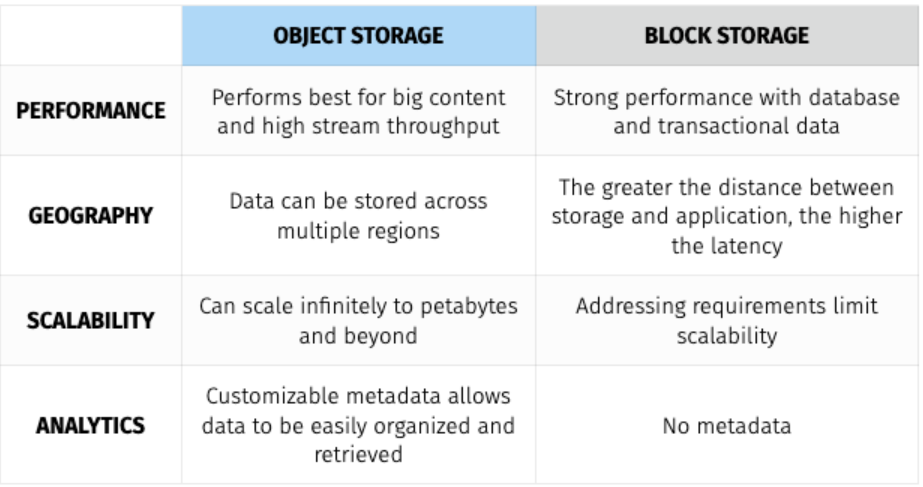
**IAM Entities:**

* **Users** - any individual end user such as an employee, system architect, CTO, etc.
* **Groups** - any collection of similar people with shared permissions such as system administrators, HR employees, finance teams, etc. Each user within their specified group will inherit the permissions set for the group.
* **Roles** - any software service that needs to be granted permissions to do its job, e.g- AWS Lambda needing write permissions to S3 or a fleet of EC2 instances needing read permissions from a RDS MySQL database.
* **Policies** - the documented rule sets that are applied to grant or limit access. In order for users, groups, or roles to properly set permissions, they use policies. Policies are written in JSON and you can either use custom policies for your specific needs or use the default policies set by AW

**Priority Levels in IAM**

* **Explicit Deny**: Denies access to a particular resource and this ruling cannot be overruled.
* **Explicit Allow**: Allows access to a particular resource so long as there is not an associated Explicit Deny.
* **Default Deny (or Implicit Deny)**: IAM identities start off with no resource access. Access instead must be granted.

**S3**

****

Data uploaded into S3 is spread across multiple files and facilities. The files uploaded into S3 have an upper-bound of 5TB per file and the number of files that can be uploaded is virtually limitless. S3 buckets, which contain all files, are named in a universal namespace so uniqueness is required. All successful uploads will return an **HTTP 200 response**.

* Objects (regular files or directories) are stored in S3 with a key, value, version ID, and metadata. They can also contain torrents and sub resources for access control lists which are basically permissions for the object itself.
* The data consistency model for S3 ensures immediate read access for new objects after the initial PUT requests. These new objects are introduced into AWS for the first time and thus do not need to be updated anywhere so they are available immediately.
* The data consistency model for S3 also ensures immediate read access for PUTS and DELETES of already existing objects.
* Amazon guarantees 99.999999999% (or 11 9s) durability for all S3 storage classes except its Reduced Redundancy Storage class.

**S3 Encryption:**

* **S3 Managed Keys / SSE - S3 (server side encryption S3 ) -** when Amazon manages the encryption and decryption keys for you automatically. In this scenario, you concede a little control to Amazon in exchange for ease of use.
* **AWS Key Management Service / SSE - KMS -** when Amazon and you both manage the encryption and decryption keys together.
* **Server Side Encryption w/ customer provided keys / SSE - C -** when I give Amazon my own keys that I manage. In this scenario, you concede ease of use in exchange for more control.

**Storage Gateway Simplified:**

Storage Gateway is a service that connects on-premise environments with cloud-based storage in order to seamlessly and securely integrate an on-prem application with a cloud storage backend. and Volume Gateway as a way of storing virtual hard disk drives in the cloud.

* The Storage Gateway service can either be a physical device or a VM image downloaded onto a host in an on-prem data center. It acts as a bridge to send or receive data from AWS.
* Storage Gateway can sit on top of VMWare's ESXi hypervisor for Linux machines and Microsoft’s Hyper-V hypervisor for Windows machines.
* The three types of Storage Gateways are below:
  + **File Gateway -** Operates via NFS or SMB and is used to store files in S3 over a network filesystem mount point in the supplied virtual machine. Simply put, you can think of a File Gateway as a file system mount on S3.
  + **Volume Gateway -** Operates via iSCSI and is used to store copies of hard disk drives or virtual hard disk drives in S3. These can be achieved via Stored Volumes or Cached Volumes. Simply put, you can think of Volume Gateway as a way of storing virtual hard disk drives in the cloud.
  + **Tape Gateway -** Operates as a Virtual Tape Library

**Stored Volumes vs. Cached Volumes:**

* Volume Gateway's **Stored Volumes** let you store data locally on-prem and backs the data up to AWS as a secondary data source. Stored Volumes allow low-latency access to entire datasets, while providing high availability over a hybrid cloud solution. Further, you can mount Stored Volumes on application infrastructure as iSCSI drives so when data is written to these volumes, the data is both written onto the on-prem hardware and asynchronously backed up as snapshots in AWS EBS or S3.
* Volume Gateway's **Cached Volumes** differ as they do not store the entire dataset locally like Stored Volumes. Instead, AWS is used as the primary data source and the local hardware is used as a caching layer. Only the most frequently used components are retained onto the on-prem infrastructure while the remaining data is served from AWS. This minimizes the need to scale on-prem infrastructure while still maintaining low-latency access to the most referenced data

**EC2 Placement Groups:**

* Clustered Placement Groups
* Spread Placement Groups
* Partitioned Placement Groups

**Elastic Network Interfaces (ENI)**

An elastic network interface is a networking component that represents a virtual network card. When you provision a new instance, there will be an ENI attached automatically and you can create and configure additional network interfaces if desired. When you move a network interface from one instance to another, network traffic is redirected to the new instance.

**Web Application Firewall (WAF)**AWS WAF is a web application that lets you allow or block the HTTP(s) requests that are bound for CloudFront, API Gateway, Application Load Balancers, EC2, and other Layer 7 entry points into your AWS environment. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that filter out specific traffic patterns that you can define. WAF's default rule-set addresses issues like the OWASP Top 10 security risks and is regularly updated whenever new vulnerabilities are discovered.