Ransomware Protection with NetBackup MSDP and FlashBlade

Your existing data protection may not be enough. Backups safeguard critical data against common scenarios, such as recovering from natural or human-caused disasters, data corruption, or accidental deletions. However, ransomware attacks can stress existing data-protection infrastructure that may be built on legacy architectures, such as disk and tape. Ransomware attacks continue to be top of mind for business and IT leaders.

This blog post will guide you through how to implement FlashBlade® SafeMode™ snapshots with Veritas NetBackup Media Server Deduplication Pool (MSDP). For general best practices for using FlashBlade with NetBackup, contact your Pure Storage® account team. For MSDP performance and best practices, please refer to the Rapid Restore of Oracle Using FlashBlade and NetBackup white paper.

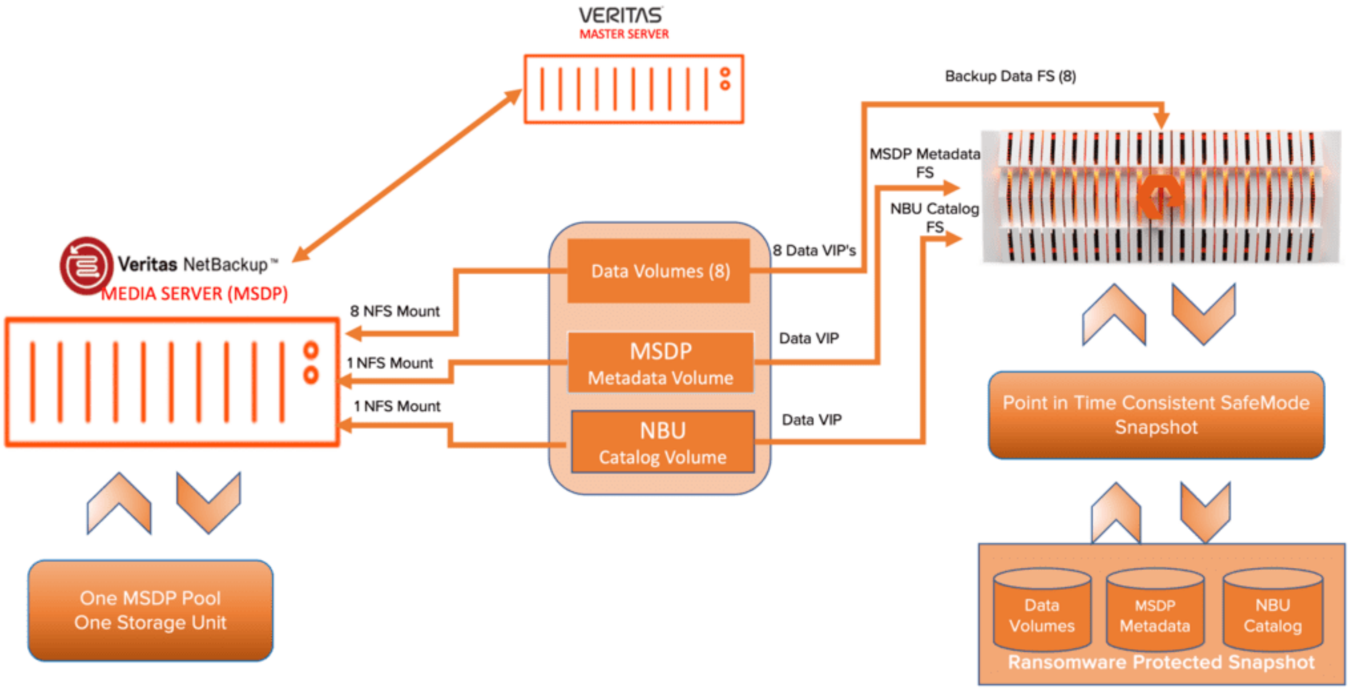
What are SafeMode snapshots in FlashBlade? Designed to secure backup data from ransomware attacks, they automatically create snapshots for the file systems from time to time and also prevent users from eradicating the snapshots from the system. If a ransomware attack causes any problems with new data, you'll have a path to recovery.

FlashBlade prevents anyone from eradicating snapshots, which means all backup data, MSDP metadata, and NetBackup catalog data is protected with read-only mode snapshots. If backup data is compromised from a ransomware attack, you can recover the backup data and metadata from a read-only snapshot with a rollover snapshot feature.

To configure NetBackup MSDP on FlashBlade, please refer to my Veritas NetBackup MSDP Integration with FlashBlade NFS post.

Implementation Overview

The logical architecture of Veritas NetBackup and Pure Storage is illustrated below. The supported primary application for backup can be hosted on any storage, but for fast backup and fast restore, it's imperative to host on a flash array like Pure Storage FlashArray™. FlashBlade acts as an NFS storage target for backups conducted by NetBackup.



The backup application NetBackup MSDP is configured on the network file system running on FlashBlade. In reality, FlashBlade is a true scale-out gateway NAS cluster file system, capable of very high-performance bandwidth. The SafeMode snapshot feature is included at no extra cost and provides insurance to recover data in the event of a ransomware attack. Meanwhile, NetBackup MSDP is a highly efficient deduplication engine and supports backup for most of the primary applications such as Oracle, VMware, and SQL.

Best Practices for Configuration

Before getting started with the implementation, we recommend that you do the following:

- Use Purity//FB 3.0 or later.
- Configure FlashBlade with NetBackup for MSDP configuration.
- Define the appropriate SafeMode snapshot policy.
- Estimate capacity requirements.
- Contact your Pure Support account team to set up FlashBlade for SafeMode.

When executing SafeMode Snapshots on the MSDP-configured file system, the SafeMode snapshot should be performed when there’s no activity on the MSDP storage server, and the storage pool is quiesced. The snapshot retention value should account for the necessary backup schedules to provide the required data availability to meet business requirements. This needs to be balanced against the additional storage required for each extra day of retention.

We recommended the following steps:

- Suspending Schedule
- Suspending SLPs

- Backing up NetBackup Catalog
- Suspending activity on the MSDP storage server
- Performing SafeMode snapshot on the FB file system
- Activating the MSDP storage server again
- Resuming the SLPs
- Resuming the NetBackup policy schedule

Snapshot Recovery and NetBackup Disaster Recovery

When faced with a ransomware event, rogue administrator, or other type of data loss event, SafeMode snapshots make restoring service simple. This section details the process to recover NetBackup MSDP metadata, NetBackup Catalog, and MSDP backed-up data on FlashBlade. For instructions on performing NetBackup DR recovery, refer to NetBackup's documentation.

Contact Pure Support

As soon as you identify an attack, it's critical that your authorized administrator contact Pure Storage Support right away. Our Support team can change the snapshot schedule and retention to ensure your data remains available during recovery. This is especially important if you need to recover from an older snapshot.

Stop Jobs and Media Server and Master Server Services

File system rollback can disrupt active file access. It's important to remove any risk of potential issues with NetBackup due to lost file access. Before starting recovery, stop any running jobs, and stop NetBackup media server and master server services.

Roll Back to Snapshot

Identify which snapshot needs to be recovered for all the file systems for the MSDP storage pool, MSDP metadata, and catalog file system, based on the time of the event and whether the data is clean. Pure Storage Support will perform the rollback of the affected file systems. If you have an MSDP data pool, there'll most likely be multiple file systems in a single MSDP storage unit. Make sure to roll back all of them.

NetBackup MSDP Metadata Recovery

Configuration of FlashBlade as an NFS target for NetBackup MSDP metadata involves creating an NFS volume on FlashBlade and exporting this share to the media server. This ensures the MSDP metadata is protected with SafeMode snapshot on FlashBlade. At the time of disaster, the MSDP metadata is recovered to the configured file system with rollback to snapshot.

NetBackup Catalog Recovery

Full catalog recovery restores the device and the media configuration information in the catalog backup. During the catalog recovery process, services may be shut down and restarted. You can generate the disaster recovery file from the catalog backup image and later use it for disaster recovery purposes.

Restart NetBackup Services and Perform the Data Verification

Once data recovery is complete, run the data verification in NetBackup to identify any data gaps and prevent future recoveries from using data that's no longer available. Veritas NetBackup has procedures for data verification of the images, refer to NetBackup's documentation for more details.

Takeaways

Ransomware attacks are on the rise. Safeguard your data infrastructure and simplify restoring service by configuring NetBackup MSDP with FlashBlade SafeMode snapshots. With these two powerful tools, you:

- Get a safety net against attacks from ransomware or rogue admins.
- Prevent manual deletions.
- Protect backup data sets, MDSP metadata, and the NetBackup Catalog.

If you already have a current FlashBlade subscription or maintenance support, you already have FlashBlade SafeMode snapshots, so why not get the most out of them?

Check out the video below for more on this implementation.