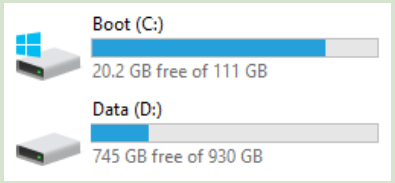
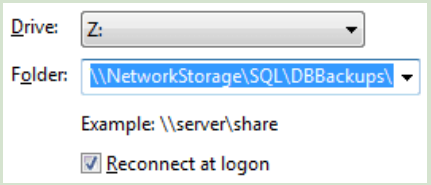
	Site-to-Site VPN	Direct Connect
Use case	Connecting remote networks to AWS VPC which doesn't require heavy data transfer or doesn't require a consistent connection	Connecting remote networks to AWS VPC which require heavy data transfer or require a consistent connection
Choose when…	Cost is important	Predictable performance is important
Supported speed	1.25 Gbps per tunnel	1 / 10 / 100 Gbps (sub 1 Gbps connections may be available from some service providers)
How it works?	Establishes a tunnel over existing internet connection	Establishes a connectivity over a dedicated network. Doesn't use Internet
High Availability	Highly available on AWS side (VGW is deployed across 2 AZs)	Single connection. No high availability by default
Encryption	Uses IPSec	Not encrypted by default
Time to establish	Can be setup in few minutes in a self-service fashion	Requires a Service Provider, may take few hours/days to get established
Cost dimension	Per connection hour and data transfer out	Variable port fees and data transfer out

Compare	Amazon DynamoDB Global Secondary Index (GSI)	Amazon DynamoDB Local Secondary Index (LSI)
Queries	Across all partitions	In a single partition
Size Limit	No size limitations	Can’t exceed 10 GB
Provisioned throughput	Separate from table	Shares with the tables
Read Consistency	Only Eventual	Strong or Eventual
Maximum	20	5
Creation	Anytime	Only with table creation
Deletion	Anytime	Only with table deletion

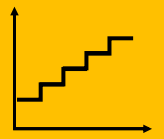
Analogies Cloud

Find detailed explanation video on - www.analogiescloud.com

	Block Storage	File Storage	Object Storage
Unit of Transaction	Blocks	Files	Objects (files with metadata)
Example	Laptop Disk 	Windows Share 	OneDrive / Google Drive / Dropbox 
How can you update?	You can directly update the file	You can directly update the file	You cannot update the object directly. You create a new version of the object and replace the existing one or keep multiple versions of the same object.
Protocols	SCSI, Fiber Channel, SATA	SMB, CIFS, NFS	REST/SOAP over HTTP/HTTPs
Support for metadata	No metadata support it stores only file system attributes	No metadata support it stores only file system attributes	Supports custom metadata
AWS Services	Amazon EBS Amazon Instance Store	Amazon EFS Amazon FSX	Amazon S3 Amazon Glacier

	Gateway Endpoint	Interface Endpoint
Used for	Private connectivity to Amazon S3 and Amazon DynamoDB	Private connectivity to 100+ AWS Services (including Amazon S3)
How it works?	An entry for prefix list (IP addresses) for supported services is added in to the routing table	An ENI(s) is provisioned in the selected subnet(s) which serves as an entry point for traffic destined to a supported service. (powered by AWS PrivateLink)
Provisioned at	VPC Level then entry added to Route Table	Subnet Level (no entry required in Route Table)
Security	Through VPC Endpoint Policy	Through Security Group

Security Group	Network ACL
Applied at Instance (ENI) Level	Applied at Subnet Level
Stateful - Response is always allowed	Stateless - Request and Response both have to be allowed
Default Rules (For Default SG) - All inbound is allowed from the same SG - All outbound is Allowed Default Rules (For a new SG) - All Inbound is Deny - All outbound in Allowed	Default Rules (For Default NACL) - All inbound is Allowed - All outbound is Allowed Default Rules (For a new NACL) - All inbound is Deny - All outbound is Deny
1 Instance can have many SG assigned	1 Subnet can have only 1 NACL
Only allow statements	Allow and Deny both statements
Order is not important	Order is important (lower order rule is applied first)
Source - IP / IP Range / Port / SG-<xxxxxxx>	Source - IP / Port / IP Range

	Scalability 	Elasticity 
What is it?	Scalability is the ability of a system to uphold the functionality when the size or volume changes.	Elasticity is the ability to dynamically manage available resources for addressing the size or volume.
Use case	To meet the static/predictable increase in the workload.	To meet the dynamic/sudden increase in the workload.
Type	Strategic operation	Tactical approach
Focuses on	Design/architecture	Operations
Resource provisioning	To exceed future demands	To meet present demand
Consideration	Medium- and long-term predictions	Short-term demand
Execution by	Typically scheduled	Typically triggered by automation

Analogies Cloud

Find detailed explanation video on - www.analogiescloud.com

	SQL (Optimized for Storage)	NoSQL (Optimized for performance)
Data Storage	Rows and Columns	Key-value, Document, Wide-column, Graph
Schema	Fixed	Dynamic
Querying	Using SQL	Focused on collection of documents
Scaling	Vertical	Horizontal
Transactions	Supported	Support varies

A — **Atomicity**
Transitions are all or nothing

C — **Consistency**
Only valid data is saved

I — **Isolation**
Transactions do not affect each other

D — **Durability**
Written data won't be lost

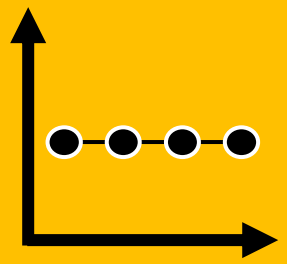
BA — **Basically Available**
System does guarantee availability

S — **Soft state**
System may change over time

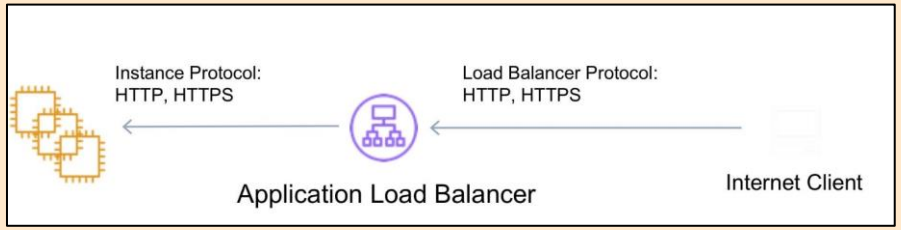
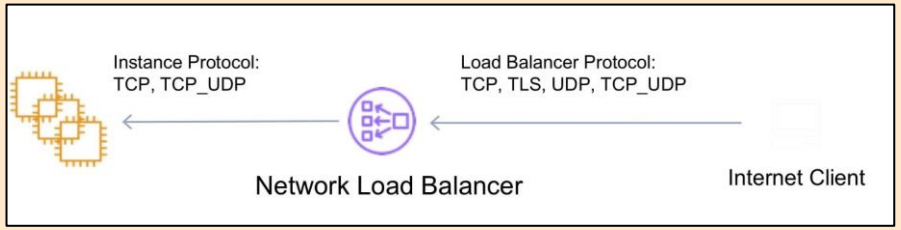
E — **Eventual consistency**
system will become consistent over time

	 Amazon SNS	 Amazon SQS
Message persistence	No	Yes
Delivery mechanism	Push (passive)	Poll (active)
Producer and consumer	Publisher and Subscriber	Send or receive
Distribution model	One to many (1:N)	One to one (1:1)
Most common use cases	Application to Application (A2A) Application to Person (A2P)	Application to Application (A2A)

- Amazon DynamoDB has two read/write capacity modes for processing reads and writes on your tables:

	Provisioned Mode 	On-Demand Mode 
What?	Provision the capacity (RCU/WCU) to run at a specific limit	No limit scaling, serving thousands of requests per second without capacity planning
Charges	Pay for provisioned capacity (whether you use it or not)	Pay only for read and write you perform
Benefit	Controls cost and supports capacity reservation	Instantly accommodates your workload as traffic ramps up or down
Suitable for	Steady state and predictable traffic	Random and unpredictable traffic
Floor and ceiling	Can be setup using Auto Scaling	Can scale to zero, no ceiling

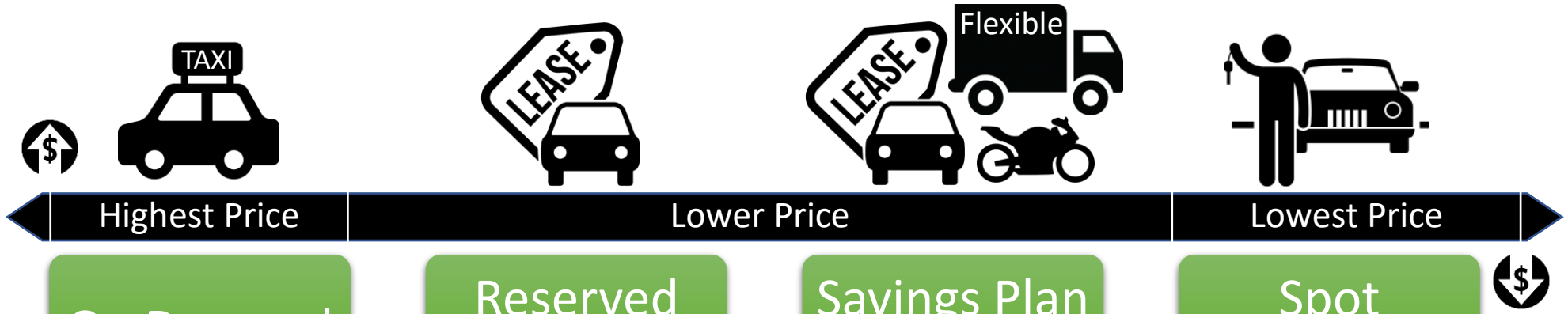
Find detailed explanation video on - www.analogiescloud.com

	Application Load Balancer (ALB)	Networks Load Balancer (NLB)
Operates at	Request Level (Application Layer / Layer 7)	Connection Level (Network Layer / Layer 3)
Routes traffic based on	Content of the Packet	Header of the Packet
Supported Protocols	HTTP, HTTPS 	TCP, UDP, TLS 
Static and Elastic IP	No	Yes
Target Types	Instances, Containers, Lambda, IP Addresses	Instances, Containers, IP Addresses

Autoscaling in AWS

	 (Launched in 2009) Amazon EC2 Auto Scaling	 (Launched in 2016) AWS Auto Scaling	 (Launched in 2018) AWS Application Auto Scaling
What?	Focus on Amazon EC2 Instance Auto Scaling	Build scaling plans for application scaling for multiple resources across multiple services	Automatically scaling resources for individual AWS services beyond Amazon EC2
How?	Automatically add or remove EC2 instances according to conditions you define in an ASG.	Automatically discover scalable resources in your application and configure scaling for all the resources in a single place using predefined guidance or configure it individually.	Through a scaling plan you can track specific CloudWatch metrics and use AWS CloudFormation templates for custom resource.
Which?	• Amazon EC2 Instances	• Amazon EC2 • Amazon EC2 Spot Fleets • Amazon ECS • Amazon DynamoDB • Amazon Aurora	• AppStream 2.0 fleets • Amazon EMR clusters • Amazon Neptune clusters • SageMaker endpoint variants • Custom Resources • And many more…

EC2 Purchase Options



On Demand

- Pay by second – Amazon Linux Ubuntu and Windows
- Pay by hours – Other Operating Systems
- Unpredictable workload

Reserved Instance

- 1 Year or 3 Year commitment
- Long running and predictable workload
- Reserve Region / AZ / Instance Type / OS

Savings Plan (RI 2.0)

- Commitment of a fixed payment
- Flexible in terms of reservation

Spot Instance

- Unused capacity of AWS infrastructure
- Supply and demand based pricing

Private, Public and Elastic IPs

	Private IP	Public IP	Elastic IP
Used for	Internal Communication	External Communication	External Communication
Mandatory / Optional	Mandatory	Optional	Optional
After Power Cycle	Stays same	Renewed	Stays same
Allocated to	Instance (ENI)	Instance (ENI)	Account (then associated)
Charges	No	No	Charged if unused

	AWS KMS	CloudHSM
Scope	AES-256 and RSA encrypt; RSA and ECC sign	Most general-purpose HSM functions (encrypt, sign /verify, derive, hash, wrap)
Secrets / keys stored in	Shared FIPS-validated HSM	Single-tenant FIPS-validated HSM in customer VPC
HSM controlled by	AWS	Customer
Scalability managed by	AWS	Customer
Keys managed by	AWS	Customer
Key access by	AWS IAM / resource policies	Customer-defined credentials
Integrated with AWS services	Yes	No
Secret / key operations implemented with	AWS CLI / SDK or Encryption SDK	Customer-built application
Rotation executed by	AWS [not for BYOK and CKS]	Customer

	RPO	RTO
Focuses on	Data loss prevention	Whole business recovery
Depends on	Backup Frequency	Speed of recovery
Describes	Maximum data loss	Maximum recovery time
Consideration	How often your data changes?	How much downtime you can handle?