AWS DataSync can be used to move large amounts of data online between on-premises storage and Amazon S3, Amazon EFS, or Amazon FSx for Windows File Server. The source datastore can be Server Message Block (SMB) file servers.

AWS DataSync can be used to automate and accelerate the replication of data to AWS storage services. Note that Storage Gateway is used for hybrid scenarios where servers need local access to data with various options for storing and synchronizing the data to AWS storage services. Storage Gateway does not accelerate replication of data.

Some facts about Amazon EBS encrypted volumes and snapshots:

1. All **EBS** types support encryption and all instance **families** now support encryption.
2. Not all **instance** types support encryption.
3. Data in transit between an instance and an encrypted volume is also encrypted (data is encrypted in trans.
4. You can have encrypted an unencrypted EBS volumes attached to an instance at the same time.
5. Snapshots of encrypted volumes are encrypted automatically.
6. EBS volumes restored from encrypted snapshots are encrypted automatically.
7. EBS volumes created from encrypted snapshots are also encrypted.

**Cross-Account Copying**. To create a copy of the encrypted EBS snapshot in another account you need to complete four simple steps:

1. Share the custom key associated with the snapshot with the target account.
2. Share the encrypted EBS snapshot with the target account.
3. In the context of the target account, locate the shared snapshot and make a copy of it.
4. Use the newly created copy to create a new volume.
5. If you make periodic snapshots of a volume, the snapshots are incremental, which means that only the blocks on the device that have changed after your last snapshot are saved in the new snapshot.
6. EBS volumes are AZ specific, but snapshots are region specific.
7. Snapshots can be copied between regions (and be encrypted). Images are then created from the snapshot in the other region which creates an AMI that can be used to boot an instance.
8. Snapshots of encrypted volumes are encrypted automatically.
9. EBS volumes restored from encrypted snapshots are encrypted automatically.
10. EBS volumes created from encrypted snapshots are also encrypted.
11. You can share snapshots, but if they’re encrypted it must be with a custom CMK key.
12. You can check the encryption status of your EBS volumes with AWS Config.
13. You cannot share encrypted volumes created using a default CMK key.
14. You cannot make encrypted snapshots public.
15. You can share encrypted snapshots with other AWS accounts using a non-default CMK key and configuring cross-account permissions to give the account access to the key, mark as private and configure the account to share with.

The following information applies to snapshots:

* Snapshots are created asynchronously and are incremental.
* You can copy unencrypted snapshots (optionally encrypt).
* You can copy an encrypted snapshot (optionally re-encrypt with a different key).
* Snapshot copies receive a new unique ID.
* You can copy within or between regions.
* You cannot move snapshots, only copy them.
* You cannot take a copy of a snapshot when it is in a “pending” state, it must be “complete”.
* S3 Server Side Encryption (SSE) protects data in transit while copying.
* User defined tags are not copied.
* You can have up to 5 snapshot copy requests running in a single destination per account.
* You can copy Import/Export service, AWS Marketplace, and AWS Storage Gateway snapshots.
* If you try to copy an encrypted snapshot without having access to the encryption keys it will fail silently (cross-account permissions are required).

**Elastic Fabric Adapter (EFA)**

An Elastic Fabric Adapter is an AWS [Elastic Network Adapter](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking-ena.html)  (ENA) with added capabilities. Elastic Fabric Adapter (EFA) is a network interface for Amazon EC2 instances that enables customers to run applications requiring high levels of inter-node communications at scale on AWS.

Common use cases for EFAs include:

* **High Performance Computing (HPC) applications** using the Message Passing Interface (MPI).
* Machine Learning (ML) applications using NVIDIA Collective Communications Library (NCCL).

When to use ENA:

* Good for use cases that require higher bandwidth and lower inter-instance latency.
* Supported for limited instance types (HVM only).

Elastic Network Adapter (ENA)" is incorrect. The ENA, which provides Enhanced Networking, does provide high bandwidth and low inter-instance latency but it does not support the features for a tightly-coupled app that the EFA does.

When you launch a new EC2 instance, the EC2 service attempts to place the instance in such a way that all of your instances are spread out across underlying hardware to minimize correlated failures. You can use *placement groups* to influence the placement of a group of *interdependent* instances to meet the needs of your workload. Depending on the type of workload, you can create a placement group using one of the following placement strategies:

* *Cluster* – packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications.
* *Partition* – spreads your instances across logical partitions such that groups of instances in one partition do not share the underlying hardware with groups of instances in different partitions. This strategy is typically used by large distributed and replicated workloads, such as Hadoop, Cassandra, and Kafka.
* *Spread* – strictly places a small group of instances across distinct underlying hardware to reduce correlated failures.

