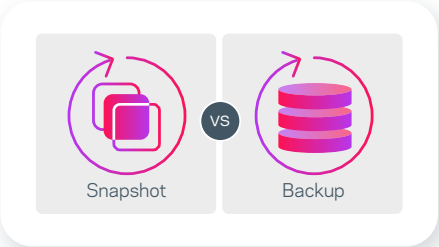
VERITAS

The Difference Between Data Snapshots and Backups

Optimizing data protection: maximizing its effectiveness.

Data protection is crucial to ensure the safety and availability of your organization's critical information. When it comes to preserving data, two popular methods are snapshots and backups. Both serve different purposes and offer unique advantages. While snapshots are helpful in certain situations, they provide a different level of protection than a backup.



What Is a Snapshot?

Snapshots are point-in-time copies of data that capture the state of a system or volume at a specific moment. A snapshot contains a singular record of your system configuration. Snapshots are compact, efficient, and avoid the lag and expense of relocating information by effortlessly restoring themselves in seconds. A snapshot preserves a moment of your server's file system, metadata, and settings. You need to store the snapshot source files in a separate location to be able to retrieve them. You can create snapshots quickly and frequently, making them great for quick testing.

What Is a True Backup?

Backups come in several forms, including full, incremental, and reverse-incremental styles, each with distinct merits. Backups are stored separately from the original data. They allow you to roll back your system to restore services and files from a previous point before a data loss or corruption event. By completely replicating your database and saving it in an alternate location, you can gain peace of mind in the event of file corruption or data loss.

How Are They Different?

In short, capturing a snapshot is not the same as making a backup.

- A snapshot is an image of all data residing on the server, but you can't select parts to keep or restore. Capturing snapshots is often done before testing or implementing significant modifications. This feature allows you to make multiple saves.
- When you initiate a backup, it overwrites the previous document with the latest version. If programs or applications are running, or a database is active, they can cause issues with the backup. For example, real-time writing processes can result in incomplete files and failed snapshots. Because backups are comprehensive, they take longer (sometimes hours) to create.

Knowing these nuances may help you identify which to use for specific use cases.

When to Use Snapshots

Snapshots offer instant recovery by allowing you to roll back to a specific point in time, eliminating a lengthier restore. Snapshots use a copy-on-write mechanism. This means they are store changes made since the prior snapshot. This reduces storage requirements and improves efficiency. Snapshots excel at recovery time objectives (RTO) due to minimal downtime, making them useful for temporary rollbacks.

When Snapshots Aren't Enough

Snapshots are:

- Not designed for long-term archiving and do not meet compliance requirements
- Typically tied to the specific system from which they are taken
- More vulnerable to risks that affect primary data because they are usually stored on the same storage system

Why Backups Are Best

1. Backups excel for flexible recovery point objectives (RPO) because you can recover from any specific point in time. They're particularly suitable if you require long-term data retention and must comply with regulations.
2. Backups involve creating multiple copies of data and storing them separately from the source. These copies serve as a safety net to recover data in case of data loss, corruption, or system failure. Backups provide a comprehensive solution. You can retain backups for extended periods, providing historical data useful for compliance, legal requirements, and long-term analytics.
3. With backups, you can selectively restore files, folders, or an entire system based on your needs. You can also restore data to different locations. Backups are more immune to vulnerabilities because they are typically housed separately from production.
4. Snapshots and backups involve duplicating data. Snapshots are great for testing software changes and updates, while backups provide a more comprehensive way to protect your data. If you want to protect your critical systems and remain compliant, backups are a superior option.
5. Data protection is not a one-size-fits-all activity. Veritas utilizes snapshots and backups. Your data management lifecycle needs the flexibility to adjust and scale to your SLAs and production. Our goal is to make your company as resilient as possible, and fill your toolbox with the best data protection solutions available.
6. By leveraging the strengths of snapshots and backups, you can ensure your data is safe, available, and recoverable.

Learn more about data protection solutions from Veritas. →

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1943 08/23