PURESTORAGE®

TECHNICAL WHITE PAPER

Ransomware Protection with Pure and Veritas

Pure FlashBlade® SafeMode™ Snaphots and Veritas NetBackup MSDP work together to protect your data in the event of a ransomware attack.

Contents

Introduction

Ransomware attacks continue to be top-of-mind for business and IT leaders. And for good reason. Ransomware compromises access to your organization's lifeblood—data. Consequences can be dire: Pay perpetrators to (maybe) unencrypt your data, stumble with decryption tools, or gamble on recovering from backups. With millions of dollars spent annually to guard entry points to data, many still underestimate the strategic value of augmenting data protection.

But your existing data protection may not be enough. Backups safeguard critical data against common scenarios such as recovering from natural or man-made disasters, data corruption, or accidental deletions. But ransomware attacks can stress existing data-protection infrastructure that may be built on legacy architectures—such as disk and tape—more than expected. First, if you're already struggling with meeting recovery SLAs, a ransomware attack can exacerbate the situation with additional downtime. Second, ransomware can compromise your backup systems and data, which could require you to reinstall and reconfigure your backup solution before you even contemplate data recovery.

This technical white paper provides an overview of the integration of Veritas NetBackup and Pure Storage® FlashBlade®. It discusses the performance and best practices of FlashBlade as an NFS target for NetBackup deduplicated data when backing up and restoring Oracle database(s). The target audience for this document includes, but is not limited to, administrators, storage administrators, IT managers, system architects, sales engineers, field consultants, professional services, and partners who are looking to design and deploy Pure Storage and Veritas solutions.

Pure FlashBlade: A Quick Recap

Pure Storage developed the FlashBlade architecture to meet the storage needs of data-driven businesses. FlashBlade is an all-flash system, primarily optimized for storing and processing unstructured data. A FlashBlade system can simultaneously host multiple file systems and multi-tenant object stores for thousands of clients. A scale-out, all-flash storage system, FlashBlade is powered by a distributed file system that was purpose-built for massive concurrency across all data types. It can scale up to multi-petabyte capacity with linear-scale performance simply by adding a single blade at a time, up to 150 blades. Due to its native scale-out architecture and ability to drive performance for workload type, it is considered a data hub that enables enterprises to consolidate a range of workloads—from backup to analytics and AI—on a single platform.

Figure 1. Features of Pure FlashBlade

Many organizations build their data protection strategy with FlashBlade, enjoying rapid backup and restore performance while investing in a platform that enables them to consolidate data lakes and other data silos. A FlashBlade system's ability to scale performance and capacity is based on five key innovations:

- **High-performance storage:** FlashBlade maximizes the advantages of an all-flash architecture by storing data in storage units and ditching the crippling, high-latency storage media such as traditional spinning disks and conventional solid-state drives. The integration of scalable NVRAM into each storage unit helps scale performance and capacity proportionally when new blades are added to a system.
- **Unified network:** A FlashBlade system consolidates high communication traffic between clients and internal administrative hosts into a single, reliable high-performing network that supports both IPv4 and IPv6 client access over Ethernet links up to 160Gb/s.
- **Purity//FB storage operating system:** With its symmetrical operating system running on FlashBlade's fabric modules, Purity//FB minimizes workload balancing problems by distributing all client operation requests evenly among the blades on FlashBlade.
- **Common media architectural design for files and objects:** FlashBlade's single underlying media architecture supports concurrent access to files via a variety of protocols such as NFSv3, NFS over HTTP, and SMB (with Samba-level functionality) and objects via Amazon S3 across the entire FlashBlade configuration.
- **Simple usability:** Purity//FB on FlashBlade alleviates system-management headaches as it simplifies storage operations by performing routine administrative tasks autonomously. With a robust operating system, FlashBlade is capable of self-tuning and providing system alerts when components fail.

A full FlashBlade system configuration consists of up to five self-contained rack-mounted chassis interconnected by high-speed links to two external fabric modules (XFM). The rear of each chassis includes two on-board fabric modules for interconnecting the blades, other chassis, and client systems using TCP/IP over high-speed Ethernet. Both fabric modules are interconnected, and each contains a control processor and Ethernet switch ASIC. For reliability, each chassis is equipped with redundant power supplies and cooling fans.

The front of each chassis holds up to 15 blades for processing data operations and storage. Each blade assembly is a self-contained compute module equipped with processors, communication interfaces, and 17TB or 52TB of flash memory for persistent data storage.

The current FlashBlade system can support more than 1.5 million NFSv3 getattrs commands per second, and up to 4.5GB/s of write and up to 15GB/s of read in a single 4U chassis with 15 blades. It can scale both compute and performance up to a 10 x 4U chassis with 150 blades.

FlashBlade SafeMode

At Pure Storage, we share the concerns around ransomware. We're pleased to introduce a new approach to mitigating[1] these attacks when using Pure FlashBlade systems. Built-in to FlashBlade, SafeMode snapshots enable you to create read-only snapshots of backup data and associated metadata catalogs after you've performed a full backup. You can recover data directly from these snapshots, helping guard against attacks by ransomware and even rogue admins. FlashBlade provides the following benefits:

- **Enhanced protection:** Ransomware can't eradicate (delete), modify, or encrypt SafeMode snapshots.
- **Employee safeguards:** Only an authorized designee from your organization can work directly with Pure Technical Support to configure the feature, modify policy, or manually eradicate snapshots.
- **Backup integration:** Utilize the same snapshot process regardless of the backup product or native utility used to manage data-protection processes.
- **Flexibility:** Snapshot cadence and eradication scheduling are customizable.
- **Rapid restore:** Leverage a massively parallel architecture and elastic performance that scales with data to speed backup—and recovery.
- **Investment protection:** FlashBlade includes SafeMode snapshots at no extra charge. Your Pure subscription or maintenance support contract cover enhancements.

Veritas NetBackup

Veritas offers industry-leading enterprise data-management solutions that integrate broadly across its product portfolio and build on the company's market-leading Veritas NetBackup™ data protection solution. Long recognized as a market-share leader of enterprise backup and recovery software, Veritas NetBackup protects the largest and most demanding multi-cloud and data center environments. NetBackup provides breakthrough capabilities for virtualized and cloud-based deployments. Features like high performance, intelligent automation, and centralized management based on a flexible, multi-tier architecture enable NetBackup to adapt to the growing needs of a fast-paced, modern enterprise.

One of the hallmarks of enterprise IT is its heterogeneity. The variety of platforms, applications, and infrastructure often grows as the enterprise grows. NetBackup supports a vast array of environments and integrates with every layer of the infrastructure stack to unify your entire data protection strategy. NetBackup software offers backup to various storage targets such as tape, storage array network (SAN), network-attached storage (NAS), and public and private cloud.

[1] FlashBlade SafeMode Snapshots allow recovery of data after a ransomware attack but does not prevent the attack from occurring.

Pure and Veritas NetBackup: Solution Overview

Figure 2 illustrates the logical architecture of Veritas NetBackup with Pure Storage arrays. You can host the supported primary application for backup on any storage. But for fast backup and fast restore, you must host it on an all-flash array like Pure FlashArray™. FlashBlade acts as an NFS storage target for backups performed by NetBackup.

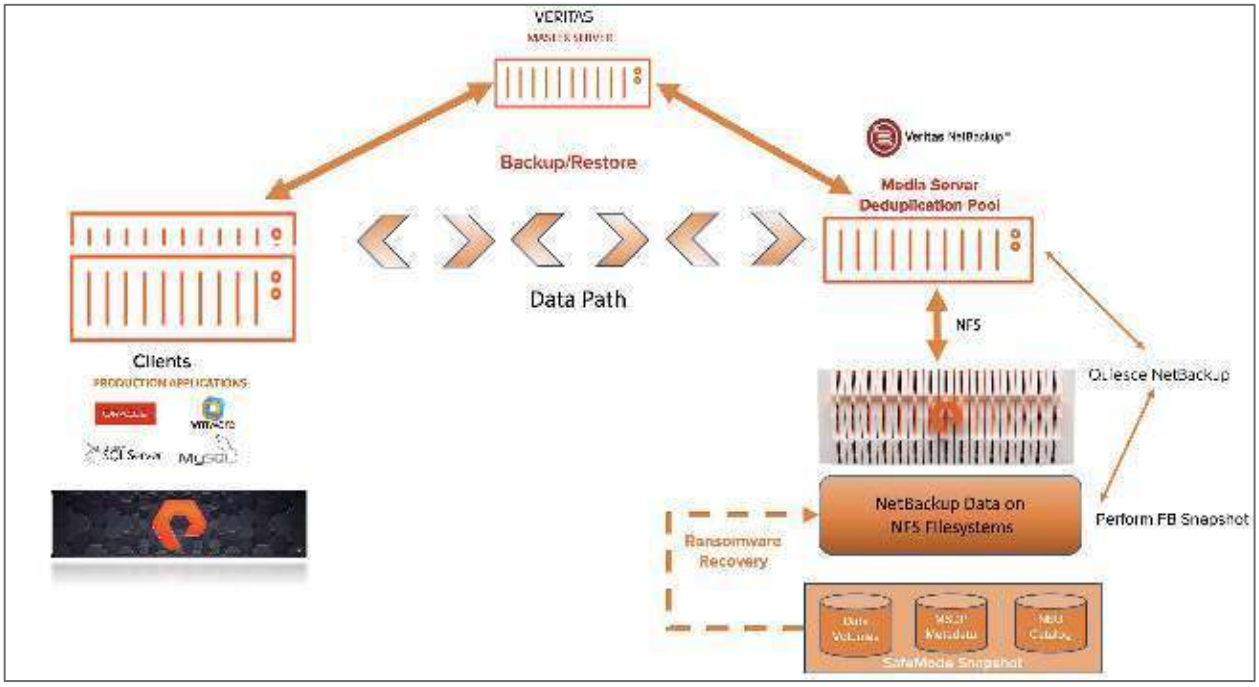

Figure 2. The logical architecture of Veritas NetBackup with Pure Storage arrays.

NetBackup can use FlashBlade as a target for deduplicated or non-deduplicated backups. To learn how to configure FlashBlade as a NetBackup deduplication pool please read the solutions guide on MSDP. This document describes how to mitigate a ransomware attack using FlashBlade SafeMode Snapshots with a NetBackup deduplication pool.

Recommended MSDP Architecture

Figure 3 illustrates NetBackup MSDP architecture configured over the NFS filesystem on Pure Storage FlashBlade. The Backup Application NetBackup MSDP is configured on the Network File System running on FlashBlade.

Configuration of FlashBlade as an NFS target for NetBackup involves creating volume(s) and exporting these volume(s) as an NFS share to the host acting as a media server. These shares are then mounted on the media server and configured to be a target storage unit for backups. It is required to have different Data Vips to mount the FlashBlade NFS file systems for backup data but it's not required to use separate data vips for metadata and catalog volumes. For more details please refer to the MSDP solutions guide.

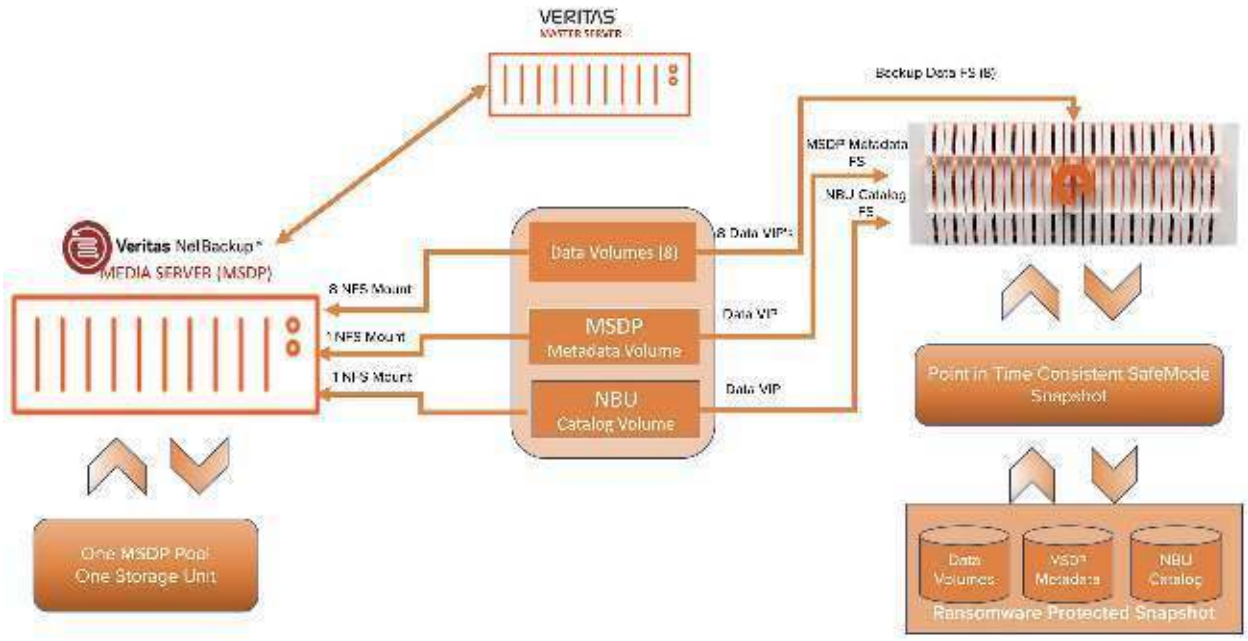

Figure 3. NetBackup MSDP architecture configured over the NFS filesystem on Storage FlashBlade.

Introduction to SafeMode Snapshots

SafeMode snapshots are designed to secure backup data from ransomware attacks. FlashBlade SafeMode for file systems does two things:

- Helps automatically create snapshots for the file systems from time to time
- Prevents the user from eradicating the snapshots from the system

If there are any problems with new data that a ransomware attack can cause, there is a path to recovery protecting against such malicious behavior. This also protects the system from mistakes, rogue admins, or compromised admin accounts.

Best Practices and Procedure

These best practices are organized to encapsulate the prerequisites, the components of the architecture from FlashBlade foundations to NetBackup Storage provisioning, and execution of the SafeMode snapshot. Each section covers the entire configuration of the component.

Prerequisites

Use Purity//FB 3.0 or Later

Purity//FB 3.0 includes significant enhancements that improve ransomware mitigation. The most impactful change is support for the rollback of SafeMode snapshots, which allows you to work with Pure's support teams to instantly restore the live file system after an event and purge compromised data.

Use Netbackup8.2 with EEB ET3981134

Utilizing FlashBlade as an NFS storage target for deduplicated data is supported with NetBackup version 8.2 with EEB ET3981134 running on Red Hat Enterprise Linux (RHEL) 7.6 and onwards. (For more information, read the Pure Storage MSDP best practices guide.

Enable the SafeMode Snapshot on FlashBlade

Before proceeding to take a snapshot, you need to configure FlashBlade to take SafeMode snapshots. To enable SafeMode, please contact your Pure support account team.

Foundations

Media Server Deduplication Pool Configuration

Veritas NetBackup provides deduplication options that let you deduplicate data everywhere, as close to the source of data as you require. MSDP provides the ability to reduce the amount of data that is stored, backup bandwidth, backup windows, and infrastructure. (For more information on NetBackup MSDP configuration, refer to the MSDP Solution Guide.)

Manual SafeMode Snapshot

The manual SafeMode snapshot should be performed when there is no activity on the MSDP storage server and the storage pool is quiesced. (For more information please refer to the next section.) Consider taking the necessary snapshot daily to provide the required data availability to meet business requirements. The snapshot retention period on this snapshot will set to the default settings. Your authorized administrator will work with Pure Support if you need to perform the deletion on the snapshots.

Estimate Capacity Requirements

You need the baseline size, daily change rate, and expected data reduction rate to estimate the capacity for SafeMode snapshot. Apply the reduction rate to the daily change rate and multiply by the number of days you will keep snapshots. Add the baseline to calculate the total expected capacity required for SafeMode snapshot implementation.

For example, in an environment with 300TiB of data, the baseline after initial data reduction could be 180TiB. If the daily change rate is 10TiB and data reduction is 2:1, the overall backup change rate is 5TiB per day. Across a seven-day retention period, there would be 35TiB of data change, plus another 35TiB kept in snapshots. The total additional capacity would be 250TiB. Your Pure Storage and Veritas sales teams can assist with estimating your data sizes.

Provisioning Storage for Data, MSDP Metadata, and NBU catalog

Configuring FlashBlade as an NFS target for NetBackup involves creating data volume(s), MSDP metadata volume, NetBackup catalog volume, and exporting these volume(s) as an NFS share to the host acting as a media server. These shares are then mounted on the media server and configured as one MSDP storage pool, a storage unit target to an NFS mount for MSDP metadata and to be a target storage unit for catalog backup as well as shown in Figures 4 and 5.

Figure 4. Storage provisioning on FlashBlade for MSDP data and metadata.

Figure 5. Storage provisioning on FlashBlade for NetBackup catalog

Executing SafeMode Snapshots

To create a useful and consistent SafeMode snapshot of the backup copies and MSDP metadata, it is important to quiesce the NetBackup Media storage server pool. The following are the recommended steps to pause the backup application intermittently before taking the SafeMode snapshot on FlashBlade. Consider automating these steps to reduce the overhead on the administrator. Each section covers the details of the procedure.

Step 1. Suspend the Policy Schedule

The foremost step is to disable the policy schedules that are configured to perform the backup on the MSDP storage pool. The NetBackup Policy Execution Manager Requisition (nbpemreq) determines which jobs are due soon. It also reads in all entered policy updates that are in a pending state: `nbpemreq - suspend_scheduling` suspends the nbpemreq scheduling activity. You can use this option to suspend scheduled backups. You can do this with the following command on the master server.

```
/usr/openv/netbackup/bin/admincmd/nbpemreq - suspend_scheduling
```

Step 2. Suspend Storage Lifecycle Policy

A storage lifecycle policy (SLP) is a storage plan for a set of backups in this case the storage is an MSDP storage server. The operations in SLP are the backup instructions for the data. Taking a point-in-time consistent snapshot would also require disabling the MSDP storage server, which will lead to failure of any SLP running abruptly. Therefore, it's recommended that you disable the SLP intermittently before taking the SafeMode Snapshot. You can do this by running the following command on the NetBackup master server:

```
/usr/openv/netbackup/bin/admincmd/nbstlutil inactive -destination <MSDP_storage server>
```

Step 3. Back Up the NBU Catalog Policy

The NetBackup catalog is the internal database that contains information about NetBackup backups and configuration. Backup information includes records of the files that have been backed up and the media on which they are stored. The catalogs also contain information about the media, the storage devices associated with its associated clients, and the general infrastructure of the environment. It is important to perform a manual backup of the catalog policy before taking the SafeMode snapshot.

Configure the NetBackup Catalog backup policy to store the catalog images on a non-deduplication storage unit. Configuring FlashBlade as an NFS target for NetBackup involves creating NetBackup catalog volume and configuring the storage unit on NetBackup on the NFS share to the host acting as a media server (Figure 6).

Because NetBackup needs the catalog information to perform restores of client backups, duplications, and other operations, it is important to configure a catalog-backup policy before using NetBackup for normal day-to-day operations.

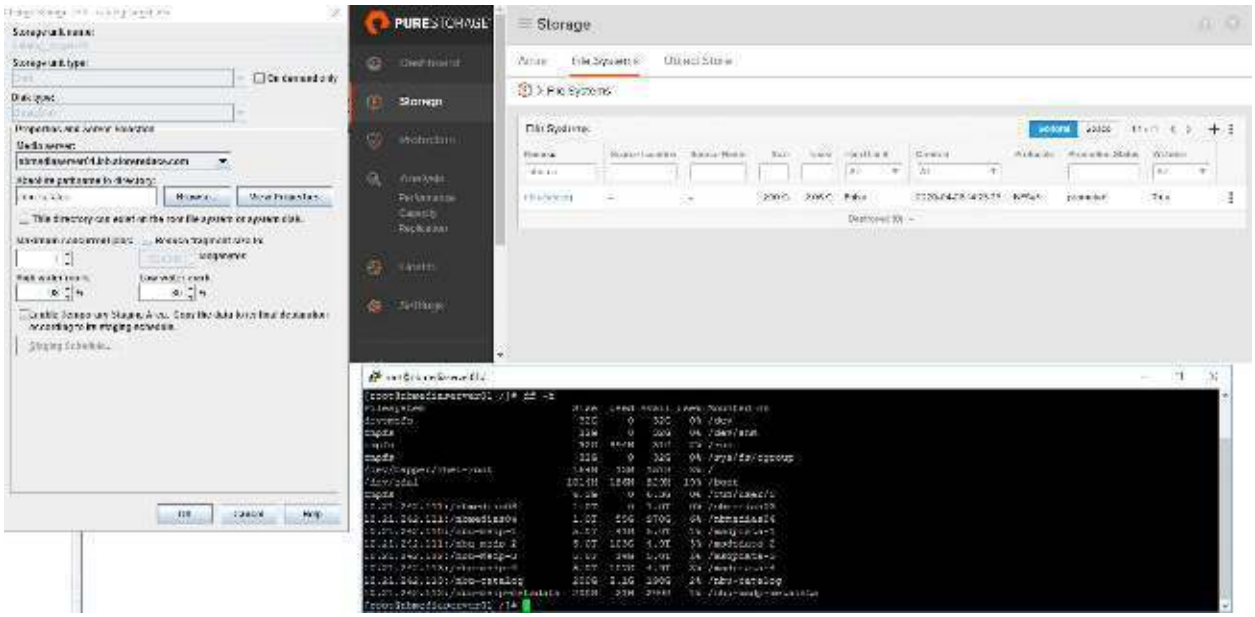

Figure 6. NetBackup Catalog data provision on FlashBlade

Step 4. Suspend Activity on the MSDP Storage Server

The final step before taking the SafeMode Snapshot is to disable the activity on the MSDP storage server. Any sort of write operations on MSDP backup filesystem or MSDP metadata filesystem will be quiesced. You can do this by running the MSDP deduplication command utility on the NetBackup Media Server Deduplication storage. The following is the full command you needs execute to quiesce the MSDP storage server:

```
/usr/openv/pdde/pdcr/bin/crcontrol -m PUT=no -m DEREF=no -m SYSTEM=no -m STORAGED=no -m COMPACTD=no
```

Step 5. Perform SafeMode Snapshot on the FlashBlade NFS File Systems

Once the NetBackup components are quiesced, it's the right time to perform the point-in-time data-consistent SafeMode snapshots. You can do this from the FlashBlade user interface by selecting the corresponding NetBackup NFS shared filesystems and creating the snapshot. To maintain data consistency across the MSDP data/metadata, it is imperative to take the snapshot on all the NFS shares (i.e. for MSDP backup data, MSDP metadata, and NetBackup catalog). For example, if there are four NFS shares created for MSDP data—one for metadata and one for catalog backup—the snapshots have to be created

on all four NFS file systems (Figure 7). At the same time, create a snapshot of MSDP metadata and a snapshot on the catalog filesystem (Figure 8).

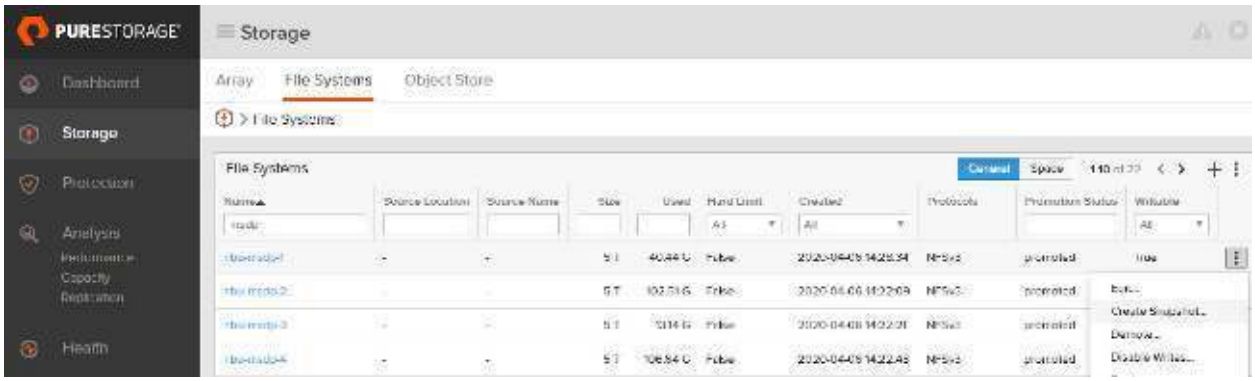

Figure 7. Create point in time snapshots on NFS shares for MSDP pool and metadata

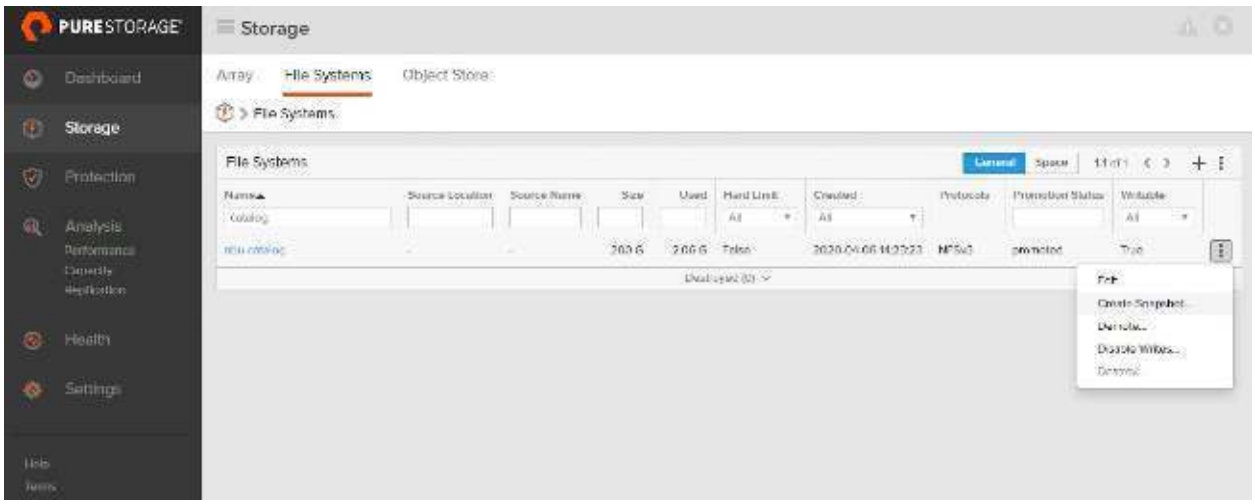

Figure 8. Create point in time Snapshot on NetBackup Catalog NFS share

Step 6. Reactivate the MSDP Storage Server

After performing the SafeMode snapshots on the FlashBlade, you need to reactivate the NetBackup services. The foremost step in unquiescing the backup application is to activate the MSDP storage server pool. Achieved this by running the following command on the appropriate NetBackup media server to enable the write operations on the MSDP data pool:

```
/usr/openv/pdde/pdcr/bin/crcontrol -m PUT=yes -m DEREF=yes -m SYSTEM=yes -m STORAGED=yes -m COMPACTD=yes
```

Step 7. Resume the NetBackup Policy Schedule

You need to activate the NetBackup policy schedule resume on the NetBackup master server. You can do this by running the following admin command:

```
/usr/openv/netbackup/bin/admincmd/nbpemreq -resume_scheduling
```

The option resume_scheduling resumes the nbpemreq the scheduling activity that a -suspend_scheduling option has interrupted.

Step 8. Resume the SLP

The nbstlutil command provides a way for users to intervene in SLP operations. Run the following command to resume backing up the storage lifecycle policy to MSDP storage target:

```
nbstlutil active -destination <msdp_storage server>
```

Snapshot Recovery and NetBackup DR

When faced with a ransomware event, rogue administrator, or another data-loss event, SafeMode Snapshots simplify restoring service. This section details the procedure to recover NetBackup MSDP metadata, NetBackup Catalog, and MSDP backed up data on FlashBlade. For instructions on performing NetBackup DR recovery, refer to NetBackup documentation.

Step 1. Contact Pure Support

The authorized administrator must contact Pure Storage Support right away when an attack is identified. Pure Support 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.

Step 2. Stop Jobs and Media Server and Master Server Services

File-system rollback can disrupt active file access. It is important to remove any risk of potential issues with NetBackup due to lost file access. Before starting recovery, stop any running jobs, the stop NetBackup media server, and the master server services. Please see this support article for more information.

Step 3. Roll Back to Snapshot

Identify which snapshot needs to be recovered for all the filesystems for MSDP storage pool, MSDP metadata, and catalog filesystem, based on the time of the event and whether the data is clean. Pure Support will perform the rollback of the affected file systems. There will be multiple file systems in a single MSDP storage unit in the case of MSDP data pool: Rollback all of them.

Step 4. Perform 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 use it later for disaster-recovery purposes. You can generate the DR file (Figure 9) with the following command on the host of catalog backup NFS mount point:

```
/usr/openv/netbackup/bin/admincmd/bpimport -drfile -id /nbu-catalog/ -drfile_dest /nbu-catalog/
```

In this example, the NFS share exposed for catalog backup is mounted on the media server on path /nbu-catalog. The DR file was generated based on the image on the recovered filesystem. The NetBackup master server can use this DR file to import all the images and devices information for disaster recovery. For more information on disaster recovery of NetBackup please refer to NetBackup documentation. See this article for more information.

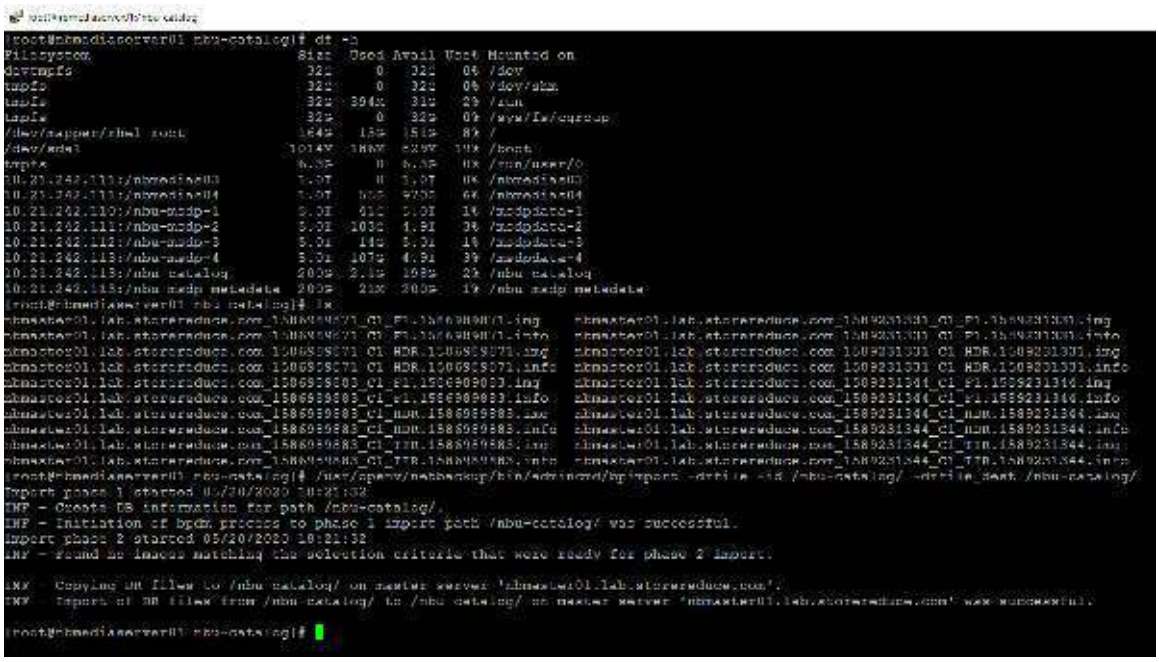

Figure 9. Creating a DR file for recovery

Step 5. Restart Media Server and Master Server Services

Start the services on the Media Server and Master server that were stopped before the snapshot rollback. Ensure that all services and storage targets come online before continuing. See this article for more information.

Step 6. Run NetBackup Data Verification after Restore

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

Conclusion

FlashBlade as a deduplicated storage target for NetBackup is the ideal solution for a high-performance, storage-efficient solution that delivers rapid restore, protection, and recovery from ransomware attacks. As a result of the close technical partnership between Pure Storage and Veritas, FlashBlade has the unique advantage of being the only supported object store with NetBackup deduplication. This solution delivers the following benefits:

- High-performance backup and recovery
- Integrated protection and recovery from ransomware
- Storage efficiency when utilizing both NetBackup MSDP deduplication and FlashBlade compression
- Full integration with Veritas NetBackup advanced deduplication features, such as client-side deduplication, optimized duplication, and Auto Image Replication (AIR).

About the Author

Mandeep Arora is a Pure Storage Data Protection Solutions Architect responsible for defining data protection solutions partnered with various backup applications. He is responsible for defining solutions and reference architecture for primary workloads such as Oracle, SQL, and VMware based on the company's products, and performance benchmarks. Mandeep has spent over 12 years of his career with the data protection industry, he has the flavor working with various data protection products meant for small and medium businesses as well as large enterprises. He started his career with IBM Tivoli Storage Manager in the core software development and test team, followed by Isilon Systems, where he was responsible for delivering the NAS backup solution to enterprise-class customers. He was also a part of the Veritas storage solutions team and was responsible for technical relationships and advising partners on data protection for VMware.

Pure Storage, Inc.
650 Castro Street, #400
Mountain View, CA 94041