

REFERENCE ARCHITECTURE

# Simplified Disaster Recovery and Ransomware Protection

With Pure Storage FlashRecover//S™, Powered by Cohesity®

# Contents

- Introduction .....3**
- Pure Storage FlashRecover//S, Powered by Cohesity.....3**
- How Pure Storage FlashRecover//S Works .....4**
  - Ransomware Protection ..... 4
  - Importance of Disaggregated Storage and Compute for Data Protection..... 4
- FlashRecover//S Architecture .....5**
- Pure Storage SafeMode Snapshots with FlashRecover//S.....6**
  - Enabling SafeMode Snapshots..... 7
- SafeMode Procedures.....8**
  - Executing SafeMode Snapshots ..... 8
- SafeMode Recovery Process ..... 10**
  - Leverage SafeMode Recovery on An Existing Cluster ..... 11
- Leverage SafeMode Recovery on a Newly Built Cluster ..... 14**
- Conclusion ..... 19**
- About the Author ..... 21**



## Introduction

Did you know that if you already have Pure Storage® FlashRecover//S™, Powered by Cohesity you can now add another level of ransomware protection, at no additional cost? This white paper shows how you can integrate the Pure Storage SafeMode™ Snapshot feature into your installation and use it to achieve multi-level ransomware protection.

Ransomware is one of the biggest threats to businesses today, and there are no signs of it abating. Attacks are getting more sophisticated, and ransomware groups are identifying and exploiting new vulnerabilities much faster than enterprise solutions can patch them. [Security Brief Australia reports](#) that “52% of widespread threats began with a zero-day exploit” and since no business is immune to ransomware attacks, enterprises need to focus more on disaster recovery (DR) to minimize the impact of an attack and ensure business continuity.

Pure Storage FlashRecover™, Powered by Cohesity is an integrated, modern all-flash data protection solution for rapid recovery at scale. The jointly developed solution offers simple, fast, reliable, and independent scaling of storage and compute for backup and recovery of enterprise data.

FlashRecover//S significantly reduces how much time you need to spend on recovery because with SafeMode, attackers are prevented from destroying days' worth of data or your ability to recover. Additionally, enterprises need performance to perform rapid recovery and restore systems quickly should a ransomware attack occur.

The best practices below apply only to configuration elements specific to Cohesity and SafeMode and not necessarily to general FlashBlade//S™ deployments.

---

## Pure Storage FlashRecover//S, Powered by Cohesity

According to a 2021 [Coveware study](#), the average downtime a company experienced in Q4 2021 due to ransomware attacks was at least 20 days. Enterprises need a data protection solution that is scalable, high performing, and capable of providing multi-point protection to recover in a matter of hours instead of days. With FlashRecover//S, enterprises will have a data protection solution that delivers:

- **High performance:** Experience up to three times faster backup and restore throughput than disk-based alternatives. Flash eliminates defragmentation-related concerns and inherently brings performance to restores.
- **Scalable and efficient data reuse:** Scale out compute and storage independently without requiring complicated services. If additional storage is required, simply add more blades to the FlashBlade® and grow your environment. Independent scaling allows efficient use of resources. You can scale from 168TB to 2PB storage in a single chassis.
- **Recovery at scale:** Restore and recover petabytes of data in hours, instead of days or weeks.



- **Simplified management:** Easily deploy, manage, and use a single integrated solution with simple architecture. FlashRecover//S will auto-discover and configure the storage required for backups in a simple, wizard-driven approach.
- **Ransomware protection:** Instantly restore the data and resurrect a new FlashRecover cluster after disaster strikes. SafeMode from Pure is built into the solution, offering multi-layered data security and faster, more flexible recoveries.

## How Pure Storage FlashRecover//S Works

The latest version of FlashRecover//S combines the new Cohesity PXG2 compute nodes and FlashBlade//S. FlashRecover//S integrates SafeMode for faster recovery from disaster and to combat ransomware.

In a disaggregated system, compute and storage are decoupled. In such a case, Cohesity doesn't control the storage system that it is writing to, which opens a possibility that the storage part of the cluster might get compromised in the event of a ransomware attack. This is where the SafeMode integration comes into play.

### Ransomware Protection

FlashRecover//S moves the metadata and configuration data to the FlashBlade NFS filesystems to create a consistent SafeMode copy of the backup data and metadata. The SafeMode copy of the system is immutable and contains the configuration of the cluster, the metadata, and the actual data in the FlashBlade, thus providing protection for the storage system. If an attack occurs, recovery can be done directly in the production environment by rolling back to the latest SafeMode copy of the system.

### Importance of Disaggregated Storage and Compute for Data Protection

Primary storage continues to grow at an unprecedented rate, and your data protection strategy must keep up with it. The traditional approach of adding a backup server and storage or another backup appliance requires not only deployment, but also calibration of backup and DR policies. Backup deduplication only works at the backup server level. So in the traditional approach to scaling out, careful policy management is needed to maintain levels of deduplication efficiency.

Contrast this to the disaggregated approach: simply add more storage. No backup policy maintenance is required, and deduplication continues to be performed across all backed up data. The disaggregated approach offers additional advantages. For example, if you want to increase backup or recovery performance, you can simply add more compute nodes. In a more traditional data protection model, that would likely require a significant redesign.

The disaggregated approach preserves a single name space, eliminates islands of deduplication, and greatly simplifies the process of scaling a data protection solution—with respect to both storage and performance.



## FlashRecover//S Architecture

The FlashRecover//S solution is made up of three main parts:

- **Cohesity DataProtect software:** Cohesity DataProtect is simple, comprehensive, enterprise-grade backup and recovery software for traditional and modern data sources.
- **Cohesity-certified compute nodes:** Cohesity DataProtect runs on Cohesity-certified compute (PXG2) nodes for FlashRecover//S with no local drives.
- **Pure Storage FlashBlade//S:** FlashBlade//S is the backend storage where the file systems are created and mounted to compute nodes via NFS v3 protocol.

The solution is built on the foundation that compute and storage are disaggregated, which enables enterprises to independently scale compute and capacity as needed. The solution is also designed with high availability in mind, with no single point of failure and no inherent bottlenecks.

FlashRecover//S can be deployed in an automated manner, which means a user would only need to supply the IP address of the existing or new FlashBlade in the datacenter and token id. Cohesity auto deployment software will auto detect the FlashBlade and will validate if existing Data VIPs are configured on FlashBlade to perform the deployment, as shown in figure 1.

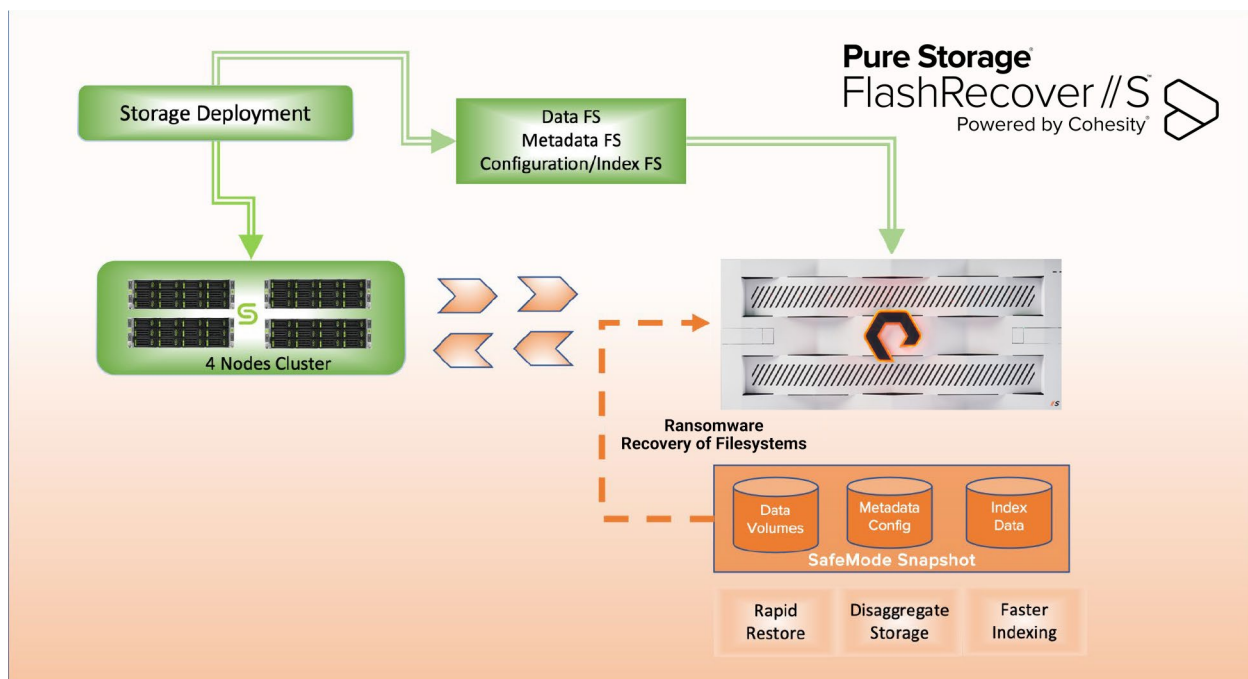


Figure 1: FlashRecover Ransomware Solution Architecture

The deployment creates the data, metadata, configuration, and indexing file systems on the FlashBlade, as shown in Figure 2. There are four main filesystem types that get created on the FlashBlade when FlashRecover is configured.



These four types of filesystems are:

- **Data filesystems:** For backup data store
- **Metadata filesystems:** Uses a distributed key:value store for cluster metadata storage
- **Configuration filesystems:** Stores FlashRecover cluster configuration and cluster node data
- **Indexing filesystems:** For indexing stores

Dashboard

Storage

Protection

Policies

Analysis

Performance

Capacity

Replication

Network

Health

Settings

Array

File Systems

Object Store

File Systems

Size

262.59 T

Virtual

93.46 T

Data Reduction

1.3 to 1

Unique

74.45 T

Snapshots

5.05 T

Total

79.50 T

File Systems

Name

1035855204745120-84461-5

FlashRecover\_FBNFS\_DATA\_1035855204745120-84461-5

-

-

536.85 G

False

2022-07-29 13:33:43

NFSv3

promoted

True

FlashRecover\_FBNFS\_INDEX\_1035855204745120-84461-5

-

-

115 G

False

2022-07-29 13:33:41

NFSv3

promoted

True

FlashRecover\_FBNFS\_LOCAL\_1035855204745120-84461-5

-

-

2719 G

False

2022-07-29 13:33:41

NFSv3

promoted

True

FlashRecover\_FBNFS\_METADATA\_1035855204745120-84461-5

-

-

33.58 G

False

2022-07-29 13:33:42

NFSv3

promoted

True

Source Location

Source Name

Size

Virtual

Hard Limit

Created

Protocols

Promotion Status

Writable

1 of 4

+

-

Destroyed (0)

Figure 2: FlashRecover//S Filesystems on FlashBlade

These four types of FlashRecover//S filesystems are mounted over the data VIPs and balanced across all the available nodes. In the case of a node failure, the logical NFS mount points are redistributed on the remaining surviving compute nodes.

When the failed compute node is back online, the mount points are rebalanced across the FlashRecover//S cluster. Any new node addition to the configuration will create a new set of NFS filesystems.

## Pure Storage SafeMode Snapshots with FlashRecover//S

There are plenty of resources available for FlashRecover, including a white paper on [rapid restore with Oracle](#) and one focused on [performance testing results with FlashRecover](#). You can find these white papers and additional resources on the [FlashRecover page](#).

In this paper, we want to get the word out about FlashRecover//S with SafeMode, because it extends protection against ransomware attacks beyond what's available with most data protection solutions.

SafeMode, a built-in feature of FlashBlade systems, mitigates ransomware attacks by preventing any modification or deletion of backup data. The backup data cannot be altered or destroyed. This helps guard against data loss due to ransomware, accidental deletion, or rogue admins. SafeMode enhances protection by capturing the FlashRecover data, metadata, and cluster configuration data in periodic read-only snapshots that are immediately available for recovery in any DR scenario.

SafeMode benefits include:

- **Enhanced protection:** Ransomware can't delete, modify, or encrypt data protected with SafeMode snapshots of backup data. 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 data.
- **System-wide security:** Once enabled, SafeMode protects all the filesystems on the FlashBlade, not just ones used by FlashRecover.
- **Backup integration:** SafeMode snapshots can be executed directly from the FlashRecover command line.



- **Rapid restore:** Restore via a massively parallel architecture and elastic performance that scales with data to speed backup and recovery.
- **Investment protection:** FlashBlade includes the SafeMode feature at no extra charge. Your Pure subscription or maintenance support contract covers enhancements.
- **Flexibility:** Snapshot cadence and eradication scheduling are customizable.

### Enabling SafeMode Snapshots

To enable SafeMode, follow these steps:

1. Ensure you meet the pre-requisites
2. Enable SafeMode Snapshots on FlashBlade
3. Estimate capacity requirements

#### Ensure you meet the prerequisites

There are prerequisites to leveraging SafeMode, discussed below:

- **Purity//FlashBlade 3.0 or later:** Purity//FlashBlade 3.0 includes significant enhancements that improve ransomware mitigation, including support for the rollback of SafeMode snapshots, which allows you to work with Pure Storage support teams to instantly restore the live file system after an event and purge compromised data.
- **Cohesity DataProtect 6.8.1\_u1 or later:** Use Cohesity DataProtect version 6.8.1\_u1 and onwards.
- **PXG1 and PXG2 support:** FlashRecover SafeMode snapshot feature is supported on both PXG1 and PXG2 nodes. Existing customers on PXG1 will need a software upgrade to Cohesity's 6.8.1\_u1 release. FlashRecover//S will support heterogeneous node configurations, for example if you have an existing PXG1 and later decided to add new PXG2 nodes this is doable.

To leverage the ransomware protection feature For an existing FlashRecover deployment, you must upgrade your cluster to the latest FlashRecover//S software version (6.8.1\_u1). When the software upgrade completes successfully, FlashRecover//S will auto-migrate the metadata and configuration data to the corresponding newly created filesystems on the FlashBlade.

**NOTE:** There will be some performance impact on the backup and recovery workflow while the migration of metadata and configuration is in progress.

#### Enable SafeMode Snapshots on FlashBlade

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

#### Estimate Capacity Requirements

To estimate the capacity required for SafeMode snapshots, you need the baseline size, daily change rate, and expected data reduction rate.



With the captured data:

- Apply the reduction rate to the daily change rate and multiply it by the number of days you will retain the SafeMode snapshots.
- Add the baseline size to calculate the total expected capacity required for SafeMode snapshot implementation.

Here's an example:

- In an environment with 300TiB of data, the baseline size after initial data reduction is 180TiB.
- If the daily change rate is 10TiB and data reduction is 2:1, the overall backup change rate is 5TiB per day.
- Across a seven-day retention period, there would be 35TiB of data change, plus another 35TiB kept in snapshots. The total additional capacity would be 250TiB.

**NOTE:** Reach out to the Pure Storage and Cohesity sales teams for assistance with estimating the right storage requirements.

## SafeMode Procedures

### Executing SafeMode Snapshots

To create a useful and consistent SafeMode snapshot of the backup copies, metadata, and configuration data, it is important to quiesce the services on the FlashRecover cluster. The current workflow requires manual intervention to perform the SafeMode snapshot.

To successfully create SafeMode snapshots on the FlashRecover//S clusters, use the following steps:

1. Login to the ssh console
  - a. Log in to any one of the nodes of the cluster using the support user access.
2. Create the cluster snapshot
  - a. Issue the `iris_cli` command:

```
iris_cli cluster create-snapshot cluster-id=<your_cluster_id> snapshot-
version=myVersion<myversion_is_optional>
```

- b. Here's an example of the command executed on a test clusters:

```
[support@restricted-ms-ransomware-cc14210033-node-1 ~]\> iris_cli cluster create-snapshot
cluster-id=2005807841383984 snapshot-version=demo-wp
Username: admin
'admin' Password:
MESSAGE                               : Cluster create snapshot request is accepted. Use command
"snapshot_helper create-snapshot-status" on this node to monitor the create snapshot status.
```





Check for the create snapshot success alert (CE03401120) before performing other cluster operations.

If the optional parameter snapshot version is not provided, the system will dynamically generate the timestamp-based snapshot version.

The FlashRecover cluster will:

1. Validate the create snapshot command
2. Logically stop the background cluster services
3. Perform an internal backup of the node local data to the appropriate FlashBlade filesystem
4. Create the SafeMode snapshot on the FlashBlade automatically.

During this process, the FlashRecover cluster services are logically stopped; hence, the `iris_cli` command line will be paused as well. A standalone tool, `snapshot_helper`, is available on the FlashRecover cluster to probe the status and any errors in the snapshot creation process.

Here's an example where the progress can be checked using `snapshot_helper`:

```
[support@restricted-ms-ransomware-cc14210033-node-1 ~]\> snapshot_helper create-snapshot-status
Request: Cluster Create Snapshot
Status: Waiting for stopping cluster services.
```

When the FlashRecover cluster services are stopped, the create snapshot command will trigger a snapshot on the corresponding configured FlashRecover filesystem on FlashBlade, as shown in Figure 3.

The screenshot displays the 'FlashRecover\_FBNFS\_DATA\_2005807841383984-57329-1' filesystem details. The 'File System Snapshots' table at the bottom contains the following data:

Name	Source Location	Source Name	Policy	Created
FlashRecover_FBNFS_DATA_2005807841383984-57329-1.demo-wp	sn1-fb-d01-29	FlashRecover_FBNFS_DATA_2005807841383984-57329-1		2022-10-06 15:42:03

The snapshot entry is circled in red, and a 'Destroyed (0)' link is visible below the table.

Figure 3: FlashRecover filesystem snapshot view



Once the snapshot creation on FlashBlade is successful, the cluster services will dynamically restart. Here's what the snapshot\_helper status would look like:

```
[support@restricted-ms-ransomware-cc14210033-node-1 ~]\> snapshot_helper create-snapshot-status
Request: Cluster Create Snapshot
Status: Waiting for starting cluster services.
```

Upon successful completion of the SafeMode snapshot creation process, an info alert will be generated, as shown in Figure 4.

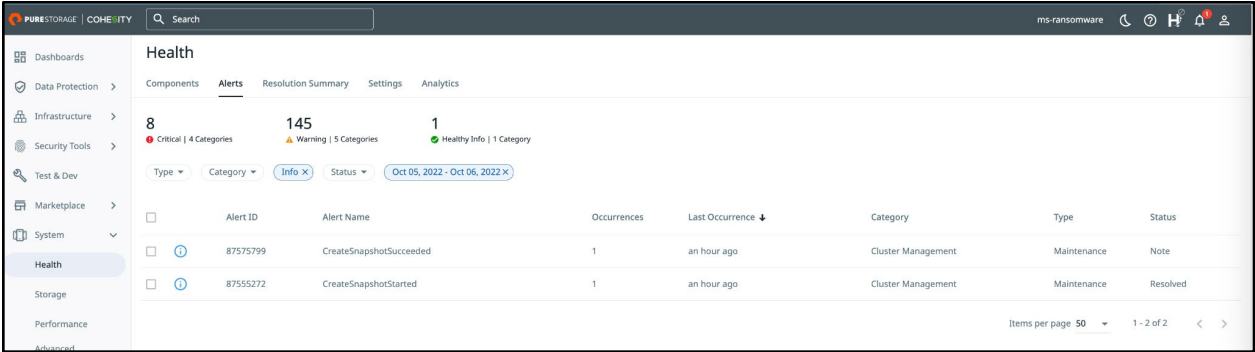


Figure 4: Successful creation of SafeMode snapshot on FlashBlade

The info alert shows that the SafeMode snapshot has been successfully created on the FlashRecover//S.

SafeMode Recovery Process

When faced with a ransomware event, SafeMode snapshots can be leveraged to bring the cluster back to a known-good state. This section details the procedure to recover FlashRecover data backed up on FlashBlade.

The following flow diagram (Figure 5) outlines the SafeMode snapshot recovery process.

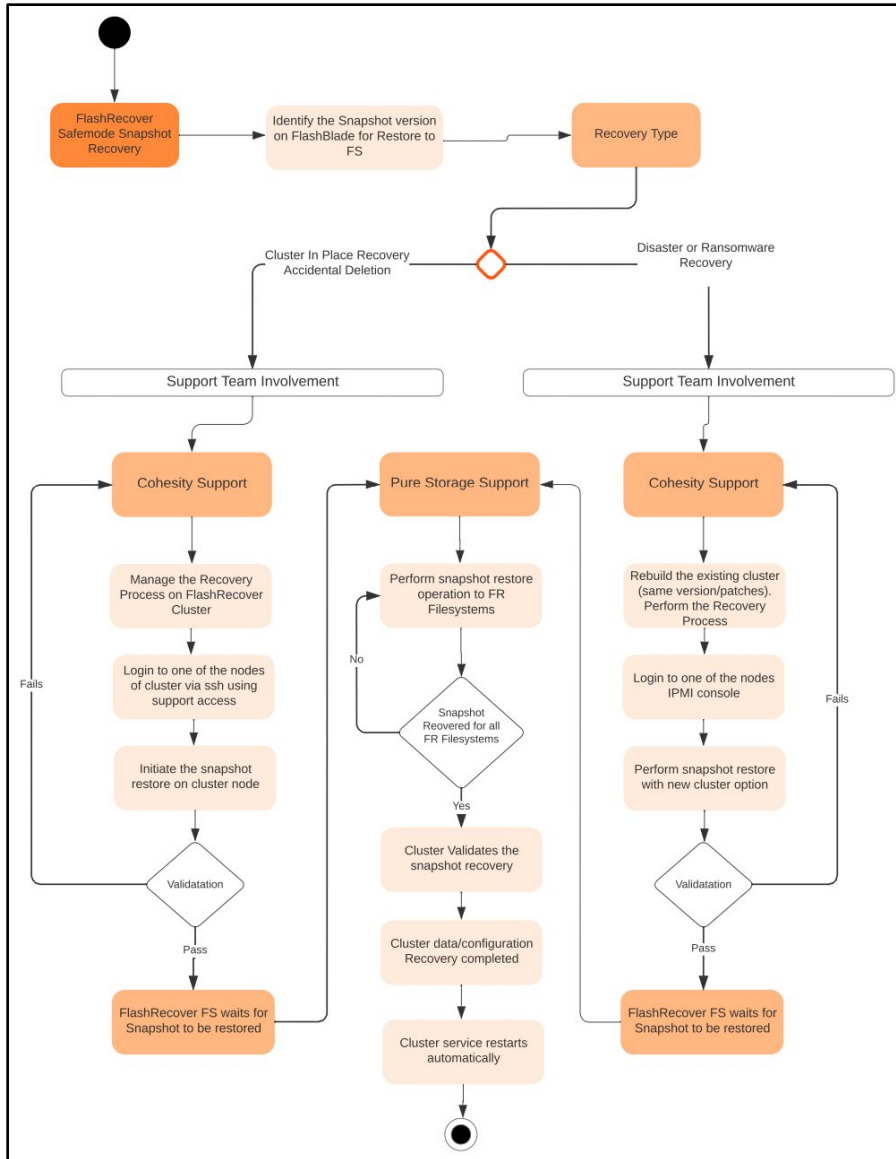


Figure 5: SafeMode Process Flow Diagram

Let's breakdown the flow diagram discussion into the following disaster recovery scenarios: leveraging SafeMode recovery on an existing cluster and leveraging SafeMode recovery on a newly built cluster.

### Leverage SafeMode Recovery on An Existing Cluster

In a DR scenario where the SafeMode recovery needs to be performed on an existing cluster, here are the steps that are needed:

1. Contact Pure Storage Support and Cohesity Support
  - a. When an attack is identified, the authorized administrator on FlashRecover must contact Cohesity support and Pure Storage support right away.
  - b. Cohesity support should administer the recovery process on the FlashRecover cluster.



- c. Pure Storage support can change the snapshot schedule and retention to ensure your data remains available during recovery and will assist in restoring the identified SafeMode snapshots on the FlashBlade. This is especially important if you need to recover from an older snapshot.
2. Log in to a FlashRecover Cohesity node via ssh
  - a. Log in into any node of the FlashRecover cluster via ssh using the support user Access.
3. Restore the cluster snapshot
  - a. Identify the snapshot version that needs to be restored, and work with the Cohesity support team in the restore process.

The following is an example of the SafeMode snapshot restore performed on a test cluster:

```
[support@restricted-ms-ransomware-cc14210033-node-1 ~]\> iris_cli cluster restore-snapshot cluster-
id=2005807841383984 snapshot-version=demo-wp
Username: admin
'admin' Password:
MESSAGE                               : Cluster restore snapshot request is accepted. Use command
"snapshot_helper restore-snapshot-status" on this node to monitor the restore snapshot status. Wait
until the status becomes "Waiting for file system snapshots are restored on the FlashBlade by the
user." to perform the manual file system snapshots restore on the FlashBlade. Check for the restore
snapshot success alert (CE03401123) before performing other cluster operations.
```

In Step 3, the FlashRecover cluster will:

- Validate the restore snapshot command
- Process the pre-restore operations on the FlashRecover cluster, for example stopping the cluster services
- Wait for the snapshots to be restored on FlashBlade

**NOTE:** It is essential that in Step 3, Pure Storage support is contacted to assist and perform the restore of the snapshots for the list of the FlashRecover filesystems.

During the restore process the cluster services will be stopped and the `iris_cli` command will be paused as well. The snapshot helper can be used to check the restore process, as shown in the following example:

```
[support@restricted-ms-ransomware-cc14210033-node-1 ~]\> snapshot_helper restore-snapshot-status
Request: Cluster Restore Snapshot
Status: Waiting for stopping cluster services.
```

### Snapshot Rollback

The `snapshot_helper restore-snapshot-status` becomes "Waiting for file system snapshots are restored on the FlashBlade by the user" as shown in Figure 6:



```
[support@restricted-ms-ransomware-cc14210033-node-1 ~]\> snapshot_helper restore-snapshot-status
Request: Cluster Restore Snapshot
Status: Waiting for file system snapshots are restored on the FlashBlade by the user. Pending file systems:
FlashRecover_FBNFS_DATA_2005807841383984-57329-11
FlashRecover_FBNFS_DATA_2005807841383984-57329-9
FlashRecover_FBNFS_INDEX_2005807841383984-57329-4
FlashRecover_FBNFS_LOCAL_2005807841383984-57329-2
FlashRecover_FBNFS_LOCAL_2005807841383984-57329-3
FlashRecover_FBNFS_METADATA_2005807841383984-57329-2
FlashRecover_FBNFS_METADATA_2005807841383984-57329-4
FlashRecover_FBNFS_DATA_2005807841383984-57329-16
FlashRecover_FBNFS_DATA_2005807841383984-57329-17
FlashRecover_FBNFS_DATA_2005807841383984-57329-2
FlashRecover_FBNFS_DATA_2005807841383984-57329-3
FlashRecover_FBNFS_METADATA_2005807841383984-57329-3
FlashRecover_FBNFS_DATA_2005807841383984-57329-21
FlashRecover_FBNFS_DATA_2005807841383984-57329-22
FlashRecover_FBNFS_DATA_2005807841383984-57329-5
FlashRecover_FBNFS_LOCAL_2005807841383984-57329-1
FlashRecover_FBNFS_METADATA_2005807841383984-57329-1
FlashRecover_FBNFS_DATA_2005807841383984-57329-1
FlashRecover_FBNFS_DATA_2005807841383984-57329-12
FlashRecover_FBNFS_DATA_2005807841383984-57329-23
FlashRecover_FBNFS_INDEX_2005807841383984-57329-1
FlashRecover_FBNFS_DATA_2005807841383984-57329-18
FlashRecover_FBNFS_DATA_2005807841383984-57329-20
FlashRecover_FBNFS_DATA_2005807841383984-57329-4
FlashRecover_FBNFS_DATA_2005807841383984-57329-13
FlashRecover_FBNFS_DATA_2005807841383984-57329-19
FlashRecover_FBNFS_DATA_2005807841383984-57329-6
FlashRecover_FBNFS_DATA_2005807841383984-57329-8
FlashRecover_FBNFS_LOCAL_2005807841383984-57329-4
FlashRecover_FBNFS_DATA_2005807841383984-57329-10
FlashRecover_FBNFS_DATA_2005807841383984-57329-14
FlashRecover_FBNFS_DATA_2005807841383984-57329-15
FlashRecover_FBNFS_DATA_2005807841383984-57329-24
FlashRecover_FBNFS_DATA_2005807841383984-57329-7
FlashRecover_FBNFS_INDEX_2005807841383984-57329-2
FlashRecover_FBNFS_INDEX_2005807841383984-57329-3
[support@restricted-ms-ransomware-cc14210033-node-1 ~]\>
```

Figure 6: Snapshot\_helper restore-snapshot-status

Pure Storage support will restore the snapshot of the affected FlashRecover filesystems on FlashBlade. The `snapshot_helper restore-snapshot-status` command can be used to query a list of filesystems that are still pending restore from snapshot.

In the following example, we can see that part of the filesystem snapshot is restored and any pending filesystems that still need to be restored for the recovery to be successful:

```
[support@restricted-ms-ransomware-cc14210033-node-1 ~]\> snapshot_helper restore-snapshot-status
Request: Cluster Restore Snapshot
Status: Waiting for file system snapshots are restored on the FlashBlade by the user. Pending file
systems:
FlashRecover_FBNFS_INDEX_2005807841383984-57329-4
FlashRecover_FBNFS_LOCAL_2005807841383984-57329-2
FlashRecover_FBNFS_LOCAL_2005807841383984-57329-3
FlashRecover_FBNFS_METADATA_2005807841383984-57329-2
FlashRecover_FBNFS_METADATA_2005807841383984-57329-4
FlashRecover_FBNFS_METADATA_2005807841383984-57329-3
FlashRecover_FBNFS_LOCAL_2005807841383984-57329-1
FlashRecover_FBNFS_METADATA_2005807841383984-57329-1
FlashRecover_FBNFS_INDEX_2005807841383984-57329-1
```



```
FlashRecover_FBNFS_LOCAL_2005807841383984-57329-4
FlashRecover_FBNFS_INDEX_2005807841383984-57329-2
FlashRecover_FBNFS_INDEX_2005807841383984-57329-3
[support@restricted-ms-ransomware-cc14210033-node-1 ~]\>
```

The restore-snapshot operation keeps monitoring the filesystems; when it detects that all the filesystems are restored from the specified version on FlashBlade, the operation will continue to restore node configuration data from the restored filesystems on the FlashBlade, and then automatically restart the cluster services, as shown in Figure 7.

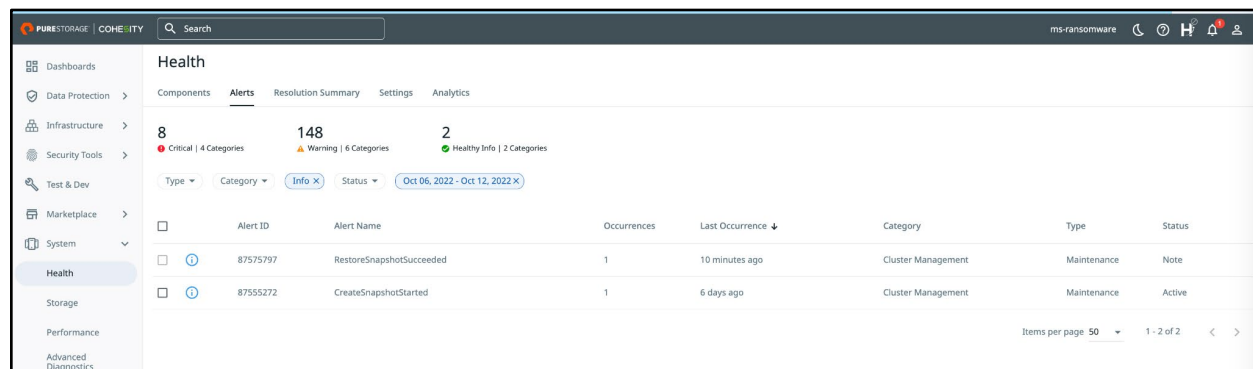
```
[support@restricted-ms-ransomware-cc14210033-node-1 ~]\> snapshot_helper restore-snapshot-status
Request: Cluster Restore Snapshot
Status: Restoring node local data from backup in remote storage.

[support@restricted-ms-ransomware-cc14210033-node-1 ~]\> snapshot_helper restore-snapshot-status
Request: Cluster Restore Snapshot
Status: Restoring node local data from backup in remote storage.

[support@restricted-ms-ransomware-cc14210033-node-1 ~]\>
```

Figure 7: snapshot\_helper restore-snapshot\_status

After the operation completes, the snapshot\_helper restore-snapshot status will show “Unable to get restore snapshot status because restore snapshot operation is currently not running on the node.” The user will receive a RestoreSnapshotSucceeded alert as shown in Figure 8. For data consistency, if the restore operation fails, the cluster won’t start automatically; it will need manual intervention from the Cohesity support team.



Alert ID	Alert Name	Occurrences	Last Occurrence	Category	Type	Status
87575797	RestoreSnapshotSucceeded	1	10 minutes ago	Cluster Management	Maintenance	Note
87555272	CreateSnapshotStarted	1	6 days ago	Cluster Management	Maintenance	Active

Figure 8: Alert for snapshot creation and successful restore

## Leverage SafeMode Recovery on a Newly Built Cluster

In this section, let’s explore the steps that are required to use SafeMode recovery on a newly built cluster. For an overview of this procedure, refer to the flow diagram (Figure 5). The steps involve:

1. Involve Cohesity Support
2. Logging in to a node in the cluster via the ipmi console
3. Initiating the cluster restore
4. Snapshot rollback



Cohesity Support

To perform a complete disaster recovery from SafeMode snapshot on a new cluster, you must rebuild the original FlashRecover cluster with the same version (with applicable patches) and the same hardware configuration as that on which the snapshots were performed. It is required that you reach out to the Cohesity support team.

- Record the cluster-id information for the older cluster. This is required to perform the recovery.
- After the FlashRecover cluster is built, do not register the FlashBlade to the cluster.

Figures 9 and 10 show the older version of the test cluster and the corresponding newly built test cluster for disaster recovery.

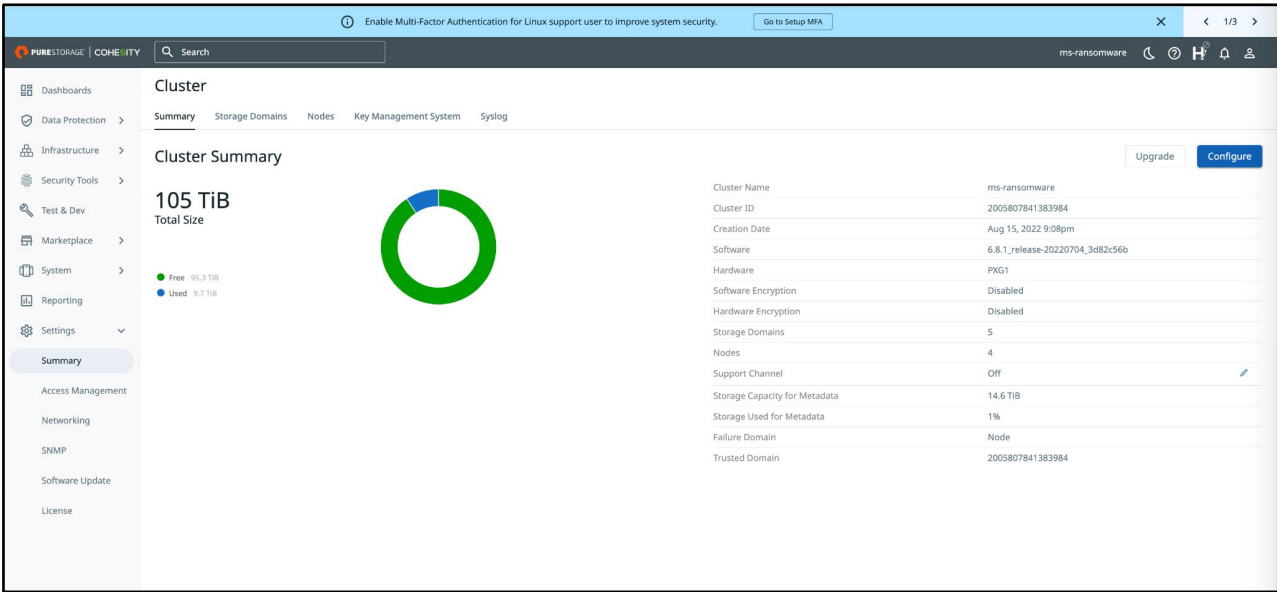


Figure 9: Older Version of the Cluster

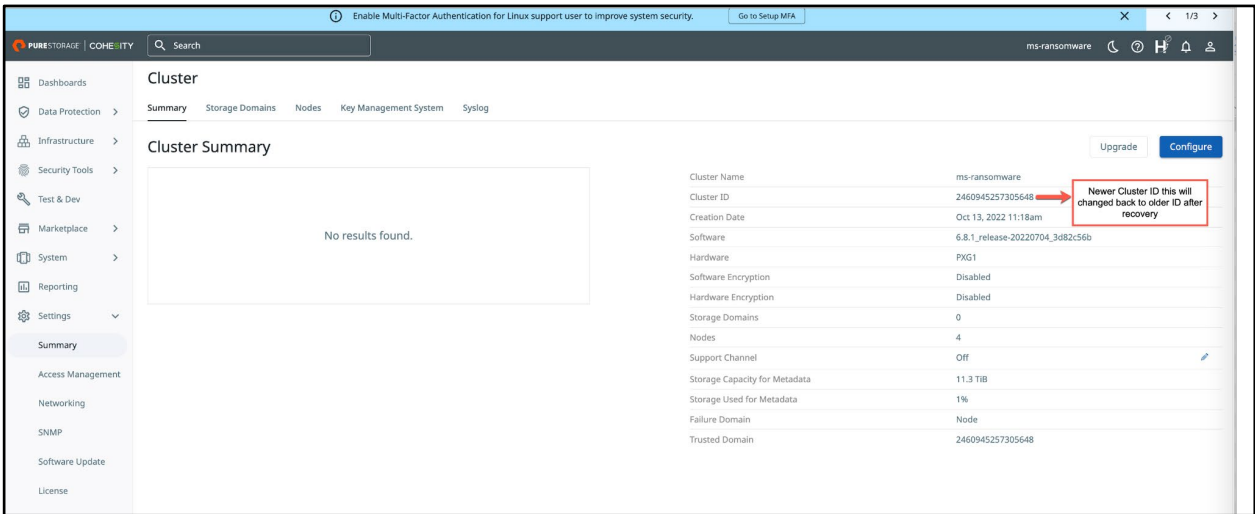


Figure 10: Rebuilt cluster for Disaster Recovery

Log in to a Node in the Cluster via the ipmi Console

For the initial version of this feature, manual intervention is required to perform the recovery of the entire cluster including backup data, metadata, and cluster configuration.



**IMPORTANT:** The authorized administrator must involve the Cohesity Support team to initiate the recovery process and will need access to one of the node IPMI consoles to perform the recovery steps as shown below Figure 11.

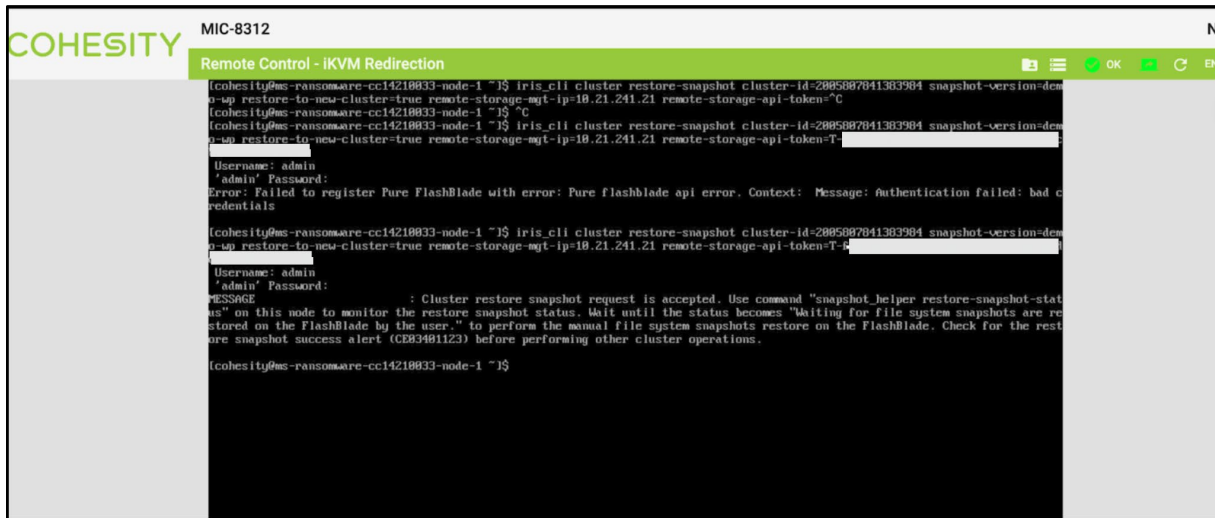


Figure 11: IPMI console for DR Recovery

### Initiate the Cluster Restore

Identify which snapshot version needs to be restored and work with the Cohesity support team for assistance in the restore process.

The `iris_cli restore-snapshot` command shown below needs to be executed as a Cohesity user on the Cohesity IPMI console node.

```
iris_cli cluster restore-snapshot cluster-id=cluster_id snapshot-version=previous_snapshot_version
restore-to-new-cluster=true remote-storage-mgt-ip=FB_ip remote-storage-api-token=FB_api_token
```

Note that `cluster-id` is the older cluster-id information that you have saved in the previous step.

Alternatively, you can grab it from the FlashRecover file system naming convention created on FlashBlade. For example, in a filesystem name `FlashRecover_FBNFS_DATA_2005807841383984-57329-1` the number "2005807841383984" is the older FlashRecover cluster-id information.

The `restore-snapshot` command also requires the management IP address and the token id of the FlashBlade. To get the FlashBlade api token id you can log in to the FlashBlade console and run the command `pureadmin list --api-token --expose`.

Here is an example of the command executed on one of the test clusters on a previously created snapshot in Figure 12.





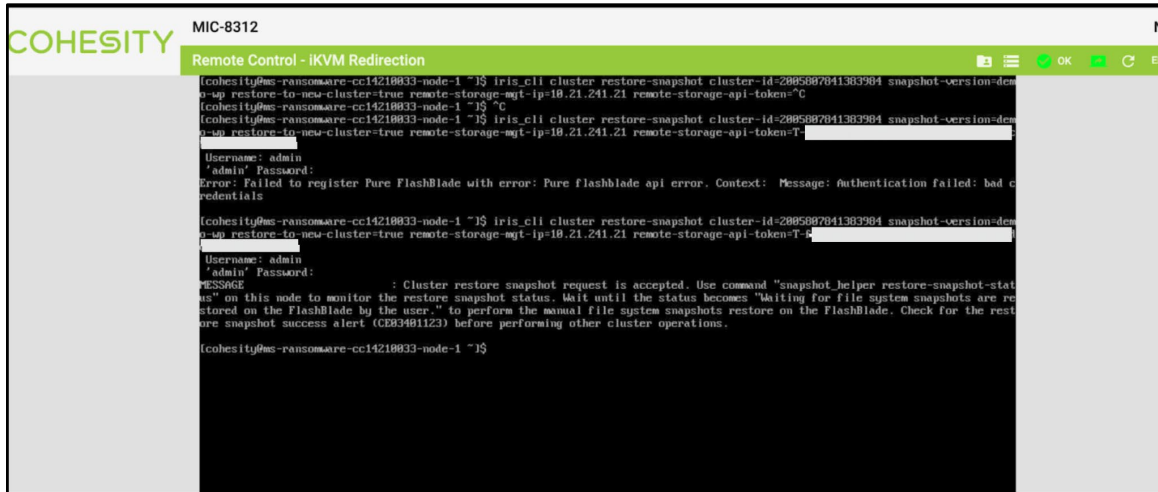


Figure 12: Restore command Execution on IPMI console

The FlashRecover cluster:

1. Validates the restore snapshot command
2. Starts processing the pre-restore operations on the cluster such as stopping the cluster services
3. Waits for the snapshots to be restored on FlashBlade

At this point Pure Storage support must restore the snapshot for the list of the FlashRecover filesystems. During the restore process the cluster services will be stopped and the `iris_cli` command will be paused as well. The `snapshot_helper` tool can be used to check the restore snapshot progress, as shown in Figure 13:

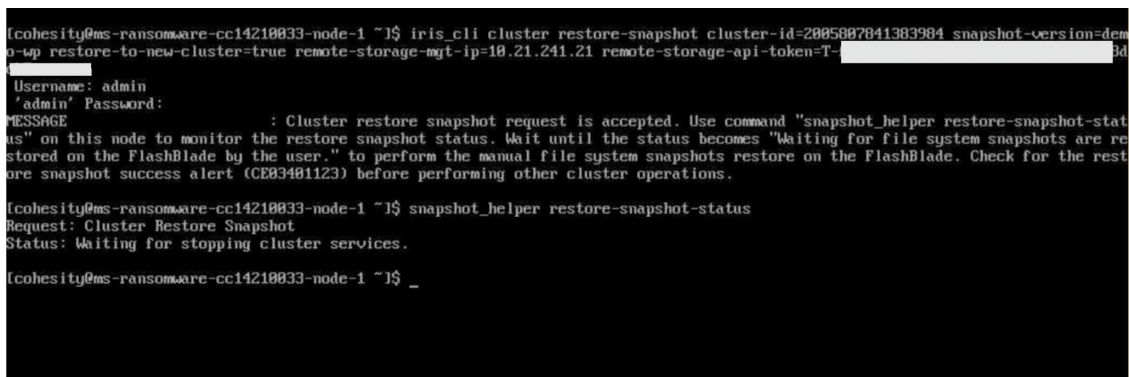


Figure 13: Snapshot Restore status

### Snapshot Rollback

At this point, the authorized administrator should contact Pure Storage support for snapshot restore on FlashRecover filesystems on FlashBlade.

The `snapshot_helper restore-snapshot-status` becomes "Waiting for file system snapshots are restored on the FlashBlade by the user."

Pure Storage support will restore the snapshot of the affected filesystems on FlashBlade. The `restore-snapshot` operation keeps monitoring the filesystems. When it detects that all the filesystems are restored from the specified version on



FlashBlade, the operation will continue to restore node configuration data from the restored filesystems on the FlashBlade, and then automatically restart the cluster services, as shown in Figure 14.

```
icohesity@ms-ransomware-cc14210033-node-1 ~$ snapshot_helper restore-snapshot-status
Request: Cluster Restore Snapshot
Status: Waiting for file system snapshots are restored on the FlashBlade by the user. Pending file systems:
lashRecover_FBNFS_DATA_2005087041383904-57329-19
lashRecover_FBNFS_DATA_2005087041383904-57329-20
lashRecover_FBNFS_INDEX_2005087041383904-57329-1
lashRecover_FBNFS_LOCAL_2005087041383904-57329-2
lashRecover_FBNFS_DATA_2005087041383904-57329-8
lashRecover_FBNFS_DATA_2005087041383904-57329-9
lashRecover_FBNFS_METADATA_2005087041383904-57329-1
lashRecover_FBNFS_LOCAL_2005087041383904-57329-4
lashRecover_FBNFS_DATA_2005087041383904-57329-10
lashRecover_FBNFS_DATA_2005087041383904-57329-21
lashRecover_FBNFS_DATA_2005087041383904-57329-7
lashRecover_FBNFS_LOCAL_2005087041383904-57329-3
lashRecover_FBNFS_DATA_2005087041383904-57329-12
lashRecover_FBNFS_DATA_2005087041383904-57329-14
lashRecover_FBNFS_DATA_2005087041383904-57329-16
lashRecover_FBNFS_DATA_2005087041383904-57329-17
lashRecover_FBNFS_LOCAL_2005087041383904-57329-1
lashRecover_FBNFS_METADATA_2005087041383904-57329-2
lashRecover_FBNFS_METADATA_2005087041383904-57329-3
lashRecover_FBNFS_METADATA_2005087041383904-57329-4
lashRecover_FBNFS_DATA_2005087041383904-57329-22
lashRecover_FBNFS_DATA_2005087041383904-57329-24
lashRecover_FBNFS_DATA_2005087041383904-57329-4
lashRecover_FBNFS_INDEX_2005087041383904-57329-2
lashRecover_FBNFS_DATA_2005087041383904-57329-6
lashRecover_FBNFS_DATA_2005087041383904-57329-15
lashRecover_FBNFS_DATA_2005087041383904-57329-2
lashRecover_FBNFS_DATA_2005087041383904-57329-23
lashRecover_FBNFS_DATA_2005087041383904-57329-3
lashRecover_FBNFS_INDEX_2005087041383904-57329-3
lashRecover_FBNFS_INDEX_2005087041383904-57329-4
lashRecover_FBNFS_DATA_2005087041383904-57329-1
lashRecover_FBNFS_DATA_2005087041383904-57329-11
lashRecover_FBNFS_DATA_2005087041383904-57329-13
lashRecover_FBNFS_DATA_2005087041383904-57329-5
lashRecover_FBNFS_DATA_2005087041383904-57329-10
icohesity@ms-ransomware-cc14210033-node-1 ~$ snapshot_helper restore-snapshot-status
Request: Cluster Restore Snapshot
Status: Restoring node local data from backup in remote storage.
icohesity@ms-ransomware-cc14210033-node-1 ~$
```

Pure Storage Support Needs to Restore the specified Snapshot for restore to FlashRecover Filesystem on FlashBlade

Figure 14: Restore snapshot progress

After the restore snapshot operation succeeds, the cluster alert “restore snapshot succeeded” will be generated, as shown in Figure 15.

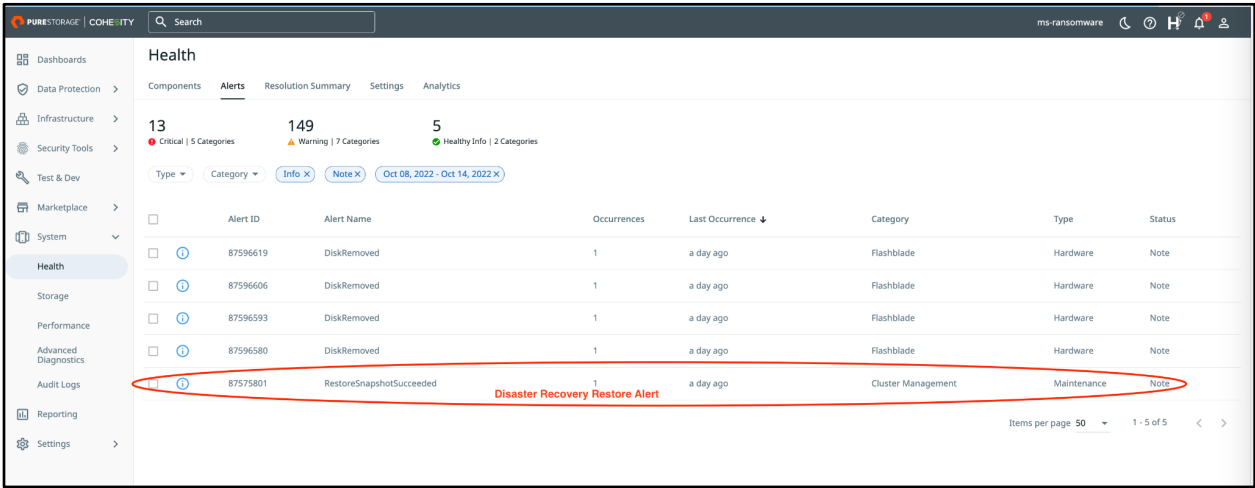


Figure 15: Restore Snapshot Succeeded alert

At this point the entire FlashRecover cluster configuration, data and metadata are restored successfully to the state when the snapshots were executed, as shown below Figures 16 and 17.



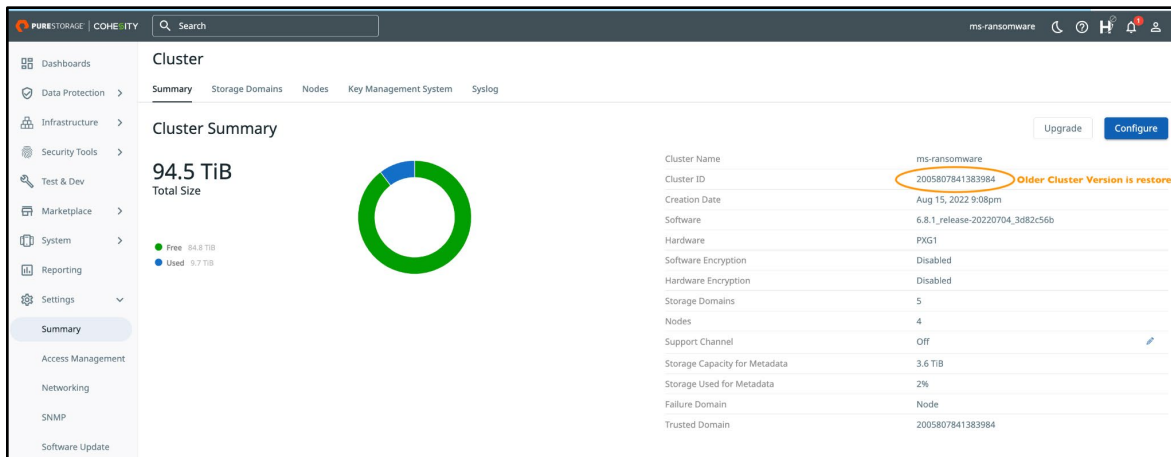


Figure 16: New cluster restored back to the original state

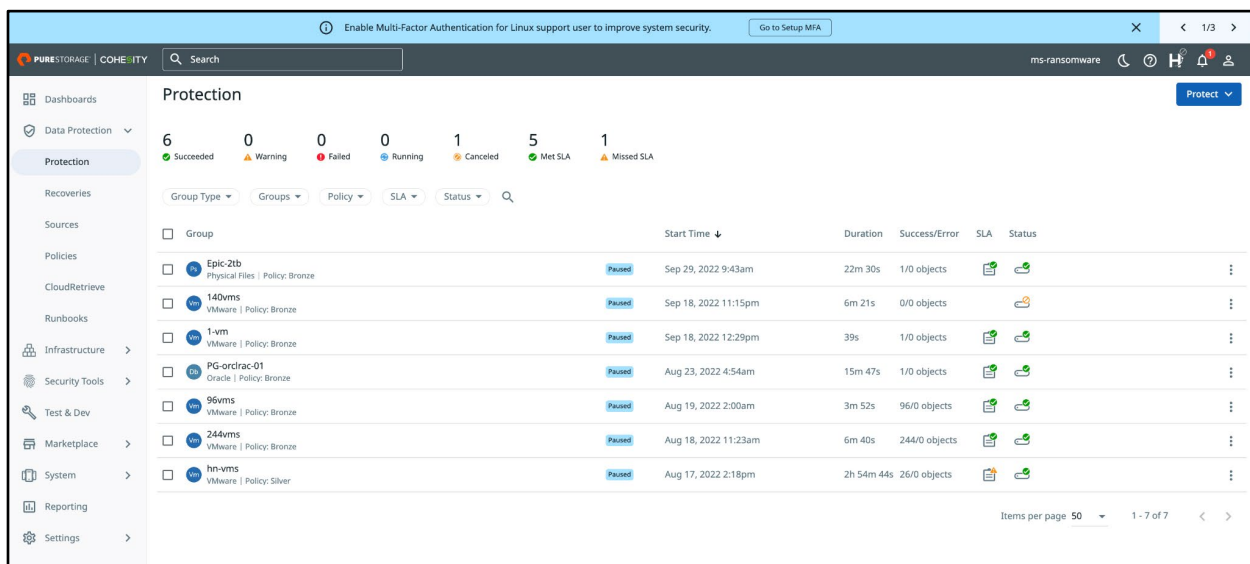


Figure 17: Backup jobs and policy restored

You have successfully restored your FlashRecover//S in a DR scenario with a newly built cluster.

## Conclusion

Pure Storage FlashRecover//S delivers a modern data protection experience, combining the best in flash-based, unified fast file and object (UFFO) storage with industry-leading, data protection from Cohesity. FlashRecover//S gives midsize and enterprise customers alike a highly performant solution designed for fast recoveries at scale.

Using FlashBlade as an NFS storage target for FlashRecover deduplicated data provides a storage-efficient solution for rapid restore at scale for an organization's virtual machines.

FlashRecover is an exclusive integration of Pure Storage FlashBlade with Cohesity DataProtect, delivering power and ease of use:

- Simplified, integrated, and rapid data protection for ransomware and disaster recovery
- Recovery of petabytes of data in hours



## REFERENCE ARCHITECTURE

- Up to three times faster backup and restore throughput than disk-based alternatives
- Recovery of 1,000s of virtual machines (VMs) a day
- Disaggregated compute and storage for independent scaling of backup and recovery processes
- Reuse of backup data on FlashBlade for modern apps

For enterprises that require the ability to do quick backup writes and fast large-scale recoveries of their data and virtual machines, Pure Storage FlashRecover//S delivers top performance.





### About the Author

Mandeep Arora is a Pure Storage Data Protection Solutions Architect and is responsible for defining data protection solutions partnered with various backup applications. He is responsible for defining solutions and reference architectures for primary workloads such as Oracle, SQL, and VMware.

Mandeep has spent over 14 years of his career with the data protection industry, with experience working with various data protection products meant for small and medium businesses as well as large enterprises. He started his career with IBM Tivoli Storage Manager in the core software development and test team, followed by Isilon Systems, where he was responsible for delivering the NAS backup solution to enterprise-class customers. He was also a part of the Veritas storage solutions team and Quorum one click recovery solutions and was responsible for technical relationships and advising partners on data protection for VMware.

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](https://purestorage.com)

800.379.PURE

