

TECHNICAL WHITE PAPER

Ransomware Protection with Pure Storage® and Commvault

Best Practices for SafeMode Snapshots with
Pure Storage FlashBlade® and Commvault.

Contents

- Introduction.....4
- Augment Data Protection with SafeMode Snapshots.....4
- FlashBlade: Quick Recap.....5
 - Storage Consumption with SafeMode Snapshots and Backups.....6
- Recommended Architecture.....6
- Best Practices and Procedures.....7
 - Foundations.....7
 - Use Purity//FB 3.0 or Later.....7
 - Use Commvault 11 SP18 or Later.....7
 - Estimate Capacity Requirements.....7
 - Define the Appropriate SafeMode Snapshot Policy.....8
 - Monitor SafeMode Snapshot Policy Alignment with DASH Copy Operations.....8
 - Secondary MediaAgent Configuration.....8
 - Use Dedicated MediaAgents for DASH Copy and Ransomware Recovery.....8
 - Deploy MediaAgents on Virtual Machines.....9
 - Use Linux for MediaAgents.....9
 - Follow Commvault Sizing Guidelines.....9
 - Primary Storage Copy.....9
 - Grant Read Access to the Cloud Library.....9
 - Rotate FlashBlade object store access keys.....10
 - Avoid Storing Access Keys.....11
 - SafeMode Storage Copy.....12
 - Minimize the Number of File Systems.....12
 - Configure a Restrictive Export Policy on File Systems.....12
 - Use Recommended NFS Mount Options.....13
 - Run Weekly Space Reclamation.....13
 - Server Plan.....14
 - Set Appropriate Retention on SafeMode Copy Data.....14
 - Use a Continuous Schedule for DASH Copy Operations.....14
 - CommServe DR Backup.....15
 - Use a Dedicated Service Account.....15

Configure SMB Export Policy.....15

Restrict Access Using ACLs16

Consolidate DR Backups for Multiple CommServe Systems16

Schedule DR Backups Close to the SafeMode Snapshot Schedule16

Use FlashBlade Replication to Provide Offsite Availability17

Upload Backups to FlashBlade Cloud Library17

Upload Backups to Commvault Cloud17

Set Appropriate DR Backup Retention17

SafeMode Snapshot Recovery Process..... 18

Run Commvault Data Verification After Restore 19

Additional Resources 19

About the Author..... 20



Introduction

Ransomware attacks continue to be top of mind for business and IT leaders. And for good reason. They compromise 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. It's important not to underestimate the economic impact of ransomware. A 2019 study found that cybercriminals had extracted over \$11.5 Billion in ransom payments. This doesn't include the loss to an organization's reputation.

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. However, 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 service-level agreements (SLAs), a ransomware attack can exacerbate the situation with additional downtime. Second, a compromise of your backup systems and data could require you to reinstall and reconfigure your backup solution, before even contemplating data recovery.

This white paper is intended as a how-to and best practices guide to assist with the design and implementation of Pure Storage® FlashBlade® SafeMode Snapshots into Commvault environments. The best practices apply only to configuration elements specific to SafeMode Snapshots and not to general FlashBlade deployments. For general best practices for using FlashBlade with Commvault, contact your Pure Storage account team. For Commvault best practices around ransomware protection, please see [Commvault's own documentation](#).

The target audience for this document includes, but is not limited to, system architects, systems engineers, IT managers, and storage administrators.

Augment Data Protection with SafeMode Snapshots

Pure Storage shares the concerns around ransomware. SafeMode snapshots, a built-in feature of FlashBlade® systems, mitigate these attacks by enabling read-only snapshots of backup data and associated metadata catalogs. You can recover data quickly using these snapshots, helping guard against the effects of ransomware attacks, accidental deletion, and even rogue admins. FlashBlade provides the following benefits:

- **Enhanced protection:** Ransomware can't eradicate (delete), modify, or encrypt SafeMode snapshots. In addition, 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:** Customize snapshot cadence and eradication scheduling.



- **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

FlashBlade: 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. FlashBlade is a scale-out, all-flash storage system, powered by a distributed file system 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 any type of workload, 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.

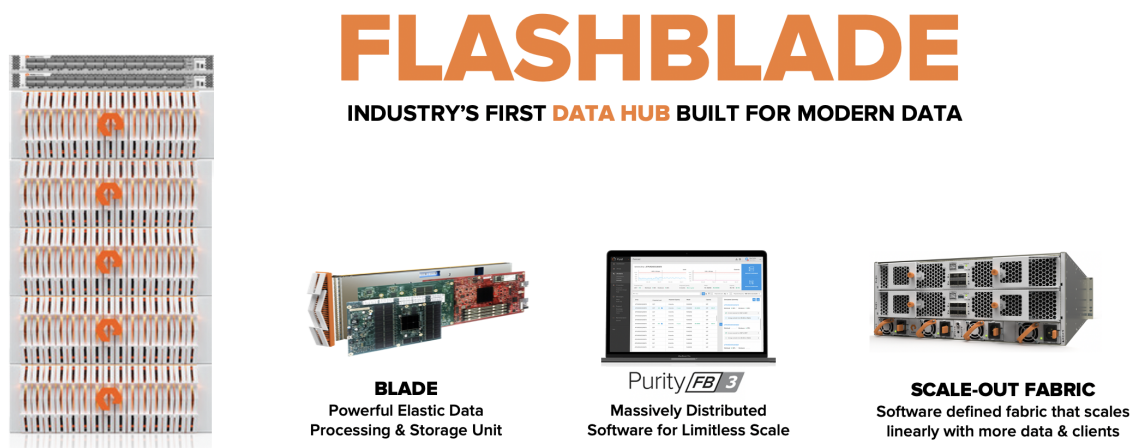


Figure 1. FlashBlade

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 device:** 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 blades.
- **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 protocol 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 10 self-contained rack-mounted chassis interconnected by high-speed links to two external fabric modules (XFM). At the rear of each chassis are 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 either 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—or >17 GiB/sec of 512KiB reads or >8 GiB/sec of 512KiB overwrites—on a 3:1 compressible dataset 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.

Storage Consumption with SafeMode Snapshots and Backups

FlashBlade snapshots operate at the file level. If a file does not change between snapshots, it consumes no extra storage. If the file is deleted or modified, it consumes capacity in the size of the file, minus any savings from compression. With backup software, most files are written once, retained for a period based on policies, then deleted. Backup data, therefore, does not consume significant snapshot space until it is pruned. With backup software, the storage used by snapshots comes primarily from deleted data.

Recommended Architecture

SafeMode Snapshots currently support FlashBlade file systems. However, the Pure Storage best practice for deploying FlashBlade with Commvault is to use object storage, accessed over Amazon S3 protocol, for the primary data copy for performance and simplicity. The recommended architecture, therefore, includes a second data copy on a FlashBlade file system, with independent retention from the FlashBlade object store copy, plus a dedicated MediaAgent to manage Commvault DASH Copy operations from object store to NFS (Figure 2).

Adding the second data copy and splitting the DASH Copy role onto a separate MediaAgent serve two purposes:

- It isolates the primary and secondary workloads so secondary copies do not impact backup throughput.
- It encapsulates the SafeMode components into a simple modular deployment model that is easily deployed, expanded, and removed, without impacting the rest of the configuration.



CommServe DR backups also benefit from SafeMode Snapshot protection when using an SMB share on FlashBlade. See [FlashBlade documentation](#) for instructions on enabling SMB support on FlashBlade and connecting to Active Directory.

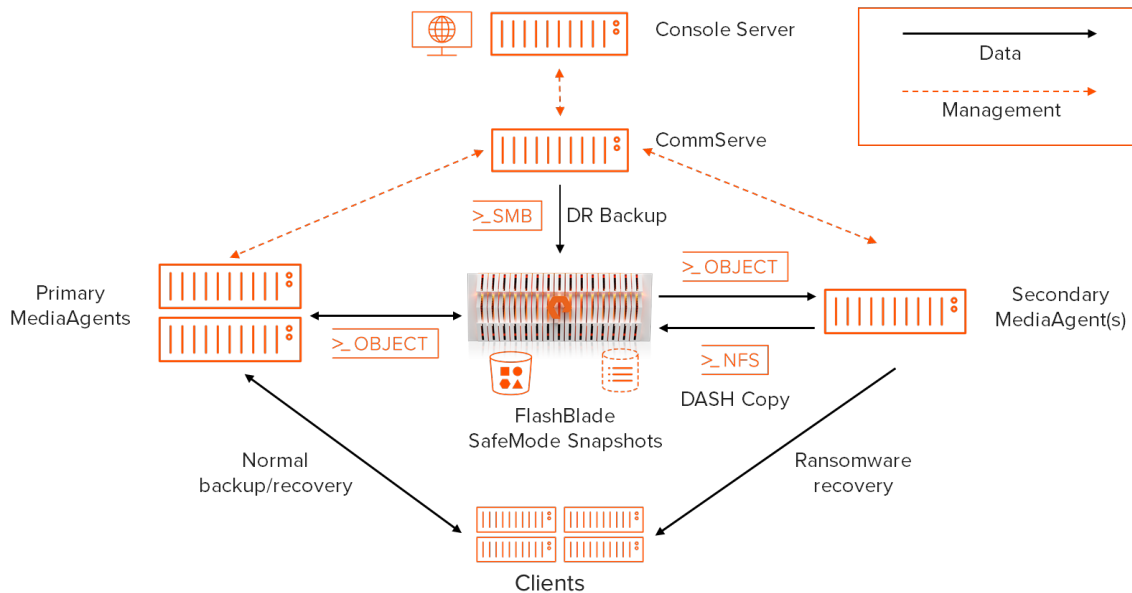


Figure 2. Reference Architecture

Best Practices and Procedures

These best practices are organized to encapsulate the components of the architecture, from foundations to MediaAgent configuration, primary copy, secondary copy, server plans, and DR backup. Each section covers the entire configuration of the component.

Foundations

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. This allows you to work with Pure Storage Support to instantly restore the live file system after an event and purge compromised data.

Use Commvault 11 SP18 or Later

Along with general improvements, Commvault has made significant enhancements to the Command Center interface in Service Pack 18 that make the solution simpler to deploy and manage. Among other items, storage and plan configuration steps are reduced, credential management simplifies Amazon S3 key rotation.

Estimate Capacity Requirements

In a Commvault environment, implementing SafeMode Snapshots will require capacity for the additional data copy and retained snapshots. Follow these guidelines to ensure you have adequate storage available on FlashBlade.



- To estimate the required capacity in an established CommCell, run a *Data Retention Forecast and Compliance* report in the CommCell Console. Set the Forecasted option to the planned retention period. If you want different retention periods between Commvault backups and SafeMode Snapshots, run one report for each value. The data copy will consume the amount in the Space to Keep (GB) field in the Disk Media Summary section of the report, while SafeMode Snapshots will use the amount in the Space to Free (GB) field. Add these amounts together to get the total additional storage needed.
- To estimate for a new CommCell, you need the baseline size, daily change rate, and expected data reduction rate. Apply the reduction rate to the daily change rate, multiply by the number of days snapshots will be kept, then double the result. Add the baseline to determine the total expected capacity required to implement SafeMode Snapshots.

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 7-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 Commvault sales teams can assist with estimating your data sizes.

Define the Appropriate SafeMode Snapshot Policy

SafeMode Snapshot policy will vary based on customer needs. Two key policy settings need to be defined: schedule and retention. Careful consideration is required when deciding what values to use since the policy applies to all file systems on the FlashBlade.

The snapshot schedule should align with the end of the normal DASH Copy window to minimize data loss if a rollback is required after a ransomware attack. For example, if copies typically finish at 7:00 a.m., the SafeMode Snapshot policy should be scheduled to occur between 7:00 a.m. and 8:00 a.m. You can schedule snapshots to repeat multiple times per day if there are multiple copy windows or lower tolerance for data loss after an attack.

The snapshot retention value should consider 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. Note that snapshots created outside policy, i.e. through the FlashBlade GUI, command line, or REST API, will also be protected from eradication based on the SafeMode Snapshot policy, which may affect storage consumption. The authorized administrator will work with Pure Support to configure the SafeMode Snapshot policy on your FlashBlade.

Monitor SafeMode Snapshot Policy Alignment with DASH Copy Operations

Once you have established the SafeMode Snapshot policy, it is critical to ensure it is working effectively. Perform regular audits of DASH Copy operations to ensure that snapshots are being created after data copies are finished and that there is not a much larger gap than expected. If the alignment is off, the authorized administrator can work with Pure Support to make any necessary adjustments.

Secondary MediaAgent Configuration

Use Dedicated MediaAgents for DASH Copy and Ransomware Recovery

For DASH Copy and post-ransomware recovery operations, one or more dedicated secondary MediaAgents should be deployed. Stacking primary and secondary copy workloads on the same MediaAgents makes decoupling more difficult and can impact the performance of production backups.



Deploy MediaAgents on Virtual Machines

Virtual machines are recommended for easy deployment and horizontal scaling. While physical servers will work fine, the costs and complexity of deployment compared to virtual machines are generally much higher, and virtual machines are easier to scale.

Use Linux for MediaAgents

Secondary MediaAgents should run Linux releases for native, performant NFS support. Windows MediaAgents will work, but the Windows NFS client is more complex to deploy and configure, only supports NFSv3, and generally does not perform as well as Linux. See [Commvault documentation](#) for supported Linux distributions and versions.

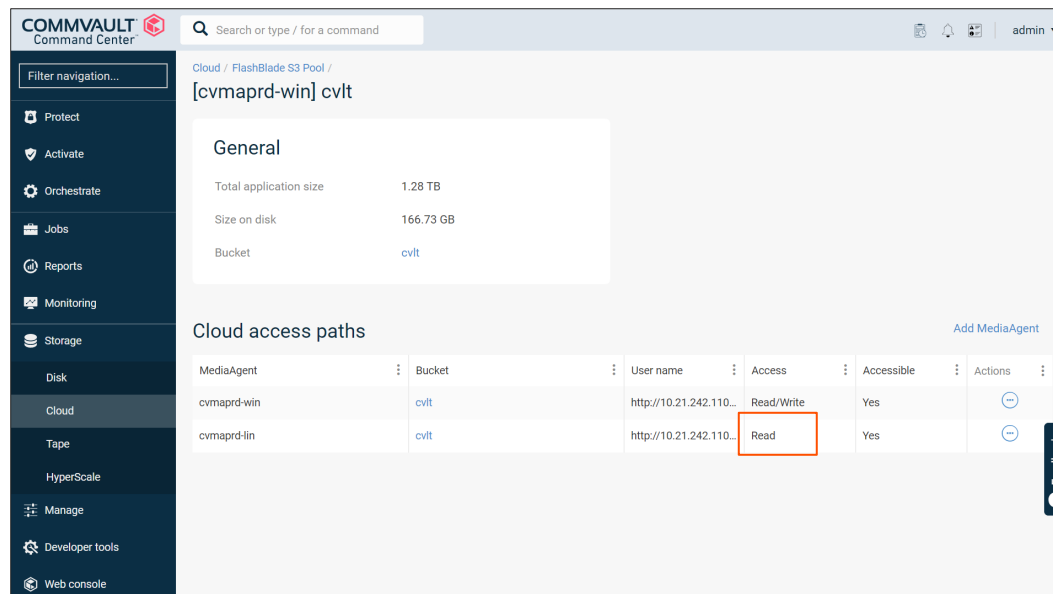
Follow Commvault Sizing Guidelines

Size MediaAgents based on Commvault specifications, available in [Commvault documentation](#). The number of MediaAgents required should be based on the amount of network throughput necessary to support the unique data being copied. For example, on a 10Gbps network, a single MediaAgent can copy 10TiB in a few hours. 50TiB would take more than 14 hours and may require a second MediaAgent depending on the environment.

Primary Storage Copy

Grant Read Access to the Cloud Library

MediaAgents dedicated to managing DASH Copy operations require access paths to the primary cloud storage target on FlashBlade. When adding a path through Commvault Command Center, Commvault will default to read/write access, which will add the secondary MediaAgents to the backup pool. The access paths should be changed to read-only to dedicate the MediaAgents to DASH Copy and recovery (Figure 3).



The screenshot shows the Commvault Command Center interface. On the left is a navigation sidebar with options like Protect, Activate, Orchestrate, Jobs, Reports, Monitoring, Storage, Disk, Cloud, Tape, HyperScale, Manage, Developer tools, and Web console. The main area displays the configuration for a cloud storage target named '[cvmaprd-win] cvlt'. Under the 'General' section, it shows 'Total application size' as 1.28 TB, 'Size on disk' as 166.73 GB, and 'Bucket' as 'cvlt'. Below this is the 'Cloud access paths' section, which contains a table with columns: MediaAgent, Bucket, User name, Access, Accessible, and Actions. Two rows are listed: one for 'cvmaprd-win' with 'Read/Write' access, and another for 'cvmaprd-fin' with 'Read' access. The 'Read' access for 'cvmaprd-fin' is highlighted with a red box.

MediaAgent	Bucket	User name	Access	Accessible	Actions
cvmaprd-win	cvlt	http://10.21.242.110...	Read/Write	Yes	⊖
cvmaprd-fin	cvlt	http://10.21.242.110...	Read	Yes	⊖

Figure 3. Cloud storage target access paths.

To enable read access, share the mount path to the secondary MediaAgents by clicking Add MediaAgent, selecting the secondary MediaAgent(s), and clicking the Save button. For the appropriate access path, click the bucket field. On the Edit cloud access path page, click Advanced (Figure 4). In the Access field, select “Read.” Click the Save button.

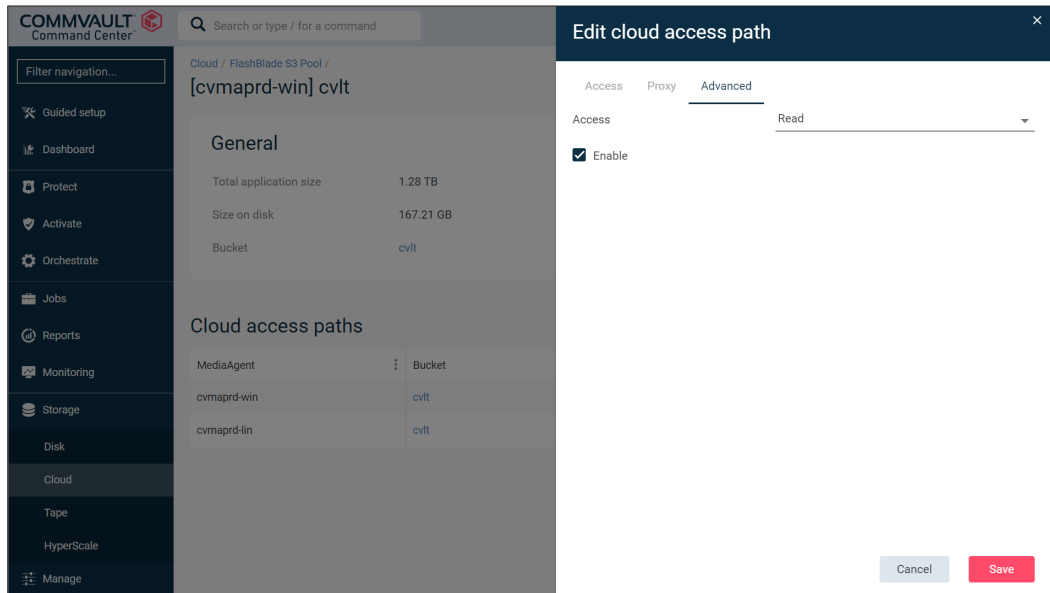


Figure 4. Enabling read access on cloud storage access paths

Rotate FlashBlade object store access keys

Access keys for FlashBlade object storage should be rotated regularly—creating a new key and deleting the old one—to minimize the risk of key compromise. The credential manager in Commvault makes the rotation process simple. To rotate keys, first, create a new key pair on the FlashBlade. Access the Object Store view for the account that contains the Commvault bucket. Click the context menu button for the user and select Create access key from the menu. A dialog will appear with the details of the new key (Figure 5).

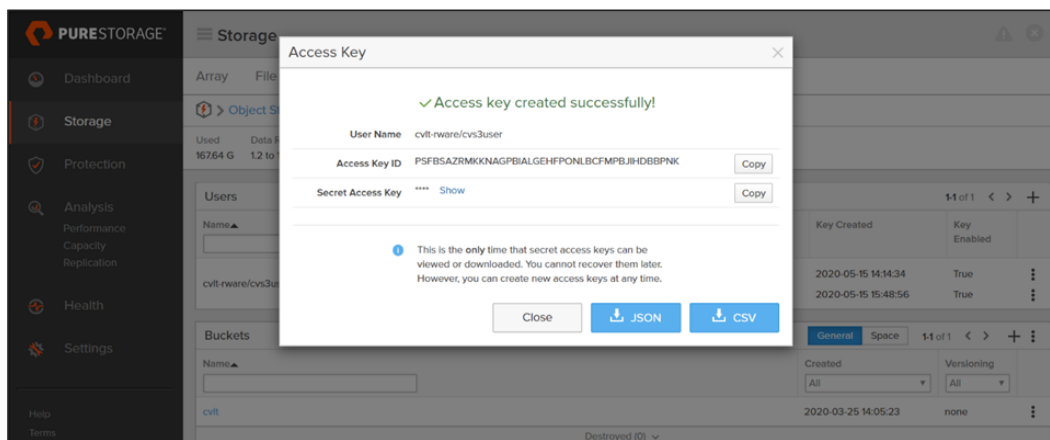


Figure 5. FlashBlade key creation

With the new keys created, access the Credential manager view in Commvault Command Center and click the stored credential for the FlashBlade bucket. Replace the Access key ID and Secret access key fields with the newly generated key values, then click the Save button. You may export the keys for future reference; however, copying the key values



between consoles using the Copy buttons will prevent an attacker from compromising the stored file. Running the consoles side by side lets you copy the keys in seconds.

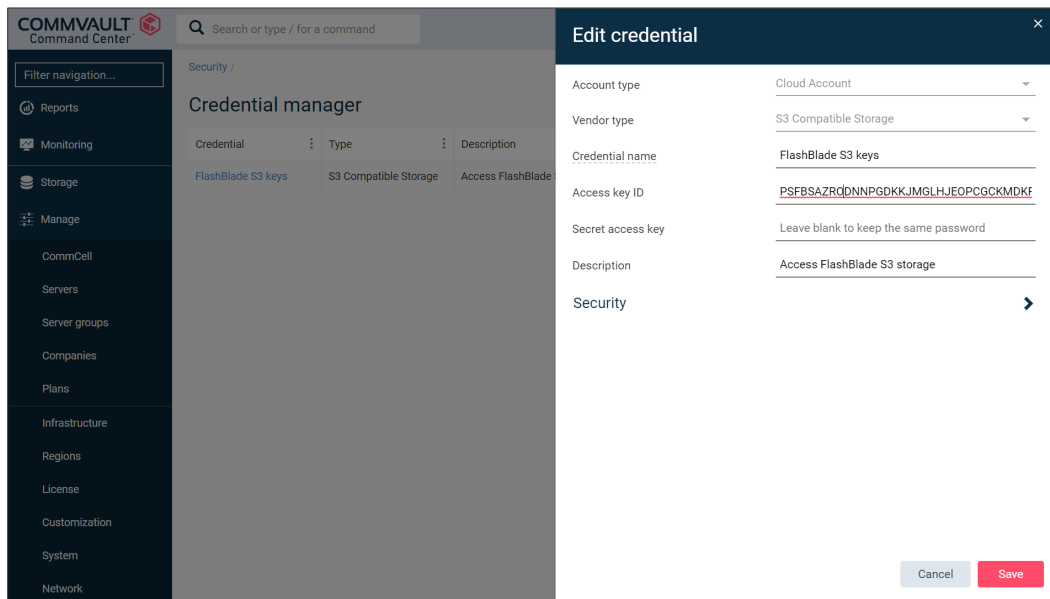


Figure 6. Updating keys with Commvault credential manager.

Once the key has been updated in Commvault, delete the old key from the FlashBlade to prevent compromise. Click the context menu for the old key, then select Delete access key. When prompted to confirm the deletion, click on Delete.

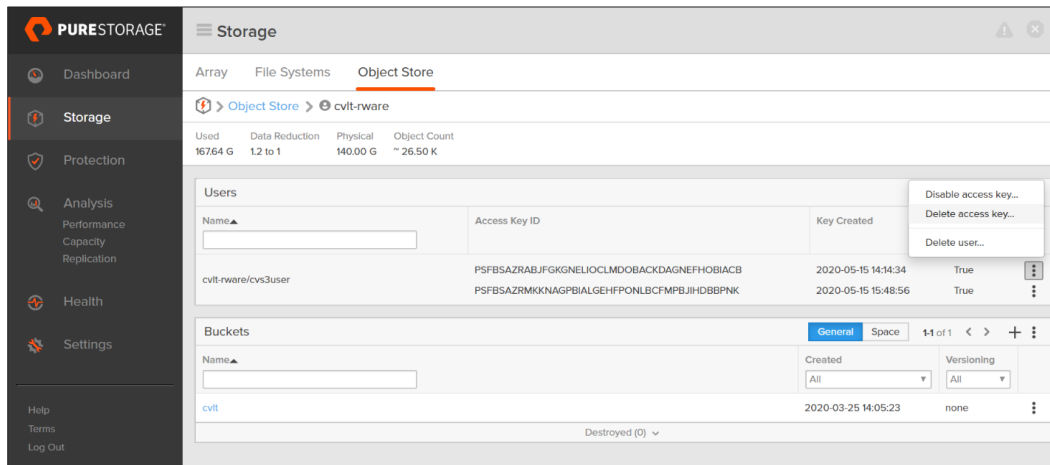


Figure 7. Deleting old access key.

Avoid Storing Access Keys

Exporting access keys, especially secret keys, to store them in a file may seem like a reasonable step given the size and complexity of the key values. However, this creates a vector for an attacker to gain access to and alter or delete your backup data without your knowledge. Commvault stores the access keys in an encrypted form and doesn't ever display the secret key. An attacker would have to gain direct access to the CommServe database and obtain and decrypt the secret key to compromise the backup storage.



Since it is simple to generate new keys, it is better to generate a separate key if you need to do any direct access testing, then delete the key when testing is complete.

SafeMode Storage Copy

Minimize the Number of File Systems

For most environments, a single FlashBlade file system can support the entire deployment. Although file system is thin provisioned and not limited on size, if you use hard quotas, they must be large enough to contain the backup data that will be in the secondary copy. Multiple file systems can be used to create more FlashBlade connections; however, each additional file system increases the complexity of managing the overall solution. Please see Pure Storage guide *Best Practices for Configuring Commvault with FlashBlade* for details on setting up multiple FlashBlade file systems with Commvault.

Configure a Restrictive Export Policy on File Systems

Minimizing the attack surface of an environment is critical to preventing a ransomware attack, and export policies are an important part of that. Properly configured policies prevent direct access to stored data outside the systems that need it. In this case, only the secondary MediaAgents should have access to the FlashBlade file systems. The export policy should include the following options:

- NFSv4.1
- NFSv3 (optional)
- Rules to restrict access to only the IP address(es) for the secondary MediaAgent(s). Enter a separate rule for each MediaAgent rather than using a subnet filter.
- rw
- root_squash

For example, a rule to grant access for a MediaAgent with the address 10.1.1.1 would be written as `10.1.1.1/32(rw,root_squash)`.



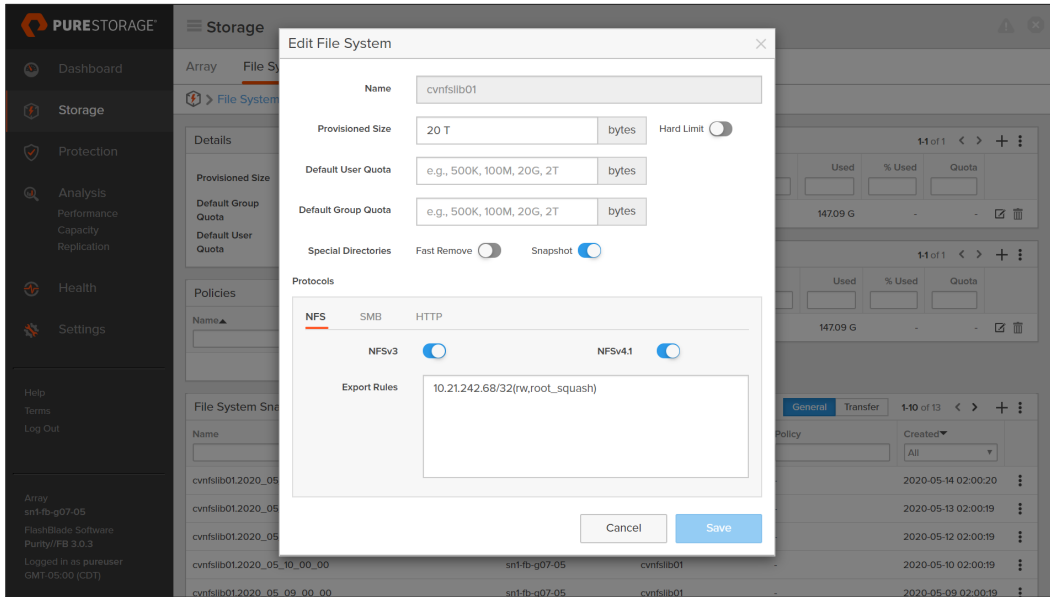


Figure 8. Mount path export policy

Use Recommended NFS Mount Options

The file system(s) should be mounted to the MediaAgent(s) using the following options.

- Type nfs4
- vers=4.1
- rsize=524288
- wsize=524268
- hard
- local_lock=none

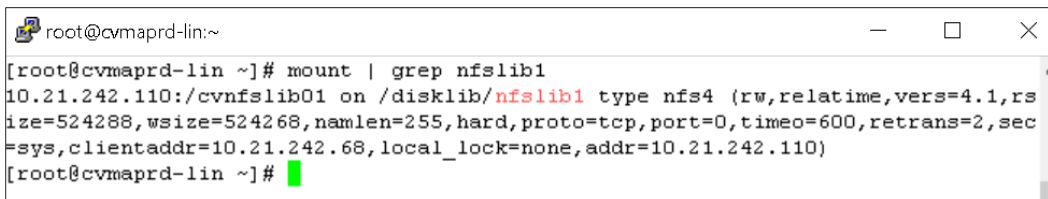


Figure 9. NFS mount options

When sharing the file system across multiple MediaAgents, mount the export to the same path on each MediaAgent.

Run Weekly Space Reclamation

In Service Pack 18 Commvault introduced a built-in schedule for reclaiming space on storage that does not support drilling holes in files. It runs daily but only reclaims space monthly for a given deduplication store. This in turn creates a wide swing in snapshot consumption, growing as data is deleted by Commvault and then shrinking when the snapshot retention expires. Run space reclamation weekly to reduce the amount of data deleted in each job and minimize the swing in consumption. Note: This will increase the I/O load on the FlashBlade but should not significantly impact DASH Copy operations.



Consider the following example: SafeMode policy is set to retain seven days of snapshots. The CommCell ages 20TiB per week, but not enough unique blocks age to delete any data files at that time. After 30 days there will be 80TiB of extra data on the file system, although snapshot growth will be minimal. The space reclamation will delete that extra 80TiB, which will then be kept in snapshots for seven days until the retention expires, during which time another 20TiB of extra data ages. Total extra FlashBlade capacity consumption will be 100TiB, with an 80TiB swing. Running space reclamation weekly will reduce the swing to 20TiB, with a peak of 40TiB extra consumption.

Space reclamation is part of the data verification process. Commvault has procedures for data verification of deduplicated and non-deduplicated data. For more details, refer to [Commvault documentation](#).

Server Plan

Set Appropriate Retention on SafeMode Copy Data

Retention on the SafeMode copy needs to balance between storage consumption and mitigating ransomware risk. Since each snapshot contains all the data that exists when it is taken, the overall retention period will be the sum of Commvault retention and FlashBlade SafeMode Snapshot retention. Figure 10 shows an illustration of copy retention. For example, if the Commvault retention on the SafeMode copy is seven days, and the SafeMode Snapshot policy retention is seven days, the system will ensure 14 days of backups are kept.

Note: Additional steps are required when recovering data Commvault has pruned. See the SafeMode Snapshot Recovery Process section for more information.

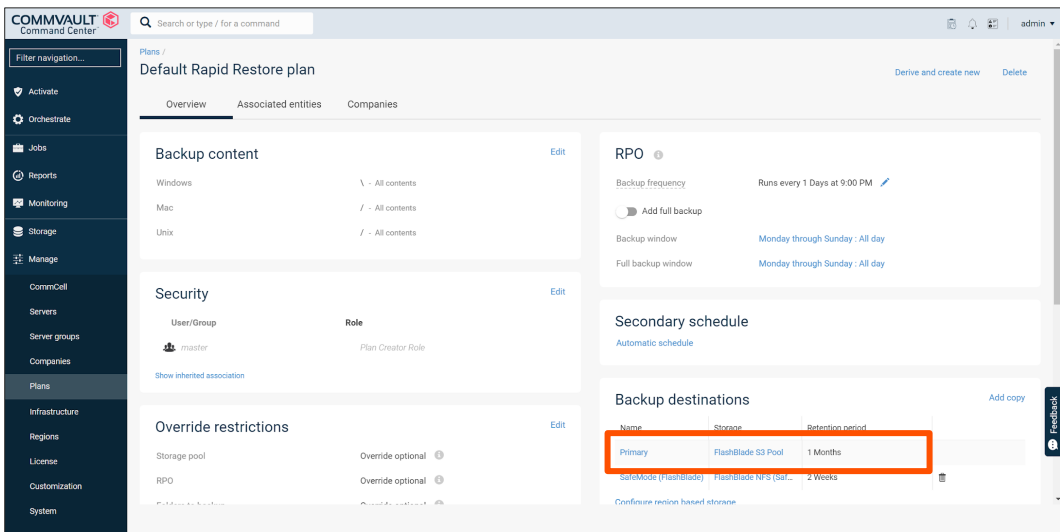


Figure 10. SafeMode copy retention in server plan

Use a Continuous Schedule for DASH Copy Operations

To most effectively use SafeMode Snapshots, it is important to minimize the time between backups completing and the snapshot being taken. A continuous DASH Copy schedule will trigger the copy process on the secondary MediaAgent shortly after a backup job completes. This removes the need for a dedicated schedule or copy window. Continuous is the default schedule for plans created in Commvault Command Center (Figure 11).



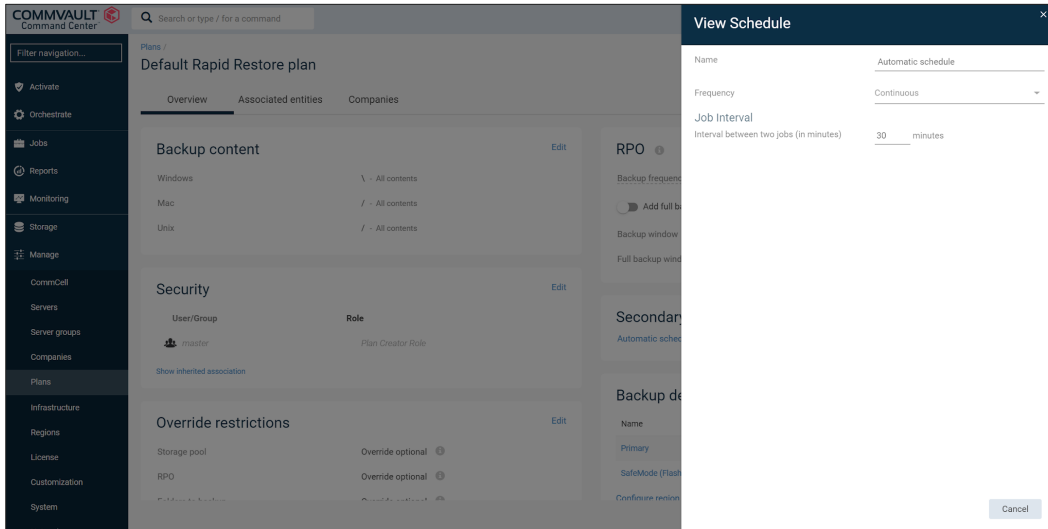


Figure 11. Continuous DASH Copy schedule.

CommServe DR Backup

Use a Dedicated Service Account

Using a dedicated service account ensures that the DR backups can't be accessed and therefore altered or deleted by any other account. The service account should not be used for any other purpose or allowed local login to any systems. If you have a password vault product, use it to store the password.

Important: The service account must have values set for the uidNumber and gidNumber attributes in Active Directory for authentication and ACLs to work properly.

Configure SMB Export Policy

Set up the DR file system with only SMB enabled (Figure 12). Set the Native SMB ACLs option.

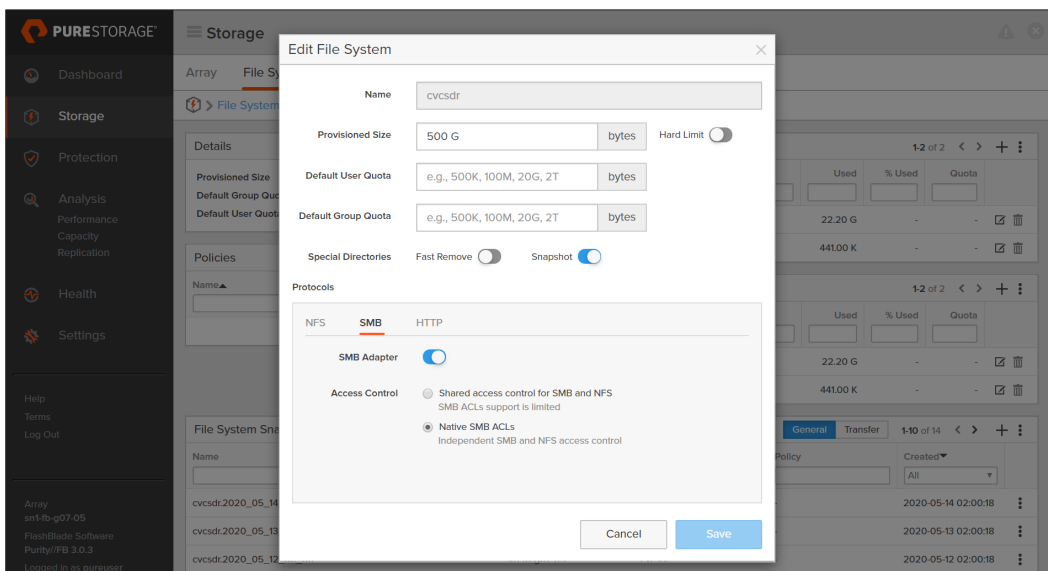


Figure 12. SMB export policy



Restrict Access Using ACLs

The DR backup share ACL needs to restrict access so that only the service account can write to and manage the file system. Grant full control access for the service account to all files and directories in the share.

The CommServe DR recovery uses a restore within Microsoft SQL Server that runs as the SQL Server service account. Using the Commvault recommended configuration, this process will access the SMB share as the CommServe computer account. For DR recovery to work, the standby CommServe computer account also needs access. The ACL should grant only read access. For DR recovery on the production CommServe, the production CommServe computer account will also need read access. For easier permissioning, create a group in Active Directory and add all the CommServe computer accounts to the group. Grant the group read access to the DR backup SMB share. Figure 13 shows the full ACL.

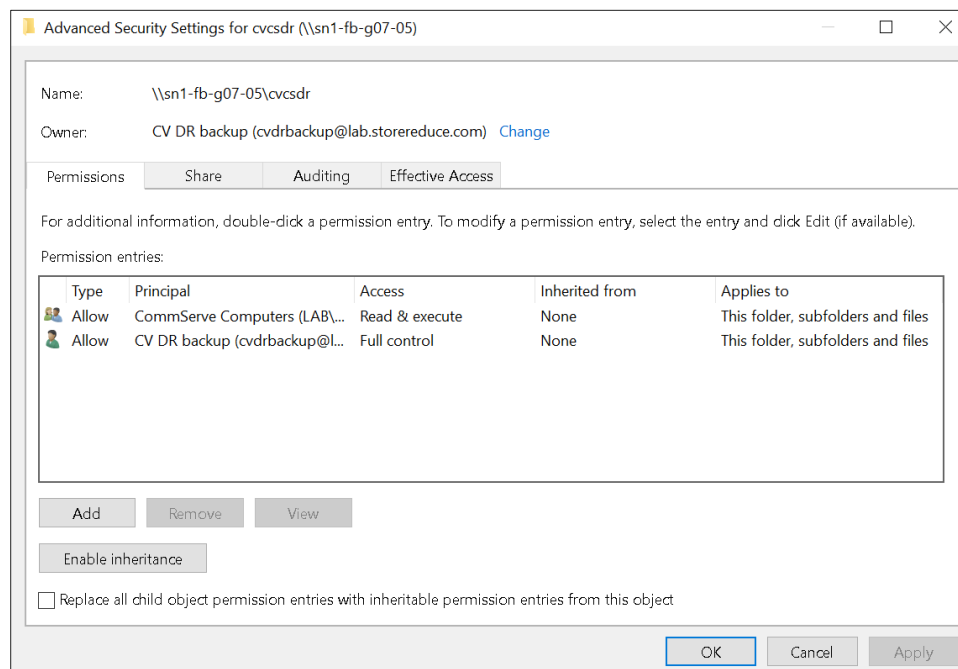


Figure 13. DR Backup SMB share ACL.

Consolidate DR Backups for Multiple CommServe Systems

Every CommServe in an environment needs to run DR backups, including standby systems. Every CommServe can benefit from SafeMode Snapshots if you consolidate the DR backups onto a single file system. Create a separate directory per CommServe to avoid conflicts between CommServe systems. All DR backups can use the same service account. The ACL on the DR backup share needs to grant read access to every CommServe computer account in Active Directory to ensure recoverability.

Schedule DR Backups Close to the SafeMode Snapshot Schedule

To minimize the period where CommServe DR backups are not protected by SafeMode Snapshots, schedule the DR backups to occur just before the snapshot policy schedule, making sure to allow enough time for the backup to complete. For example, if the SafeMode schedule runs at 10:00 a.m., and the backup completes in one minute, schedule DR backups for 9:55 a.m.



Use FlashBlade Replication to Provide Offsite Availability

While not detailed as part of this architecture, native replication between FlashBlade systems coupled with SafeMode will provide an extra layer of defense for CommServe DR backups. Enabling replication with SafeMode can have broader implications, which you should discuss with your Pure Storage account team before implementing it. Refer to [FlashBlade documentation](#) for more detail on enabling replication.

Upload Backups to FlashBlade Cloud Library

DR backups can be uploaded automatically to a configured cloud library, with longer retention than the first stage network share backup. Enabling this option is an easy way to get a longer-term copy of DR backups on FlashBlade Object Store.

To enable cloud library upload using Commvault Command Center, navigate to Manage/System view, then select Maintenance. Click the DR backup (Daily) tile to fetch the settings, then click the Edit button (gear icon) to open the properties. As shown in figure 14, enable the Upload backup metadata to cloud library option, then select the FlashBlade Amazon S3 target in the Cloud library dropdown. Click the Save button to commit any changes.

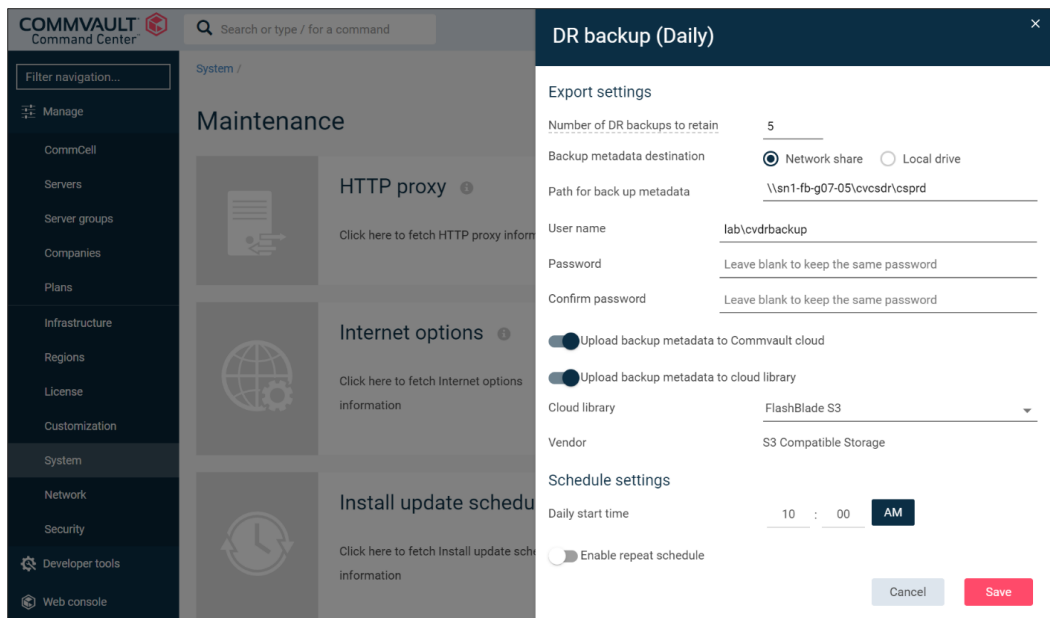


Figure 14. DR Backup configuration in Commvault Command Center

Upload Backups to Commvault Cloud

Commvault provides cloud storage for DR backups as part of a paid support agreement. This ensures an offsite copy is available in case of site loss or other situation that prevents using the local copies. This option should be enabled if allowed by your company policies.

Set Appropriate DR Backup Retention

By default, Commvault will keep five daily DR backups on the FlashBlade SMB share. SafeMode Snapshots will extend that period based on the retention policy you define. For example, if the DR backup retention in Commvault is set to five and the SafeMode Snapshot retention policy keeps seven days, then 12 days of DR backups will be available for recovery.



SafeMode Snapshot Recovery Process

When faced with a ransomware event, rogue administrator, or other data loss event, SafeMode Snapshots make restoring service simple. This section details the procedure to recover Commvault disk storage on FlashBlade. For instructions on performing CommServe DR recovery, refer to the [Commvault documentation](#).

1. Contact Pure Support

When an attack is identified, the authorized administrator must contact Pure Storage Support right away. 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.

2. Stop Jobs and MediaAgent Services

File system rollback can disrupt active file access. It is important to remove any risk of potential issues with Commvault due to lost file access. Before starting recovery, stop any running jobs, and stop Commvault MediaAgent services on the secondary MediaAgent.

3. Roll Back to Snapshot

Identify which snapshot needs to be recovered, 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 are using multiple file systems in a single disk storage target, roll back all of them.

4. Restart MediaAgent Services

Start the services on the MediaAgent(s) that were stopped before the snapshot rollback. Ensure that all services and storage targets come online before continuing.

5. Restore Data from the SafeMode Copy

Once services and storage are online, client recovery can begin. Restore data as normal but select the options to restore from the SafeMode data copy (Figure 15).

Note: If you wish to restore data that Commvault has pruned, contact Commvault Support to catalog the data before attempting recovery.

Note: Commvault Command Center does not support choosing a data copy for some agent types. Use the CommCell Console if you need to restore data for one of these agents.

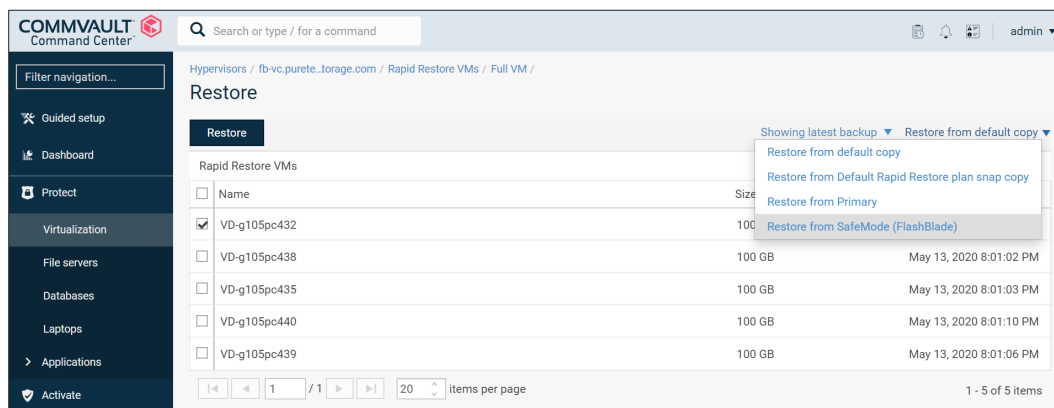


Figure 15. Restoring from an alternate data copy



6. Restore the Latest Data from Before SafeMode Snapshot

Also select the option to restore from a time before the SafeMode snapshot (Figure 16). If you try to use a recovery point newer than the snapshot, the job will fail because not all the data is available on the FlashBlade file system.

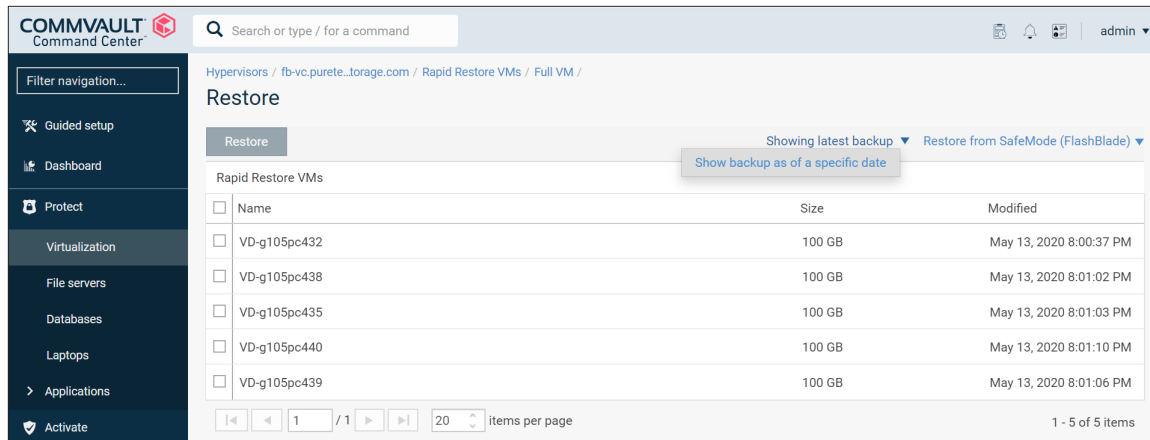


Figure 16: Showing backup as of a specific date.

When recovering data after rollback, you should start with the last backups from before the snapshot was created, unless you have rolled back to the oldest snapshot and are not sure of data integrity. In that case, you may have to try restoring from multiple snapshots; however, start with the newest data likely to be intact and work backward as necessary.

Run Commvault Data Verification After Restore

Priority should be placed on restoring service after an event. Once data recovery is complete, run data verification in Commvault to identify any data gaps and prevent future recoveries from using data that is no longer available. Commvault has procedures for data verification of deduplicated and non-deduplicated data. For more details, refer to Commvault documentation.

Additional Resources

- [Pure FlashBlade documentation](#)
- [Commvault documentation](#)



About the Author

Roy Child is a Senior Solution Architect with Pure Storage, responsible for defining data recovery solutions around various data protection applications. He is responsible for defining Pure Storage solutions and reference architectures for protecting and recovering primary workloads such as Oracle, SQL, and VMware. Roy has worked in and with the data protection industry for 20 years, from an end user to IT architect with multiple backup and recovery products, followed by product management with Commvault. Roy joined Pure Storage in April 2019.



©2020 Pure Storage, Inc. All rights reserved. Pure Storage, Pure1, Pure1 Meta, Pure-On-The-Go, the P Logo, AIRI, the AIRI logo, CloudSnap, DirectFlash, Evergreen, FlashBlade and FlashStack, and ObjectEngine are trademarks or registered trademarks of Pure Storage, Inc. in the U.S. and other countries. All other trademarks are registered marks of their respective owners.

The Pure Storage products and programs described in this documentation are distributed under a license agreement restricting the use, copying, distribution, and decompilation/reverse engineering of the products. No part of this documentation may be reproduced in any form by any means without prior written authorization from Pure Storage, Inc. and its licensors, if any. Pure Storage may make improvements and/or changes in the Pure Storage products and/or the programs described in this documentation at any time without notice.

THIS DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. PURE STORAGE SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

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

purestorage.com

800.379.PURE

