PURESTORAGE®
Uncomplicate Data Storage, Forever

TECHNICAL WHITE PAPER

Minimizing the Impact of Cyberattack Recovery

Reduce risk and downtime with Pure Storage® FlashBlade//S™ and Commvault.

Contents

Introduction 3

Solution Overview 3

- Recommended Architecture 4
- Deduplication and Immutability 5
- Layered Vaulting 5
- Backup Scheduling 7
- Sizing 7

Best Practices 7

Implementing the Solution 9

- Prerequisites 9
- Configure FlashBlade//S and Credentials 9
- Configure Commvault 14
- Configure Hardware WORM on Storage Pool 21
- Recommended: Modify DDB Backups 23
- Modify Index Backups 24
- Configure DR Backups 25

Recovering from a Cyber Event 28

- Clean Room Recovery 28
- Contact Pure Support 28

Conclusion 29

Appendix 29

- Caveats 29
- Pure Storage FlashBlade//S 29
- Commvault Backup and Recovery and Metallic 30

Additional Resources 30

About the Author 30

Introduction

According to the FBI's Internet Crime Report, potential losses from cyber crimes increased by 64% from 2018 to 2021, totaling $6.9 billion. Cyberattacks are constantly evolving, too. A quick web search will show that experts agree a breach of your defenses is a question of when, not if. When an attacker does get through, they can do a lot of damage, even if you detect and stop them quickly. Attack prevention is critical, of course, but you also need to be prepared for large-scale recovery.

Cyberattacks have broad impacts. From lost revenue and customers to reputational damage to scrutiny from investors, all layers of an organization are affected. And everyone feels the stress of recovery. How long will you be down? Will you be able to get all your data back, or has the attacker destroyed it? How much business data do you have to sacrifice or rebuild afterward? Pure Storage and Commvault are committed to getting you back in business as fast as possible, with minimal data loss, so you can breathe easier.

Minimizing the impact of an attack means setting yourself up to get back online quickly, with as little data loss as possible. The less time you're down, the less revenue you're missing out on, and the smaller a hit your reputation takes. The more recent your recovery data is, the less business history you've lost. Pure Storage® FlashBlade//S™, combined with Commvault, provides a Rapid Restore experience like no other. Features like Object Lock, Freeze Objects, and SafeMode™ Retention Lock ensure your data is ready and waiting after an attack, just like it always is. You can start recovery immediately, from your most recent clean backups, following familiar day-to-day processes. To top it all off, you have the speed and simplicity you've come to expect from Pure Storage to get you back online faster than you might think possible.

The target audience for this document includes, but is not limited to, system architects, systems engineers, IT managers, and storage administrators. This guidance applies equally to FlashBlade//S and first-generation FlashBlade®, except as noted.

Solution Overview

The joint FlashBlade//S and Commvault solution reduces the impact and cost of an attack by ensuring your backup data is immutable and can't be affected by an external attacker, rogue admin, or accidental action. FlashBlade//S data protection features protect your backup data from an attacker, even if they gain access to the FlashBlade. Commvault compliance lock prevents someone from deleting records of the backups–without requiring physical isolation or extra hardware to do so. You can be confident your most recent backups are intact when you need them. You can start recovery faster, taking full advantage of the speed of FlashBlade//S. Available Commvault features can further limit or prevent attacks to both your backup and production systems, detect an attacker before they can damage your data, and proactively monitor your backups so you can be confident you're not restoring malware.

Recommended Architecture

The architecture is based on FlashBlade//S object storage, accessed over Amazon S3 protocol, for the primary data copy, which is the Pure Storage best practice with Commvault. FlashBlade//S fast object storage reduces backup and restore times to collect and secure your data sooner. The simplicity of object storage means easier deployment and management. Commvault's Storage Accelerator component more fully utilizes your available network bandwidth by distributing storage access across your protected systems rather than funneling it through a small number of MediaAgent data movers, to protect and restore more data in parallel.

Object Lock on FlashBlade//S seamlessly adds object-level immutability, managed by Commvault. The SafeMode Retention Lock and Freeze Objects features add extra protection against direct attacks on the object buckets and their contents. With these features enabled, locked objects cannot be destroyed or overwritten, and the bucket itself cannot be deleted, even if credentials are compromised.

CommServe DR backups can leverage File SafeMode protection when using an SMB share on FlashBlade//S, protecting against a worst-case scenario that requires recovery of Commvault itself. File SafeMode will create and preserve immutable snapshots of your DR backups that an attacker cannot destroy. For instructions on enabling SMB support on FlashBlade//S and connecting to Active Directory, please see FlashBlade//S documentation.

Figure 1 shows the logical architecture with both Object Lock and SafeMode Retention Lock protecting backups of primary data and File SafeMode snapshots protecting CommServe DR backups.

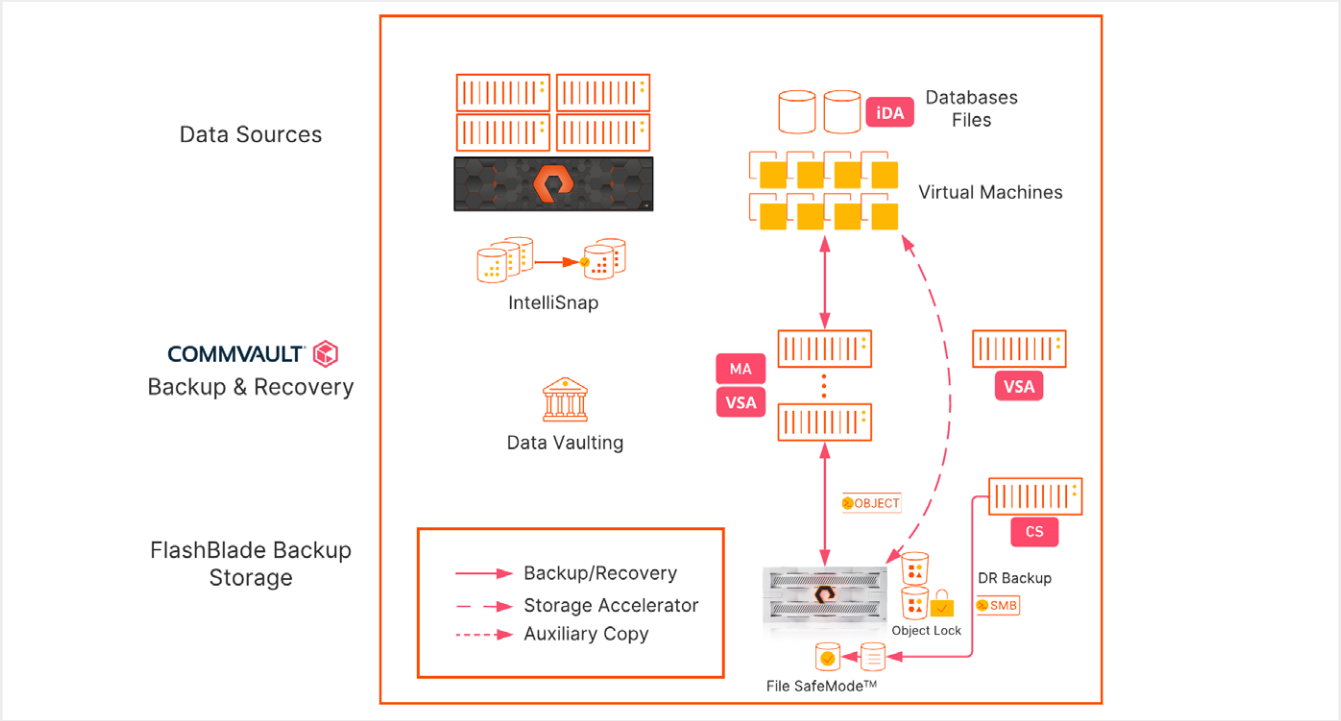


FIGURE 1 Solution logical architecture

Deduplication and Immutability

Global deduplication is a well-established technology for reducing storage consumption. It tracks data patterns that have been written, and when those patterns show up again, the existing data gets referenced rather than written again. While this is indisputably valuable, it has major implications for object-level immutability. It's important to understand that impact to make the right design decisions. Deduplication and immutability are directly at odds; virtually all of your backups will depend on data that was written during earlier backups, and that complicates when it's safe to unlock objects.

As an example, assume you need to keep your backups for 14 days. After two weeks, your first backups have met their service level agreement (SLA) and are ready to delete. However, in that time, you've added more backups with dependencies on the first week, so the first week actually needs to stay immutable until those backups expire. Each week adds more dependencies on the previous weeks, and none of that data can be exposed without risking the more recent backups. The nature of deduplication means that to add immutability you have to lock all your data forever–which defeats the very purpose of deduplication. Figure 2 illustrates these relationships and dependencies.

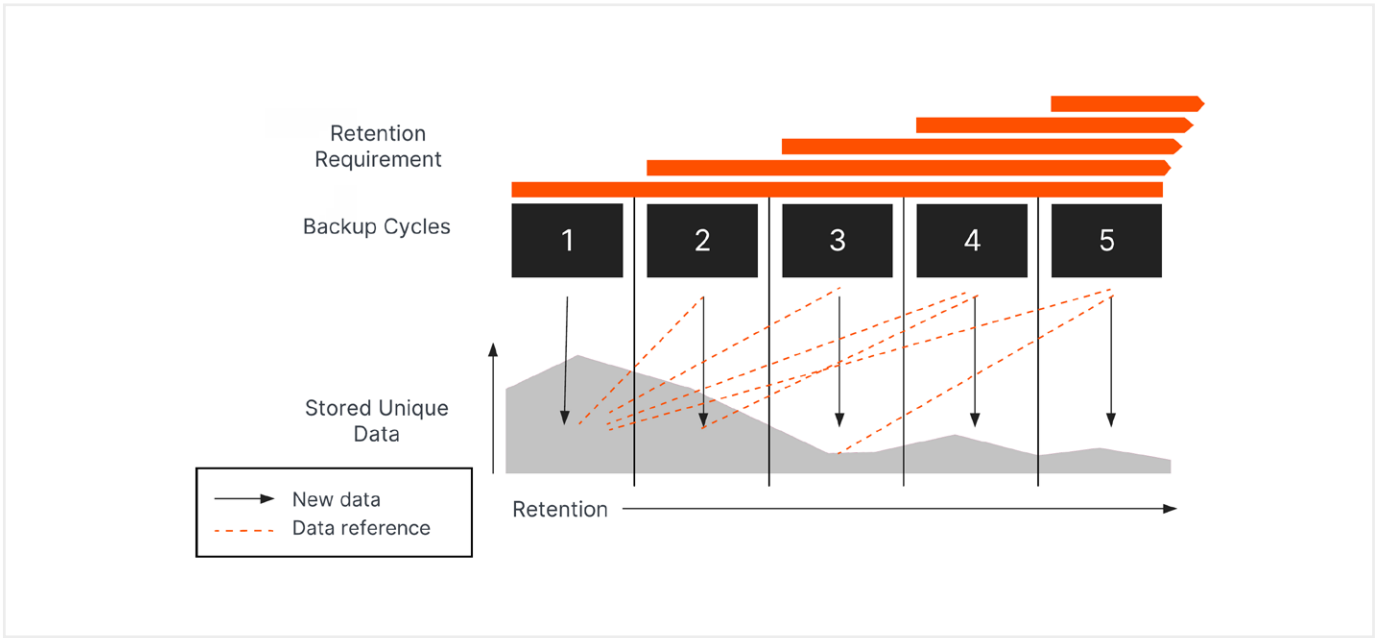


FIGURE 2 Deduplication dependencies

There are two ways to solve this problem. The first is to turn off deduplication. This entirely avoids the dependencies between backups. But it also means you can't get any of the capacity savings of deduplication, so you'll spend more on storage.

Layered Vaulting

The better solution is to use a layered data vaulting concept. Commvault periodically "closes" the vault against any new data and starts a new one, putting a finite timeline on the dependencies. Within each vault, Commvault leverages its dynamic locking technology and FlashBlade//S Object Lock to align the object locks for the entire vault to expire at the same time.

For example, consider a vault with a 14-day retention requirement. The last backups, taken day 14, will need to exist until day 28 to meet the SLA. The earliest data in the vault must also be protected until day 28 to ensure that all jobs in the vault have their

dependencies covered. To accomplish this, Commvault sets the object locks for the first day's backups to expire after 28 days. On the second day, locks are set to expire after 27 days. This continues until the 14th day, when locks are set to expire after 14 days–also on day 28. Commvault then closes the vault on the 15th day and starts the cycle over. This approach gives granular control over immutability and backup scheduling while allowing the entire vault to be deleted at the same time, which frees up capacity as quickly as possible after meeting immutability and retention SLAs.

Over time, you will have two vaults at any given time: the active vault, with new data being written to it, and the most recently sealed vault. The previous sealed vault expires when the new open vault is being created. Having two vaults ensures the immutability SLA is met; there will be dependencies going back to the oldest data in the sealed vault, and both vaults are fully protected. The immutability Figure 3 illustrates the vaulting timeline and the immutability window, which covers the backups that must be immutable to meet your SLA.

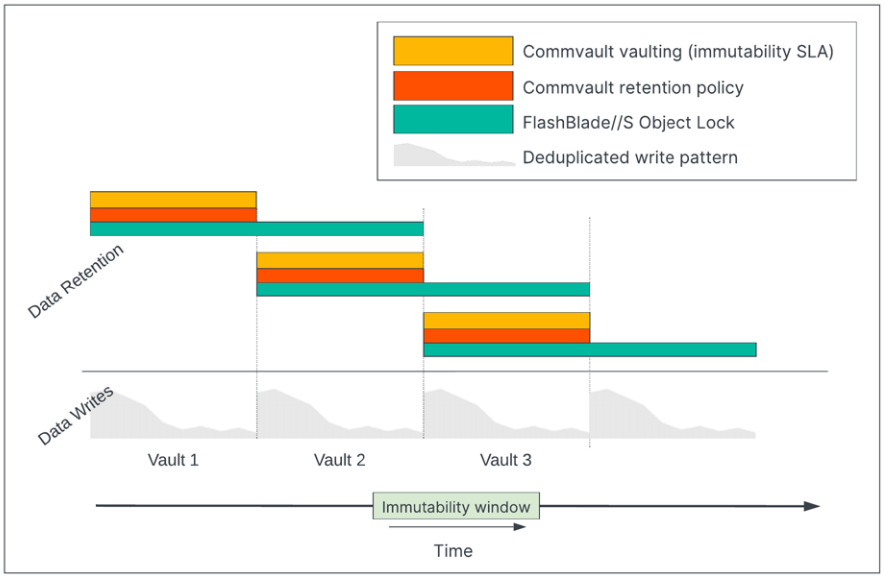


FIGURE 3 Layered data vaulting timeline

The layered vaulting system protects your data for the entire SLA period. Data is protected immediately as it is written and does not require any periodic point-in-time snapshots. You can get your production systems online sooner after an attack since your backup data is immediately available to start recovery without first having to roll anything back to an earlier recovery point. With hourly recovery costs ranging up to millions of dollars, this faster, simpler recovery can have a huge impact when it matters most.

Layered vaulting does require additional storage since each deduplication baseline will age after the next one is created, but it requires less storage and reduces downtime costs more than solutions based on snapshots and no deduplication.

The Freeze Objects feature of FlashBlade//S protects the vaulted backup data from direct attacks. FlashBlade//S SafeMode retention lock further prevents an attacker from deleting an object bucket, even if they were to gain administrative access.

Dynamic locking in Commvault aligns the object locks in the vault so they all expire at the same time. For example, to provide 14 days of protection, the first data into the vault must be locked for 28 days. Data written the second day is locked for 27 days, the third day is locked for 26 days, and so on until the 14th day, which is locked for 14 days. All object locks therefore align to day 28, and the vault can be deleted on day 29. This approach minimizes the extra storage consumption.

Backup Scheduling

Each time Commvault closes the vault, all clients using that storage pool will be flagged to run a baseline backup. The next time they run any backup, it will automatically convert to a full or synthetic full based on the agent type. For best results, you should configure full or synthetic full backups to run on the same schedule as the retention policy. This gives the most consistent behavior and minimizes the number of backup conversions.

Sizing

It is critical that you work with your Pure or Commvault account team to properly size the solution. After each vault is closed, the next baseline will quickly consume a significant amount of storage. An improperly sized solution can fill up quickly and potentially exhaust capacity. Object locking makes recovering from that situation much more difficult.

Best Practices

This section outlines the best practices for using Object Lock on FlashBlade//S with Commvault.

Use Commvault Workflow to Provision FlashBlade//S

Pure Storage and Commvault developed a workflow to simplify provisioning object storage on FlashBlade//S. The workflow simplifies the provisioning process and applies the best practices. You can install the workflow from the Commvault store using either Command Center or the CommCell Console.

Create Restrictive Object Access Policies

You should configure privileged and unprivileged object access policies on FlashBlade//S. Both policies should have the minimum required permissions.

- The privileged policy will allow deleting objects. You should define source IP addresses or subnets that are allowed to use the policy. It should only be used by MediaAgents. Required permissions:
  - `s3:DeleteObject`
    `s3:DeleteObjectVersion`
    `s3:GetBucketVersioning`
    `s3:GetObject`
    `s3:GetObjectAcl`
    `s3:GetObjectRetention`
    `s3:GetObjectTagging`
    `s3:GetObjectVersion`
    `s3:GetObjectVersionTagging`
    `s3:ListBucket`
    `s3:PutObject`
    `s3:PutObjectRetention`
- The unprivileged policy will not allow deleting objects. It should be used for Storage Accelerator clients and does not need IP address restrictions. Required permissions:

```
- s3:GetBucketVersioning
  s3:GetObject
  s3:GetObjectAcl
  s3:GetObjectRetention
  s3:GetObjectTagging
  s3:GetObjectVersion
  s3:GetObjectVersionTagging
  s3:ListBucket
  s3:PutObject
  s3:PutObjectRetention
```

Place Object Access Keys in Saved Credentials

You should store object access keys in Commvault as saved credentials. This will let you reuse them across buckets on the same FlashBlade/S and simplifies key replacement and rotation. You can only apply saved credentials to Storage Accelerator.

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.

Configure Restrictive Object Lock Settings

When you enable object lock on a FlashBlade//S bucket, you should use apply the most restrictive settings, specifically:

- Set the Versioning value to none.
- Enable Freeze Locked Objects.
- Set Retention Lock to ratcheted (locked) to enable SafeMode Retention Lock.
- Commvault will lock its own objects, so do not set a default object lock policy

Do Not Share Buckets for Locked and Unlocked Data

While a bucket with object lock enabled can store unlocked objects, doing so can cause issues if you ever have to separate the data in the future.

Rotate FlashBlade//S Object Storage Access Keys

You should regularly rotate access keys for FlashBlade//S object storage—creating a new key and deleting the old one—to minimize the risk of key compromise. If you use saved credentials in Commvault, the rotation process is fast and simple.

Designate SafeMode Contacts

Since disabling SafeMode Retention Lock requires Pure Support assistance, you can save time by having your designated contacts onboarded before you start implementation. Your Pure account team can assist.

Implementing the Solution

Prerequisites

FlashBlade//S must be running Purity//FB release 4.1.5 or later.

This guide is intended for use with Commvault release 2023E (11.32.15) or later. Commvault must be running release 2023 (11.30) or later, but 11.32 and its latest maintenance release are strongly recommended. Previous releases are not fully compatible with object lock on FlashBlade//S.

If you wish to use transport layer security (TLS) to secure FlashBlade//S communication from clients and MediaAgents, we recommend that you acquire and apply a certificate signed by a trusted certification authority (CA). Follow instructions in the CA Signed Certificate section of the FlashBlade Security - Comprehensive FAQ to generate the request and apply the signed certificate to the FlashBlade//S. You must include the IP address and DNS name, both fully qualified and unqualified, for every FlashBlade//S data VIP Commvault will access.

You may use the self-signed certificate provided with the FlashBlade//S, but you must disable certificate validation in Commvault. This is not recommended for production implementations.

Download and install the Provision Pure FlashBlade Object Storage workflow from the Commvault store. While not required, it greatly simplifies deployment and configuration of best practices.

Create a saved credential in Commvault to store an API token to access the FlashBlade//S management REST API.

Configure FlashBlade//S and Credentials

The optimal configuration for FlashBlade//S incorporates the best practices for using FlashBlade//S object storage with Commvault, using the workflow to handle the basic storage provisioning. The workflow will configure:

- An object account on FlashBlade//S.
- Two object access policies on FlashBlade//S, with best practice permissions, one with and one without object delete access.
- Two object users attached to the object access policies.
- Object access keys for each object user.
- Saved credentials in Commvault to store the keys.
- One or more object buckets, with or without best practice object lock settings. We recommend creating at least one bucket without object lock.

To execute the workflow:

1. In Commvault Command Center, navigate to the Workflows page. Locate the Provision Pure FlashBlade Object Storage workflow and click its title.
2. Complete the initial workflow form (Figure 4) as follows:
   a. In the dropdown, select the saved credential containing the API token.
   b. In the field, enter the management name or IP address of the FlashBlade//S. If you have applied a TLS certificate, use the name matching the certificate common name.

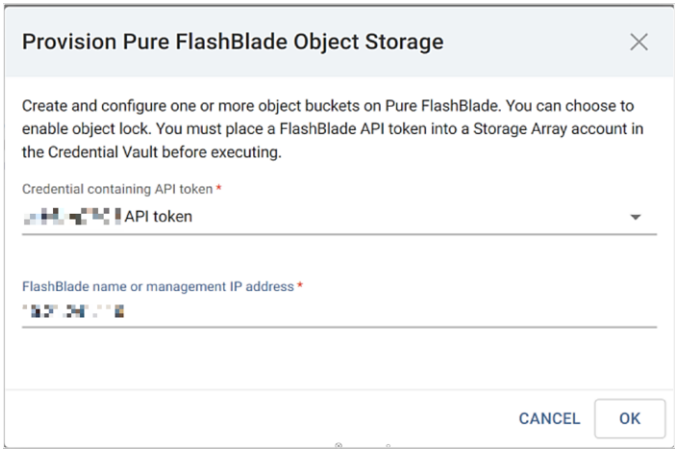


FIGURE 4 Initial workflow form

3. In the object account form (Figure 5), select the account to store the object users and buckets. If you want to create a new account, select New account and enter the name in the New account name field.

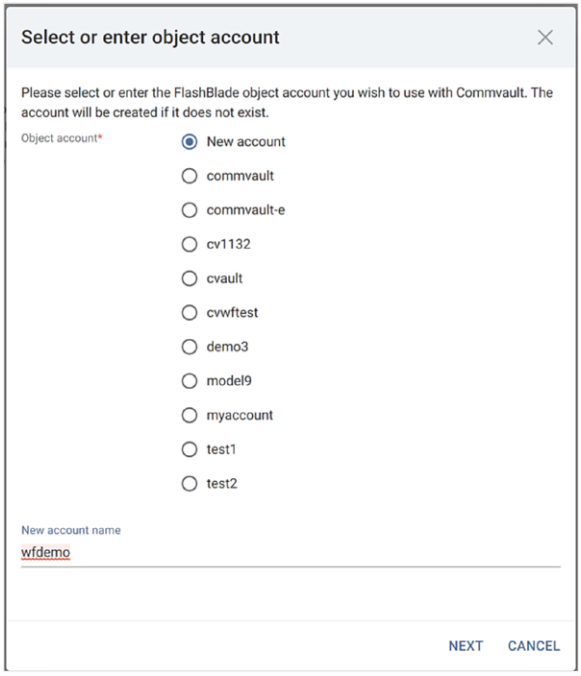


FIGURE 5 Object account form

4. On the IPs or subnets form (Figure 6), select the option you want to use to restrict bucket access in the FlashBlade//S privileged object access policy. You can choose to restrict MediaAgents, IP subnets, or no restrictions. Selecting MediaAgents will use specific IP addresses in the privileged access policy. Selecting IP subnet will allow access for any IP address on the IP subnets you define. Selecting None will skip the access restrictions and allow any address to use the privileged keys–and is therefore not recommended.

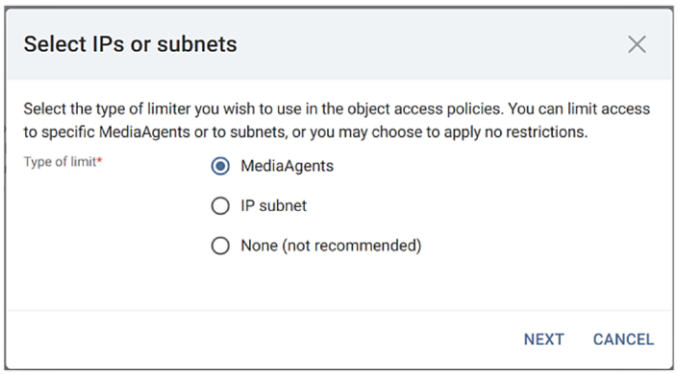


FIGURE 6 IPs or subnets form

   a. If you select MediaAgents, on the Select MediaAgents form (Figure 7), check the boxes for the MediaAgents that need access. Their IP addresses will be added to the policy.

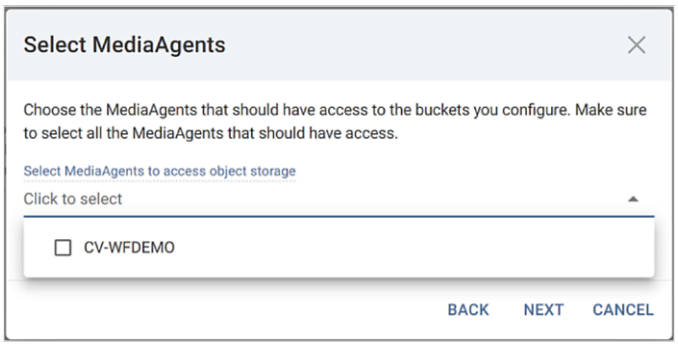


FIGURE 7 MediaAgent selection form

b. If you select IP subnet, on the IP subnets form (Figure 8), click the + button to add a field for each subnet. Enter the subnets in x.x.x.x/n format, where x.x.x.x is the IP range and n is the subnet mask bit length.

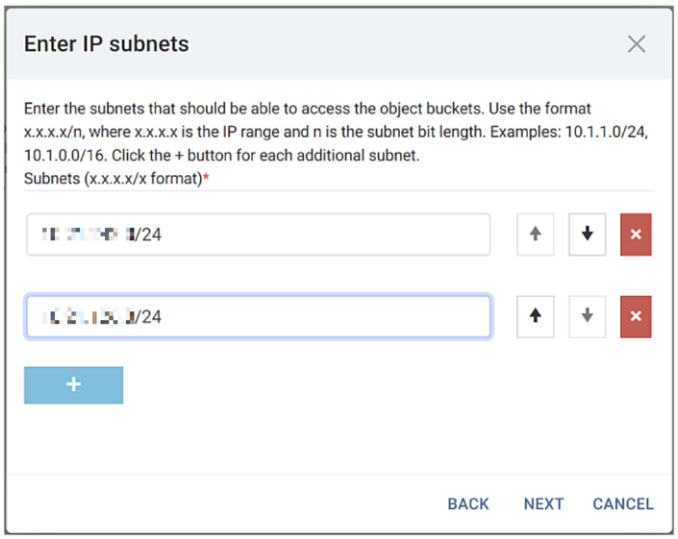


FIGURE 8 IP subnets form

5. On the bucket details form (Figure 9), enter a name for the bucket you want to create. To enable object lock on the bucket, move the Enable object lock slider to the right. The form has SafeMode retention lock selected by default, but you can disable it by moving the SafeMode slider to the left; however, SafeMode retention lock will only be enabled if you also enable object lock.

If you choose to enable object lock, versioning will be disabled, and the freeze objects setting will be enabled.

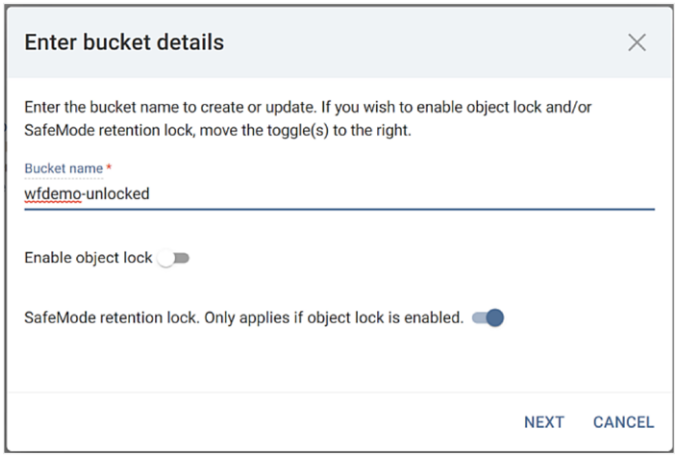


FIGURE 9 Bucket details form

6. The result form (Figure 10) will display success or failure. If you wish to create another bucket, move the slider to the right, click Next, then repeat step 5. To stop creating buckets, move the slider to the left and click Next.

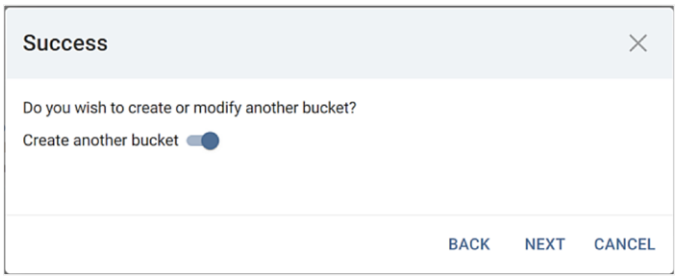


FIGURE 10 Result form

7. A summary form (Figure 11) will show the objects that were created on the FlashBlade//S and in Commvault.

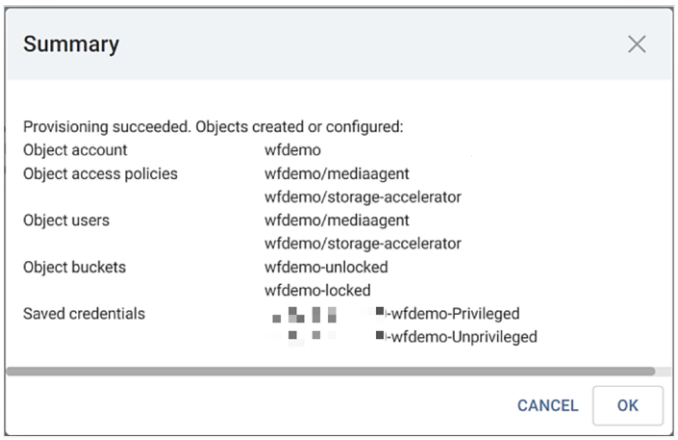


FIGURE 11 Summary form

You are now ready to create storage pools and enable object lock.

Configure Commvault

Add Cloud Storage Pools

You need to create storage pools that connect Commvault deduplication stores with object buckets. Your server plans or storage policies will associate with the storage pools.

NOTE: *Never add a bucket that uses object lock as the first storage pool in a new CommCell.*

To create a storage pool:

1. In Commvault Command Center, navigate to Storage/Cloud. Click the Add link to open the Add cloud storage wizard.
2. Complete the first section of the form (Figure 12) as follows:
   a. From the Type dropdown, select Pure Storage FlashBlade. (On 11.30 CommCells, select S3 Compatible Storage.)
   b. In the Name field, enter a display name for the storage pool.
   c. From the MediaAgent dropdown, select a MediaAgent to be the owner of the storage pool.
   d. In the Service host field, enter the name of the FlashBlade//S data VIP. You may bypass TLS by putting "http://" at the front of the name. This is not a recommended production configuration. You may use the same data VIP and DNS name for any locked and unlocked FlashBlade//S buckets.
   e. In the Bucket field, enter the name of the bucket.

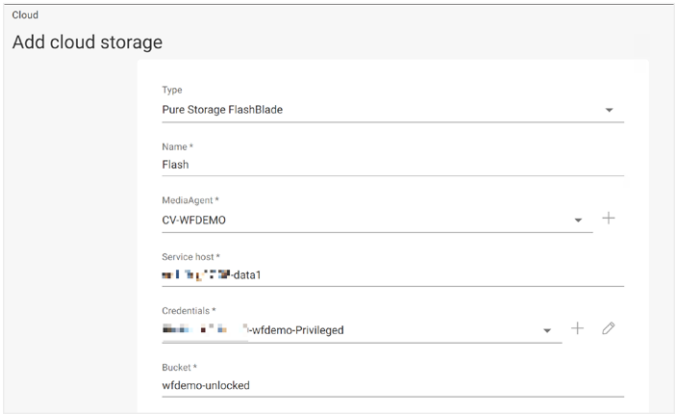


FIGURE 12 Add cloud storage form in Commvault Command Center

3. In the Deduplication DB location section (Figure 13), click the Add link to add a DDB partition.
4. In the Add Deduplication DB location popup window, select the MediaAgent that will host the DDB partition, then enter or browse to the path where the DDB should be stored. For best backup performance, this path should be located on high-speed, low-latency storage such as a PCIe NVMe drive or SSD, or Pure FlashArray//X. Click the Add button to update the DDB locations list.
5. Repeat steps 3 and 4 for any additional partitions you wish to add, up to a maximum of four.
6. Click the Save button to create the storage pool.

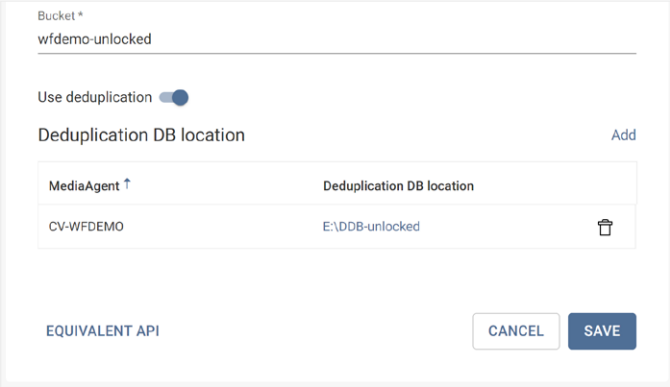


FIGURE 13 Deduplication DB location section

Repeat this procedure for each FlashBlade//S bucket.

When complete, you will have two or more storage pools, one for each bucket (Figure 14).

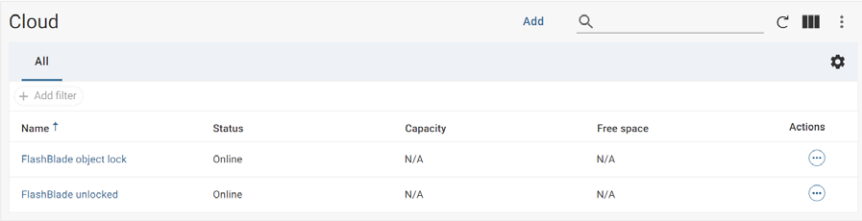


FIGURE 14 Commvault storage pools for locked and unlocked FlashBlade//S buckets

Add Storage Accelerator Credential

We recommend using separate access keys for Storage Accelerator clients and MediaAgents to mitigate the effects of a key compromise. Storage Accelerator keys should not grant access to delete objects. The workflow will have created the separate keys and added them to stored credentials in Commvault.

To apply Storage Accelerator credentials to a cloud storage pool:

1. From the cloud storage pool list, click the name of the storage pool.
2. In the page that opens, click the Backup locations tab.
3. Click the bucket name in the Bucket section.
4. In the Configuration tile (Figure 15), from the Storage accelerator credentials dropdown, select the appropriate unprivileged stored credential, then click the checkmark button.

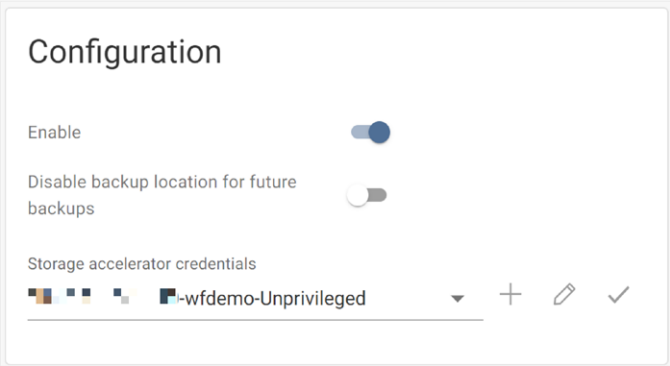


FIGURE 15 Setting Storage Accelerator credential

Repeat this procedure for each storage pool. If you have multiple buckets in the pool, you must set the credential on each one.

Add Server Backup Plans

A server backup plan sets the backup schedule for clients, as well as the progression of storage targets and the data retention for each target. You must create a backup plan for each

To create a server backup plan:

1. In Commvault Command Center, navigate to Manage/Plans. Click the Create Plan dropdown, then select Server backup to start the Create Server Backup Plan wizard.
2. On the General page (Figure 16), select the Create a new plan option. In the Plan name field, enter a name for the plan. Click the Next button to continue.

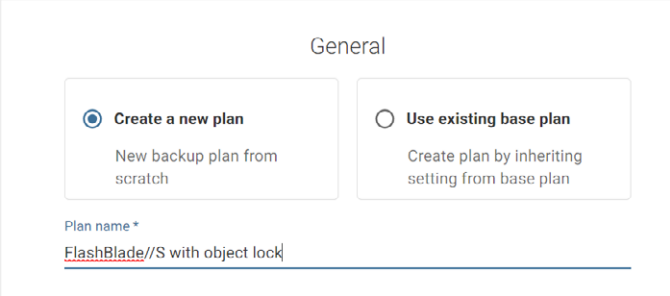


FIGURE 16 Create Server Backup Plan wizard General page

3. On the Backup Destinations page, click the Add Copy button. Fill out the Add copy popup window (Figure 17) as follows:
   - **a.** Optionally change the Name field to a descriptive name.
   - **b.** From the Storage dropdown, select the locked storage pool you created.
   - **c.** Set the retention period based on your immutability requirements. We recommend using a number of weeks to ensure alignment with backup cycles. This value will become the vaulting frequency later.
   - **d.** Do not enable the Extended Retention rules toggle.
   - **e.** Click the Save button to add the copy.

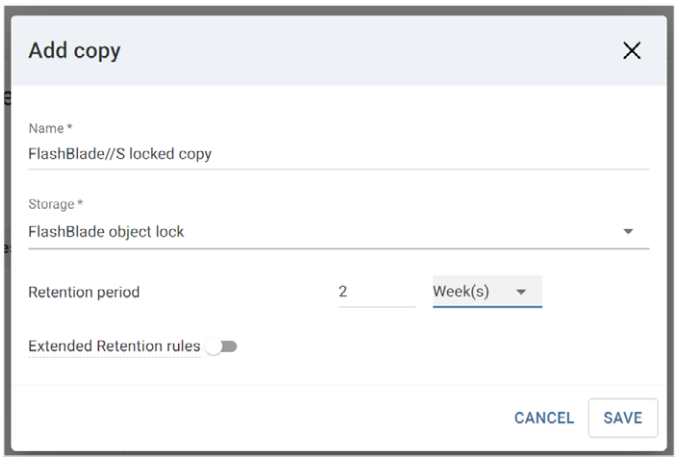


FIGURE 17 Adding a locked copy

4. To add an optional unlocked copy for longer retention, click the Add Copy button again. Fill out the Add copy popup window (Figure 18) as follows:

   a. In the Name field, enter a descriptive name.

   b. From the Storage dropdown, select the unlocked storage pool you created.

   c. If you wish to only copy certain full backups for longer retention, select the appropriate option from the Backups to copy dropdown; otherwise, the plan will copy all backups to the unlocked bucket.

   d. You can set a start date before which backups will not be copied by enabling the Backups on and after toggle and selecting a date. This is most useful when adding a secondary copy to an existing plan.

   e. Enter the desired retention period. Unlike the locked copy, the unlocked copy will not vault and will only contain a single baseline, regardless of retention.

   f. If you wish to set extended retention for certain backup jobs, enable the Extended Retention rules toggle and set the desired rules.

   g. Click Save to add the copy.

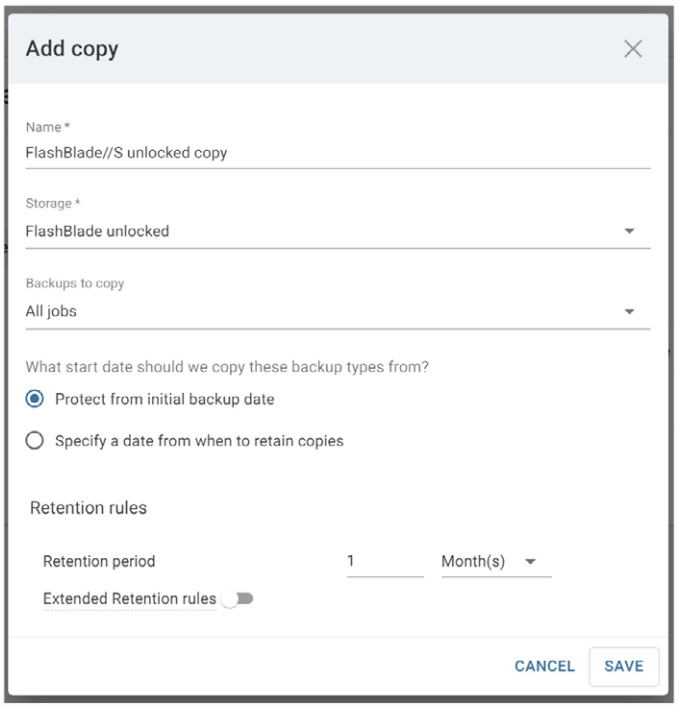


FIGURE 18 Adding an unlocked secondary copy

3. You should now see your copies listed in the Backup Destinations page (Figure 19). If you wish to add any other storage targets, such as public cloud, you should do so before proceeding. Click the Next button to continue.

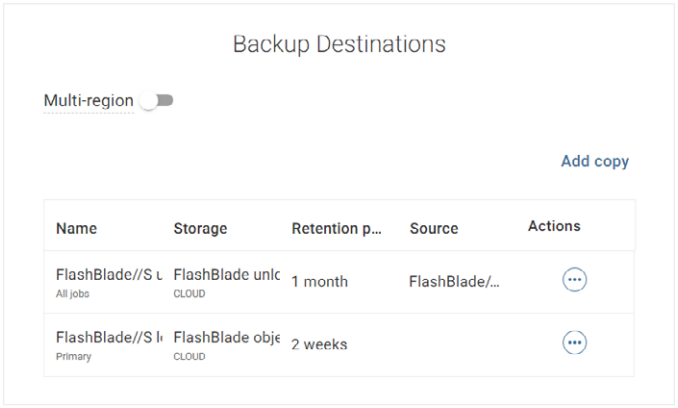


FIGURE 19 Backup destinations

4. Configure the schedule and backup window options on the Recovery Point Objective page (Figure 20) to meet your organization's needs, including database log backups. Click the Next button to continue.

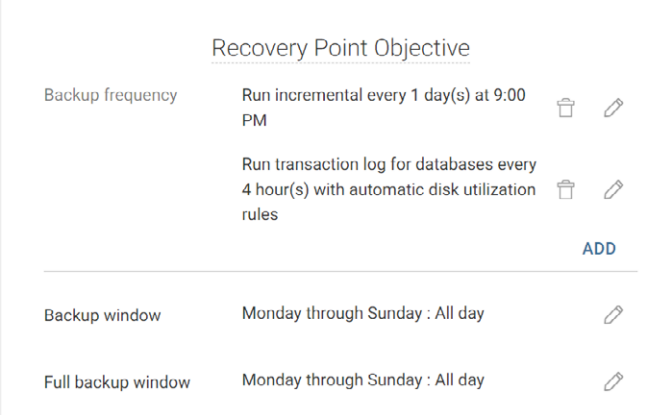


FIGURE 20 Recovery Point Objective settings

5. On the Options page (Figure 21), adjust any snapshot options to meet your needs. Click Submit to create the server backup plan.

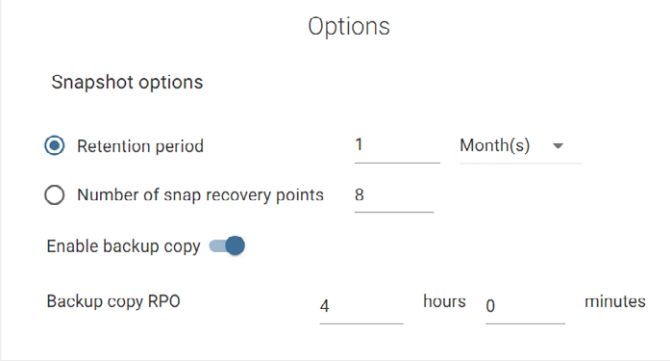


FIGURE 21 Snapshot backup options

When complete, you should have a server backup plan with two or more destinations, one of which is the FlashBlade//S bucket with object lock enabled (Figure 22).

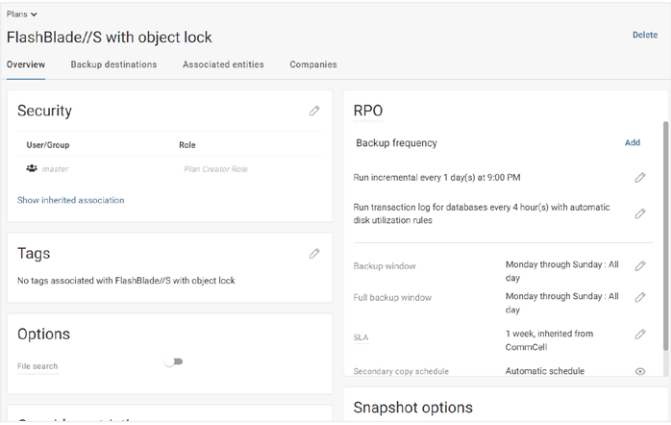


FIGURE 22 Completed server backup plan

You can verify backup destinations on the Backup destinations tab (Figure 23).

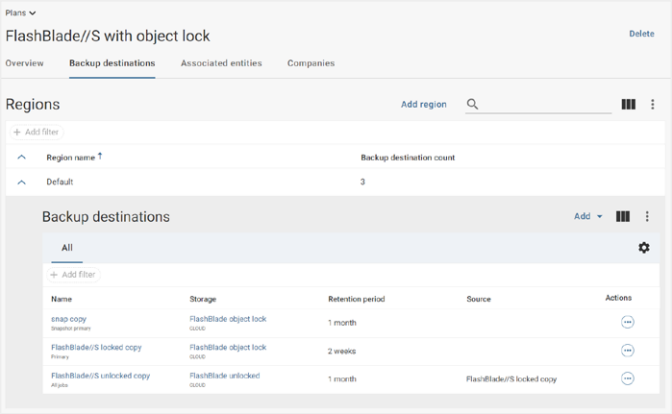


FIGURE 23 Server backup plan destinations

You should repeat this procedure to create a second backup plan that does not use the locked storage pool. When completed, you will have two new server backup plans, one with object lock and one without (Figure 24).

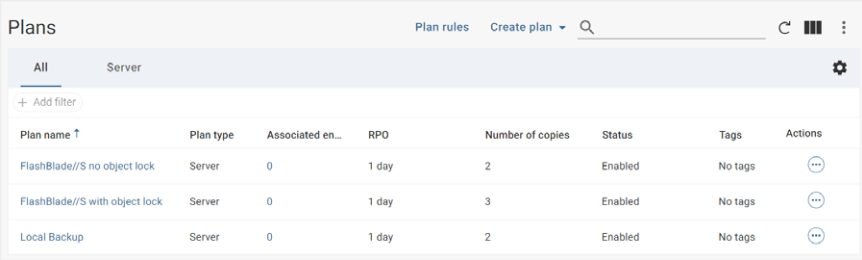


FIGURE 24 Completed server backup plans

Set Deduplication Block Size

Cloud targets in Commvault default to a deduplication block size of 512KB. For the optimal use of FlashBlade//S capacity, you should lower the size to 128KB. Deduplication block size is managed in the CommCell Console.

To change the deduplication block size for a FlashBlade//S storage pool:

1. In the CommCell Console, navigate in the CommCell Browser pane to the Storage Resources node. Expand Storage Resources, then Storage Pools. Right-click the FlashBlade//S object lock pool, then click Properties>Storage Pool (Figure 25).

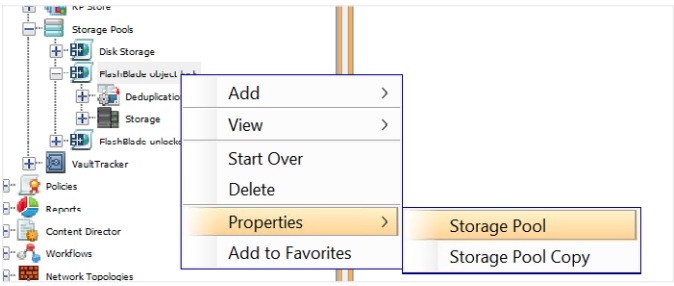


FIGURE 25 Accessing storage pool properties

2. In the Storage Pool Properties popup window, click the Advanced tab (Figure 26). From the dropdown, select 128. Click the OK button to apply the change.

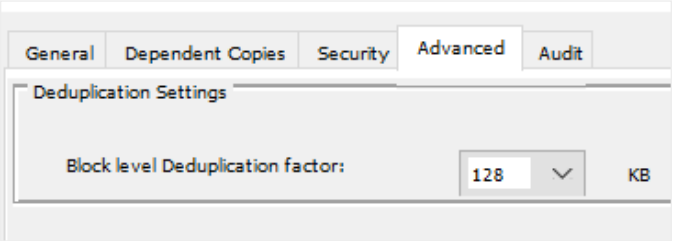


FIGURE 26 Setting deduplication block size

3. In the confirmation popup window (Figure 27), enter the confirmation text as instructed, then click the OK button.

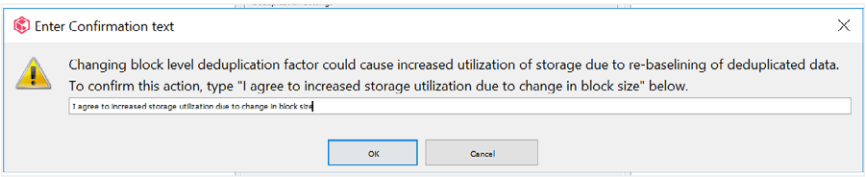


FIGURE 27 Block size change confirmation

Repeat steps 1-3 for all FlashBlade//S cloud storage pools.

Configure Hardware WORM on Storage Pool

You must enable hardware WORM support on the storage pool. This will perform several functions within Commvault. It will activate object lock commands, configure automatic sealing of the DDB for the storage pool, and apply an enforced retention. It will also enable compliance lock on all plan copies associated with the pool and enforce it on any new copies you create later.

To enable hardware WORM on a storage pool:

1. In Commvault Command Center, navigate to the Storage/Cloud page. Click the Configuration tab.
2. In the WORM tile (Figure 28), move the WORM storage lock toggle to the right.

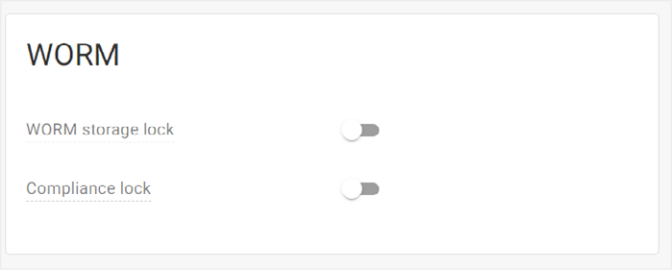
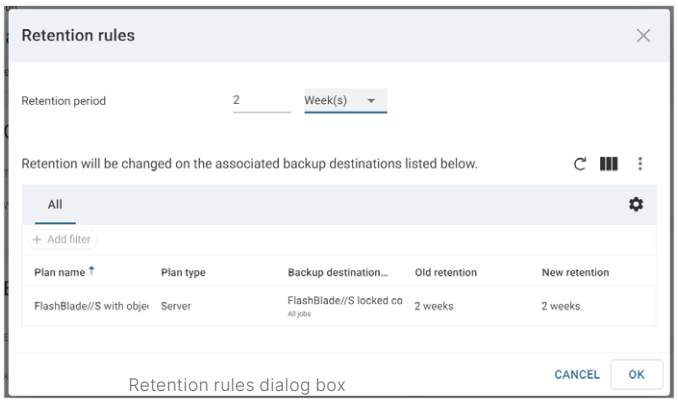


FIGURE 28 WORM tile

3. The Retention rules dialog box (Figure 29) appears. Set the Retention period to match the original retention you set during plan creation, then click the OK button..



Retention rules dialog box

4. A confirmation dialog box (Figure 30) appears. Enable both the checkboxes and type “Confirm” in the field, then click the Confirm button.

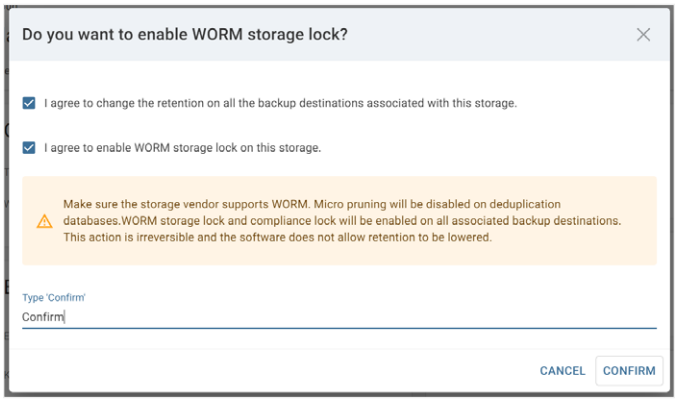


FIGURE 30 WORM confirmation dialog box

5. In the WORM tile (Figure 31), the WORM storage lock and Compliance lock toggles will move to the right, and both will be disabled for further changes. The retention period is also shown.

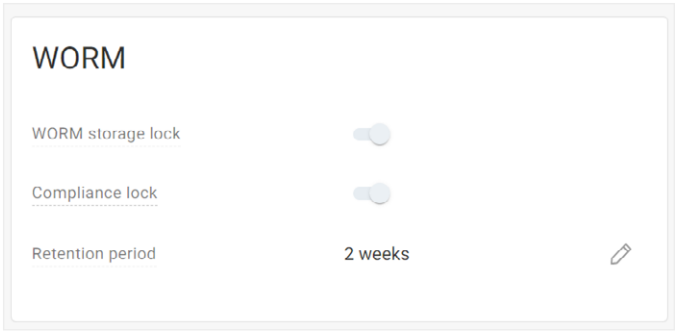


FIGURE 31 WORM tile reflecting changes

Object lock is now fully enabled, and all new backup data using the server backup plan will be protected with object lock on the FlashBlade, and the backup jobs will be protected within Commvault against deletion until they have reached the retention age.

Recommended: Modify DDB Backups

DDB backups follow a different retention scheme than normal backups, and you must avoid having these backups go to a locked storage pool to prevent pruning problems and excess capacity utilization. The backups should, however, still reside on FlashBlade//S for fast recovery and simplest protection.

NOTE: *DDB backup settings for a MediaAgent are used by all the DDBs it hosts. If the MediaAgents hosting the FlashBlade//S DDBs already had other DDBs on them, the backups will already be configured to land on other storage.*

You can change the DDB backup settings using the CommCell Console. To change the policy for DDB backups:

1. In the CommCell Browser pane, expand Client Computers, then the MediaAgent you wish to update. Expand the File System node underneath the client, then click the defaultBackupSet node.
2. In the right pane, right-click the DDBBackup subclient, then click Properties.
3. In the Subclient Properties dialog box, click the Storage Device tab (Figure 32). From the Storage Policy tab, select the unlocked FlashBlade//S server backup plan you created, then click the OK button.

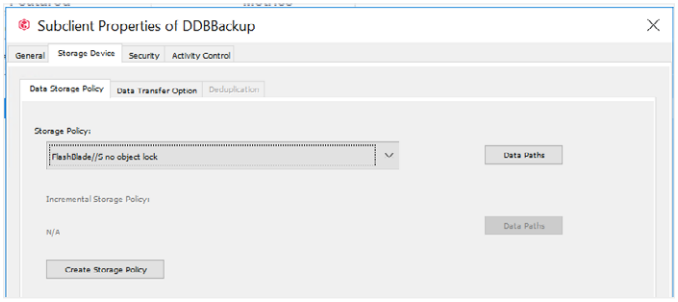


FIGURE 32 Setting DDBBackup storage policy

The Storage Policy column will update to reflect the new setting (Figure 33).

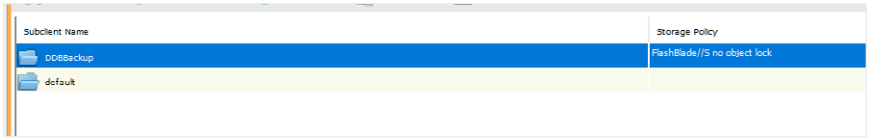


FIGURE 33 Updated DDBBackup storage policy

Modify Index Backups

Similar to DDB backups, index backups follow their own schedule and retention settings, independent of any policies you create. You should associate these to an unlocked storage pool on the same FlashBlade//S system.

NOTE: *Commvault creates index backup clients automatically upon the first index backup. You may need to wait up to a day after your first backups in new server backup plans to be able to reconfigure them.*

You can change the index backup client settings using the CommCell Console. To change the policy for index backups:

1. In the CommCell Browser pane, right-click the Client Computers node, then click Customize View.
2. In the User Preferences dialog box (Figure 34), enable the Show Index Servers checkbox, then click the OK button.

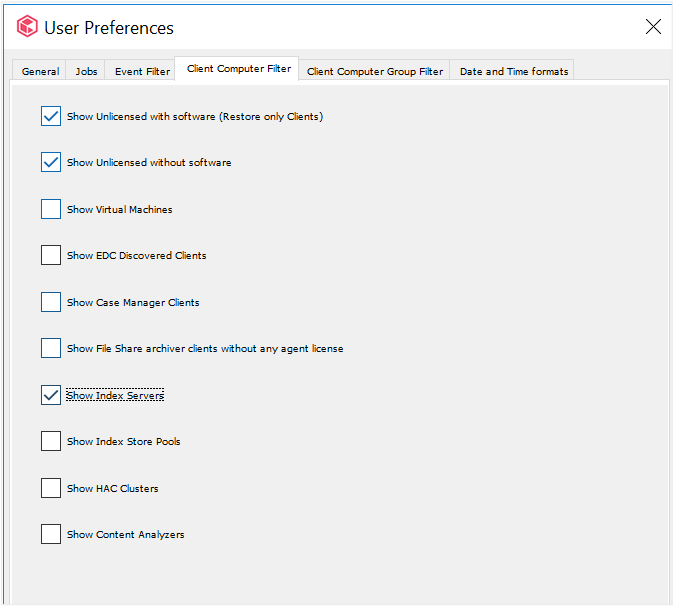


FIGURE 34 Showing index server clients

3. Once the index server for the locked server backup plan has been created, it will appear in the Client Computers list. It will follow the naming convention <plan name>_IndexServer, so the index server for a plan called FlashBlade//S with object lock would be named "FlashBlade//S with object lock_IndexServer." After it is visible–you may have to refresh the client computers list–expand the client node, then expand the Big Data Apps node, then click the classicIndexInstance node. In the right pane, right-click the default subclient, then click Properties. Click the Storage Device tab.

4. From the Storage Policy dropdown (Figure 35), select the unlocked FlashBlade//S plan you created. You will see a warning popup window twice, when you click the dropdown and again when you choose the policy. Click the OK button on both popups. Click the OK button on the Subclient Properties dialog box to commit the policy change.

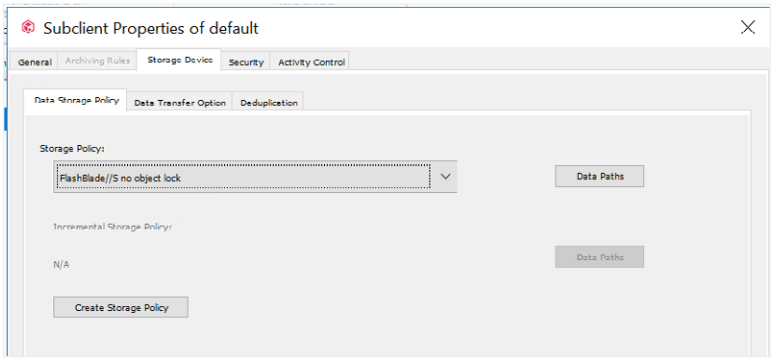


FIGURE 35 Setting index server storage policy

When complete, the default subclient will show the unlocked FlashBlade//S plan as its storage policy (Figure 36).

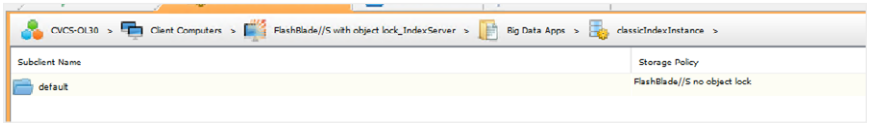


FIGURE 36 Updated index backup subclient

NOTE: *Commvault will create an index server for each server backup plan. If you create any new plans that use the same object lock pool, you will need to reassociate their index servers the same way.*

Configure DR Backups

Following are the best practices for using FlashBlade//S and File SafeMode with Commvault DR backups to provide an extra immutable layer of protection.

Use a Dedicated Service Account: Using a dedicated service account in Active Directory 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 and manage the password.

NOTE: *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: As shown in Figure 37, set up the DR file system with only SMB enabled. On Purity//FB release 3.0 and earlier, set the Native SMB ACLs option, which was removed in release 3.1.

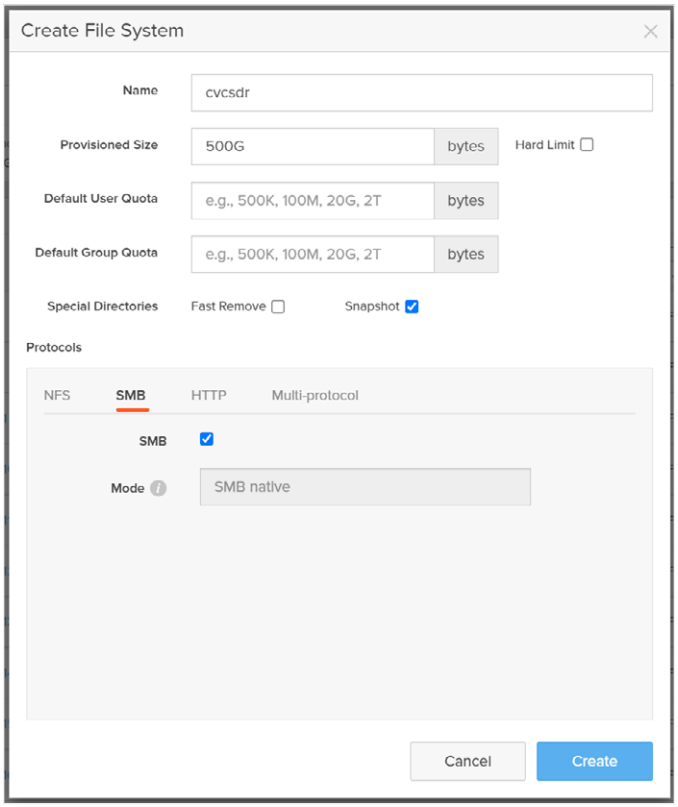


FIGURE 37 SMB export policy

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 38 shows the full ACL.

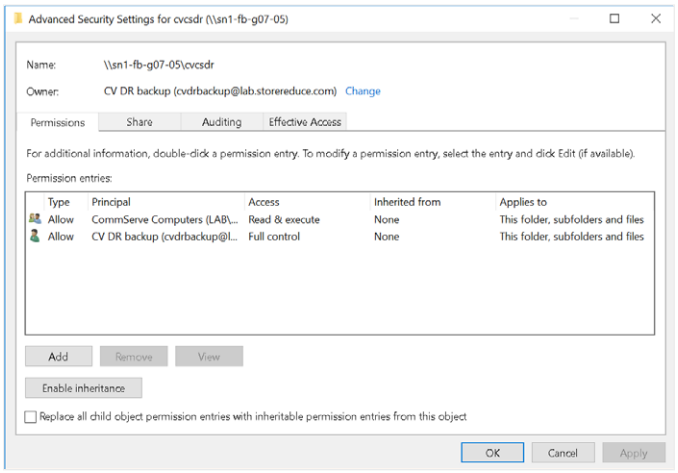


FIGURE 38 DR Backup SMB share ACL

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 snapshot schedule runs at 10:00 am, and the DR backup completes in one minute, schedule DR backups for 9:55 am.

Use FlashBlade Replication to Provide Offsite Availability: While not detailed as part of this architecture, native replication between FlashBlades 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 account team before implementing. 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 storage.

To enable cloud library upload using Commvault Command Center, navigate to the **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 39, enable the **Upload backup metadata to cloud library** option, then select the FlashBlade storage pool in the **Cloud library** dropdown. Click the **Save** button to commit any changes.

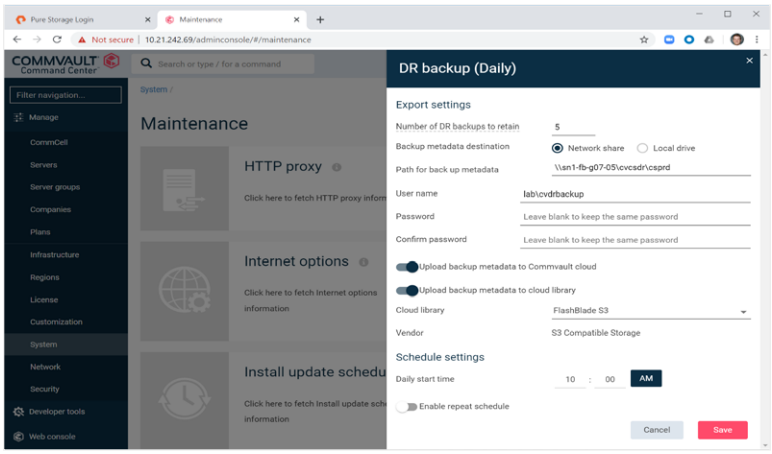


FIGURE 39 DR Backup configuration in Commvault Command Center

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 5 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 5, and the SafeMode snapshot retention policy keeps 7 days, 12 days of DR backups will be available for recovery.

Recovering from a Cyber Event

Object Lock and SafeMode Retention Lock prevent ransomware, rogue administrators, or other cyberattacks from affecting your backup data, so you can focus on getting affected systems back online faster. You don't need to take any action on the FlashBlade//S since your immutable data remains available and uncompromised.

Clean Room Recovery

As part of the recovery, you should use a "clean room" approach to restore systems and data in an isolated space. You can then remove any malware before reintroducing the systems to the production environment. Pure Storage can help define what changes you need to make to make the FlashBlade//S accessible from the clean room.

Contact Pure Support

While you can begin restoring your primary systems right away, we recommend contacting Pure Storage Support, especially if you store production data on FlashBlade//S file systems or any other Pure Storage products. Support is ready to assist with any issues you might encounter.

Conclusion

Pure FlashBlade//S and Commvault minimize the impact of a cyberattack, reducing the risk to your organization if you get hit by ransomware or other cyberattacks. You can be confident that your backups are intact, protected from an attacker by Object Lock and SafeMode. and that you can recover systems as fast as you need to.

Learn more about how Pure Storage helps protect you from ransomware and recover your data faster. When you're ready to have a conversation, reach out to your Pure account team.

Appendix

Caveats

- Synthetic full backups that run after a vault is closed will take longer to complete as the baseline is rebuilt. Depending on your environment, traditional full backups may complete faster than synthetic full, but they will add load to your production systems. Other synthetic full backups will be faster.
- Locked objects cannot be deleted before the lock expires. If you need to delete objects sooner, you will need to work with Pure Support.
- Once enabled on a bucket, SafeMode Retention Lock can only be disabled by Pure Support, working with your authorized designees.
- Object Lock cannot be enabled on a bucket that contains objects.
- Disabling and removing schedules from subclients will affect data aging for entire vault copies. To ensure Commvault can delete data on schedule, you must manually delete backups for retired subclients. If you want to archive the data from these subclients, use a separate storage pool for the archive copy.
- Delays in auxiliary copy can prevent DDBs from sealing on the expected schedule. Monitor aux copy jobs to ensure they are completing reliably.

Pure Storage FlashBlade//S

Pure Storage® FlashBlade//S is the next generation of enterprise scale-out unified fast file and object (UFFO) storage that delivers rich data services with high density, capacity, performance, and scalability to meet the needs of modern applications. Using a distributed metadata architecture, FlashBlade//S offers multi-dimensional performance on a consolidated platform with NFS, SMB, and S3 protocol access.

With a modular architecture that delivers massive scalability, and density and efficiency to save you on data center costs, FlashBlade//S can enhance just about any unstructured workload. And an Evergreen//Forever™ subscription means never having to migrate to get the latest capabilities or enhancements. Learn more about how FlashBlade//S can benefit you.

Commvault Backup and Recovery and Metallic

Commvault Backup & Recovery (Commvault) is an industry-leading data protection software for medium to large enterprises. Commvault is known for a flexible, scalable architecture, broad application integration and cloud capabilities. A suite of ransomware detection and mitigation features, such as anomaly detection, proactive threat scanning, and honey pot techniques, makes Commvault an ideal platform for both securing backup data against attack and reducing the risk of an attack occurring.

Metallic ThreatWise is a cyber detection and deception offering that uses decoy sensors to detect incursions before an attack and collect detailed information to help with a security response. Metallic Recovery Reserve is a fully operational cloud storage backup target for Commvault Backup & Recovery, fully integrated with Commvault data management software. With this cloud service, customers can simplify their cloud data management with pre-configured networking and storage, reduce costs via efficient deduplication and no egress fees, and mitigate ransomware with secure air-gapped cloud data protection.

Additional Resources

- Pure FlashBlade//S documentation
- Best Practices for Configuring Commvault with FlashBlade//S
- 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 end user to IT architect with multiple backup and recovery products, followed by product management with Commvault. Roy joined Pure Storage in April 2019.

©2023 Pure Storage, Inc. All rights reserved. Pure Storage, the P logo mark, FlashArray, FlashArray//C, FlashArray//X, FlashArray//XL, Pure Cloud Block Store, and SafeMode are trademarks or registered trademarks of Pure Storage, Inc. All other names may be trademarks of their respective owners.

PS2483-01-en 09/23