FabricPool

FlexPod

NetApp
June 08, 2021

Table of Contents

FabricPool

FabricPool overview

FabricPool is a hybrid storage solution in ONTAP that uses an all-flash (SSD) aggregate as a performance tier and an object store in a public cloud service as a cloud tier. This configuration enables policy-based data movement, depending on whether or not data is frequently accessed. FabricPool is supported in ONTAP for both AFF and all-SSD aggregates on FAS platforms. Data processing is performed at the block level, with frequently accessed data blocks in the all-flash performance tier tagged as hot and infrequently accessed blocks tagged as cold.

Using FabricPool helps to reduce storage costs without compromising performance, efficiency, security, or protection. FabricPool is transparent to enterprise applications and capitalizes on cloud efficiencies by lowering storage TCO without having to rearchitect the application infrastructure.

FlexPod can benefit from the storage tiering capabilities of FabricPool to make more efficient use of ONTAP flash storage. Inactive virtual machines (VMs), infrequently used VM templates, and VM backups from NetApp SnapCenter for vSphere can consume valuable space in the datastore volume. Moving cold data to the cloud tier frees space and resources for high-performance, mission- critical applications hosted on the FlexPod infrastructure.

Fibre Channel and iSCSI protocols generally take longer before experiencing a timeout (60 to 120 seconds), but they do not retry to establish a connection in the same way that NAS protocols do. If a SAN protocol times out, the application must be restarted. Even a short disruption could be disastrous to production applications using SAN protocols because there is no way to guarantee connectivity to public clouds. To avoid this issue, NetApp recommends using private clouds when tiering data that is accessed by SAN protocols.

In ONTAP 9.6, FabricPool integrates with all the major public cloud providers: Alibaba Cloud Object Storage Service, Amazon AWS S3, Google Cloud Storage, IBM Cloud Object Storage, and Microsoft Azure Blob Storage. This report focuses on Amazon AWS S3 storage as the cloud object tier of choice.

The composite aggregate

A FabricPool instance is created by associating an ONTAP flash aggregate with a cloud object store, such as an AWS S3 bucket, to create a composite aggregate. When volumes are created inside the composite aggregate, they can take advantage of the tiering capabilities of FabricPool. When data is written to the volume, ONTAP assigns a temperature to each of the data blocks. When the block is first written, it is assigned a temperature of hot. As time passes, if the data is not accessed, it undergoes a cooling process until it is finally assigned a cold status. These infrequently accessed data blocks are then tiered off the performance SSD aggregate and into the cloud object store.

The period of time between when a block is designated as cold and when it is moved to cloud object storage is modified by the volume tiering policy in ONTAP. Further granularity is achieved by modifying ONTAP settings that control the number of days required for a block to become cold. Candidates for data tiering are traditional volume snapshots, SnapCenter for vSphere VM backups and other NetApp Snapshot- based backups, and any infrequently used blocks in a vSphere datastore, such as VM templates and infrequently accessed VM data.

Inactive data reporting

Inactive data reporting (IDR) is available in ONTAP to help evaluate the amount of cold data that can be tiered from an aggregate. IDR is enabled by default in ONTAP 9.6 and uses a default 31-day cooling policy to determine which data in the volume is inactive.

> The amount of cold data that is tiered depends on the tiering policies set on the volume. This amount may be different than the amount of cold data detected by IDR using the default 31-day cooling period.

Object creation and data movement

FabricPool works at the NetApp WAFL block level, cooling blocks, concatenating them into storage objects, and migrating those objects to a cloud tier. Each FabricPool object is 4MB and is composed of 1,024 4KB blocks. The object size is fixed at 4MB based on performance recommendations from leading cloud providers and cannot be changed. If cold blocks are read and made hot, only the requested blocks in the 4MB object are fetched and moved back to the performance tier. Neither the entire object nor the entire file is migrated back. Only the necessary blocks are migrated.

> If ONTAP detects an opportunity for sequential readaheads, it requests blocks from the cloud tier before they are read to improve performance.

By default, data is moved to the cloud tier only when the performance aggregate is greater than 50% utilized. This threshold can be set to a lower percentage to allow a smaller amount of data storage on the performance flash tier to be moved to the cloud. This might be useful if the tiering strategy is to move cold data only when the aggregate is nearing capacity.

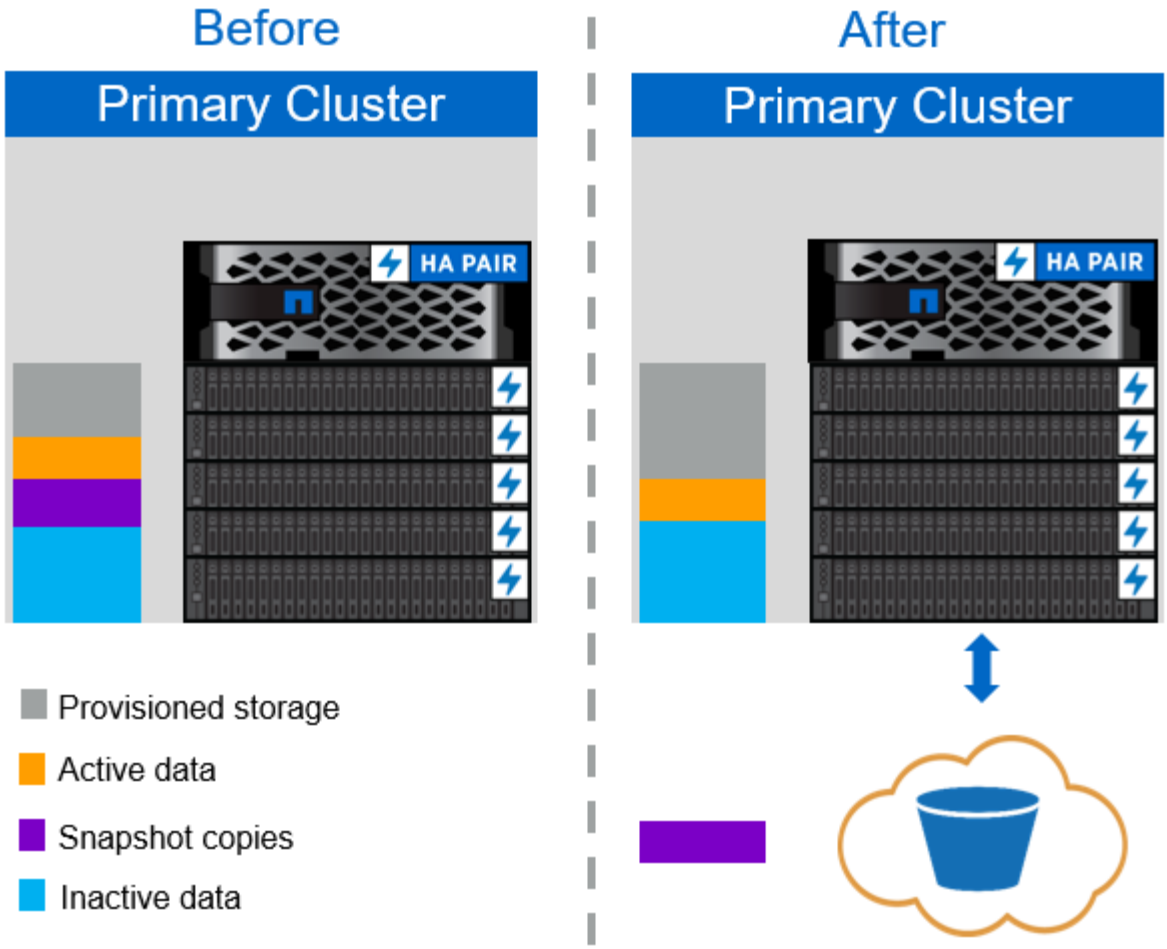
If performance tier utilization is at greater than 70% capacity, cold data is read directly from the cloud tier without being written back to the performance tier. By preventing cold data write-backs on heavily used aggregates, FabricPool preserves the aggregate for active data.

Reclaim performance tier space

As previously discussed, the primary use case for FabricPool is to facilitate the most efficient use of high-performance on-premises flash storage. Cold data in the form of volume snapshots and VM backups of the FlexPod virtual infrastructure can occupy a significant amount of expensive flash storage. Valuable performance- tier storage can be freed by implementing one of two tiering policies: Snapshot-Only or Auto.

Snapshot-Only tiering policy

The Snapshot-Only tiering policy, illustrated in the following figure, moves cold volume snapshot data and SnapCenter for vSphere backups of VMs that are occupying space but are not sharing blocks with the active file system into a cloud object store. The Snapshot-Only tiering policy moves cold data blocks to the cloud tier. If a restore is required, cold blocks in the cloud are made hot and moved back to the performance flash tier on the premises.

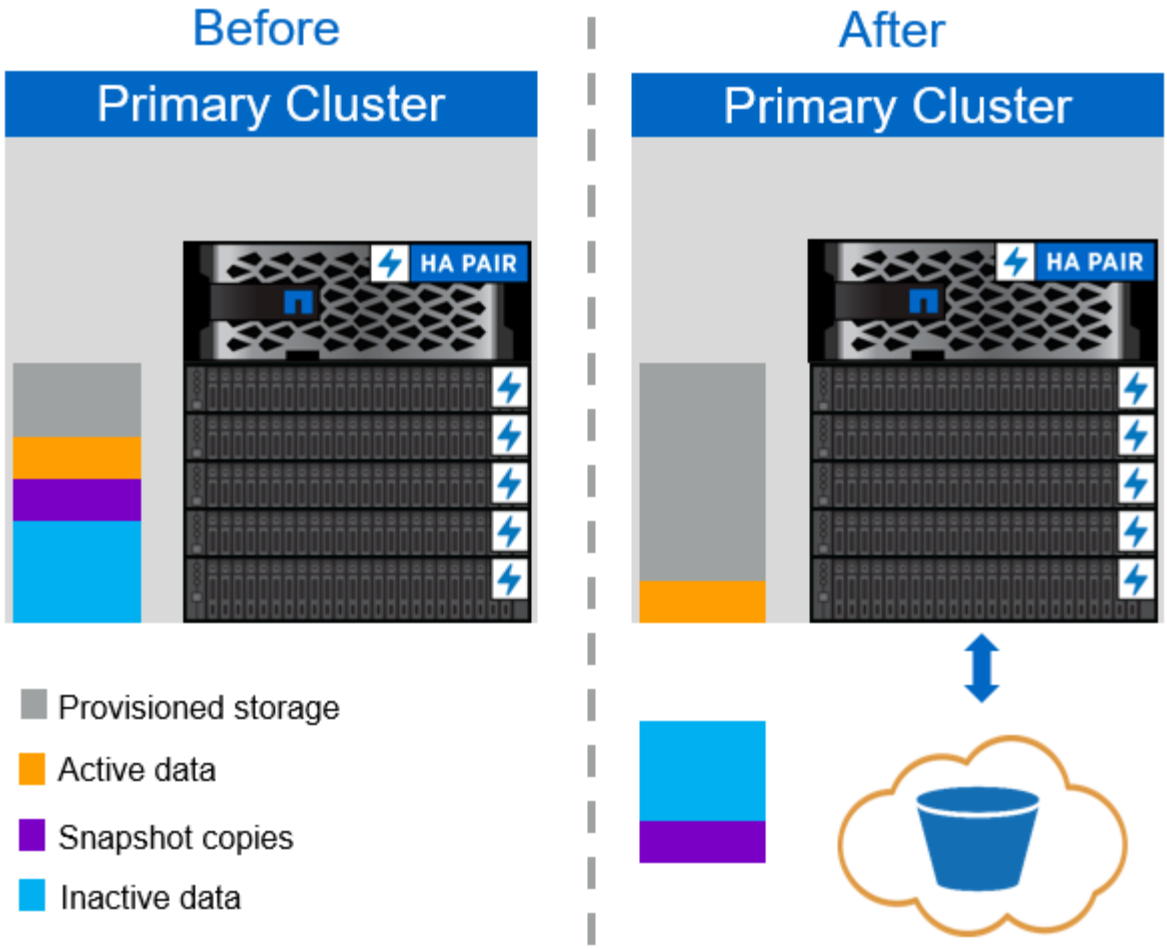


Auto tiering policy

The FabricPool Auto tiering policy, illustrated in the following figure, not only moves cold snapshot data blocks to the cloud, it also moves any cold blocks in the active file system. This can include VM templates and any unused VM data in the datastore volume. Which cold blocks are moved is controlled by the `tiering-minimum-cooling-days` setting for the volume. If cold blocks in the cloud tier are randomly read by an application, those blocks are made hot and brought back to the performance tier. However, if cold blocks are read by a sequential process such as an antivirus scanner, the blocks remain cold and persist in the cloud object store; they are not moved back to the performance tier.

When using the Auto tiering policy, infrequently accessed blocks that are made hot are pulled back from the cloud tier at the speed of cloud connectivity. This may affect VM performance if the application is latency sensitive, which should be considered before using the Auto tiering policy on the datastore. NetApp recommends placing Intercluster LIFs on ports with a speed of 10GbE for adequate performance.

The object store profiler should be used to test latency and throughput to the object store before attaching it to a FabricPool aggregate.



All tiering policy

Unlike the Auto and Snapshot-only policies, the All tiering policy moves entire volumes of data immediately into the cloud tier. This policy is best suited to secondary data protection or archival volumes for which data must be kept for historical or regulatory purposes but is rarely accessed. The All policy is not recommended for VMware datastore volumes because any data written to the datastore is immediately moved to the cloud tier. Subsequent read operations are performed from the cloud and could potentially introduce performance issues for VMs and applications residing in the datastore volume.

Security

Security is a central concern for the cloud and for FabricPool. All the native security features of ONTAP are supported in the performance tier, and the movement of data is secured as it is transferred to the cloud tier. FabricPool uses the AES-256-GCM encryption algorithm on the performance tier and maintains this encryption end to end into the cloud tier. Data blocks that are moved to the cloud object store are secured with transport layer security (TLS) v1.2 to maintain data confidentiality and integrity between storage tiers.

Communicating with the cloud object store over an unencrypted connection is supported but not recommended by NetApp.

Data encryption

Data encryption is vital to the protection of intellectual property, trade information, and personally identifiable customer information. FabricPool fully supports both NetApp Volume Encryption (NVE) and NetApp Storage

Encryption (NSE) to maintain existing data protection strategies. All encrypted data on the performance tier remains encrypted when moved to the cloud tier. Client-side encryption keys are owned by ONTAP and the server-side object store encryption keys are owned by the respective cloud object store. Any data not encrypted with NVE is encrypted with the AES-256-GCM algorithm. No other AES-256 ciphers are supported.

The use of NSE or NVE is optional and not required to use FabricPool.