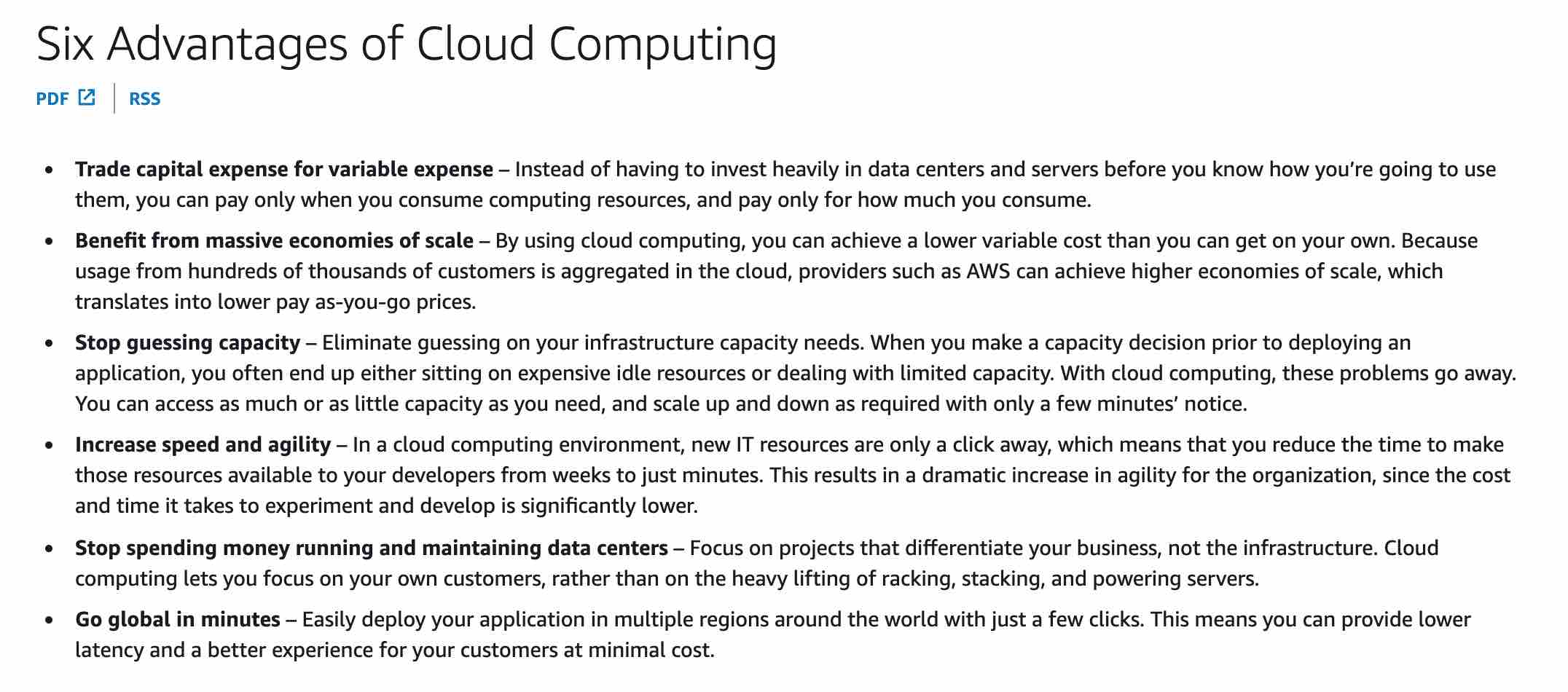
**Six advantages of cloud computing**



**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.

AWS Trusted Advisor can check Amazon Elastic Block Store (Amazon EBS) volume configurations and warns when volumes appear to be underused. Charges begin when a volume is created. If a volume remains unattached or has very low write activity (excluding boot volumes) for a period of time, the volume is probably not being used

AWS Trusted Advisor checks the Amazon Elastic Compute Cloud (Amazon EC2) instances that were running at any time during the last 14 days and alerts you if the daily CPU utilization was 10% or less and network I/O was 5 MB or less on 4 or more days.

**Service Quotas** enables you to view and manage your quotas for AWS services from a central location. Quotas, also referred to as limits in AWS, are the maximum values for the resources, actions, and items in your AWS account.

**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.

**AWS CloudFormation** - AWS CloudFormation provides a common language to model and provision AWS and third-party application resources in your cloud environment. 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. Think infrastructure as code; think CloudFormation. It is **Infrastructure as Code service.**

**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**. Think resource performance monitoring, events, and alerts; think CloudWatch.

To build the solution for the given use-case, you can create a CloudWatch Events rule that triggers on a schedule via a cron expression. You can then set the Lambda as the target for this rule.

**AWS Cost Explorer** has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time. AWS Cost Explorer also **supports forecasting** to get a better idea of what your costs and usage may look like in the future so that you can plan.

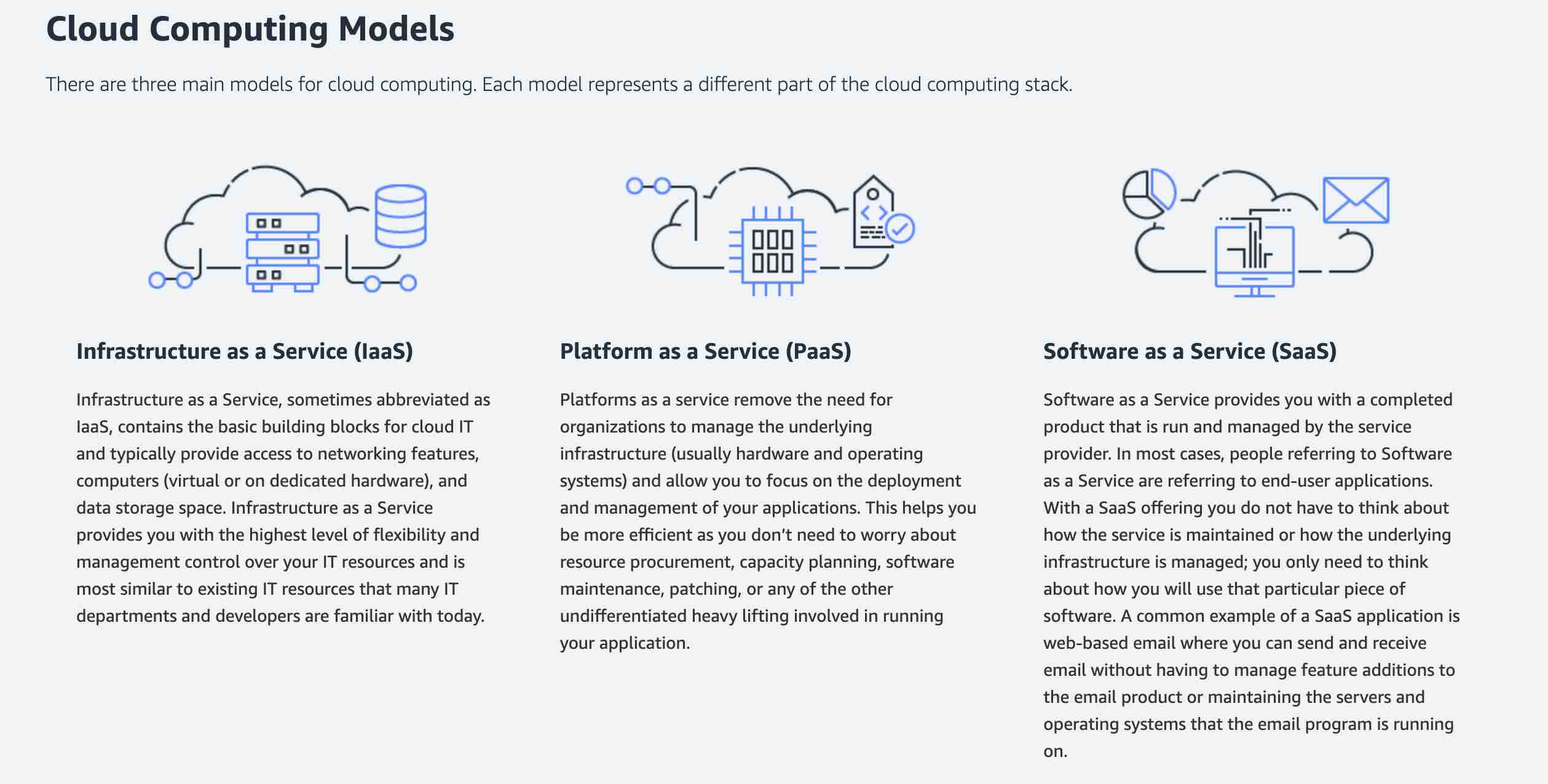
**AWS Cost and Usage Reports** - The AWS Cost and Usage Reports (AWS CUR) contains the most comprehensive set of cost and usage data available. You can use Cost and Usage Reports to publish your AWS billing reports to an Amazon Simple Storage Service (Amazon S3) bucket that you own. You can receive reports that break down your costs by the hour or month, by product or product resource, or by tags that you define yourself. AWS updates the report in your bucket once a day in a comma-separated value (CSV) format. **AWS Cost and Usage Reports cannot forecast your AWS account cost and usage.**

**AWS Budgets** - AWS Budgets gives the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount. **AWS Budgets cannot forecast your AWS account cost and usage.** You can also use AWS Budgets to set reservation utilization or coverage targets and receive alerts when your utilization drops below the threshold you define. Reservation alerts are supported for Amazon EC2, Amazon RDS, Amazon Redshift, Amazon ElastiCache, and Amazon Elasticsearch reservations.

**AWS Pricing Calculator** - AWS Pricing Calculator lets you explore AWS services and create an estimate for the cost of your use cases on AWS. You can plan your AWS costs and usage or price out setting up a new set of instances and services.

**AWS Elastic Beanstalk** makes it even easier for developers to **quickly deploy and manage applications** in the AWS Cloud. Developers simply upload their application, and Elastic Beanstalk automatically handles the deployment details of **capacity provisioning, load balancing, auto-scaling, and application health monitoring.**

It is a **Platform as a Service** as you only manage the applications and the data.



**AWS Config** is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations.

**Amazon Inspector** is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices.

**S3 One Zone-Infrequent Access** is for data that is accessed less frequently but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA. S3 One Zone-IA offers the same high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee.

**S3 Glacier** is a secure, durable, and low-cost storage class for **data archiving.** Although Glacier is cheaper than One Zone-IA, however the retrieval time ranges **from a minute to hours**.

**Horizontal Scaling** - A "horizontally scalable" system is one that can increase capacity by adding more computers to the system.

**Vertical Scaling** is adding more resources (like CPU, RAM) to a single node or machine. Example- Resizing an instance of EC2.

**Auto Scaling Group** is an example of Horizontal Scaling on AWS.

**Performance Efficiency** - Is the ability to use computing resources efficiently to meet system requirements and to maintain that efficiency as demand changes and technologies evolve.

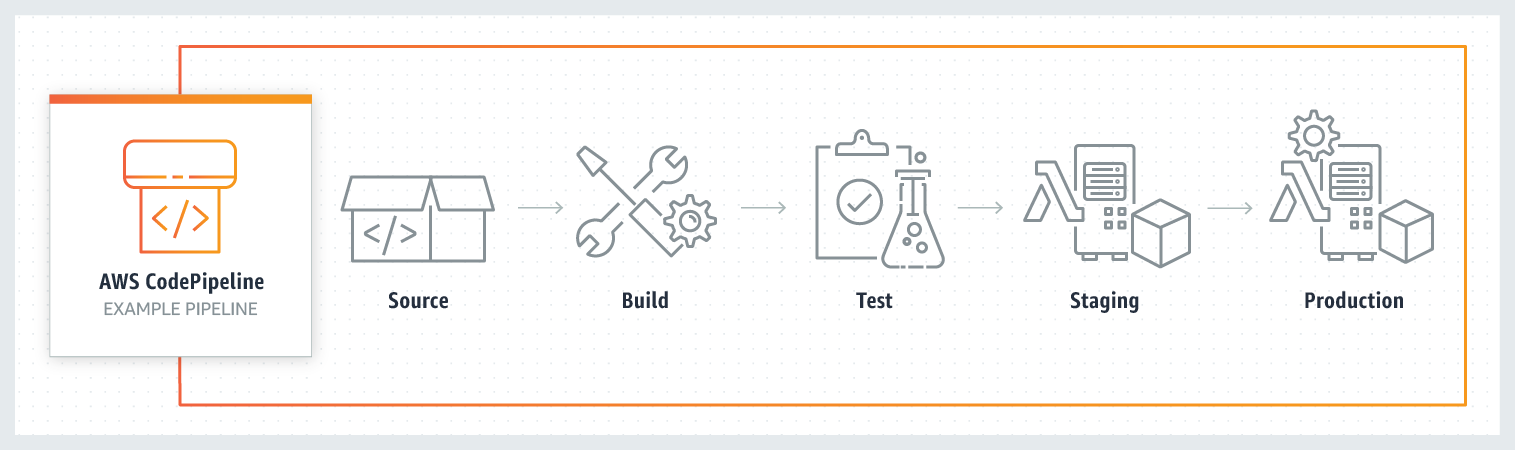
**AWS Directory Service** - AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud. It is not used to deploy resources.

**Amazon LightSail** - Amazon Lightsail is designed to be the easiest way to launch and manage a virtual private server with AWS. It is not best suited when deploying more complex resources, while CloudFormation can. Simpler alternative to using EC2, RDS, ELB, EBS, Route 53…. Great for people with little cloud experience.

**AWS CodeDeploy** - AWS CodeDeploy is a service that automates code deployments to any instance, including EC2 instances and instances running on-premises. Unlike CloudFormation, it does not deal with infrastructure configuration and orchestration.

**AWS CodeCommit** - AWS CodeCommit is a fully managed source control service that hosts secure **Git-based repositories**. It makes it easy for teams to collaborate on code in a secure and highly scalable ecosystem. CodeCommit eliminates the need to operate your own source control system or worry about scaling its infrastructure. It cannot be used to automate code deployment.

**AWS CodePipeline** - AWS CodePipeline is a continuous delivery service that enables you to model, visualize, and automate the steps required to release your software. With AWS CodePipeline, you model the full release process for building your code, deploying to pre-production environments, testing your application and releasing it to production.



**AWS Local Zones** allow you to use select AWS services, like compute and storage services, closer to more end-users, providing them very low latency access to the applications running locally. AWS Local Zones are also connected to the parent region via Amazon’s redundant and very high bandwidth private network, giving applications running in AWS Local Zones fast, secure, and seamless access to the rest of AWS services.

**AWS Edge Locations** - An AWS Edge location is a site that CloudFront uses to **cache copies** of the content for faster delivery to users at any location.

**AWS Wavelength** - AWS Wavelength extends the AWS cloud to a **global network of 5G** edge locations to enable developers to innovate and build a whole new class of applications that require ultra-low latency. Wavelength Zones provide a high-bandwidth, secure connection to the parent AWS Region, allowing developers to seamlessly connect to the full range of services in the AWS Region through the same APIs and toolsets.

**AWS Direct Connect** - WS 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 cannot be used to interconnect VPCs.

**VPC Endpoint** - 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.

**Identity and Access Management (IAM)** - AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. IAM is a feature of your AWS account offered at no additional charge.

**AWS Auto Scaling** - AWS Auto Scaling monitors your applications and automatically adjusts the capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it’s easy to setup application scaling for multiple resources across multiple services in minutes. AWS Auto Scaling is available at no additional charge. You pay only for the AWS resources needed to run your applications and Amazon CloudWatch monitoring fees.

**Elastic Compute Cloud (Amazon EC2)** - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. This is not a free service. You pay for what you use or depending on the plan you choose. It is an Infrastructure as a service (IAAS). There is a one-minute minimum charge for Linux based EC2 instance

**Simple Storage Service (Amazon S3)** - Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. S3 service is not free and you pay to depend on the storage class you choose for your data.

**DynamoDB** - 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, multi-master, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications. DynamoDB is not free and you are charged for reading, writing, and storing data in your DynamoDB tables, along with any optional features you choose to enable.

**DynamoDB global tables** replicate data automatically across your choice of AWS Regions and automatically scale capacity to accommodate your workloads. With global tables, your globally distributed applications can access data locally in the selected regions to get single-digit millisecond read and write performance. DynamoDB offers active-active cross-region support that is needed for the company.

**Amazon DynamoDB with DynamoDB Accelerator** - DynamoDB Accelerator (DAX) is an in-memory cache that delivers fast read performance for your tables at scale by enabling you to use a fully managed in-memory cache. Using DAX, you can improve the read performance of your DynamoDB tables by up to 10 times—taking the time required for reads from milliseconds to microseconds, even at millions of requests per second. DAX does not offer active-active cross-Region configuration.

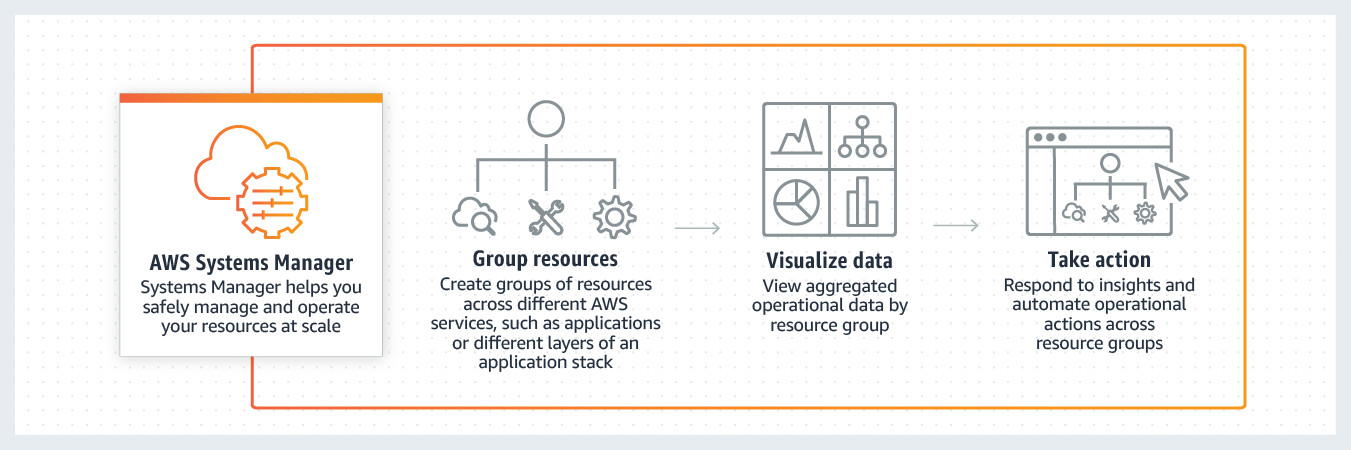
**Amazon RedShift** - Amazon Redshift is a fully-managed petabyte-scale cloud-based data warehouse product designed for **large scale data set storage and analysis**. Amazon Redshift requires a well-defined schema.

**Amazon Aurora** - Amazon Aurora (Aurora) is a fully managed relational database engine that's compatible with MySQL and PostgreSQL. With some workloads, Aurora can deliver up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications. The AWS Product team is responsible for applying patches to the underlying OS for AWS Aurora.

**Amazon RDS** - Amazon RDS is an AWS service for relational databases. RDS requires a well-defined schema.

**Amazon Aurora with multi-master cluster** - In a multi-master cluster, all DB instances have read/write capability. Currently, all DB instances in a multi-master cluster must be in the same AWS Region. You can't enable cross-Region replicas from multi-master clusters.

**Amazon Relational Database Service (Amazon RDS) for MYSQL** - Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security and compatibility they need. RDS does not support active-active configuration with cross-region support.

**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 SSM Session Manager** is a fully-managed service that provides you with an interactive **browser-based shell and CLI experience**. It helps provide secure and auditable instance management without the need to open inbound ports, maintain bastion hosts, and manage SSH keys. Session Manager helps to enable compliance with corporate policies that require controlled access to instances, increase security and auditability of access to the instances while providing simplicity and cross-platform instance access to end-users.

**Amazon EC2 Instance Connect** - Amazon EC2 Instance Connect provides a simple and secure way to connect to your **Linux instances using Secure Shell** (SSH). With EC2 Instance Connect, you use AWS Identity and Access Management (IAM) policies and principals to control SSH access to your instances, removing the need to share and manage SSH keys. Instance Connect will need **port 22** to be open for traffic.

**Step Function** - AWS Step Function lets you coordinate multiple AWS services into **serverless workflows**. You can design and run workflows that stitch together services such as AWS Lambda, AWS Glue and Amazon SageMaker. Step Function cannot be used to run a process on a schedule.

**AWS Personal Health Dashboard** - AWS Personal Health Dashboard provides **alerts and remediation guidance** when AWS is experiencing events that might affect you. It is not used to get operational insights of AWS resources.

**AWS Service Health Dashboard** - AWS Service Health Dashboard publishes most **up-to-the-minute** information on the status and availability of **all AWS services** in tabular form for all Regions that AWS is present in.

AWS Service Health Dashboard offers the possibility to subscribe to an RSS feed to be notified of interruptions to each service.

**Exam Alert:**

While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view of the performance and availability of the AWS services underlying **your AWS resources.**

**AWS Lambda** - AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second. Lambda does not support running container applications.

**Amazon SNS** - Amazon Simple Notification Service (Amazon SNS) is a highly available, durable, secure, fully managed **pub/sub** messaging service that enables you to **decouple microservices**, distributed systems, and serverless applications. It can be used to deliver notifications, but it does not provide current services' status.

**SQS** - Amazon Simple Queue Service (SQS) is a fully **managed message queuing service** that enables you to **decouple and scale microservices**, distributed systems, and serverless applications. Using SQS, you can **send, store, and receive messages between software components** at any volume, without losing messages or requiring other services to be available.

**Elastic Load Balancing (ELB)** automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses. It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones. Elastic Load Balancing offers three types of load balancers:

**Application Load Balancer** (best suited for HTTP and HTTPS traffic)

An Application Load Balancer serves as the single point of contact for clients. The load balancer distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. It distributes traffic, does not scale resources.

**Network Load Balancer** is best suited for load balancing of Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Transport Layer Security (TLS) traffic where extreme performance is required. It distributes traffic, does not scale resources.

Classic Load Balancer.

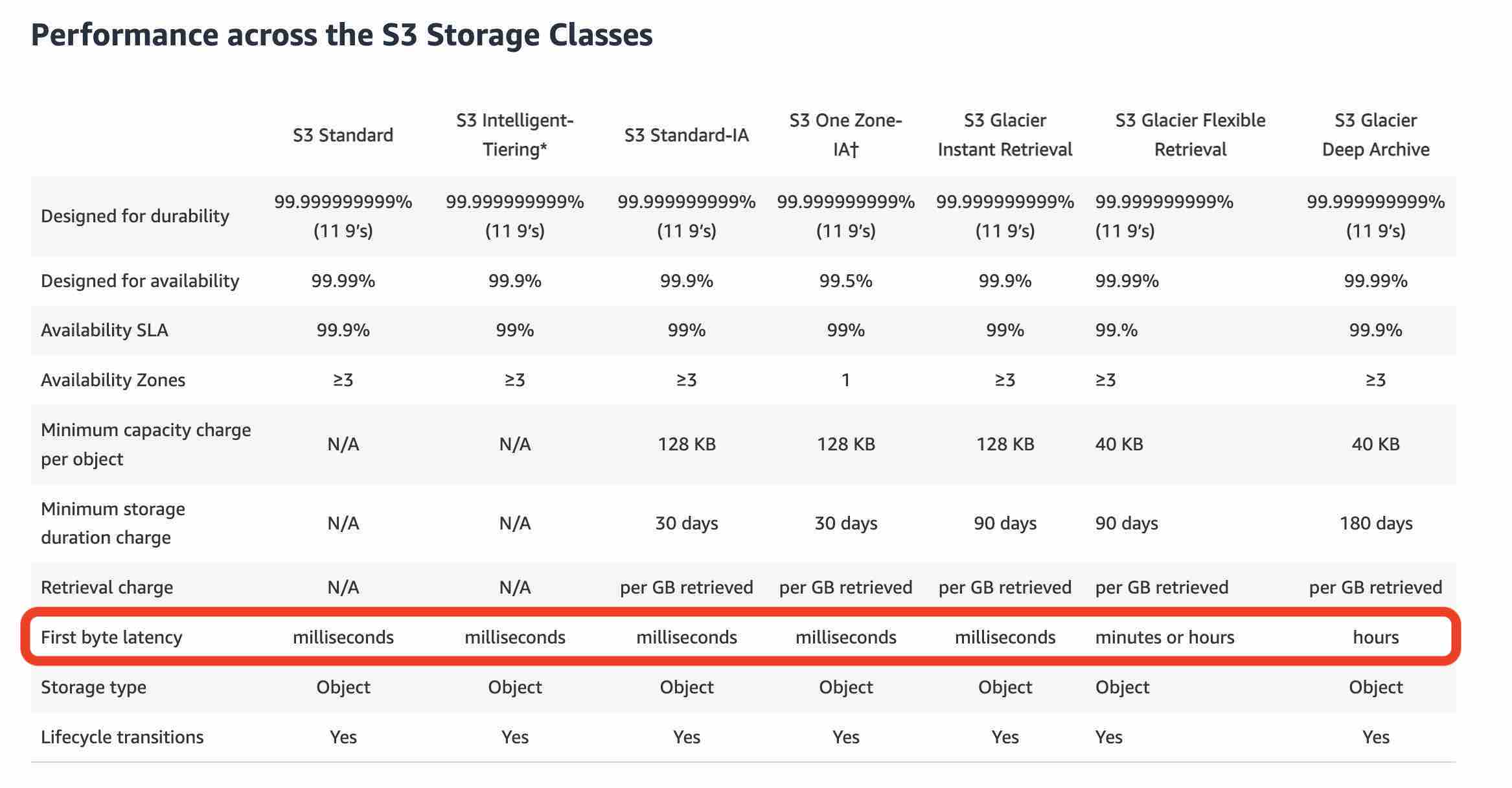
**Agility** - Agility refers to new IT resources being only a click away, which means that you reduce the time to make those resources available to your developers from weeks to just minutes.

**AWS Quick Starts references** - Quick Starts are built by AWS solutions architects and partners to help you **deploy popular technologies on AWS**, based on AWS best practices for security and high availability. These accelerators reduce hundreds of manual procedures into just a few steps, so you can build your production environment quickly and start using it immediately.

**AWS Forums** - AWS Forums is an AWS community platform where people can help each other. It is not used to deploy technologies on AWS.

**AWS Whitepapers** - AWS Whitepapers are technical content authored by AWS and the AWS community to **expand your knowledge of the cloud.** They include technical whitepapers, technical guides, reference material, and reference architectures diagrams. You can find useful content for your deployment, but it is not a service that will deploy technologies.

**"S3 Glacier Deep Archive"** - S3 Glacier Deep Archive is Amazon S3’s **lowest-cost** storage class and supports long-term retention and digital preservation for data that may be accessed **once or twice in a year**. It is designed for customers — particularly those in highly-regulated industries, such as the Financial Services, Healthcare, and Public Sectors — that **retain data sets for 7-10 years** or longer to meet regulatory compliance requirements. S3 Glacier Deep Archive can also be used for backup and disaster recovery use cases. **It has a retrieval time (first byte latency) of 12 to 48 hours.**



Think resource performance monitoring, events, and alerts; think CloudWatch.

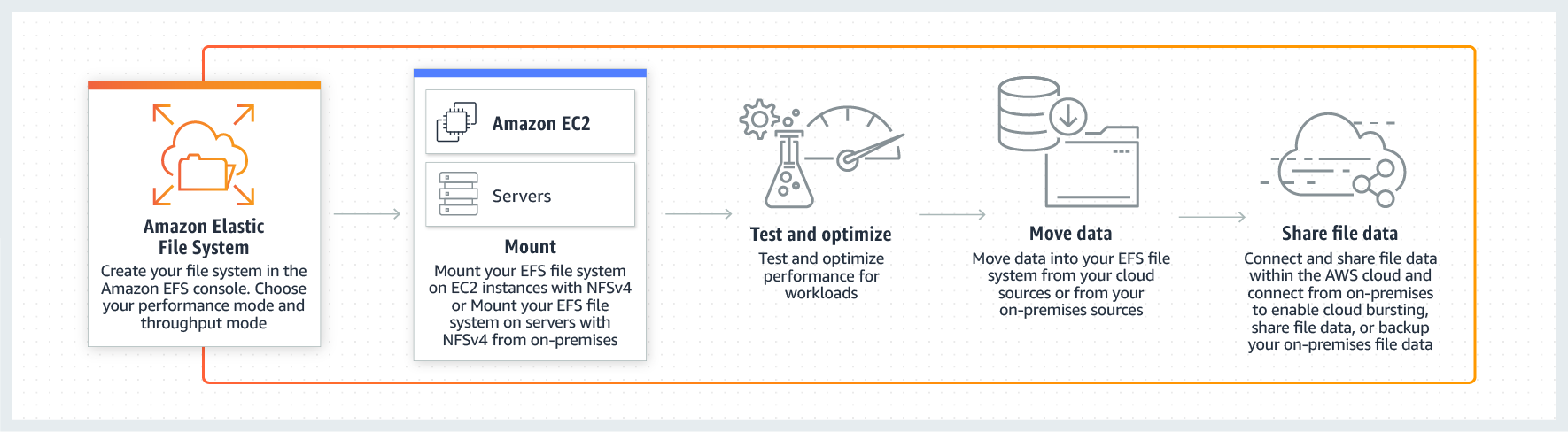
Think account-specific activity and audit; think CloudTrail.

Think resource-specific change history, audit, and compliance; think Config.

**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)** for both throughput and transaction-intensive workloads at any scale. A broad range of workloads, such as **relational and non-relational databases, enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows are widely deployed on Amazon EBS.**

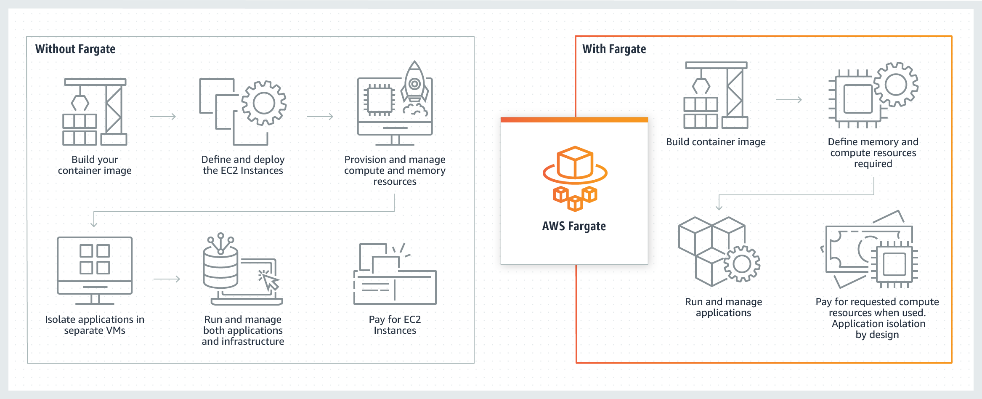
**Instance Store** - An instance store provides **temporary block-level** storage for your EC2 instance. This storage is located **on disks that are physically attached to the host computer.** Instance store is ideal for the temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers. Instance storage is temporary, data is lost if instance experiences failure or is terminated. EC2 instance store cannot be used for file sharing between instances.

**EFS** - Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed, elastic NFS (Network File System) file system. It is built to scale on-demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth. Amazon EFS is designed to provide massively parallel shared access to thousands of **Amazon EC2 instances**, enabling your applications to achieve high levels of aggregate throughput and IOPS with consistent low latencies. **It is a regional service, this means that EC2 instances can access files on an EFS file system across many Availability Zones, Regions and VPCs**



**ECS** - Amazon Elastic Container Service (ECS) is a highly scalable, high-performance container management service that supports Docker containers and allows you to easily run applications on a managed cluster of Amazon EC2 instances. **This is not a storage service** and has been added as a distractor. This is not a fully managed service and you can manage the underlying servers yourself.

**AWS Fargate** - AWS Fargate is a **serverless compute** engine for containers. It works with both **Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS).** Fargate makes it easy for you to focus on building your applications. Fargate removes the need to provision and manage servers, lets you specify and pay for resources per application, and improves security through application isolation by design. With Fargate, you do not **have access to the underlying servers.**



**Amazon Elastic Container Registry (ECR)** - Amazon Elastic Container Registry (ECR) can be used to **store, manage, and deploy Docker container** images. Amazon ECR eliminates the need to operate your container repositories. ECR does not support running container applications.

**Virtual MFA device**

A software app that runs on a phone or other device and emulates a physical device. The device generates a six-digit numeric code based upon a time-synchronized one-time password algorithm. The user must type a valid code from the device on a second webpage during sign-in. Each virtual MFA device assigned to a user must be unique. A user cannot type a code from another user's virtual MFA device to authenticate.

**U2F security key** - A device that **you plug into a USB port** on your computer. U2F is an open authentication standard hosted by the FIDO Alliance. When you enable a U2F security key, you sign in by entering your credentials and then tapping the device instead of manually entering a code.

**Hardware MFA device** - A hardware device **that generates a six-digit numeric code** based upon a time-synchronized one-time password algorithm. The user must type a valid code from the device on a second webpage during sign-in. Each MFA device assigned to a user must be unique. A user cannot type a code from another user's device to be authenticated.

**APN = AWS Partner Network**

The AWS Partner Network (APN) is the global partner program for technology and consulting businesses that leverage Amazon Web Services to build solutions and services for customers.

• APN Technology Partners: providing hardware, connectivity, and software

• APN Consulting Partners: professional services firm to help build on AWS

• APN Training Partners: find who can help you learn AWS

**Concierge Support Team** - The Concierge Support Team are AWS billing and account experts that specialize in working with enterprise accounts. They will quickly and efficiently assist you with your billing and account inquiries. The Concierge Support Team is only available for the Enterprise Support plan. Concierge Support Team cannot help in migrating to AWS and managing applications on AWS Cloud.

You can use **Amazon Transcribe** to add **speech-to-text capability** to your applications. Amazon Transcribe uses a deep learning process called automatic speech recognition (ASR) to convert speech to text quickly and accurately. Amazon Transcribe can be used to transcribe customer service calls, to automate closed captioning and subtitling, and to generate metadata for media assets.

You can use **Amazon Polly** to turn **text into lifelike speech** thereby allowing you to create applications that talk. Polly's Text-to-Speech (TTS) service uses advanced deep learning technologies to synthesize natural sounding human speech.

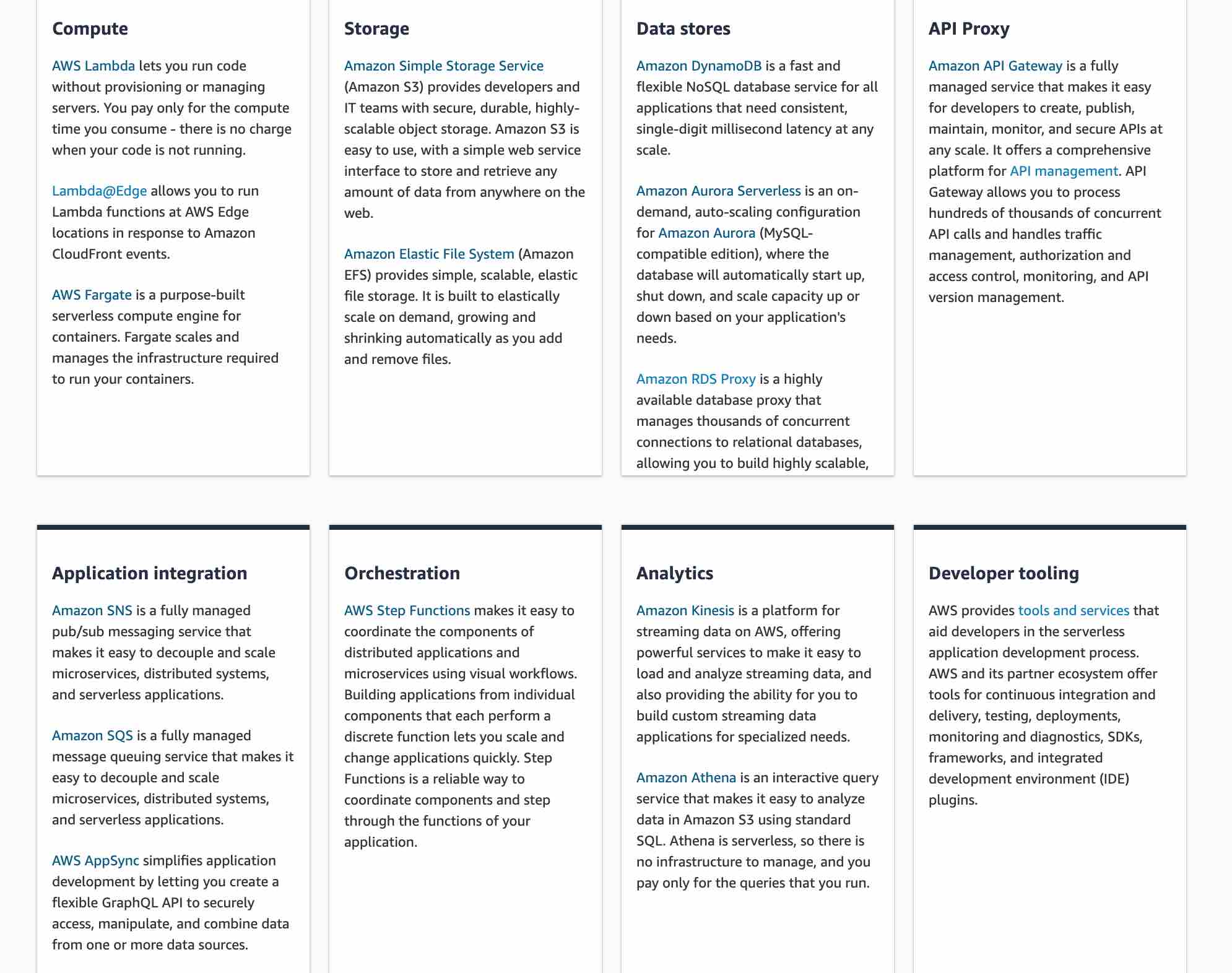
**Amazon Translate** is used for language translation. Amazon Translate uses neural machine translation via deep learning models to deliver more accurate and more natural-sounding translation than traditional statistical and rule-based translation algorithms.

**AWS CloudHSM** - AWS CloudHSM is a **cloud-based Hardware Security Module (HSM)** that enables you to easily generate and use your encryption keys on the AWS Cloud. With CloudHSM, you can manage your encryption keys using FIPS 140-2 Level 3 validated HSMs. It is a fully-managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching, high-availability, and backups.

**AWS Key Management Service (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. KMS cannot be used as a Hardware Security Module for data encryption operations in AWS Cloud.

**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. Secrets Manager cannot be used as a Hardware Security Module for data encryption operations in AWS Cloud.

The AWS serverless platform overview:



**AWS X-Ray** - You can use AWS X-Ray to analyze and **debug serverless and distributed applications** such as those built using a microservices architecture. With X-Ray, you can understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors.

**Amazon Pinpoint** - Amazon Pinpoint allows marketers and developers to deliver customer-centric engagement experiences by capturing customer usage data to draw real-time insights.

**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.

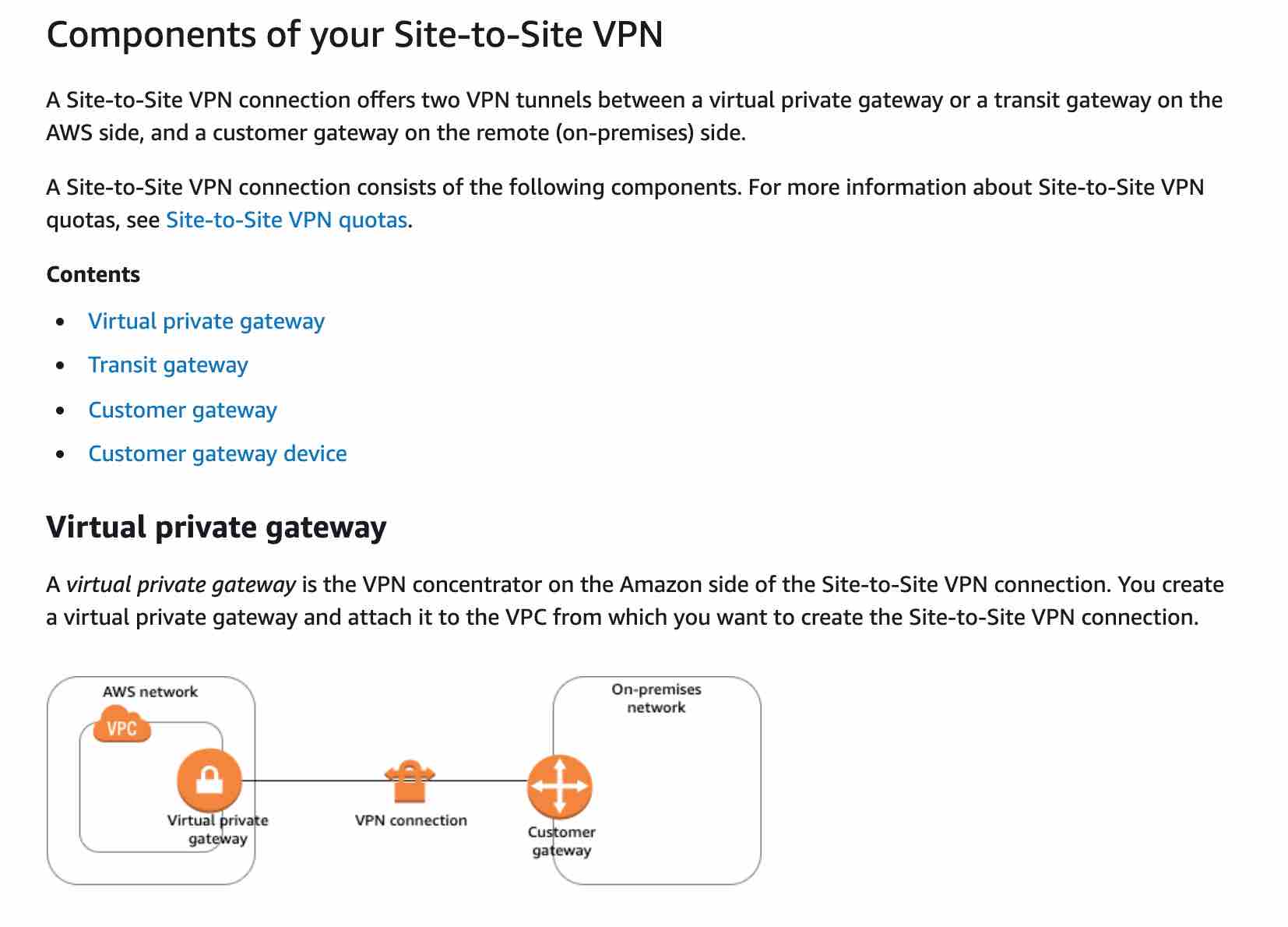
**Penetration Testing**

AWS customers can carry out security assessments or penetration tests against their AWS infrastructure without prior approval for few common AWS services. Customers are not permitted to conduct any security assessments of AWS infrastructure, or the AWS services themselves.

**VPC Peering**

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. 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 VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region. **VPC peering is not transitive.**

**Site to Site VPN** - AWS Site-to-Site VPN creates a secure connection between your data center or branch office and your AWS cloud resources. This connection goes over the public internet. Site to Site VPN cannot be used to interconnect VPCs.



**AWS Single Sign-On (SSO)**

AWS SSO is an AWS service that enables you to makes it easy to centrally manage access to multiple AWS accounts and business applications and provide users with single sign-on access to all their assigned accounts and applications from one place.

**AWS Cognito** - Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. With Amazon Cognito, you also have the option to authenticate users through **social identity providers such as Facebook, Twitter, or Amazon,** with SAML identity solutions, or by using your own identity system. It is an identity management solution for customers/developers building B2C or B2B apps for their customers.

**AWS Command Line Interface (CLI)** - The AWS Command Line Interface (CLI) is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

**AWS Acceptable Use Policy**

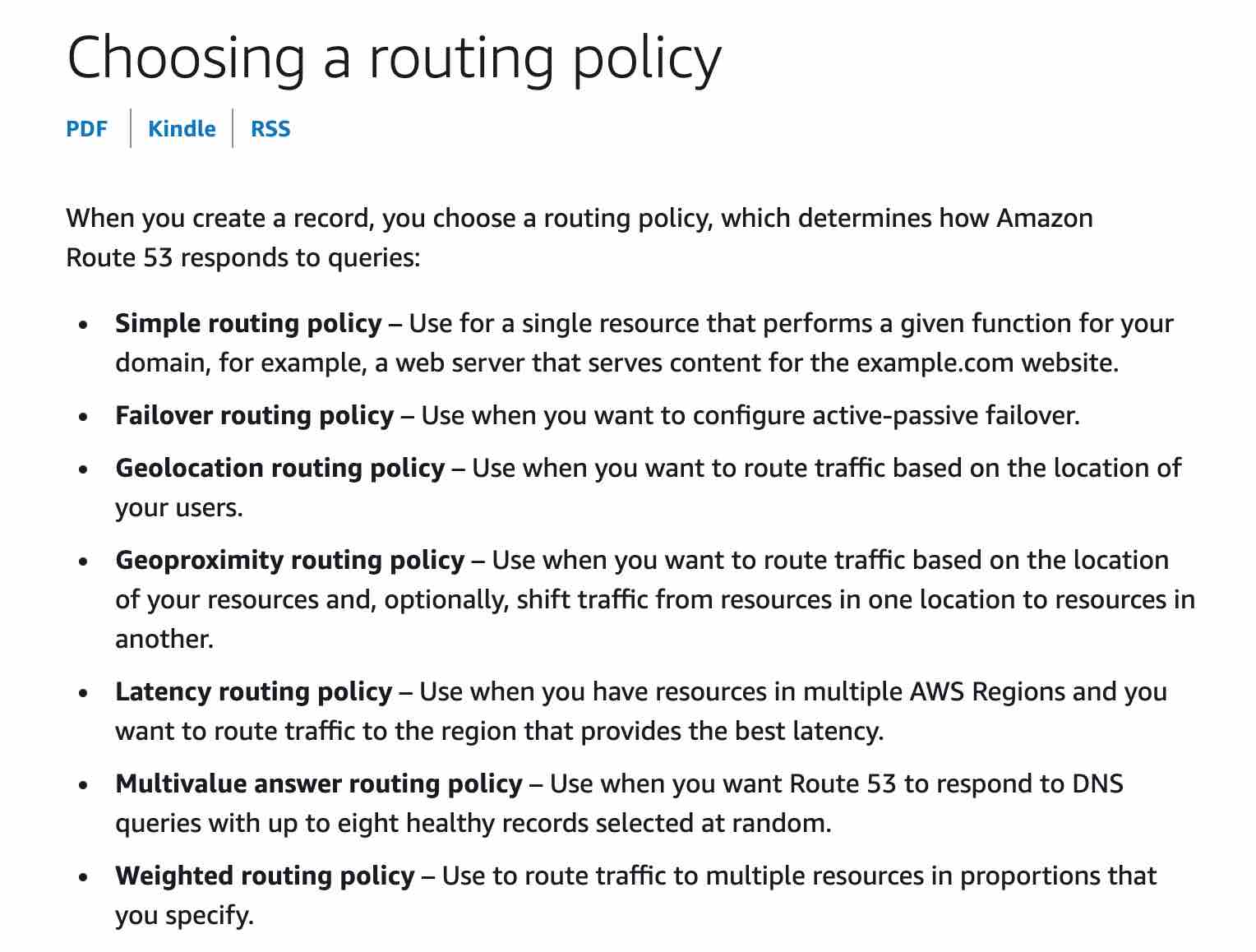
The Acceptable Use Policy describes prohibited uses of the web services offered by Amazon Web Services, Inc. and its affiliates (the “Services”) and the website located at http://aws.amazon.com (the “AWS Site”). This policy is present at https://aws.amazon.com/aup/ and is updated on a need basis by AWS.

**AWS Fair Use Policy** - This is a made-up option and has been added as a distractor.

**AWS Applicable Use Policy** - This is a made-up option and has been added as a distractor.

**Amazon Route 53** - Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating names like www.example.com into the numeric IP addresses like 192.0.2.1 that computers use to connect to each other.

**Route 53 Routing Policy Overview:**



**The AWS Well-Architected Framework** helps you understand the pros and cons of decisions you make while building systems on AWS. By using the Framework you will learn architectural best practices for designing and operating reliable, secure, efficient, and cost-effective systems in the cloud. It provides a way for you to consistently measure your architectures against best practices and identify areas for improvement.

The AWS Well-Architected Framework is based on six pillars —

Operational Excellence,

Security,

Reliability,

Performance Efficiency,

Cost Optimization

Sustainability.

**AWS OpsWorks** - AWS OpsWorks is a configuration management service that provides managed instances of **Chef and Puppet**. OpsWorks lets you use Chef and Puppet to a**utomate how servers are configured, deployed and managed across your Amazon EC2 instances or on-premises compute environments.** You cannot use OpsWorks for running commands or managing patches on servers. You cannot use this service to provision AWS infrastructure.

**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 automatically provides an inventory of Amazon S3 buckets including a list of unencrypted buckets, publicly accessible buckets, and buckets shared with AWS accounts outside those you have defined in AWS Organizations. Then, Macie applies machine learning and pattern matching techniques to the buckets you select to identify and alert you to sensitive data, such as personally identifiable information (PII).

**AWS Glue** - AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. AWS Glue job is meant to be used for batch ETL data processing.

**AWS Compute Optimizer** helps you identify the optimal AWS resource configurations, **such as Amazon EC2 instance types, Amazon EBS volume configurations, and AWS Lambda function** memory sizes, using machine learning to analyze historical utilization metrics. AWS Compute Optimizer delivers recommendations for selected types of EC2 instances, EC2 Auto Scaling groups, EBS volumes, and Lambda functions.

**AWS Batch** - AWS Batch enables developers, scientists, and engineers to easily and efficiently run hundreds of thousands of batch computing jobs on AWS.

**An Amazon Machine Image (AMI)** provides the information required to launch an instance. You must specify an AMI when you launch an instance. You can launch multiple instances from a single AMI when you need multiple instances with the same configuration.

The AMI must be in the same region as that of the EC2 instance to be launched. If the AMI exists in a different region, you can copy that AMI to the region where you want to launch the EC2 instance. The region of AMI has no bearing on the performance of the EC2 instance.

**Amazon SageMaker** - Amazon SageMaker is a fully managed service that provides every developer and data scientist with the ability to build, train, and deploy machine learning (ML) models quickly. SageMaker removes the heavy lifting from each step of the machine learning process to make it easier to develop high-quality models.

**AWS Storage Gateway** - AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. All data transferred between the gateway and AWS storage is encrypted using SSL (for all three types of gateways - **File, Volume and Tape Gateways).**

**Spot Instance** - A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts (up to 90%), you can lower your Amazon EC2 costs significantly. Spot Instances are well-suited for data analysis, batch jobs, background processing, and optional tasks. These can be terminated at short notice, so these are not suitable for critical workloads that need to run at a specific point in time. So this option is not correct for the given use-case.

**Dedicated Host** - Amazon EC2 Dedicated Hosts allow you to **use your eligible software licenses from vendors such as Microsoft and Oracle on Amazon EC2** so that you get the flexibility and cost-effectiveness of using your licenses, but with the resiliency, simplicity, and elasticity of AWS. An Amazon EC2 Dedicated Host is a physical server fully dedicated for your use, so you can help address corporate compliance requirement. They're not cost-efficient compared to On-Demand instances.

**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.

**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.**

**Note:** Per AWS pricing, data transfer between S3 and EC2 instances within the same region is not charged, so there would be no data transfer charge for moving 500 GB of data from an EC2 instance to an S3 bucket in the same region.

**A security group** acts as a virtual firewall for your instance to control inbound and outbound traffic. Security groups act **at the instance level**, not at the subnet level. You can specify allow rules, but not deny rules. You can specify separate rules for inbound and outbound traffic. **They are stateful.**

**A Network Access Control List (NACL)** is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets (i.e. it works at subnet level). A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic. **NACL is stateless**, which means that responses to allowed inbound traffic are subject to the rules for outbound traffic.

You can use a **network address translation (NAT)** gateway or a NAT Instance to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances. NAT Gateway is managed by AWS but NAT Instance is managed by you.

**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.

**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**.

**Basic** - The basic plan only provides access to the following:

Customer Service & Communities - 24x7 access to customer service, documentation, whitepapers, and support forums. **AWS Trusted Advisor - Access to the 7 core Trusted Advisor checks** and guidance to provision your resources following best practices to increase performance and improve security. **AWS Health - Your Account Health Dashboard** : A personalized view of the health of your AWS services, and alerts when your resources are impacted. This plan does **not support any architectural guidance.**

**Developer** - AWS recommends Developer Support if you are testing or doing early development on AWS and want the ability to get **email-based technical support during business hours** as well as **general architectural guidance** as you build and test. You do not get access to Infrastructure Event Management with this plan. This plan only supports general architectural guidance. This plan provides access to just the **7 core Trusted Advisor checks**.

**Business -** AWS recommends Business Support if you have production workloads on AWS and want **24x7 phone, email and chat access** to technical support and **architectural guidance in the context of your specific use-cases**. You get full access to AWS Trusted Advisor Best Practice Checks. You also get access to **Infrastructure Event Management for an additional fee**. You get access to guidance, configuration, and troubleshooting of AWS interoperability with many common operating systems, platforms, and application stack components.

**Enterprise** - AWS Enterprise Support provides customers with **concierge-like service** where the main focus is helping the customer achieve their outcomes and find success in the cloud. With Enterprise Support, you **get online training with self-paced labs, 24x7 technical support from high-quality engineers,** tools and technology to automatically manage the health of your environment, consultative review and guidance based on your applications, **and a designated Technical Account Manager (TAM)** to coordinate access to proactive/preventative programs and AWS subject matter experts. This plan supports architectural guidance contextual to your application. You get access to guidance, configuration, and troubleshooting of AWS interoperability with many common operating systems, platforms, and application stack components.

**Internet Gateway** - An Internet Gateway is a horizontally scaled, redundant, and highly available VPC component that **allows communication between your VPC and the internet.** An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic and to perform network address translation (NAT) for instances.

**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.**

**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.

**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.

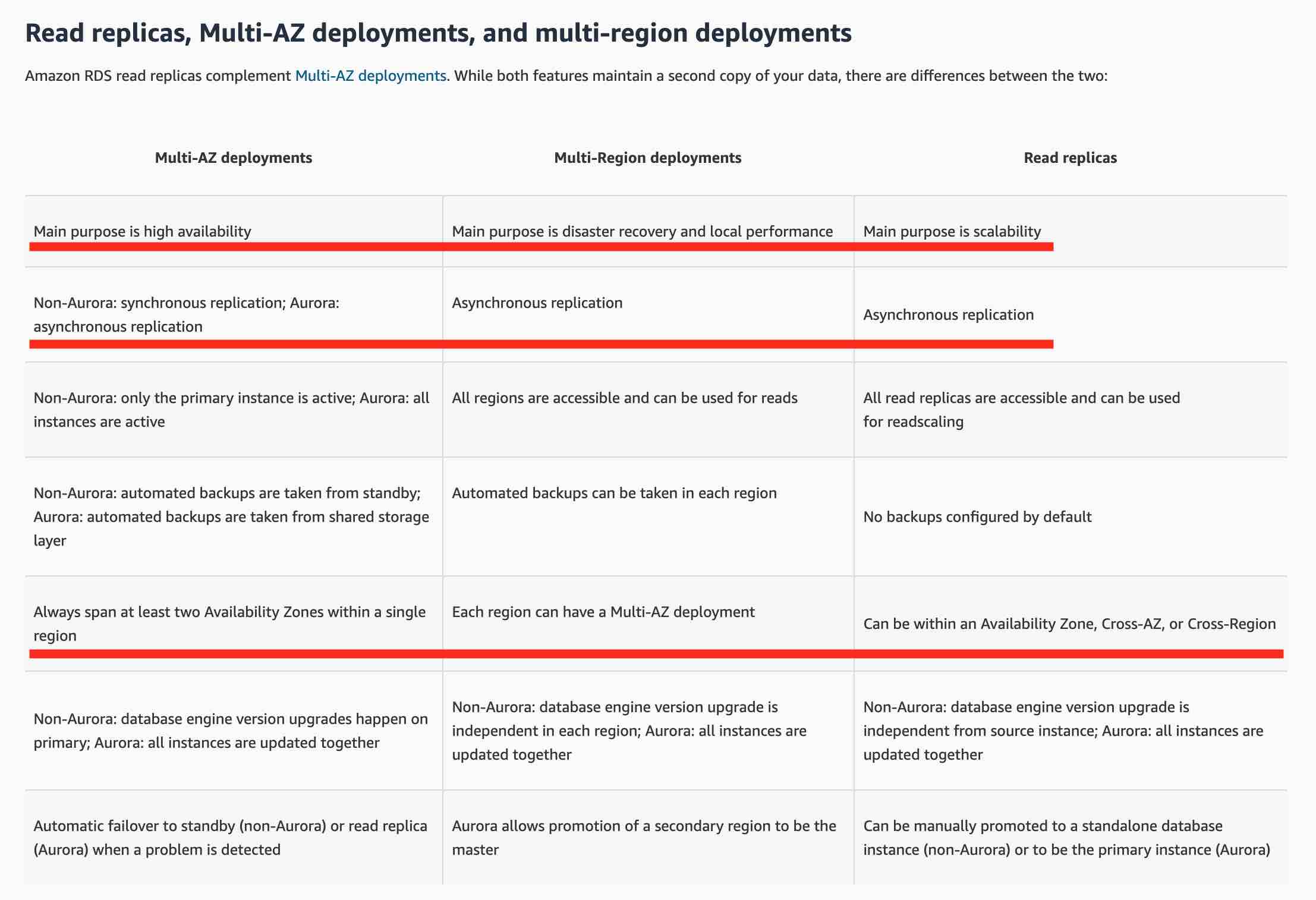
**AWS Web Application Firewall (AWS WAF)** - AWS WAF is a web application firewall that lets you monitor the HTTP(S) requests that are forwarded to an **Amazon CloudFront distribution, an Amazon API Gateway API, or an Application Load Balancer**. AWS WAF charges based on the number of web access control 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). HTTP and HTTPS requests are part of the Application layer, which is layer 7.

**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.

**AWS Software Developer Kit (SDK)** - SDKs take the complexity out of coding by providing **language-specific APIs for AWS services**. For example, the AWS SDK for JavaScript simpliﬁes the use of AWS Services by providing a set of libraries that are consistent and familiar for JavaScript developers. It provides support for API lifecycle considerations such as **credential management, retries, data marshaling, serialization, and deserialization.** AWS SDKs are offered in several programming languages to make it simple for developers working on different programming and scripting languages. So, AWS SDK can help with using AWS services from within an application using language-specific APIs.

**DocumentDB** - Amazon DocumentDB (with MongoDB compatibility) is a fast, scalable, highly available, and fully managed document database service that supports MongoDB workloads. As a document database, Amazon DocumentDB makes it easy to store, query, and index JSON data.





**AWS Service Catalog** - AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures.

**AWS Partner Network** - Organizations can take help from the AWS Partner Network (APN) to identify the right AWS services to build solutions on AWS Cloud. APN is the global partner program for technology and consulting businesses that leverage Amazon Web Services to build solutions and services for customers.

**Amazon Elastic Container Registry (ECR)** - Amazon Elastic Container Registry (ECR) can be used to store, manage, and deploy Docker container images. Amazon ECR eliminates the need to operate your container repositories. You can then pull your docker images from ECR and run those on Amazon Elastic Container Service (ECS).

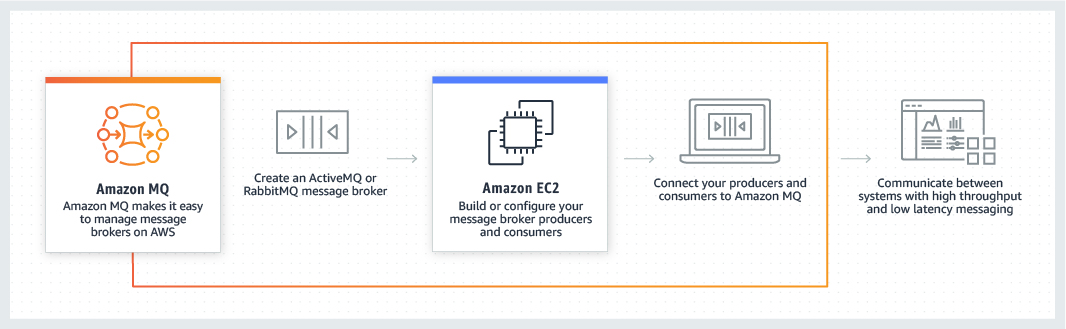
**Amazon Elastic Container Service (ECS)** - Amazon Elastic Container Service (Amazon ECS) is a highly scalable, fast, container management service that makes it easy to run, stop, and manage **Docker containers** on a cluster.

**Global Accelerator** - AWS Global Accelerator is a service that improves the availability and performance of your applications with local or global users. It provides **static IP addresses** that act as a fixed entry point to your application endpoints in a single or multiple AWS Regions, such as your Application Load Balancers, Network Load Balancers, or Amazon EC2 instances. AWS Global Accelerator uses the AWS global network to optimize the path from your users to your applications, improving the performance of your traffic by as much as 60%.

**Amazon CloudFront** - Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

**Amazon Athena** - Amazon Athena is an interactive query service that makes it easy to analyze data in **Amazon S3 using standard SQL**. Athena is **serverless**, so there is no infrastructure to manage, and you **pay** only for the **queries that you run.**

**Amazon MQ** - Amazon MQ is a managed message broker service for Apache **ActiveMQ and RabbitMQ** that makes it easy to set up and operate message brokers on AWS. Amazon MQ reduces your operational responsibilities by managing the provisioning, setup, and maintenance of message brokers for you. Because Amazon MQ connects to your current applications with industry-standard APIs and protocols, you can easily migrate to AWS without having to rewrite code.



**Amazon Kinesis data stream** - Amazon Kinesis Data Streams enables you to build custom applications that process or analyze streaming data for specialized needs. You can continuously add various types of data such as clickstreams, application logs, and social media to an Amazon Kinesis data stream from hundreds of thousands of sources. Within seconds, the data will be available for your Amazon Kinesis Applications to read and process from the stream.

**Amazon FSx for Windows File Server** - Amazon FSx for Windows File Server provides fully managed, highly reliable, and scalable file storage that **is accessible over the industry-standard Service Message Block (SMB) protocol**. It is built on Windows Server, delivering a wide range of administrative features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration.

**Amazon FSx for Lustre** - For compute-intensive and fast processing workloads, like high-performance computing (HPC), machine learning, EDA, and media processing, Amazon FSx for Lustre, provides a file system that’s optimized for performance, with input and output stored on Amazon S3. FSx for Lustre is only compatible with Linux.

**Amazon Rekognition** - With Amazon Rekognition, you can identify objects, people, text, scenes, and activities in images and videos, as well as detect any inappropriate content. Amazon Rekognition also provides highly accurate facial analysis and facial search capabilities that you can use to detect, analyze, and compare faces for a wide variety of user verification, people counting, and public safety use cases. Rekognition is a regional service.

**AWS Transit Gateway** - **AWS Transit Gateway connects VPCs and on-premises networks through a central hub**. This simplifies your network and puts an end to complex peering relationships. It acts as a **cloud router** – each new connection is only made once. This service is helpful in reducing the complex topology of VPC peering when a lot of systems are involved.

You can monitor your estimated AWS charges by using Amazon CloudWatch. Billing metric data is stored in the US East (N. Virginia) Region and represents worldwide charges. This data includes the estimated charges for every service in AWS that you use, in addition to the estimated overall total of your AWS charges.

An IT company is on a cost-optimization spree and wants to identify all EC2 instances that are under-utilized. Which AWS services can be used off-the-shelf to address this use-case without needing any manual configurations? (Select two)

ANS: AWS Cost explorer

AWS Trusted advisor

**Amazon Kendra** - Amazon Kendra is an **intelligent search service** powered by machine learning. Kendra reimagines enterprise search for your websites and applications so your employees and customers can easily find the content they are looking for, even when it’s scattered across multiple locations and content repositories within your organization.

Using Amazon Kendra, you can stop searching through troves of unstructured data and discover the right answers to your questions, when you need them. Amazon Kendra is a fully managed service, so there are no servers to provision, and no machine learning models to build, train, or deploy. Kendra supports unstructured and semi-structured data in **.html, MS Office (.doc, .ppt), PDF, and text formats.**

Unlike conventional search technology, natural language search capabilities return the answers you’re looking for quickly and accurately, no matter where the information lives within your organization.

**Amazon Personalize** - Amazon Personalize enables developers to build applications with the same machine learning (ML) technology used by Amazon.com **for real-time personalized recommendations.** Amazon Personalize makes it easy for developers to build applications capable of delivering a wide array of personalization experiences, including specific product recommendations, personalized product re-ranking, and customized direct marketing.

**Amazon Comprehend** - Amazon Comprehend is a natural-language processing (NLP) service that uses machine learning to **uncover information in unstructured data**. Instead of combing through documents, the process is simplified and unseen information is easier to understand.

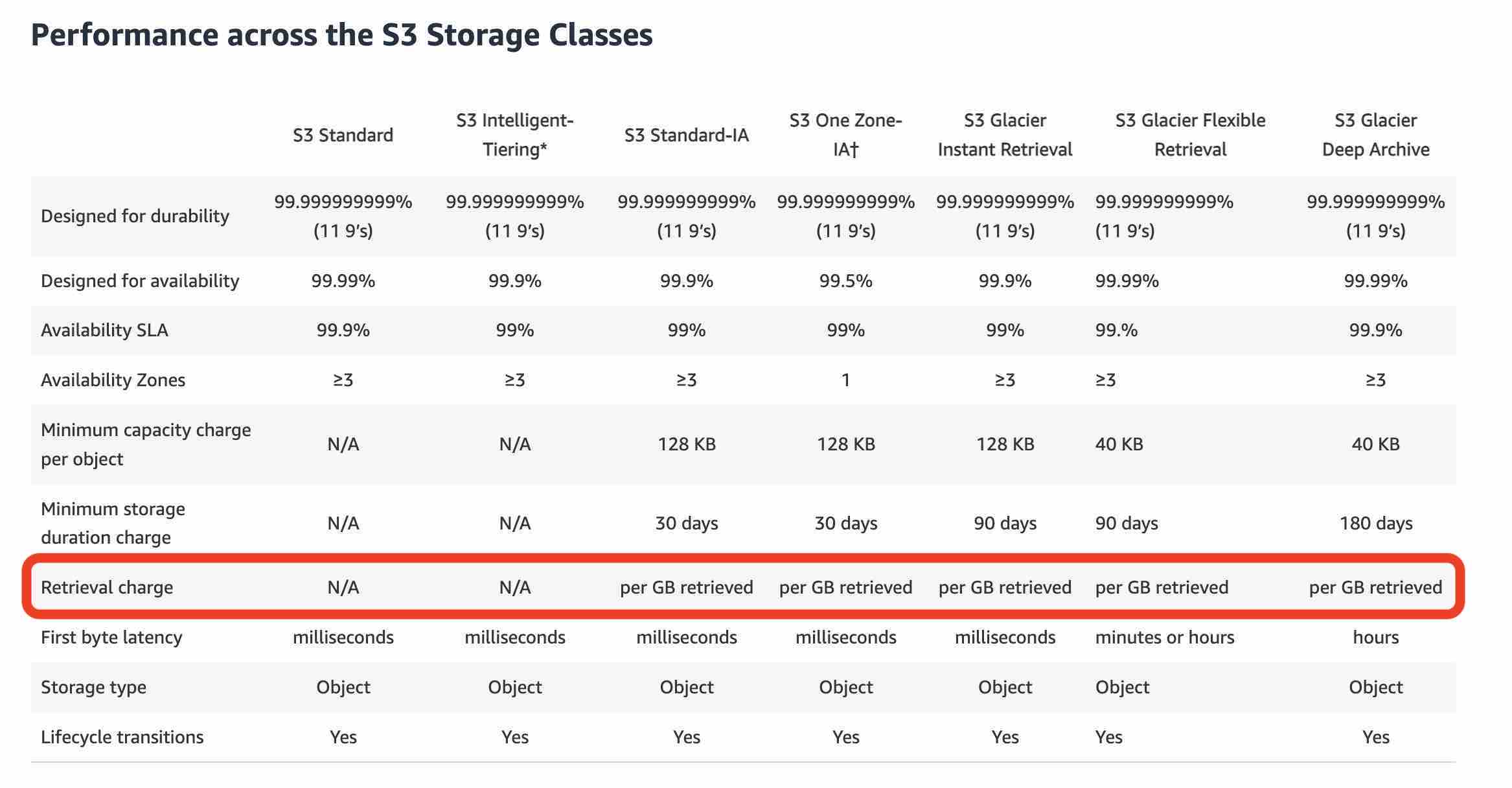
**Amazon Lex** - Amazon Lex is a service for building conversational interfaces into any application using voice and text. Amazon Lex provides the advanced deep learning functionalities of automatic speech recognition (ASR) for converting speech to text, and natural language understanding (NLU) to recognize the intent of the text, to enable you to build applications with highly engaging user experiences and lifelike conversational interactions.

**Data Encryption is enabled automatically for AWS storage gateway and AWS S3 Glacier.**

**Amazon S3 Glacier** - Amazon S3 Glacier (S3 Glacier), is a storage service optimized for infrequently used data, or "cold data. Data at rest stored in S3 Glacier is automatically **server-side encrypted** using 256-bit Advanced Encryption Standard (AES-256) with keys maintained by AWS.

**AWS Migration Evaluator:** Migration Evaluator (Formerly TSO Logic) is a complimentary service to **create data-driven business cases** for AWS Cloud planning and migration.

Migration Evaluator quickly provides a business case to make sound AWS planning and migration decisions. With Migration Evaluator, your organization can build a data-driven business case for AWS, gets access to AWS expertise, visibility into the costs associated with multiple migration strategies, and insights on how reusing existing software licensing reduces costs further.



**AWS Device Farm** - AWS Device Farm is an application testing service that lets you improve the quality of your web and mobile apps by testing them across an extensive range of **desktop browsers and real mobile devices**; without having to provision and manage any testing infrastructure. The service enables you to run your tests **concurrently** on multiple desktop browsers or real devices to speed up the execution of your test suite, and generates videos and logs to help you quickly identify issues with your app.

You can manage your objects on S3 so that they are stored cost-effectively throughout their lifecycle by configuring their Amazon S3 Lifecycle. An S3 Lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects.

There are two types of actions:

Transition actions — Define when objects transition to another storage class. For example, you might choose to transition objects to the S3 Standard-IA storage class 30 days after you created them, or archive objects to the S3 Glacier storage class one year after creating them.

Expiration actions — Define when objects expire. Amazon S3 deletes expired objects on your behalf.

**S3 Transfer Acceleration**: Amazon S3 Transfer Acceleration (S3TA) enables fast, easy, and secure transfers of files over long distances between your client and your Amazon S3 bucket. S3 Transfer Acceleration leverages **Amazon CloudFront’s globally distributed AWS Edge Locations**. As data arrives at an AWS Edge Location, data is routed to your Amazon S3 bucket over an optimized network path. **S3 Transfer Acceleration is designed to optimize transfer speeds from across the world into S3 buckets**. If you are uploading to a centralized bucket from geographically dispersed locations, or if you regularly transfer GBs or TBs of data across continents, you may save hours or days of data transfer time with S3 Transfer Acceleration.

**EC2 instance user data** EC2 instance user data is the data that you specified in the form of a **bootstrap script** or configuration parameters while launching your instance.

**EC2 instance metadata** - EC2 instance metadata is **data about your instance** that you can use to manage the instance. You can get instance items such as ami-id, public-hostname, local-hostname, hostname, public-ipv4, local-ipv4, public-keys, instance-id by using instance metadata. You cannot use EC2 instance metadata to run a bootstrap script while launching an EC2 instance. So this option is incorrect.

**AWS Snowmobile** - AWS Snowmobile is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS. You can transfer up to **100PB per Snowmobile**, a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck. Snowmobile makes it easy to move massive volumes of data to the cloud, including video libraries, image repositories, or even a complete data center migration. Transferring data with Snowmobile is more secure, fast and cost-effective.

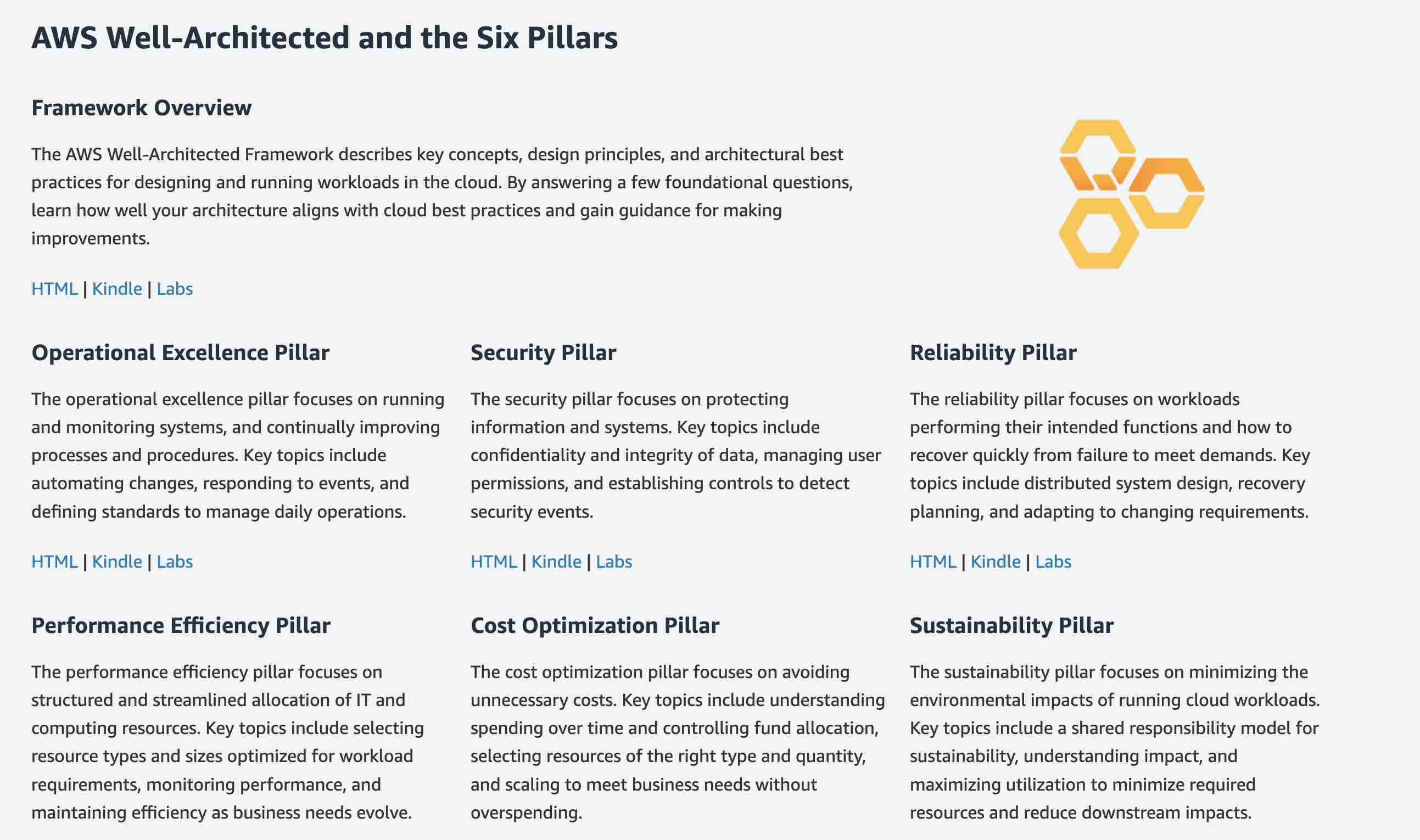
**AWS Snowball Edge** - Snowball Edge is an edge computing and data transfer device provided by the AWS Snowball service. It has on-board storage and compute power that provides select AWS services for use in edge locations. However, one Snowball Edge only provides up to **100 TB of capacity**. Therefore, to transfer 50 PBs, AWS Snowball Edge is not the most cost-effective option.

**AWS Snowball** - AWS Snowball is a **petabyte-scale** data transport solution that uses secure appliances to transfer large amounts of data into and out of AWS. The use of Snowball addresses common challenges with large- scale data transfers including high network costs, long transfer times, and security concerns. Transferring data with Snowball is simple, fast, secure, and can be as little as one-fifth the cost of high-speed Internet. However, one Snowball only provides up to **80 TB of capacity.** Therefore, to transfer 50 PBs, AWS Snowball is not the most cost-effective option.

**S3 Lifecycle management**: To manage your objects so that they are stored cost-effectively throughout their lifecycle, configure their Amazon S3 Lifecycle. An S3 Lifecycle **configuration is a set of rules** that define actions that Amazon S3 applies to a group of objects. There are two types of actions: **Transition actions** (define when objects transition to another storage class) and **expiration actions** (define when objects expire. Amazon S3 deletes expired objects on your behalf).

**AWS Fault Injection Simulator:** AWS Fault Injection Simulator is a fully managed service for running fault injection experiments on AWS that makes it easier to improve an application’s performance, observability, and resiliency. **Fault injection experiments are used in chaos engineering**, which is the practice of stressing an application in testing or production environments by creating disruptive events, such as a sudden increase in CPU or memory consumption, observing how the system responds, and implementing improvements. Fault injection experiment helps teams create the real-world conditions needed to uncover the hidden bugs, monitoring blind spots, and performance bottlenecks that are difficult to find in distributed systems.

**IAM access advisor: Access advisor shows the service permissions granted to a user and when those services were last accessed.** You can use this information to revise your policies. To summarize, you can identify unnecessary permissions so that you can revise your IAM policies accordingly.



**S3 Access Logs** - Server access logging provides detailed records for the requests that are made to a bucket. Server access logs are useful for many applications. For example, access log information can be useful in security and access audits.

**AWS Security Token Service (AWS STS)** - AWS Security Token Service (AWS STS) is a web service that enables you to request **temporary, limited-privilege** credentials for AWS Identity and Access Management (IAM) users or for users that you authenticate (federated users).

**Convertible Reserved Instances** - Purchase Convertible Reserved Instances if you need additional **flexibility**, such as the ability to use different instance families, operating systems, or tenancies over the Reserved Instance term. Convertible Reserved Instances provide you with a significant **discount (up to 54%)** compared to On-Demand Instances and can be purchased for a 1-year or 3-year term.

Convertible Reserved Instances can be useful when workloads are likely to change. In this case, a Convertible Reserved Instance enables you to adapt as needs evolve while still obtaining discounts and capacity reservations.

**AWS DataSync** - AWS DataSync is a secure **online data transfer service** that simplifies, automates, and accelerates copying terabytes of data to and from AWS storage services. Easily migrate or replicate large data sets without having to build custom solutions or oversee repetitive tasks. DataSync can copy data between Network File System (NFS) shares, or Server Message Block (SMB) shares, self-managed object storage, AWS Snowcone, Amazon Simple Storage Service (Amazon S3) buckets, Amazon Elastic File System (Amazon EFS) file systems, and Amazon FSx for Windows File Server file systems.

**Amazon CodeGuru** - Amazon CodeGuru is a developer tool that provides intelligent recommendations to **improve code quality** and identify an application’s most expensive lines of code. Integrate CodeGuru into your existing software development workflow to **automate code reviews** during application development, continuously monitor application performance in production, provide recommendations and visual clues for improving code quality and application performance, and reduce overall cost.

**AWS Cloud Development Kit (CDK)** - The AWS Cloud Development Kit (AWS CDK) is an open-source software development framework to define your cloud application resources using familiar programming languages.

AWS CDK uses the familiarity and expressive power of programming languages for modeling your applications. It provides you with high-level components called constructs that preconfigure cloud resources with proven defaults, so you can build cloud applications without needing to be an expert. AWS CDK provisions your resources in a safe, repeatable manner through AWS CloudFormation. It also enables you to compose and share your own custom constructs that incorporate your organization's requirements, helping you start new projects faster.