COHESITY | LASER VAULT

Version 1.0

April 2025

Protect IBM Power Systems iSeries with Cohesity using LaserVault ViTL

ABSTRACT

IBM iSeries Servers, now part of the broader IBM Power Systems family, are designed to handle mission-critical workloads with a focus on security, reliability, and control. IBM iSeries is a fully integrated operating system, database, middleware, security, runtime and hypervisor are all integrated into the stack and licensed as one. This integration helps clients lower TCO, simplify systems management, and do more with fewer resources. This guide will walk you through the process of setting up Cohesity Data Cloud, which is simple, secure, scalable and AI/ML-ready, offering much-needed data protection, security, mobility, access, and insights to IBM iSeries workloads.

Table of Contents

Figures

Using Cohesity with LaserVault ViTL

ViTL is the virtual tape library solution from LaserVault, designed specifically for IBM Power Systems. It simplifies backup and recovery operations by saving backups to hard drive, NAS, SAN, deduplication appliance or the cloud - no more physical tape required. ViTL reduces storage costs with its deduplication feature and integrates seamlessly via Fibre Channel or SAS with iSeries, AS/400, System i, Linux or AIX systems. It runs on a Microsoft Windows server. It attaches to one or several iSeries servers via FC and emulates up to dozens of tape devices.

IBM iSeries Servers, now part of the broader IBM Power Systems family, are designed to handle mission-critical workloads with a focus on security, reliability, and control.

IBM i is a fully integrated operating system; the database, middleware, security, runtime, and hypervisor are all integrated into the stack and licensed as one.

This integration helps clients lower TCO, simplify systems management, and do more with fewer resources.

LaserVault ViTL is a Fibre Channel or SAS-connected non-flash, hybrid, or all flash appliance that appears as a tape library to IBM Power Systems host (AS/400, iSeries, System i, AIX, Linux) automating the backup & recovery process.

Users can seamlessly replace your existing tape library with ViTL, continuing backup and restore operations without the need for programming changes.

Supporting QLogic 8, 16, 32 and 64Gb HBA, ViTL enables NPIV to emulate multiple devices (tape drives/tape libraries) over a single physical connection. This optimizes bandwidth utilization, enhances capacity management, and reduces overhead, maximizing the efficiency of your Fibre Channel connection.

LaserVault ViTL is compatible with BRMS, Robot Save, and other backup software. Virtual tapes are recognized as standard tape media by IBM i and your backup software, giving you more flexibility with additional drives and slots without the need for extra hardware.

LaserVault ViTL serves as a crucial gateway that enables seamless storage of IBM i backups on your Cohesity deduplication appliance.

LaserVault ViTL offers more cartridges and drives for a lower cost compared to other VTLs, delivering greater value at a competitive price.

For enhanced security and reliability, you can pair ViTL's virtual tape with physical tape for an extra layer of protection. This hybrid solution safeguards your critical data with immutable backups that prevent unauthorized changes and data loss, further complementing ViTL's built-in data protection features.

ViTL Requirements:

- IBM Power System (iSeries, AS/400, System i, AIX, Linux)
- Any OS/400 version capable of Fibre Channel (FC) or SAS (Serial Attached SCSI)
- Fibre Channel (NPIV support for 8, 16, 32, and 64Gb FC) or SAS connection (Serial Attached SCSI)
- LaserVault connectivity to Cohesity DataProtect Cluster with 10Gbe or 40Gbe ethernet link for matching speed from IBM iSeries

The complete ViTL solution includes both hardware and software, featuring a Windows server appliance that connects via Fibre Channel or SAS. ViTL is also available as a software only option, compatible with your existing hardware or virtual machine (VM).

When LaserVault customers use Cohesity as the storage repository for their backups, they benefit immediately from Cohesity's many features:

- **Web-scale.** Capacity grows with your business.
- **Performance.** Improved backup and restore times.
- **Storage efficiency.** Extremely high storage efficiency with global, variable-length deduplication and compression.
- **Security.** Data is always secure and encrypted both at rest and in flight. A Cohesity File-level DataLock provides additional security checks on the view's configuration.
- **Resilience.** Highly resilient, fault-tolerant architecture.

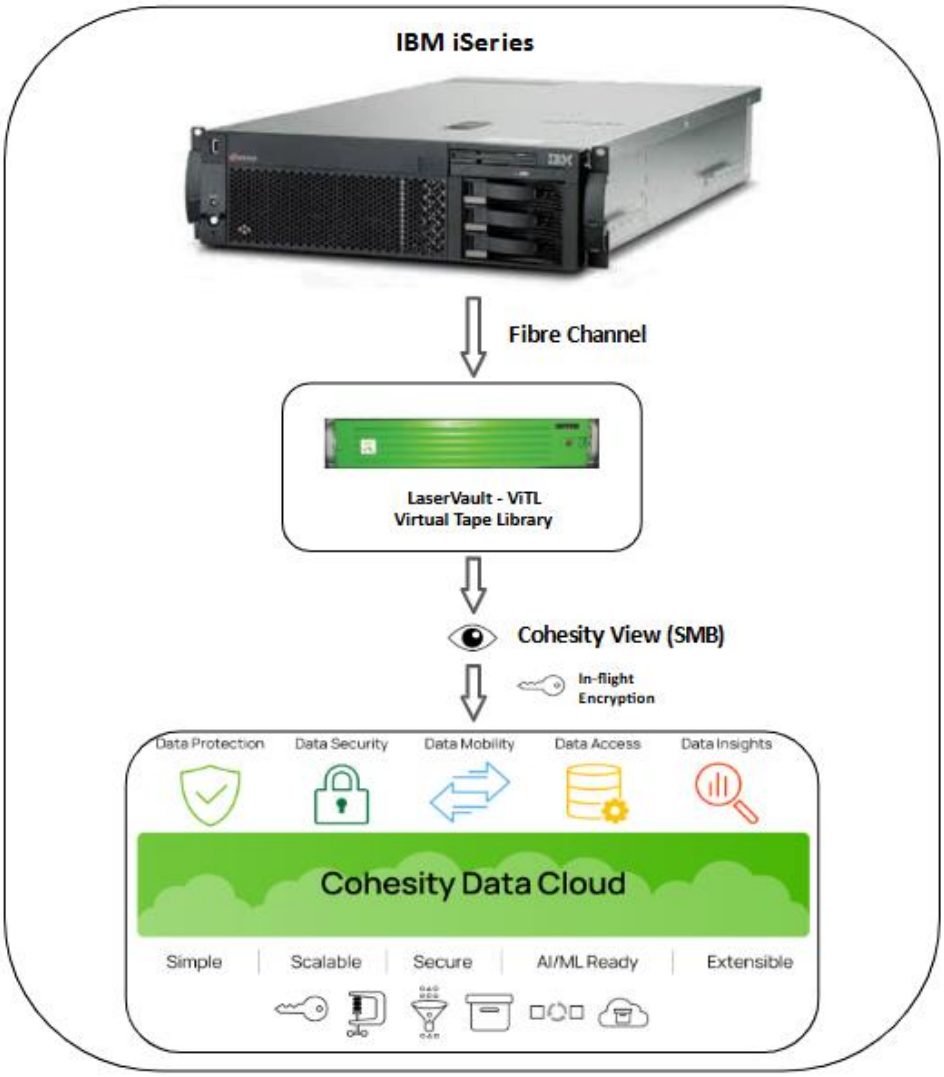
This guide focuses on IBM iSeries systems, which hosts mission-critical services and whose backup target is tape, especially the ViTL Virtual Tape Controller from LaserVault. Due to its high data change rate and throughput, it uses FC connections to backup to Virtual Tape Controllers. The LaserVault ViTL host (Windows Server) uses recommended FC HBAs. The choice of card depends on the bandwidth requirements of both IBM iSeries and LaserVault devices.

You can configure IBM iSeries system backups with LaserVault ViTL using the following paradigms:

- Single IBM iSeries systems connected to Single LaserVault ViTL Server
- Single IBM iSeries systems connected to Multiple LaserVault ViTL Servers
- Multiple IBM iSeries systems connected to a Single LaserVault ViTL Server
- Multiple IBM iSeries systems connected to Multiple LaserVault ViTL Servers

Together, these features provide a complete, reliable web-scale data protection solution. Our solution uses Cohesity's SMB Views as a single or scale-out storage repository for LaserVault ViTL. Combining LaserVault ViTL with Cohesity provides a comprehensive, highly scalable, and flexible backup solution that fits the data protection needs of any size organization.

Figure 1: Cohesity as a Backup Repository of IBM iSeries with LaserVault ViTL



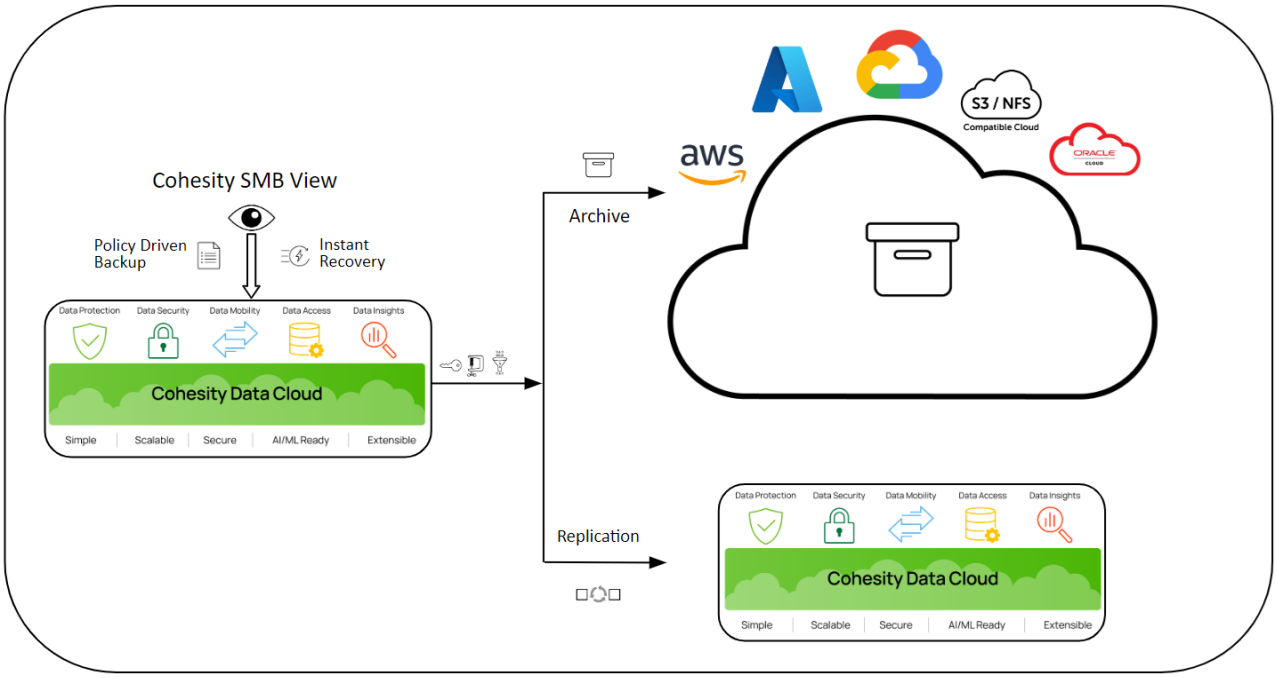
Benefits of Using Cohesity with LaserVault ViTL

Organizations that rely on IBM iSeries systems need a fast, powerful, and simple backup and recovery solution that scales well to grow with their ever-growing data. To meet these needs in a reliable and efficient ecosystem, Cohesity's Distributed architecture provides a solution that eliminates the complexities and operational inefficiencies of traditional NAS protection solutions. The solution unifies your data protection and recovery infrastructure—including target storage, backup, recovery, replication, archiving, and disaster recovery—on a single platform. With Cohesity functioning as a storage target for the virtual tapes. Cohesity cluster handles all the encryption, deduplication, replication, and compression. With Cohesity, you can protect your critical files and directories, ensuring data security, protection, and scalability.

Once you start using Cohesity as a backup repository, you can immediately take advantage of Cohesity's powerful features, including:

- **Live view** of data being written on the Cohesity storage from IBM iSeries systems.
- **Restricted access** to the view by allowing only an authorized set of IP addresses.
- **NTFS permissions** - to restrict access at the File level viz., read/write/modify/delete.
- **Data Immutability** - Once Data is written on Cohesity, it will not be overwritten, also popularly known as WORM (Write Once, Read Many).
- **File-level DataLock** provides additional security on the files in the view. It is the Cohesity WORM (**W**rite **O**nce **R**ead **M**any) feature that locks and retains files in a view.
- **File auditing** to record and monitor events occurring on your SMB view.
- **Inflight Encryption** - Not all vendors offer SMB Encryption. Inflight Encryption enables you to use existing network infrastructure and not create isolated/dark/deadnet infrastructure to avoid man-in-the-middle attacks.
- **Inline deduplication and compression** - Deduplication occurs when the Cohesity cluster writes the data to the Cohesity View, and Compression occurs when the Cohesity cluster saves the blocks to the Cluster.
- **Data Protection** - to take local snapshots of live View.
- **Policy-based data replication** from one cluster to another cluster for disaster recovery.
- **CloudArchive** and **Cloud Retrieve** your data for long-term retention and disaster recovery in AWS, Azure, GCP, NAS, and S3-compatible storage platforms. Use Cloud Tier to reduce TCO.

Figure 2: Benefits of Using Cohesity



Create and Configure Cohesity SMB View

To protect IBM iSeries systems, you need to associate a backup policy. The backup policy includes the backup configuration, a list of File Systems to Volume/Volume Group mappings, backup schedules, and retention rules. This helps invoke IBM iSeries systems backups that land in the LaserVault ViTL Tape Library. A Tape library has multiple Tapes/Tape Drives which are defined on ViTL. The Tape library (defined on ViTL) is the endpoint that maps to the Cohesity SMB share path (which supports both FQDN and VIP). Cohesity provides this SMB share, which is the Cohesity View — web-scale, globally deduplicated, compressed storage. To use a Cohesity View as a storage repository for the IBM iSeries system via LaserVault Virtual Tape Controller, complete the recommended steps below.

To the IBM iSeries system, a LaserVault ViTL virtual tape drive appears as a physical drive connected by SCSI or Fiber Channel. The drive appears as media type L8 (i.e., using LTO Gen 8) by default unless otherwise specified in the Virtual Tape Library internal configuration files. Catalog information is stored in IBM iSeries, which has a mapping of storage pools. Catalog status on both IBM iSeries and LaserVault ViTL must be in SYNC. If it goes out of SYNC, Catalog on iSeries takes precedence over LaserVault ViTL, and the conflict is resolved.

Optimize SMB Performance with GFlags

Before creating a View in Cohesity, Cohesity recommends tuning your Cohesity system settings to optimize SMB performance as follows:

1. See Recommended settings when using Cohesity as a filer in the Cohesity Support portal for more details.
2. Contact Cohesity Support to help you change the settings.

> **IMPORTANT**: If your network equipment supports LACP, Cohesity recommends configuring your Cohesity network data ports to use it. LACP can provide additional network throughput to and from the Cohesity cluster and among its nodes. To take advantage of this, both the network switches and the Cohesity cluster need to be configured for LACP. For instructions, see the Cohesity Networking Quick Start Guide.

Create and configure the View to be shared via SMB. To create an SMB, share to store IBM iSeries system backups:

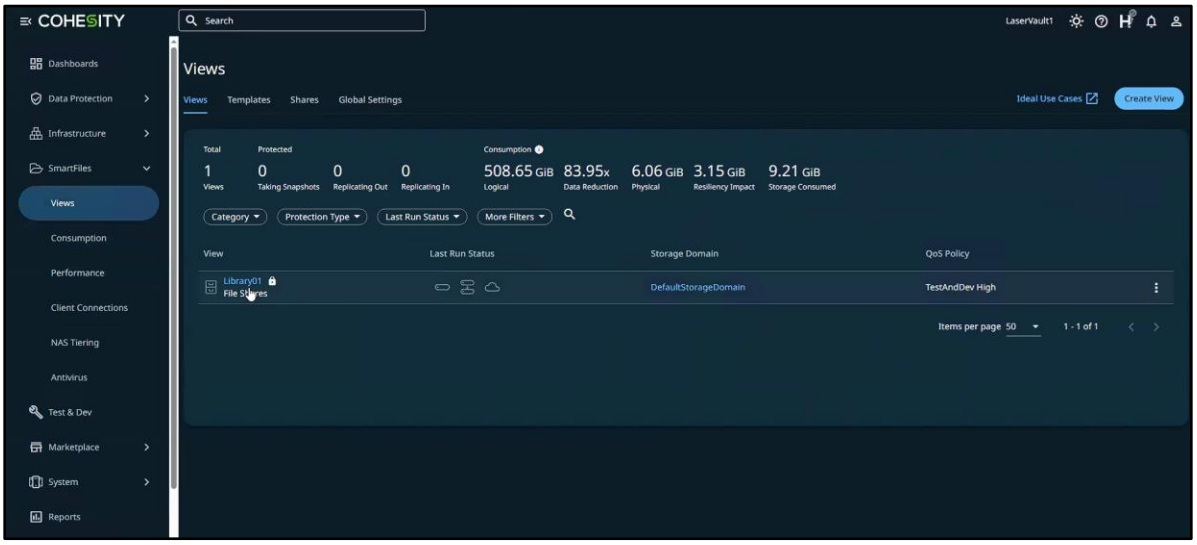
1. Ensure that Cohesity is connected to the Active Directory.
2. Create a Cohesity View, select the Optimal QoS policy, and set SMB access type and permissions. For LaserVault ViTL, Cohesity recommends using the “Test and Dev High” as QoS policy in the Cohesity SMB View.
3. Add a Share Allowlist. If you add more LaserVault ViTLs in the future, ensure they are added to the SMB Share Whitelist/Allowlist in this View.
4. Enable the File DataLock setting to make the files in the view immutable. Cohesity File DataLock has been validated with LaserVault ViTL.

IMPORTANT:

1. While enabling File DataLock, under Manually Lock Using, select the Future A Time option.
2. While choosing the Retention or Lock Period of File DataLock, set it to a period less than the corresponding Backup Expiry time, configured in the Laservault ViTL settings.

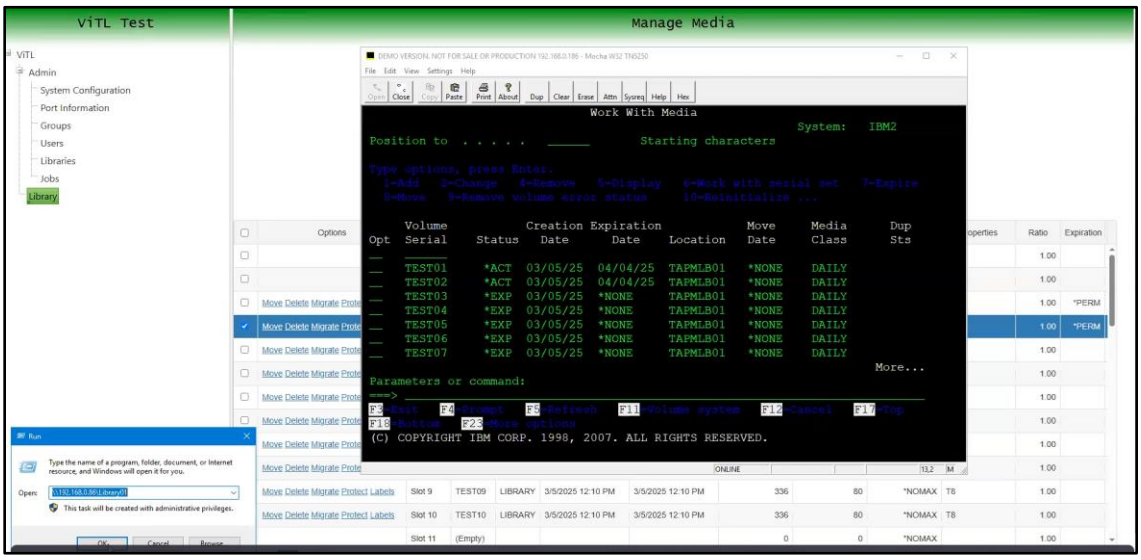
3. Tune Cohesity Cluster to Optimize SMB View for Performance.
4. Configure your LaserVault ViTL to use Cohesity View as IBM iSeries Backup Target.

View on Cohesity Data Cloud



Now that you have created the Cohesity SMB View. Verify that the SMB share (which has the same name as the View) is accessible by using the **\\<vip>\<View_Name>** format on the LaserVault ViTL hosting Windows Server.

Mapping of **Cohesity SMB Share/View** > **ViTL LIBRARY** > **Tape/Tape Drive** > **Volumes on IBM iSeries**.

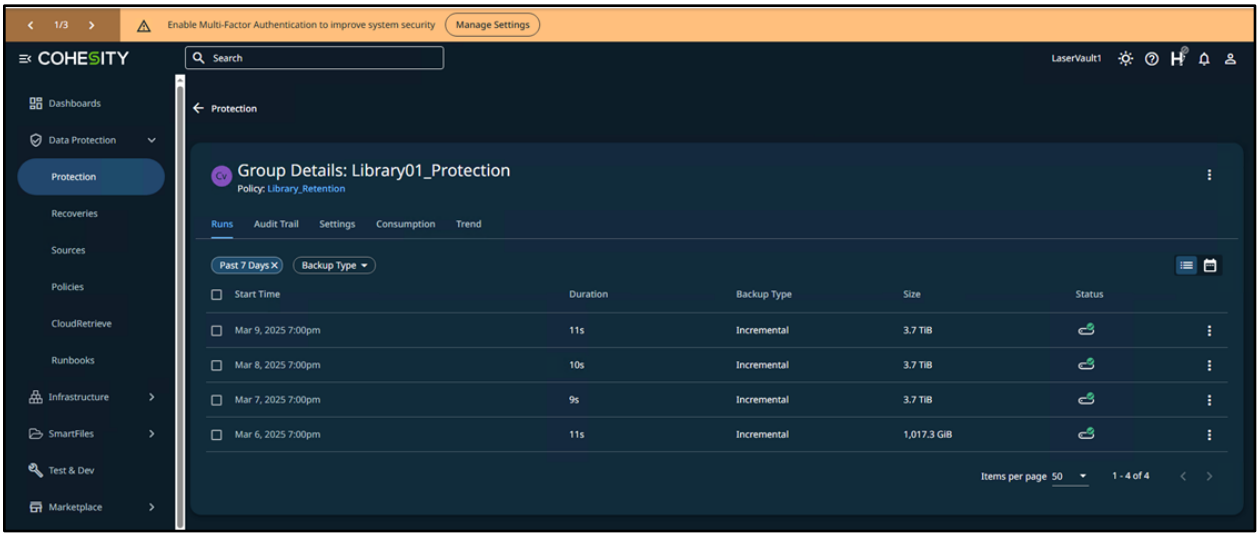


TIP: Should you encounter access issues, which appear most commonly as ‘Access Denied’ and ‘Can’t open for writing’ error messages in LaserVault ViTL, the most likely cause is an issue with the IP allowlist or Active Directory permissions. To troubleshoot these issues, use Cohesity filer audit logging on the Cohesity View, which will indicate the cause. For instructions, see Enable File Services Audit Logs in the online Help.

For this solution, Cohesity recommends that you enable Inflight Encryption, Inline Deduplication, and Inline Compression on the Storage Domain where you create the View.

Setting up Protection Group for ViTL SMB View

Once the SMB view is created, protect the SMB View as shown below with the Protection Group name. Policies can be applied to manage the backups and their retention.



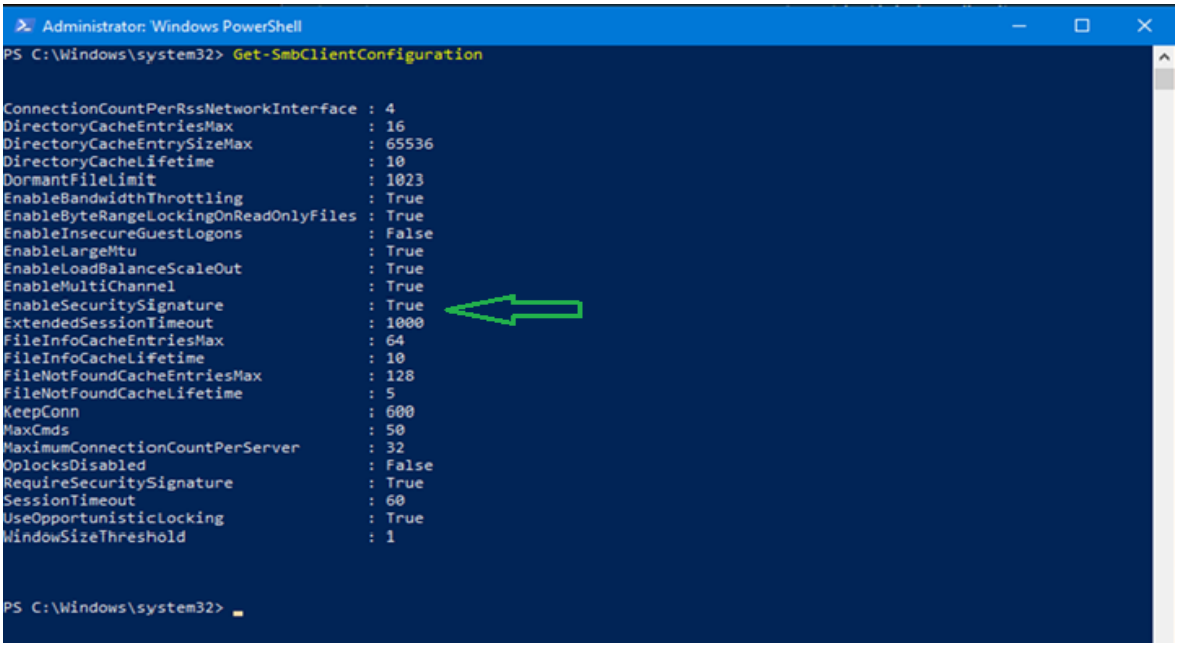
Setting up SMB Signing for ViTL SMB View

Enable ‘SMB Encryption’ on the SMB View created as shown below screen grab.

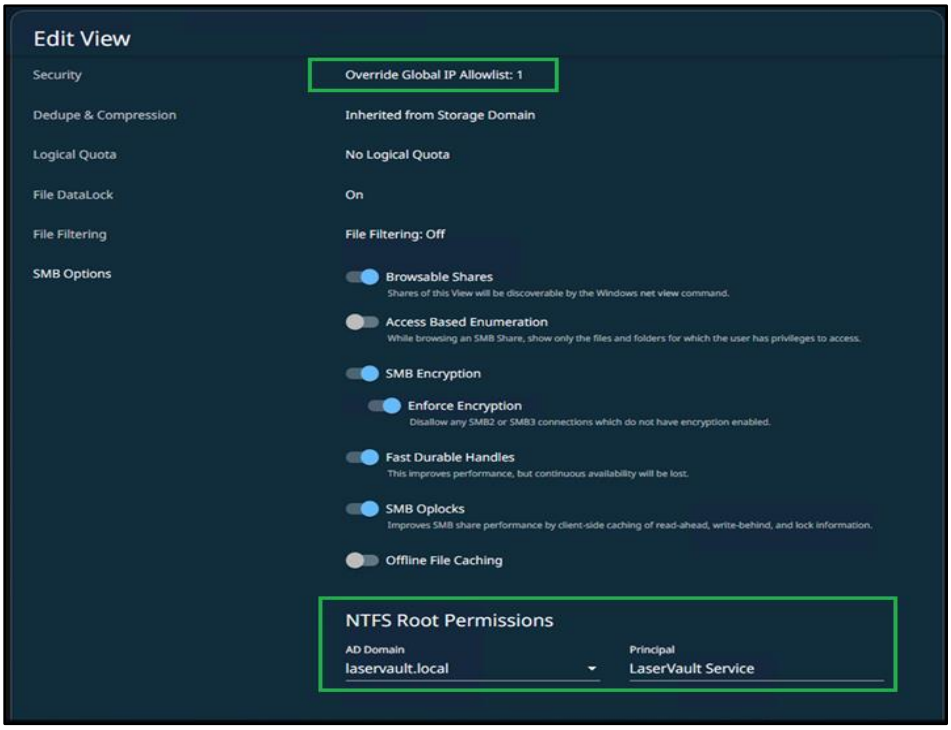
Configure the below listing of gflags with the values shown below and restart ‘bridge’ service for the gflags to take effect.

```
bridge_smb_portal_enable_oplocks=true
bridge_smb_portal_enable_share_level_permissions=true
bridge_smb_portal_enable_signing=true
bridge_smb_portal_enable_wtf8_encoding=true
```

On the LaserVault installed Windows Server, set the SMB Client attributes for signing to True.



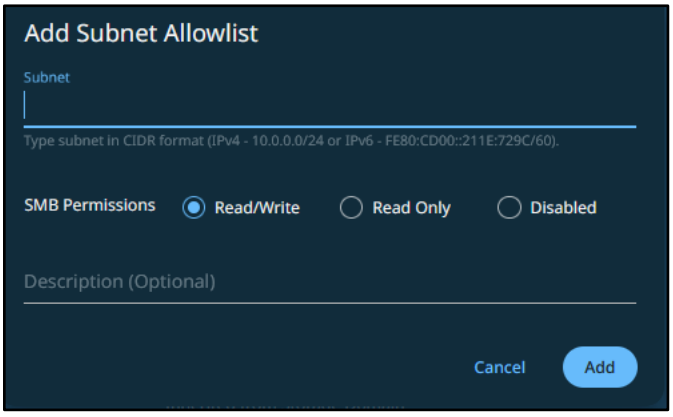
Setting up ACL for ViTL SMB View



Refer to SMB Shares for detailed information.

Hover the mouse over ‘Security’ to see the ‘Pencil’ icon, Click and proceed to see the option to choose between ‘Override Global IP Allowlist’ and ‘Extend Global IP Allowlist’. We recommend choosing ‘Override Global IP Allowlist’. In the widget click on ‘Add’ to add Subnet Allowlist, to see the widget below.

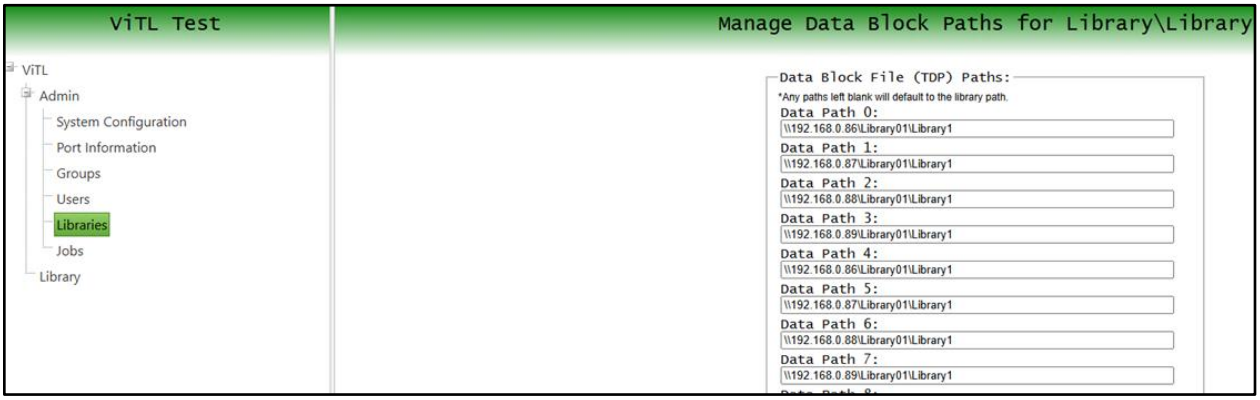
Provide the subnet in CIDR format and click on ‘Add’.



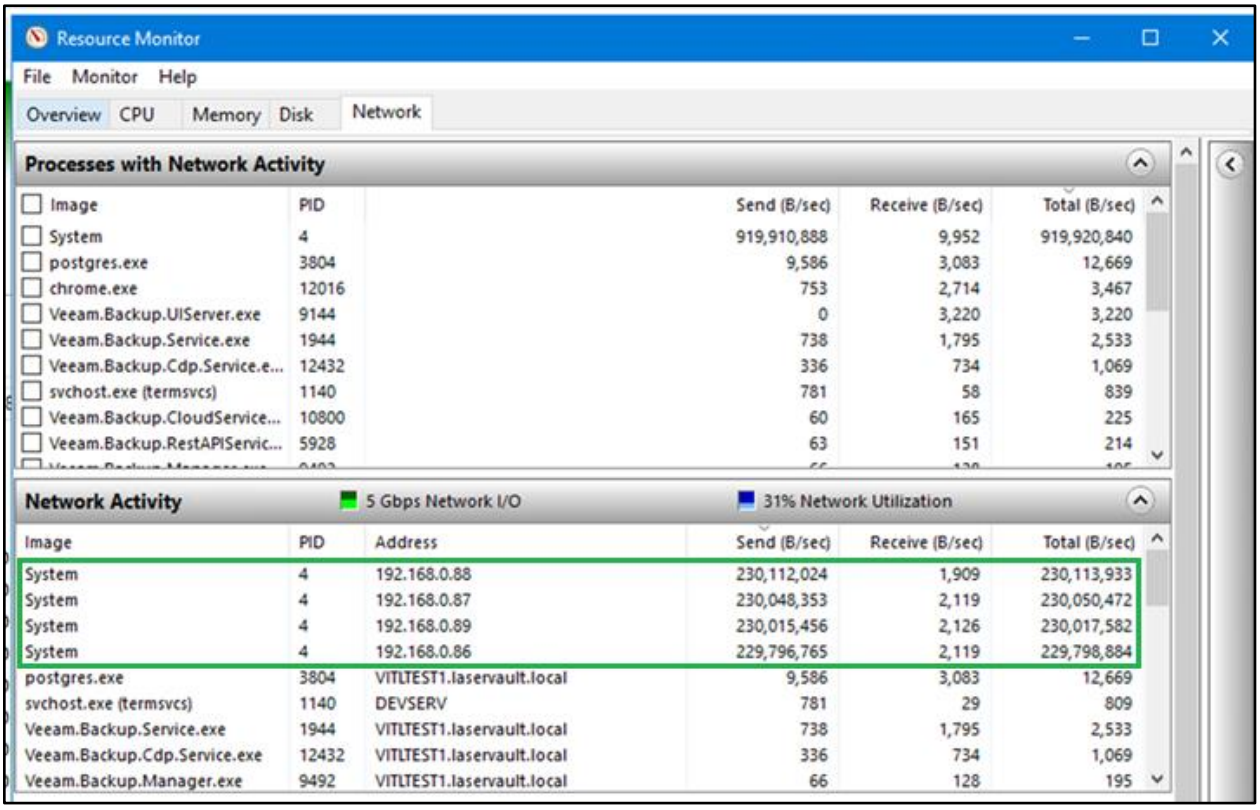
Refer to Add Subnets to Allowlists for detailed information.

Setting up Multiple Backup Streams to multiple nodes

On the LaserVault Configure Tape Library to use ALL nodes for read/write to maximize the throughput. Below is a screenshot of the configuration at LaserVault UI. The maximum number of data block paths LaserVault ViTL currently supports is 32.

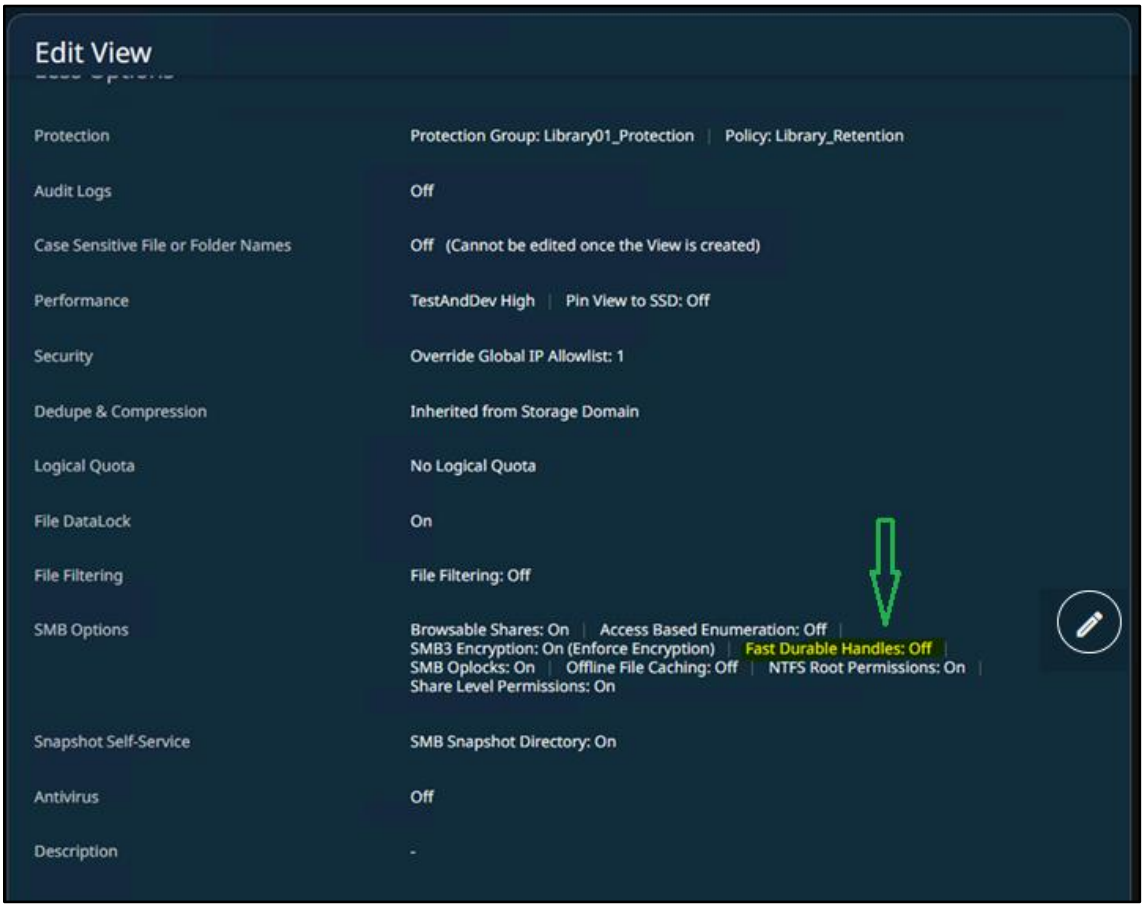


For the above configuration observe/monitor the throughput or bandwidth utilization. Below is a screenshot of data sent and received through all the nodes of the Cohesity Data Protect Cluster.

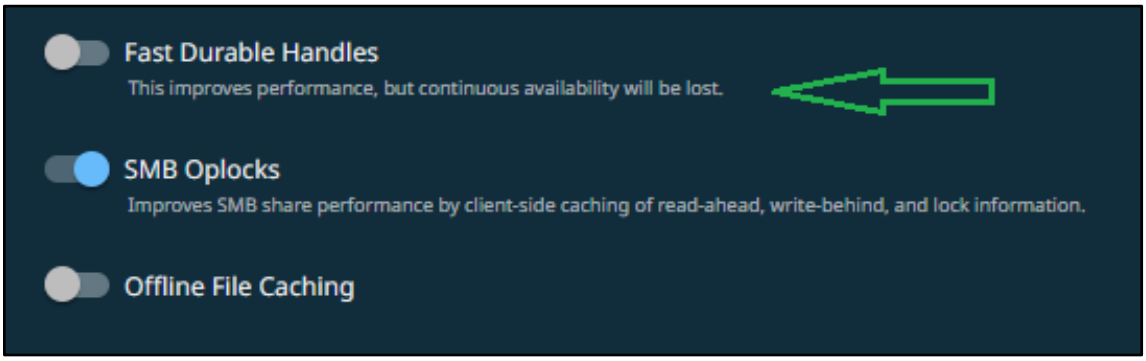


Setting up SMB View resiliency

Cohesity SMB View extends SMB Features viz., Persistent Handles enabled by default and Fast Durable Handles disabled by default. The Persistent Handles allows SMB clients to reconnect to a different node in case of a node failure and seamlessly continue their operations with the same file handle. The Fast Durable Handles option is designed to enhance performance for SMB clients by improving I/O operations, metadata operations, file listing, and more. It offers improved resiliency against service restarts of the Cohesity data service and short network failures.



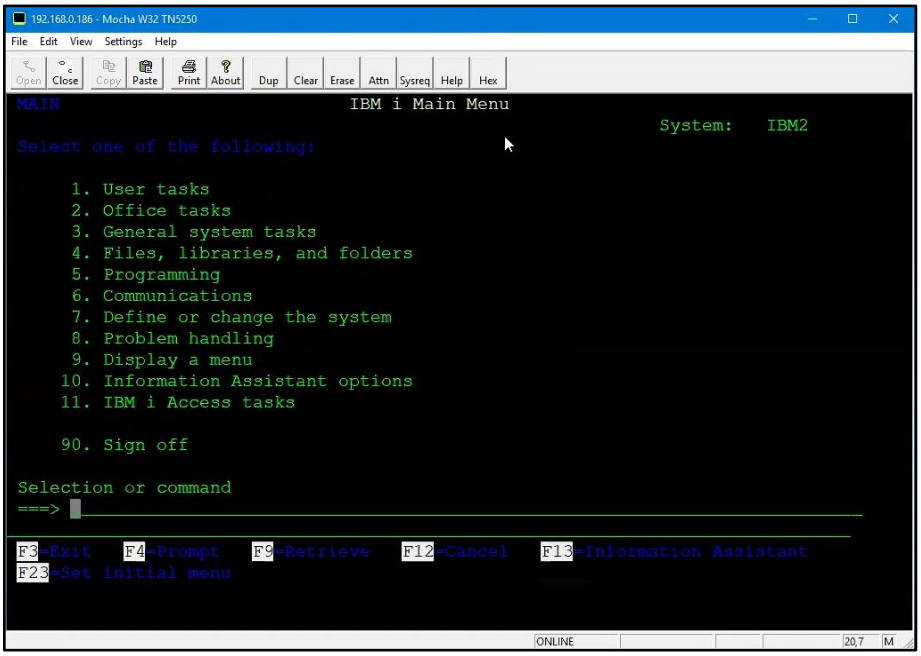
However, it's important to note that Fast Durable Handles might not be able to handle more significant events such as node failures or crashes of the SMB server service. Recommend keeping it Disabled.



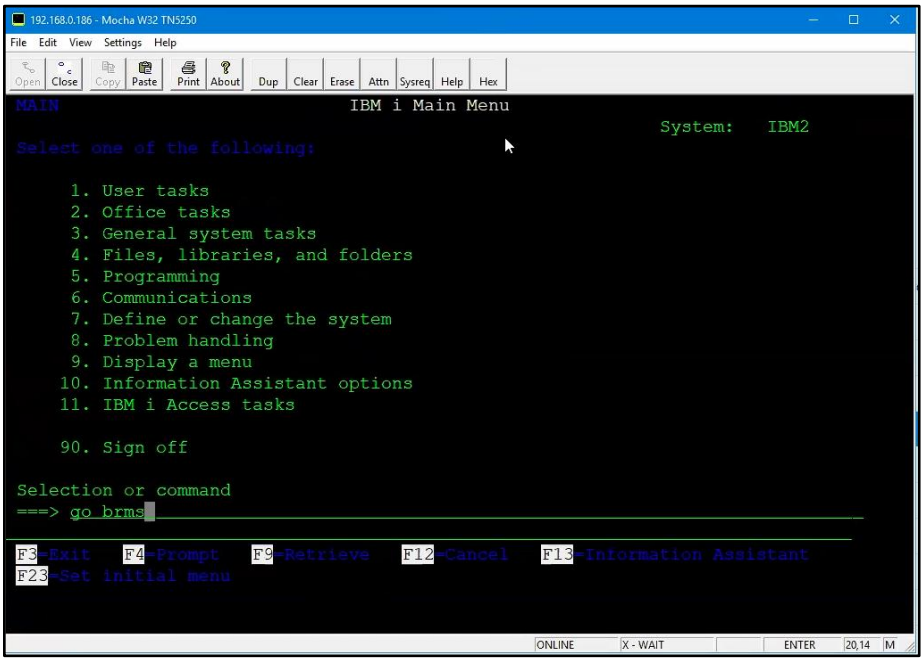
Configure IBM iSeries Server

On the IBM iSeries system, ensure the compatible FC Card with node ports are connected to FC switch ports and they are in the same zone as LaserVault FC ports. Validate and confirm communication between IBM iSeries and LaserVault Server is live and that there are no issues. The below screenshots show how to check the FC connectivity on the IBM iSeries server.

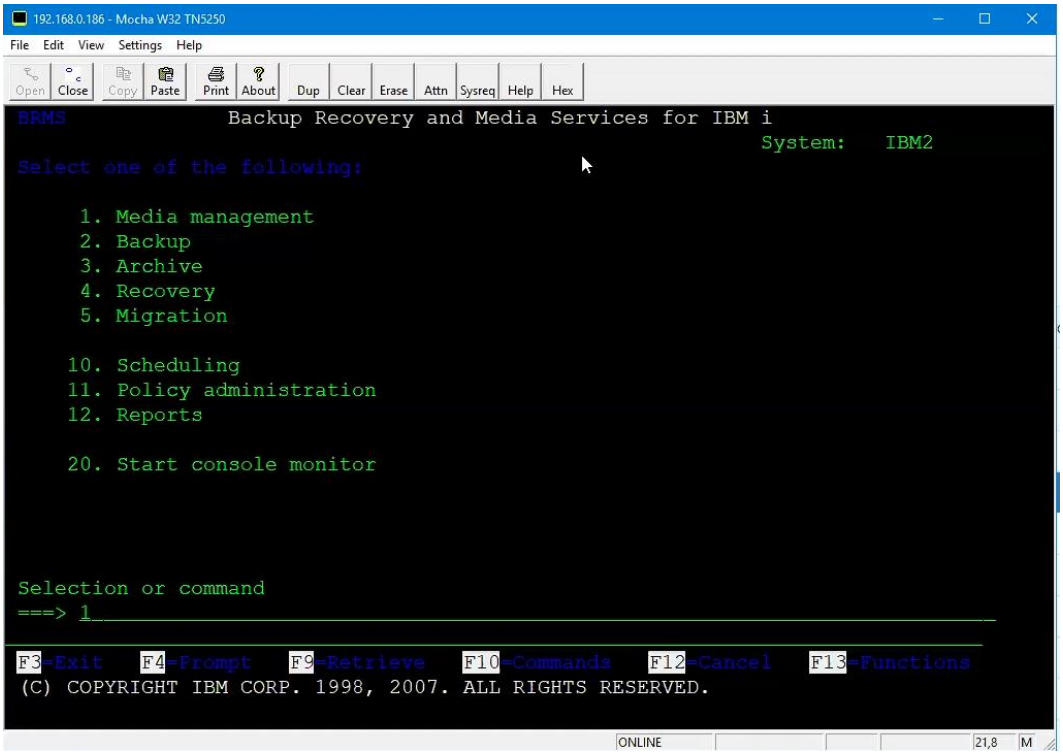
Launch or open the IBM i Main Menu.



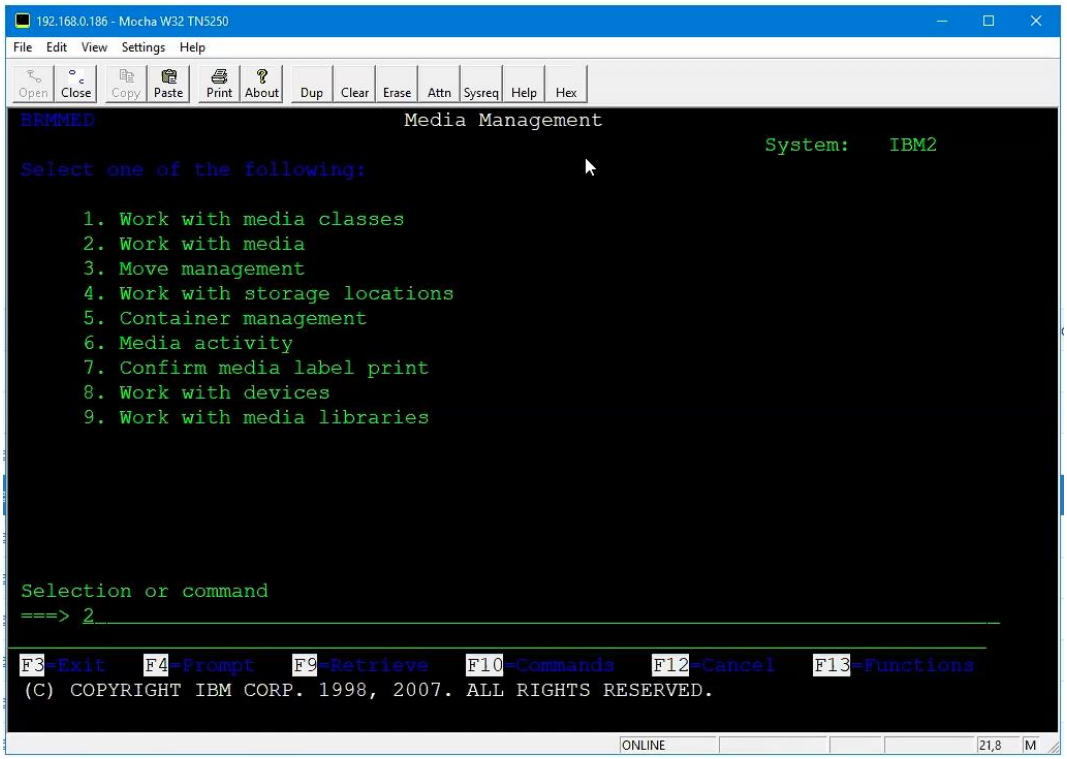
Switch to BRMS using ‘go brms’ command.



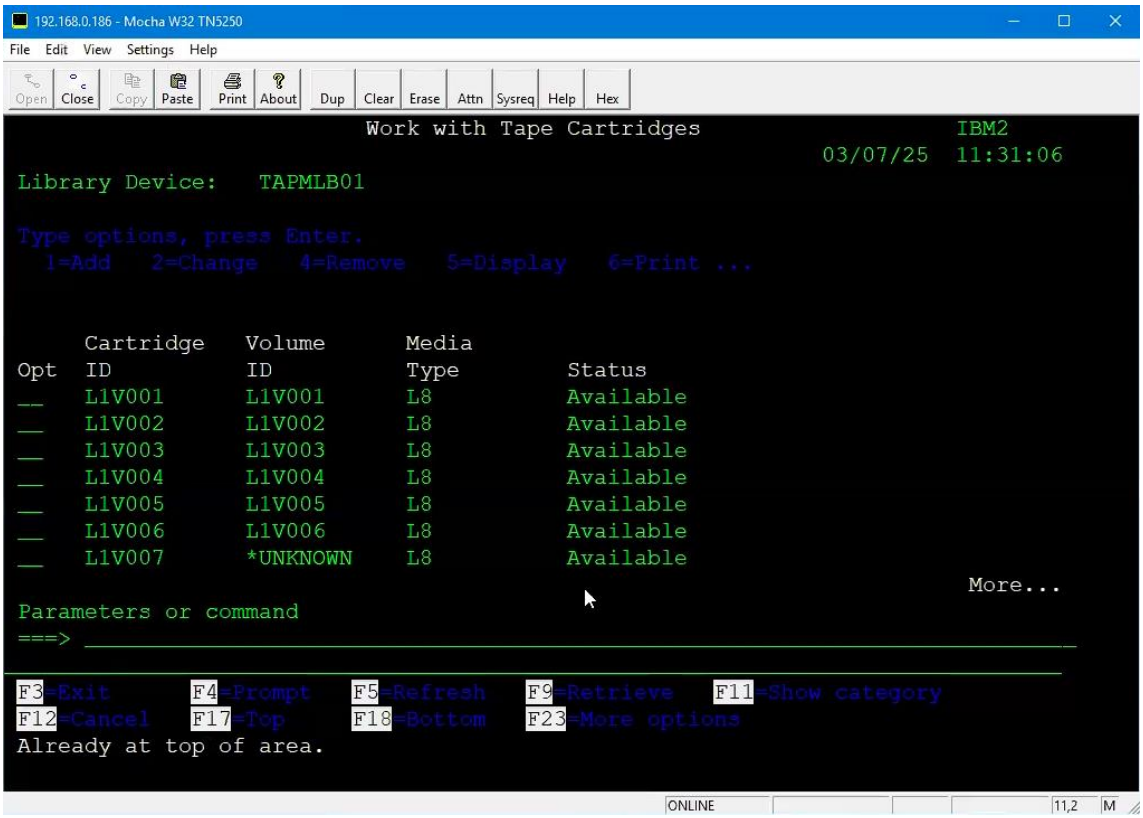
Once on the Backup Recovery and Media Services (BRMS), go to Media Management.



Once in Media Management, go to ‘Work with media’.



Below is a view of Library ‘TAPMLB01’ consisting of six Tape drives L1V001 to L1V006 each mapped to IBM volumes with the same names.



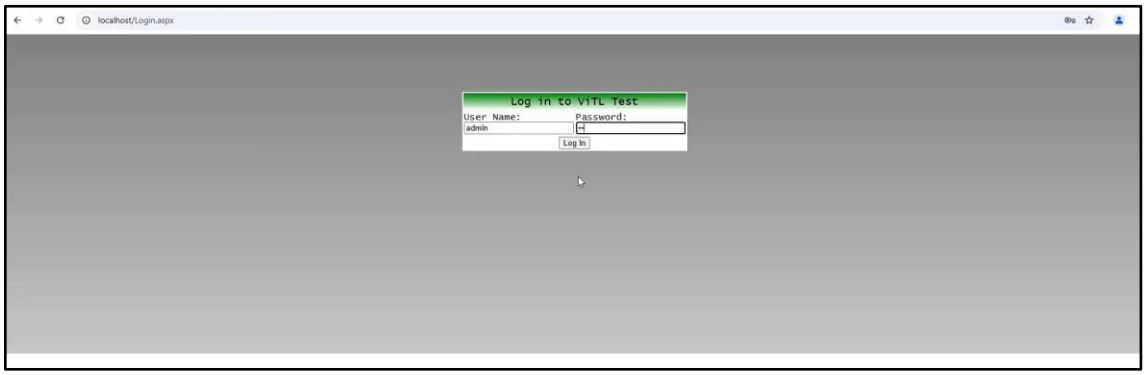
Configure LaserVault ViTL to Use Cohesity View

On commodity x86 architecture-based hardware, running Microsoft Windows Server 2019 or 2022 Operating System, can be used as LaserVault ViTL appliance. Ensure the necessary and appropriate drivers and utilities are deployed for corresponding FC Card. Validate the FC Card with ports are configured and enabled and the IBM iSeries system can communicate.

On the other end LaserVault ViTL communicates to Cohesity DataProtect Cluster through Ethernet via SMB Protocol, ensure that port 445 is opened between them for SMB traffic. Hence the ethernet connectivity of 10Gbe or 25Gbe should match the incoming speed from IBM iSeries.

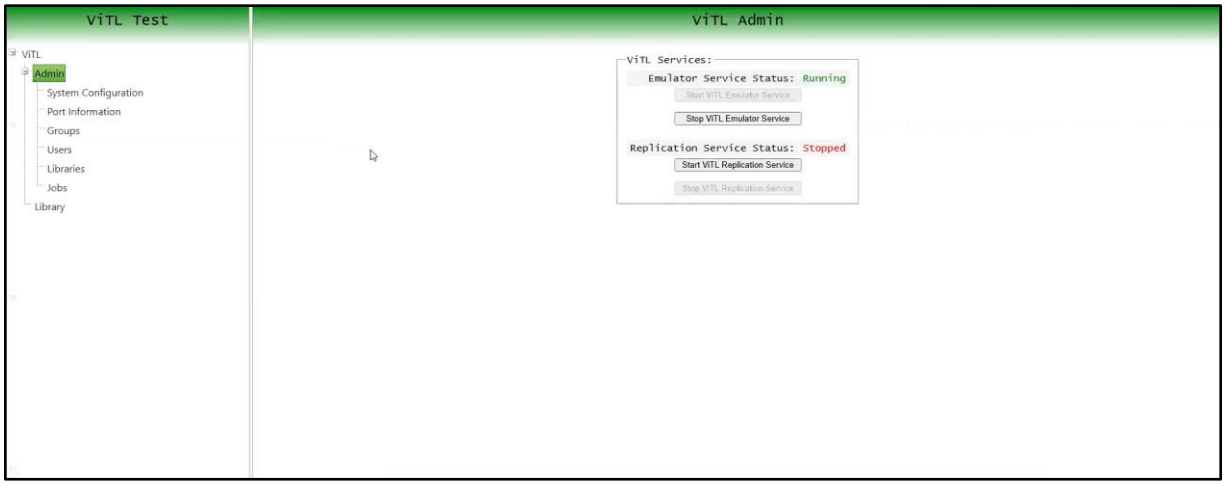
Download and install the LaserVault ViTL software. Install LaserVault ViTL software components on the Windows Server where you mapped the Cohesity view as SMB Share. For detailed network ports that need to be opened for communication between various entities like IBM iSeries system and LaserVault hosting Windows Server, refer to LaserVault ViTL Technical Manuals. Below screen grabs show how to login to LaserVault ViTL and validate the connectivity. Once installations are complete, you can launch the ViTL UI and administer the storage topology.

1. Login to LaserVault ViTL through web browser.



2. Check the LaserVault ViTL version and other details.

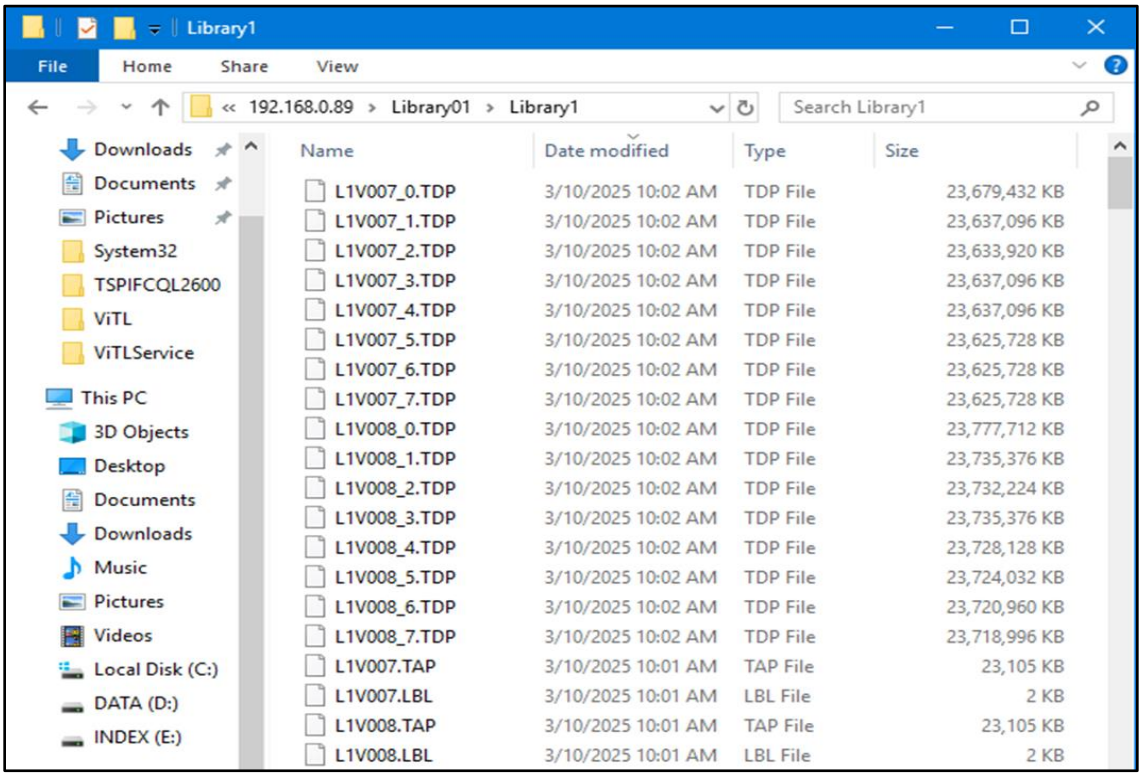
LaserVault ViTL Admin screen



3. LaserVault ViTL communicates with IBM iSeries through Fibre Channel connectivity. In this guide, we have taken the example of LaserVault ViTL communicating via QLogic FC cards.

IMPORTANT: On the Cohesity Storage, the File DataLock retention should be set to a period lesser than the one configured in the LaserVault ViTL Volume Group settings.

The following are the file extensions viz., ‘.TAP’ file, ‘.LBL’ file and ‘.TDP’ file. Data files are made up of the following and are pre-allocated. Label File ‘.LBL’ (VOL LABEL INFO), File Index ‘.TAP’ file (pointers to the data blocks on 'tape'), and Data Block Files ‘.TDP’ - Per Tape Device. The Data Block files are the actual tape out data and will be scaled based on the number of tape drives used. When one 'tape' is opened - it is actually one index file, one label file, and nine data block files. So a ViTL could have 10 tape drives opening 10 tapes which would look like 120 file sessions on the SMBServer. The Data block files are tunable up to 32 files per tape. This is configured on the Laservault based on throughput, change rates, and concurrent saves from source to destination. The below snippet shows how the IBM iSeries systems backup looks once they are written onto the Cohesity View.

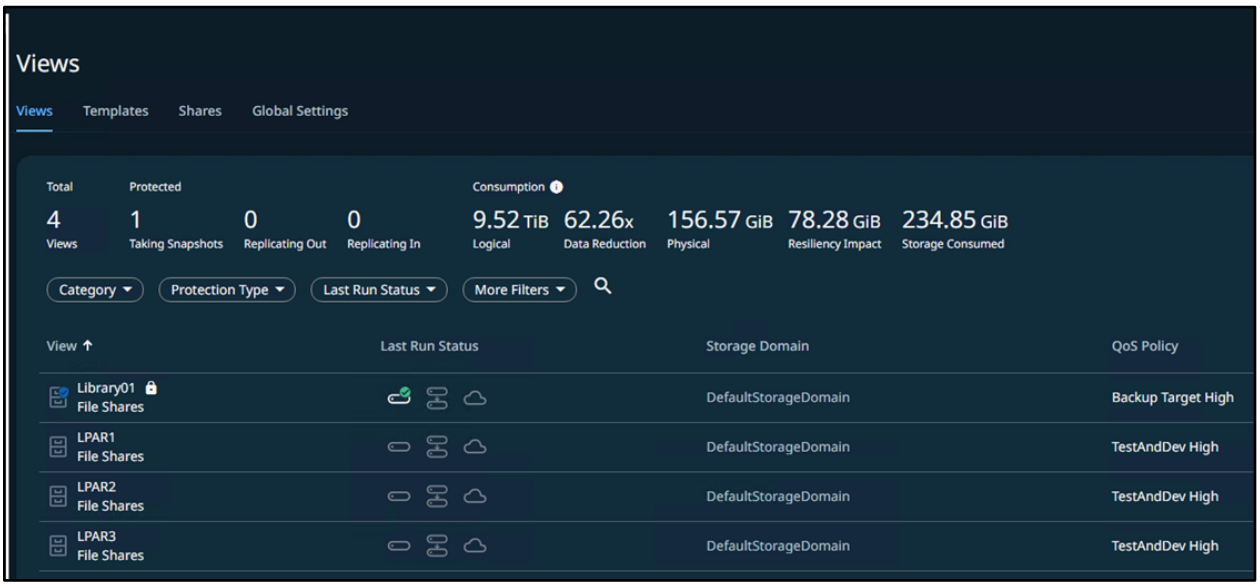


Use Cases

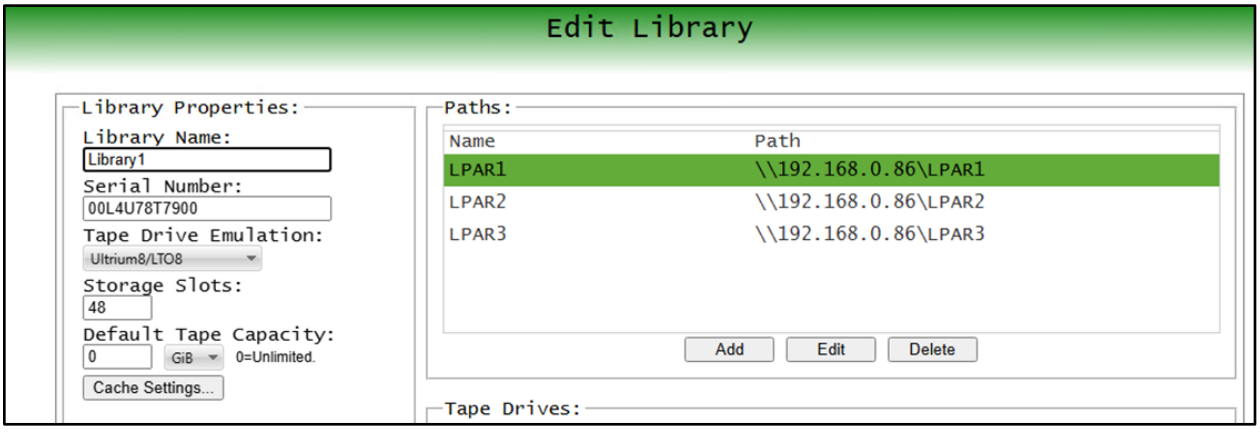
Below are a few use cases with illustrations using screen grabs that help users to deploy the solution efficiently.

Run Parallel Backups to Cohesity Views

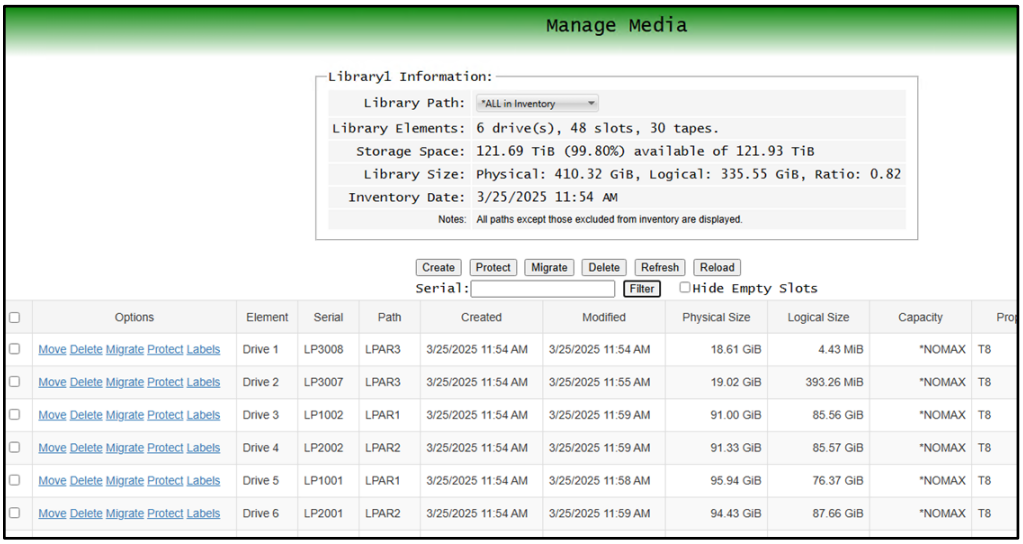
Below are Cohesity views ‘LPAR1’, ‘LPAR2’ and ‘LPAR3’ configured for a Backup job.



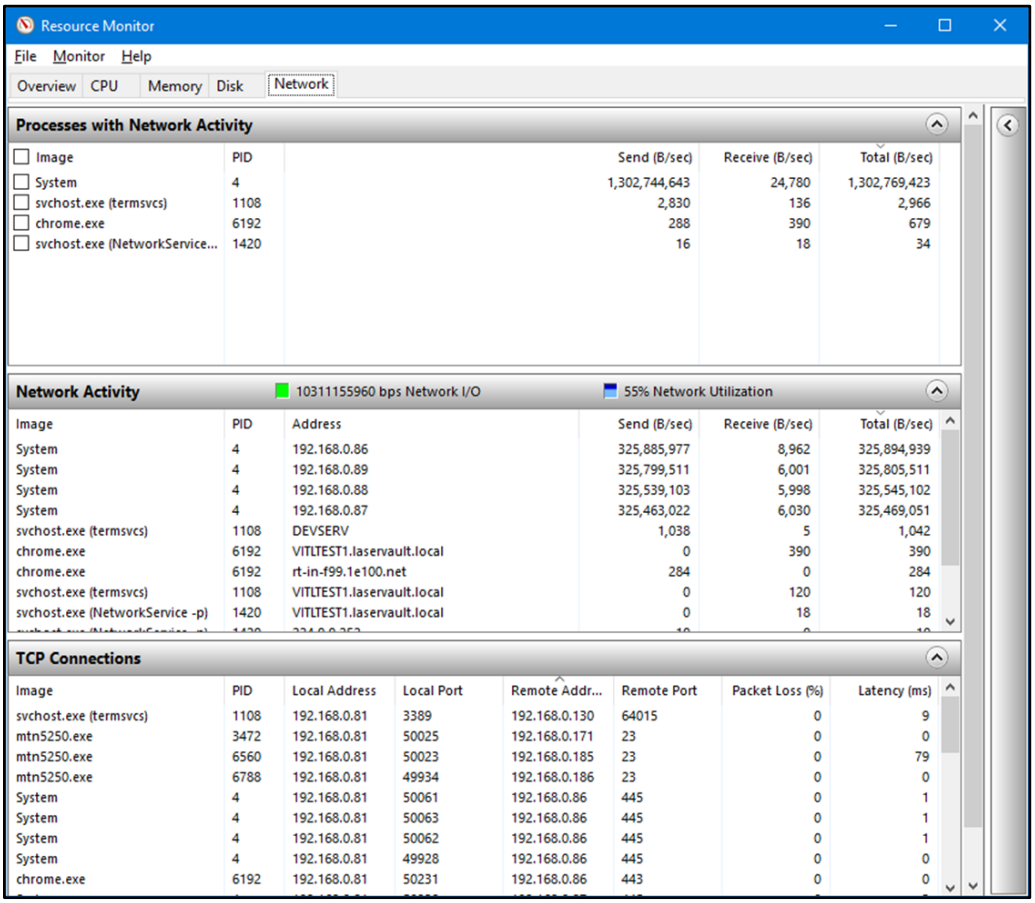
Run 3 Parallel Backups one each from multiple IBM i-Series (LPAR) Instances to respective Cohesity View using QoS as TestDevHigh. Each LPAR has its own view.



3 LPARs saving in parallel each LPAR using 2 tape drives. In the below screen, grab LPAR1 writing to tape drives LP1001 & LP1002, LPAR 2 writing to LP2001 & LP2002 and LPAR 3 writing to LP3007 & LP3008.



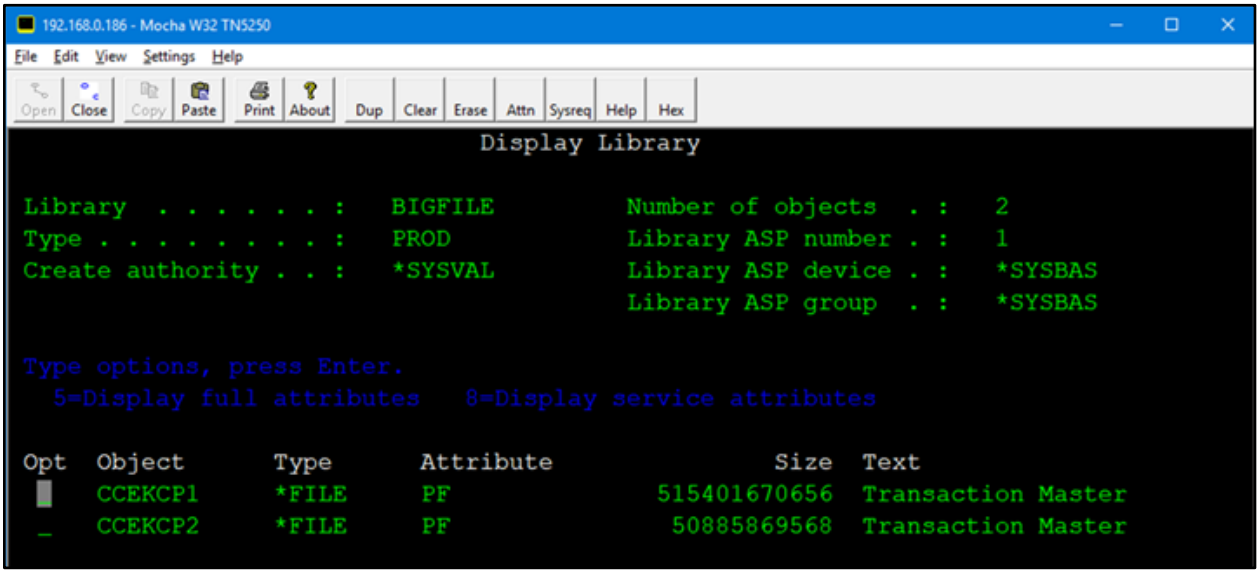
Observe the Backup Throughput, Data writes and read, Backup Time. Validate how many Nodes are used for Backups. In this case, all nodes are being used.



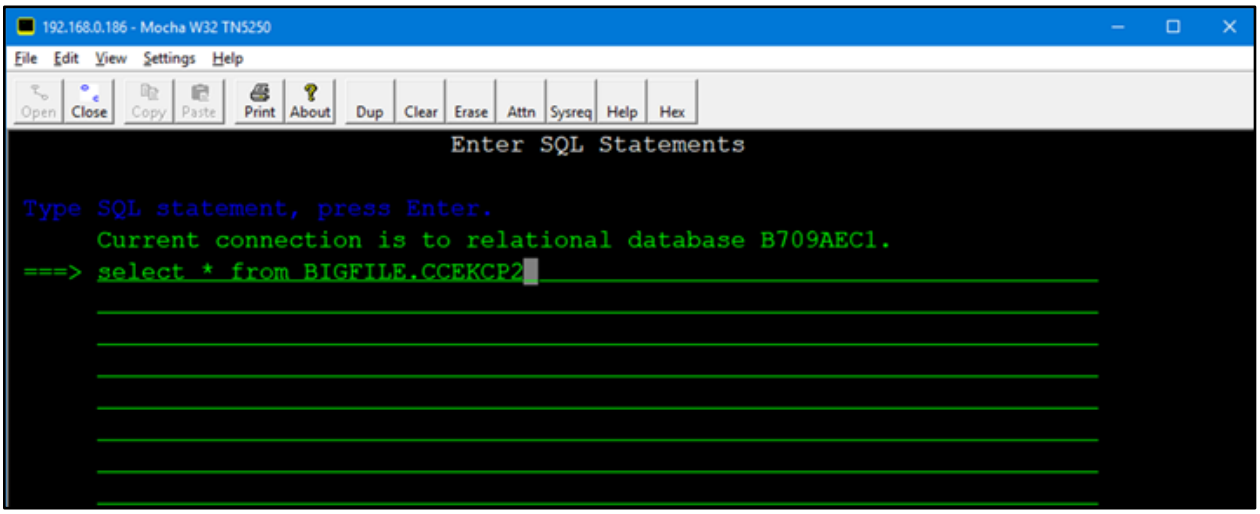
DB2 Backup and Recovery

DB2 is tightly integrated with IBM i and hence its Backup and Recovery is one of the important use case Customers wish to have it supported. DB2 backups and restore can be orchestrated from BRMS UI.

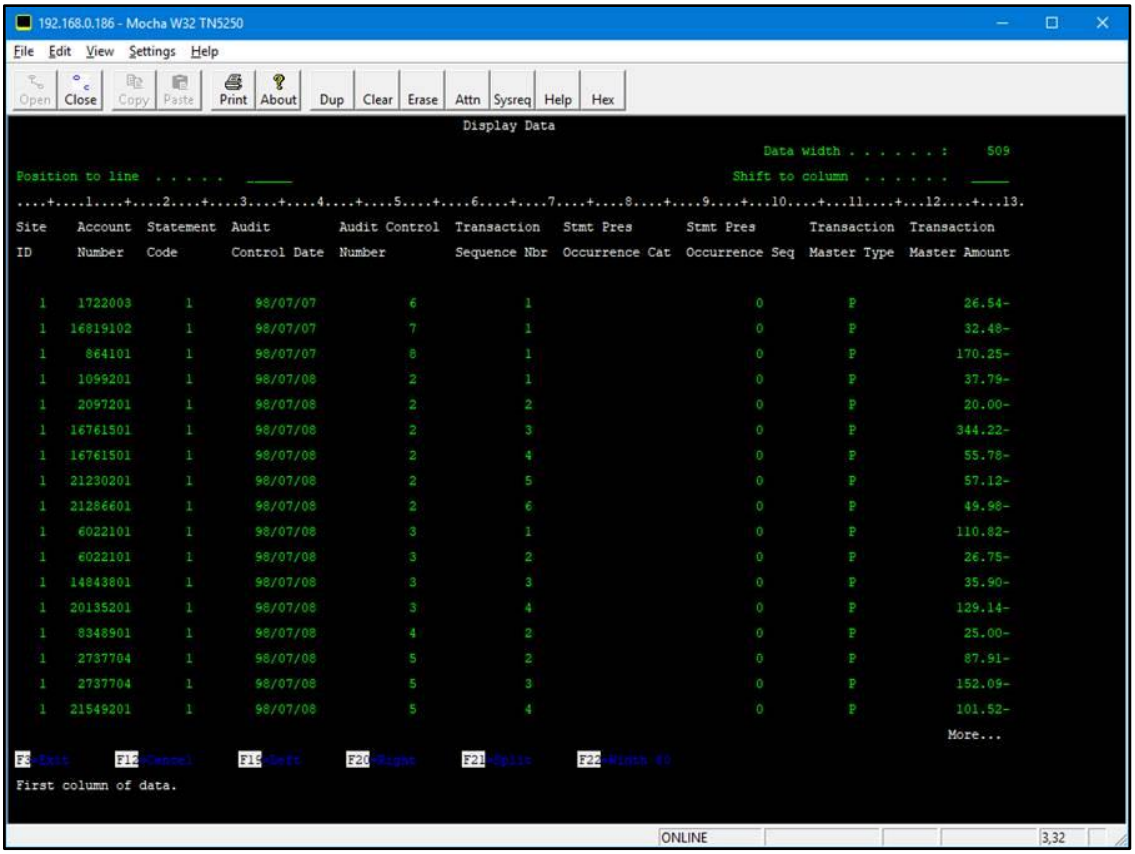
DB2 database table named ‘CCEKCP2’ located in a library named ‘BIGFILE’.



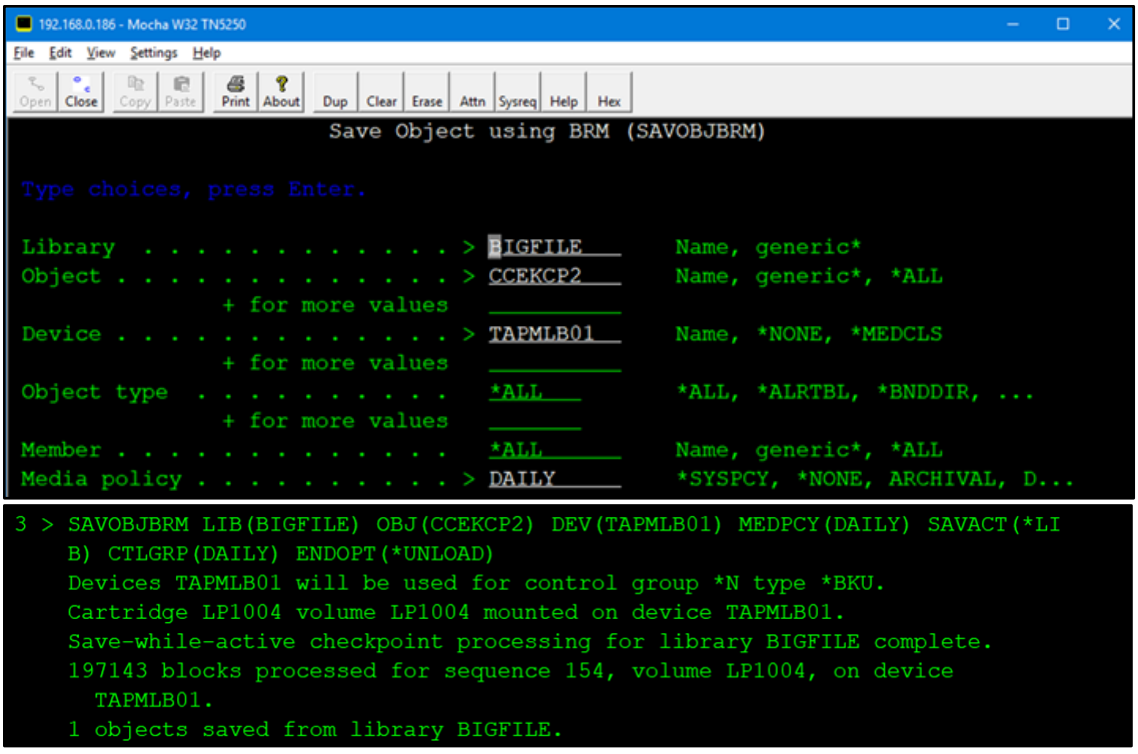
Query of data table



Contents of data table



Data table was saved



The table ‘CCEKCP2’ is being deleted to be restored from the Backup.

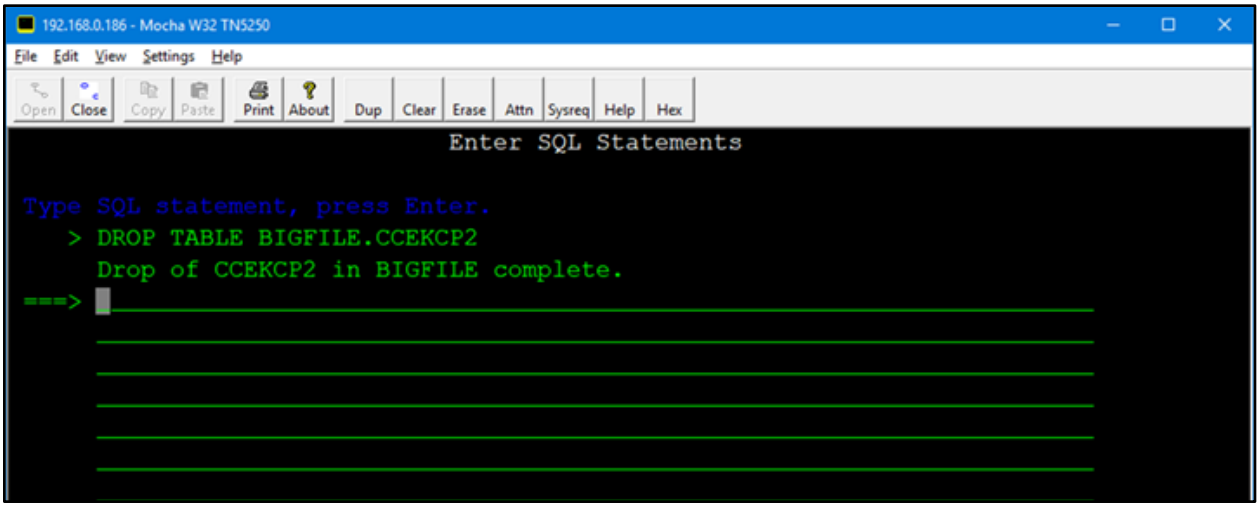
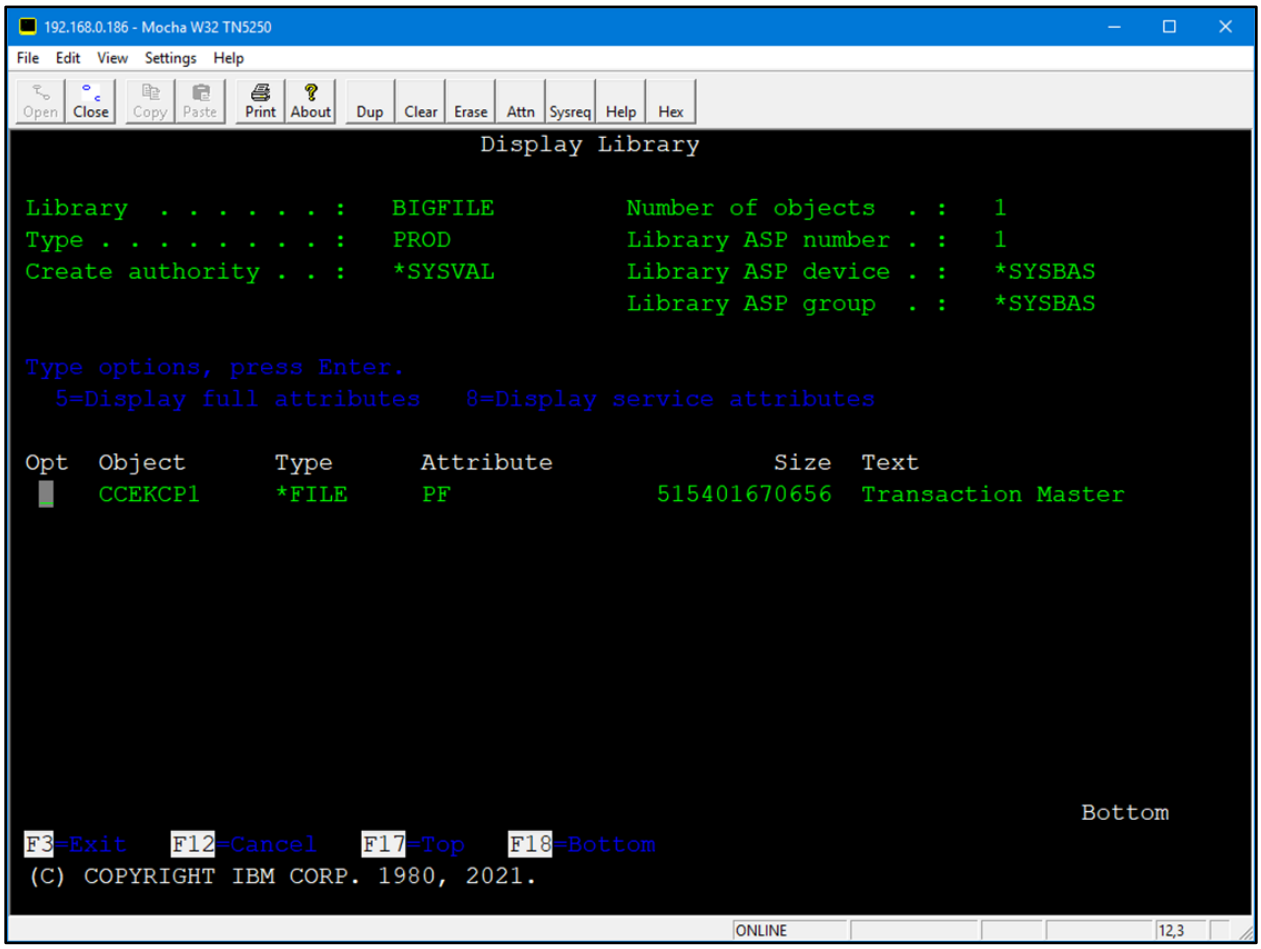
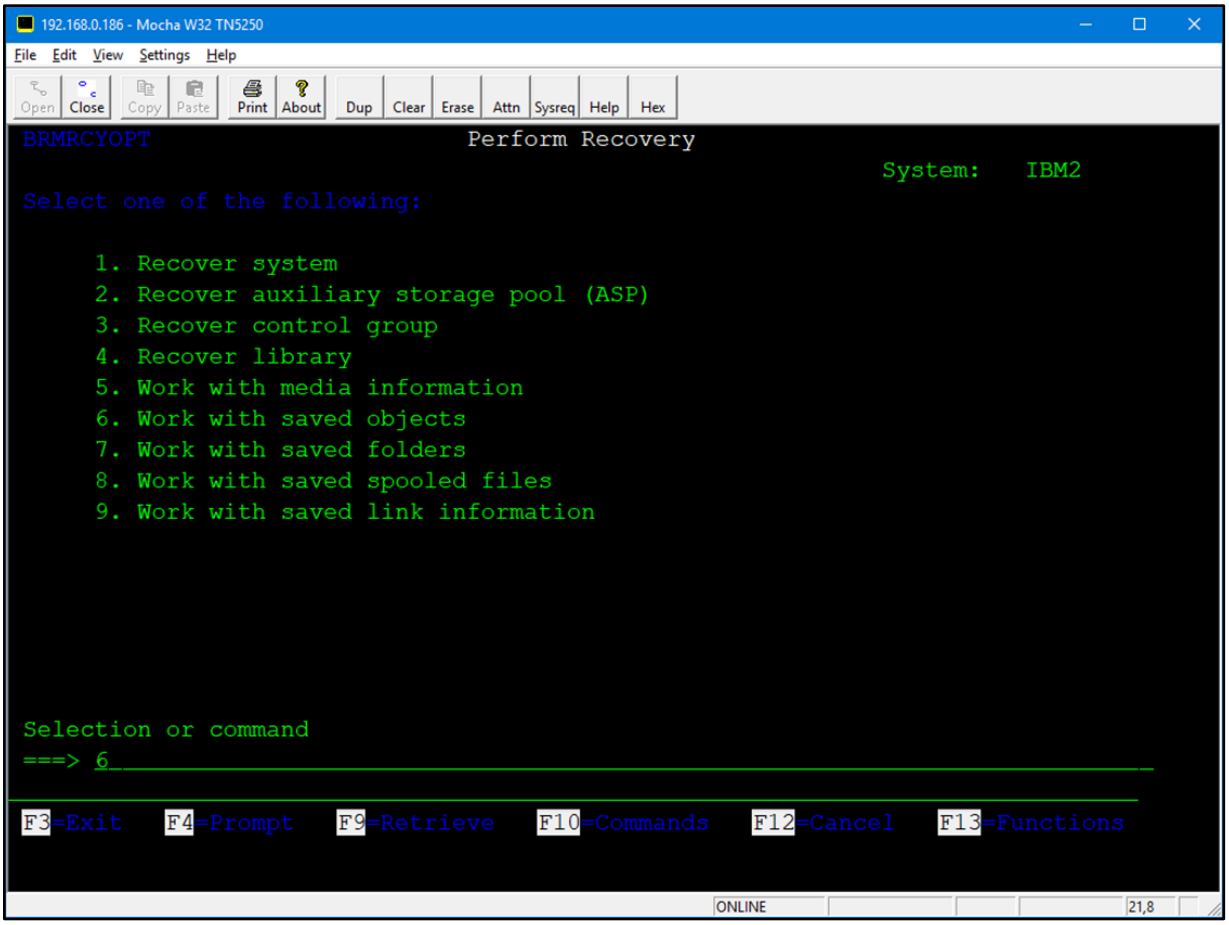


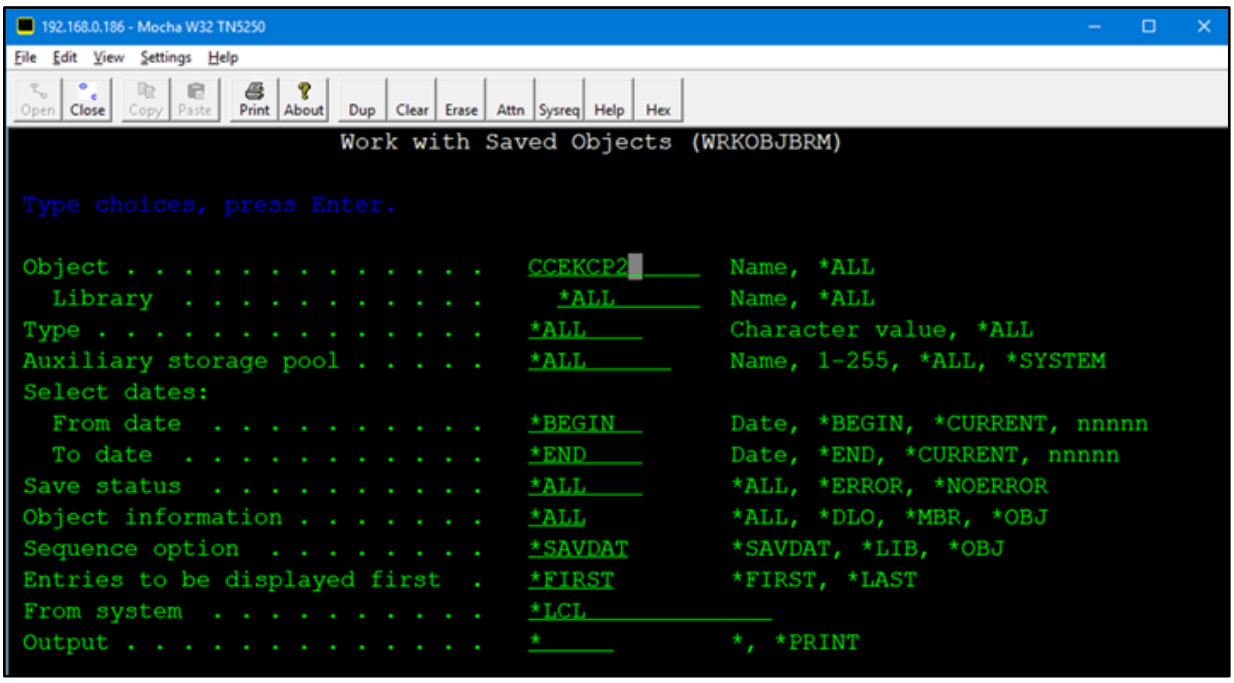
Table ‘CCEKCP2’ is no longer in the library named ‘BIGFILE’.



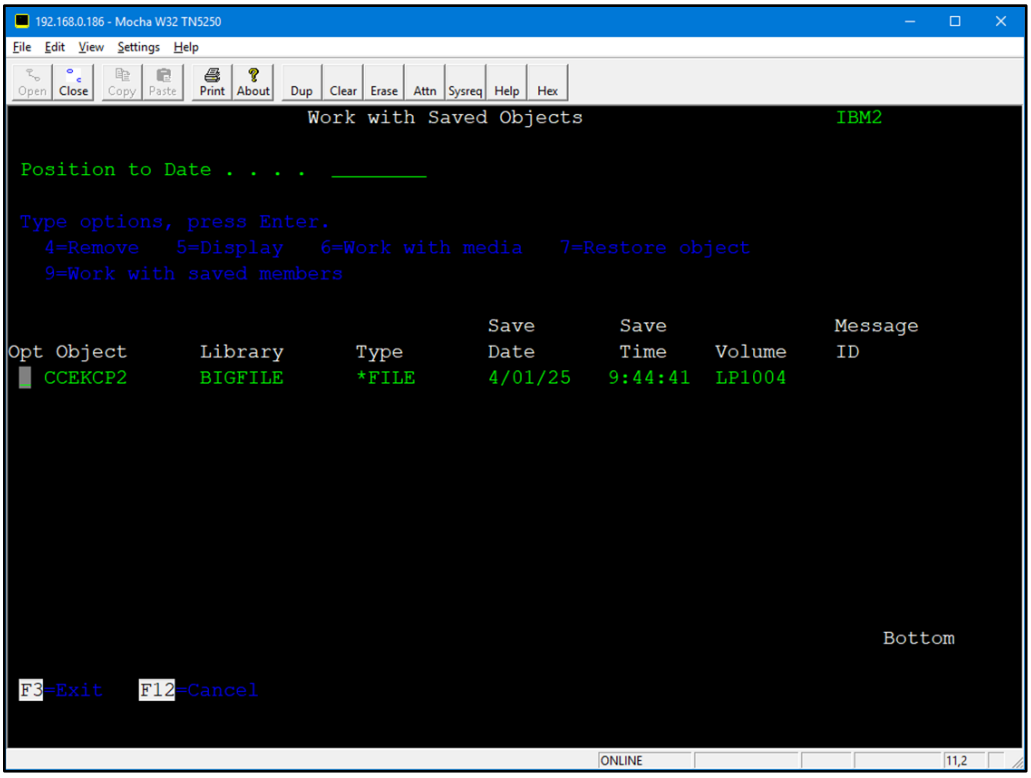
Choose option 6 to Perform Recovery from Saved Objects.



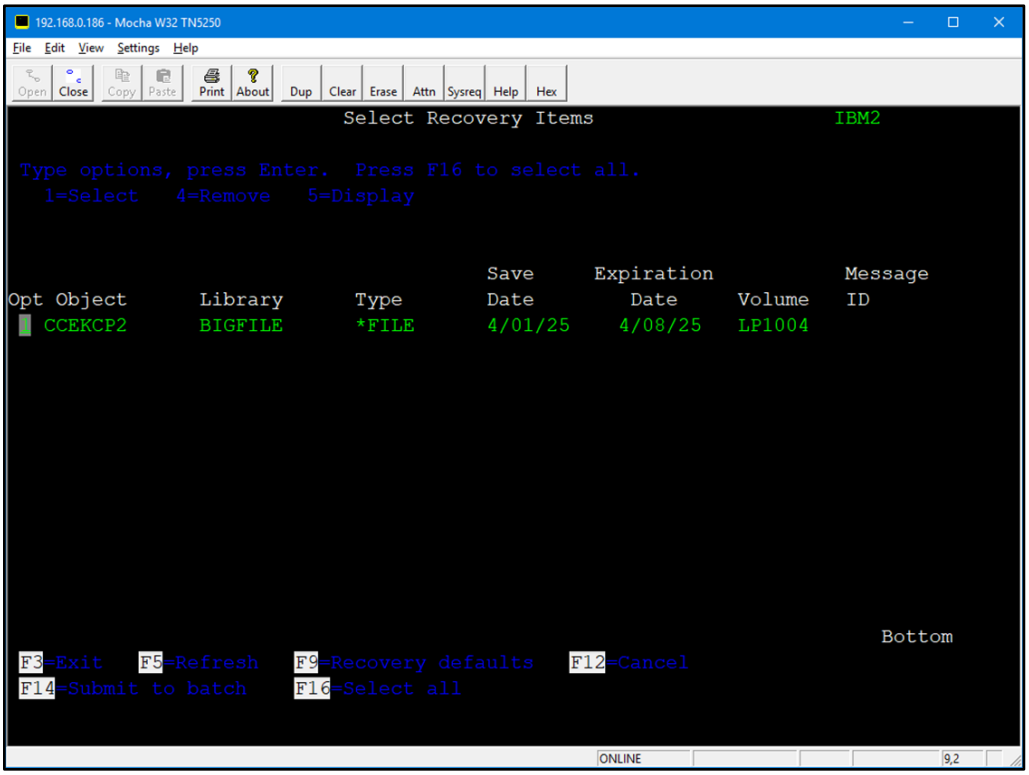
Restoring the object ‘CCEKCP2’.



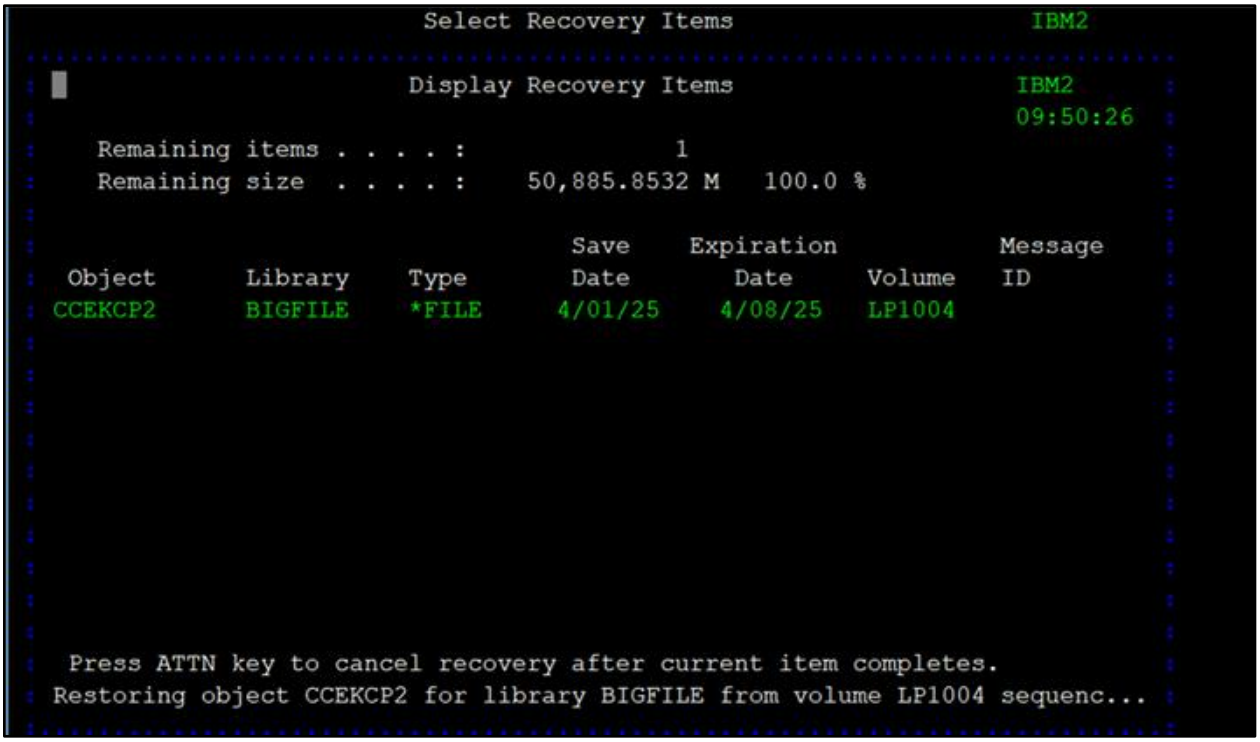
Intermediate step before Restoring the object ‘CCEKCP2’.



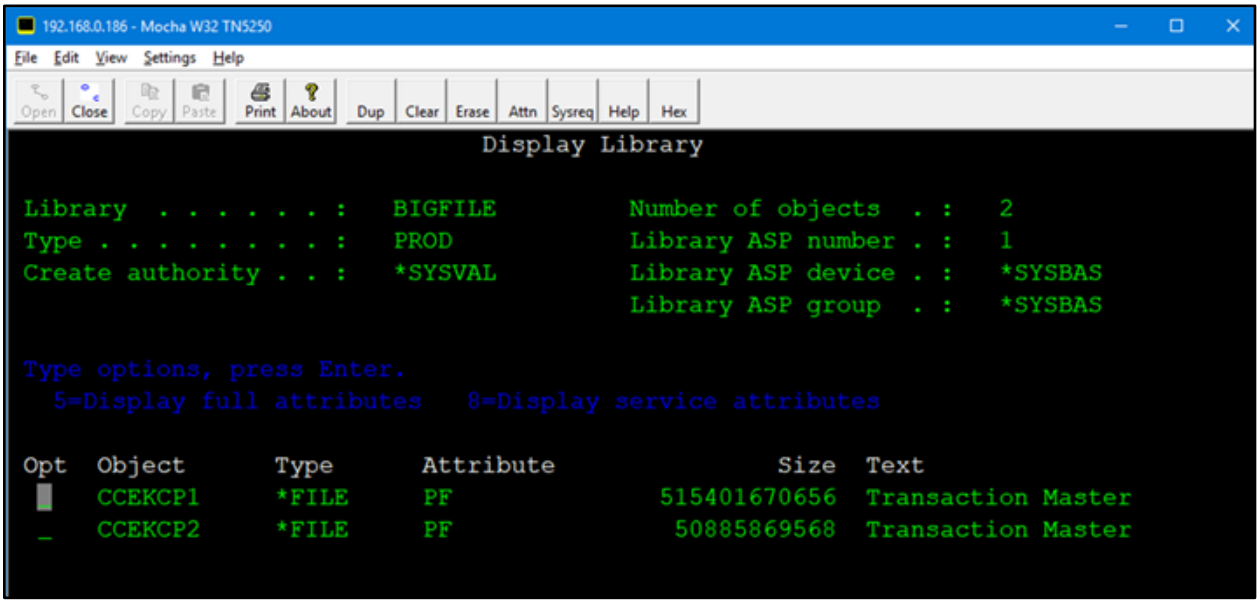
Select the object ‘CCEKCP2’ to restore.



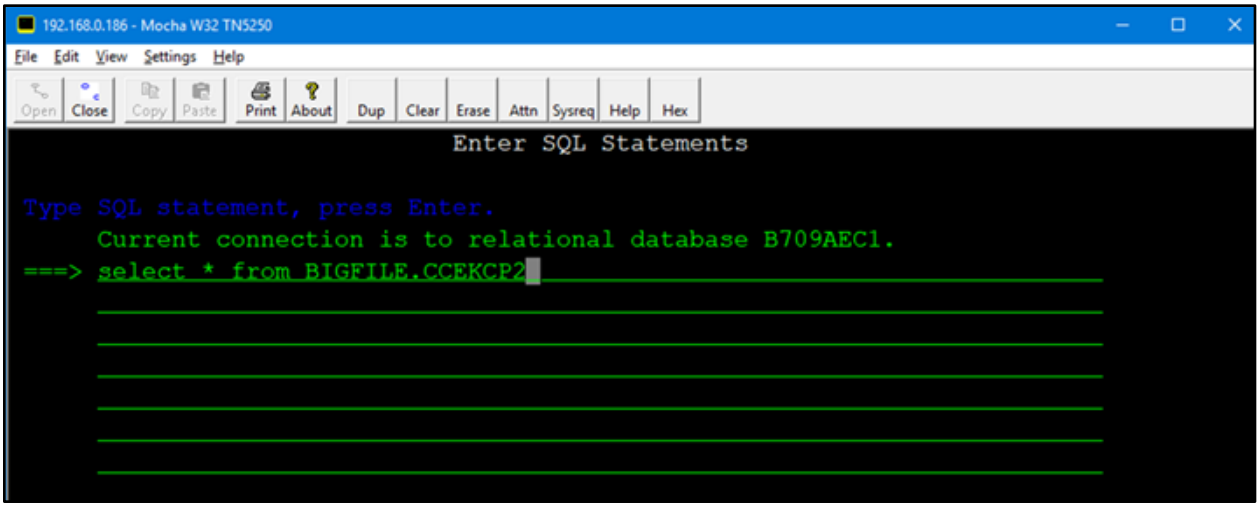
Recovery progress monitoring.



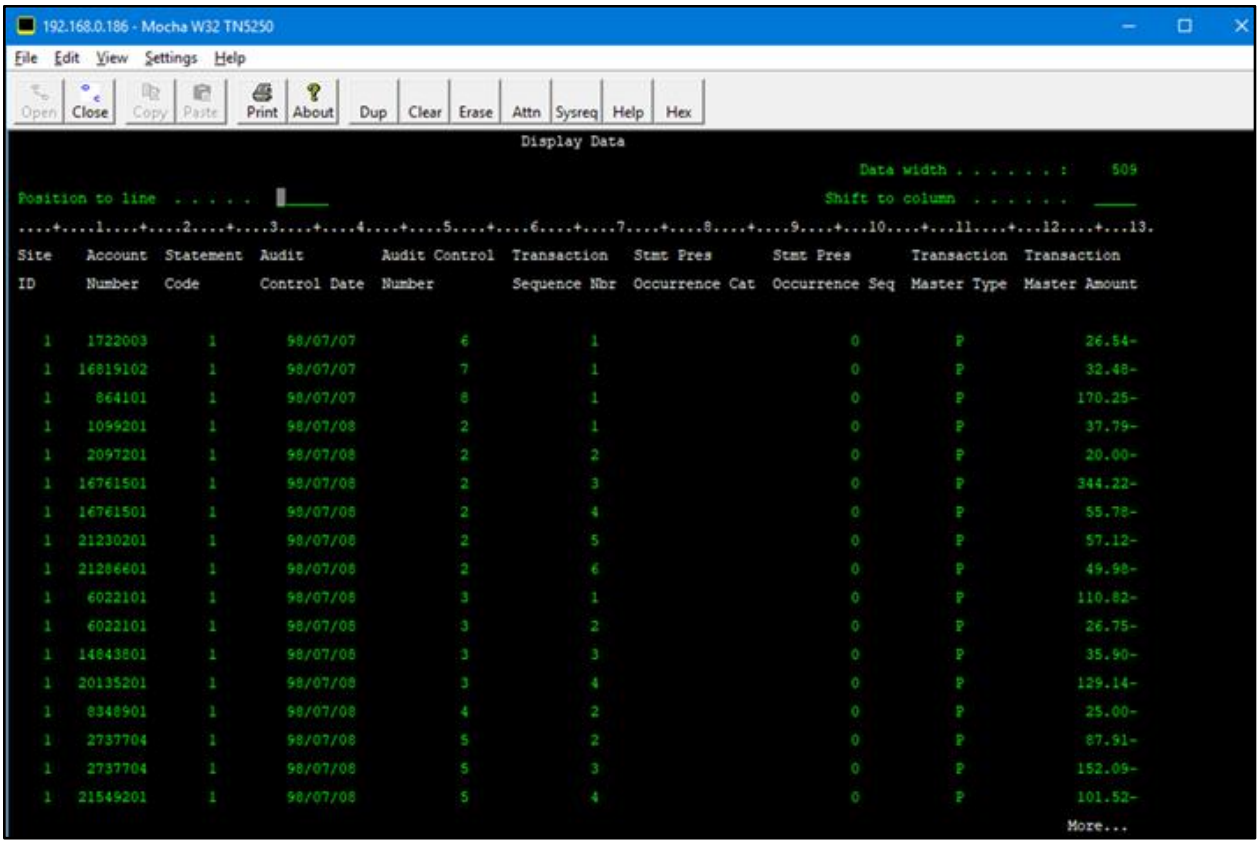
Database table ‘CCEKCP2’ restored to library ‘BIGFILE’.



Validate the DB2 Table ‘CCEKCP2’ recovery by running query.

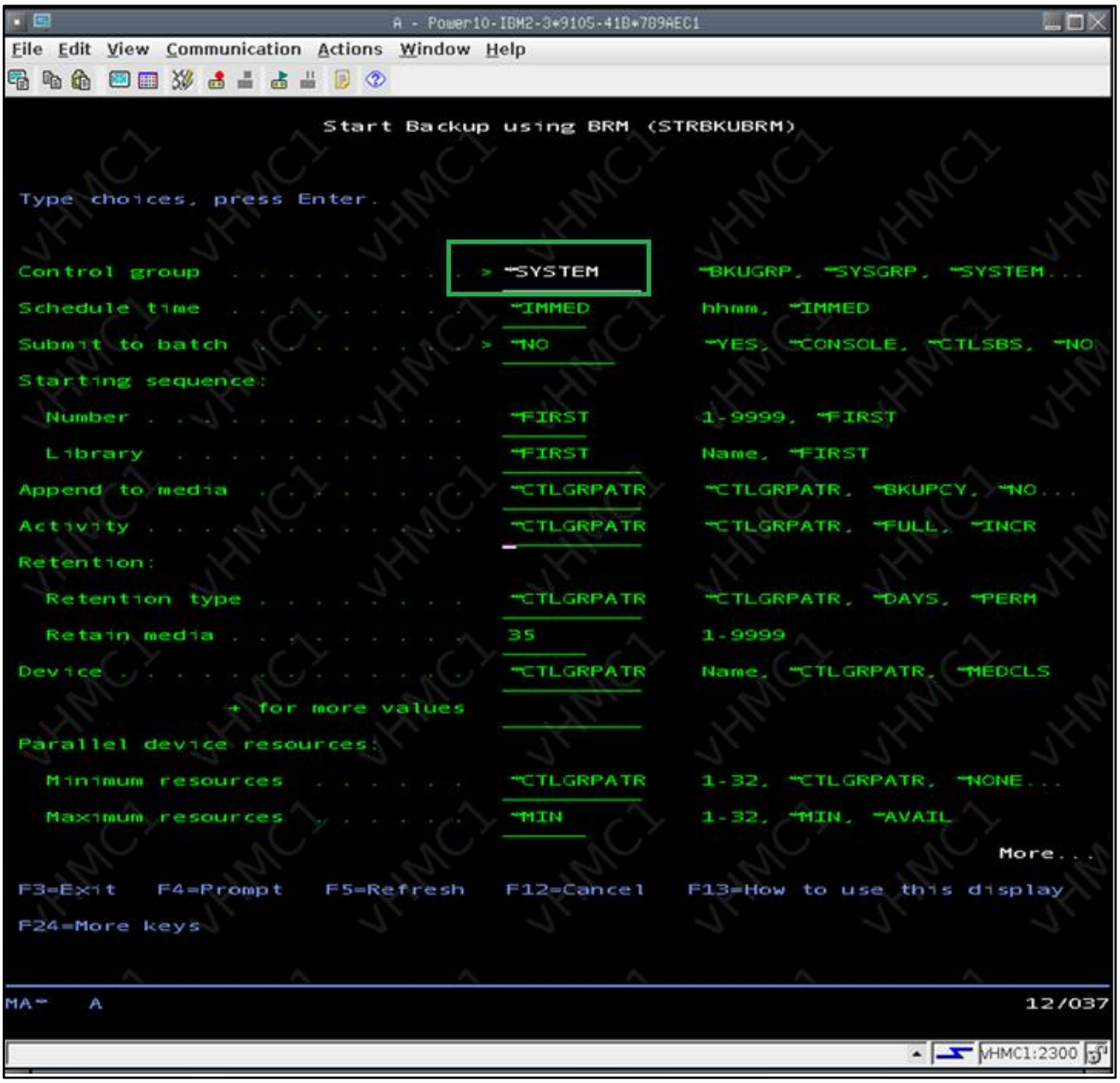


The query should return all the records in the Table ‘CCEKCP2’.

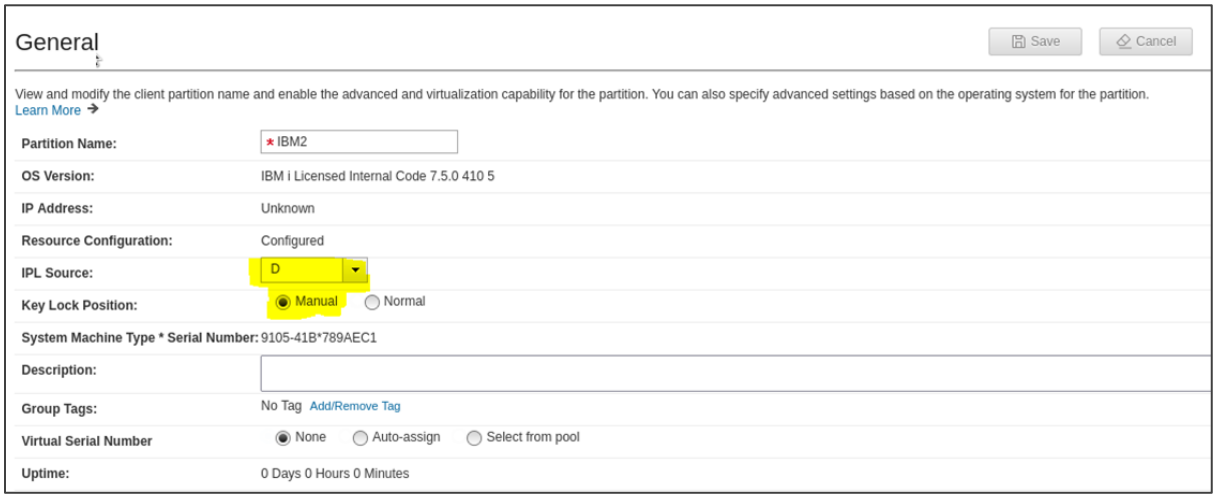


BMR (Bare Metal Restore) save and restore

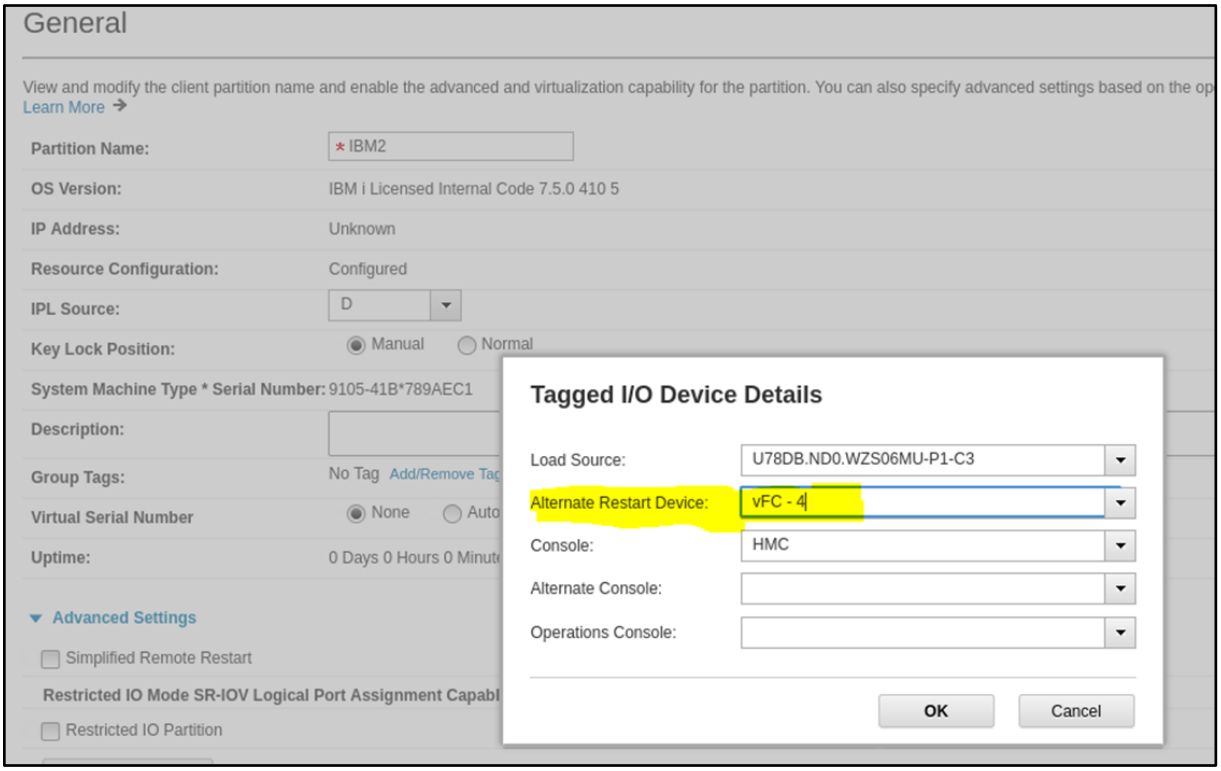
Running full system save in BRMS from the IBM i console.



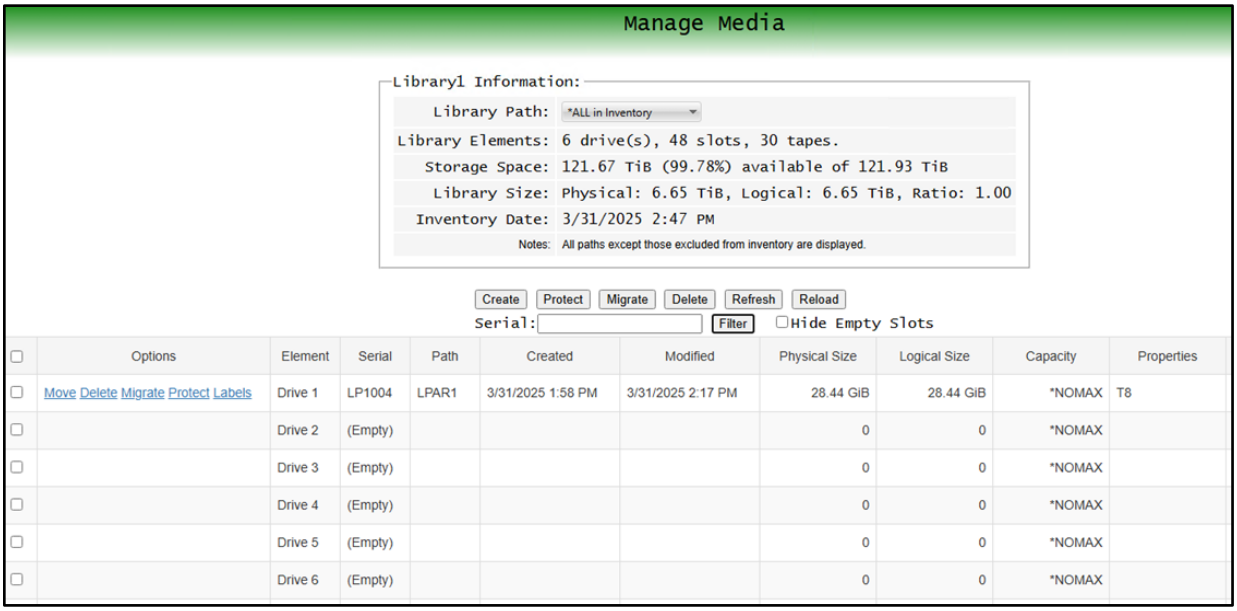
D-Mode, Manual Initial Program Load (IPL) selected for the LPAR:



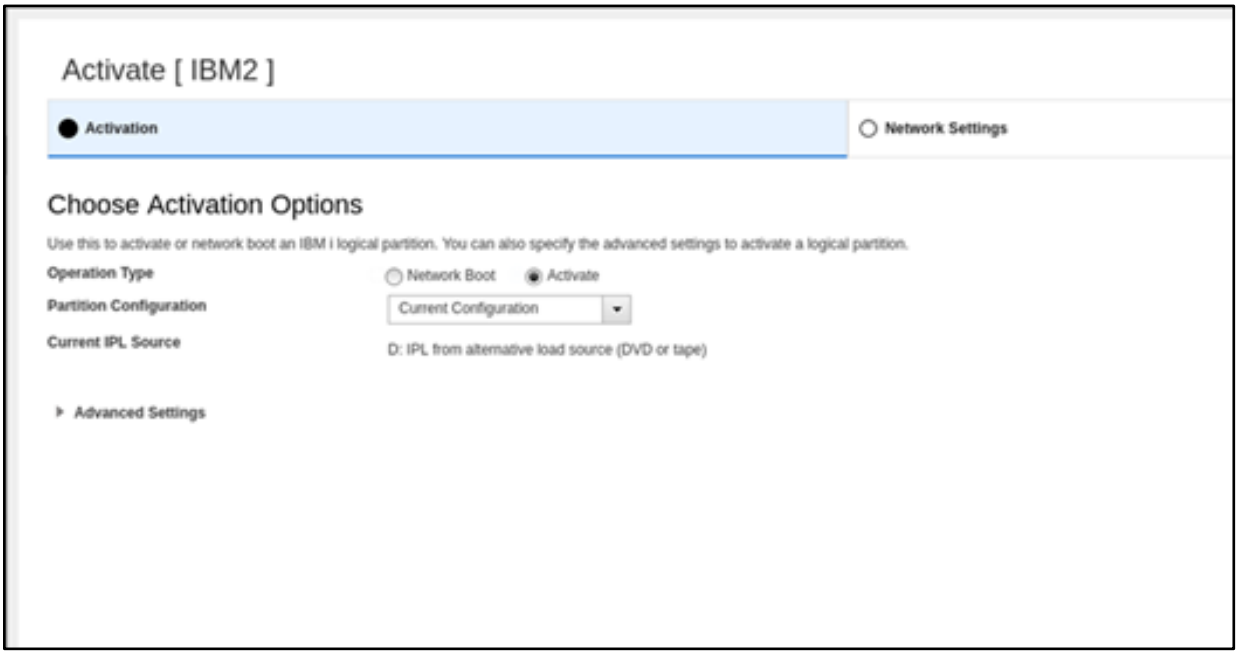
Tagged I/O set with virtual FibreChannel device vFC-4 as the alternate restart device.



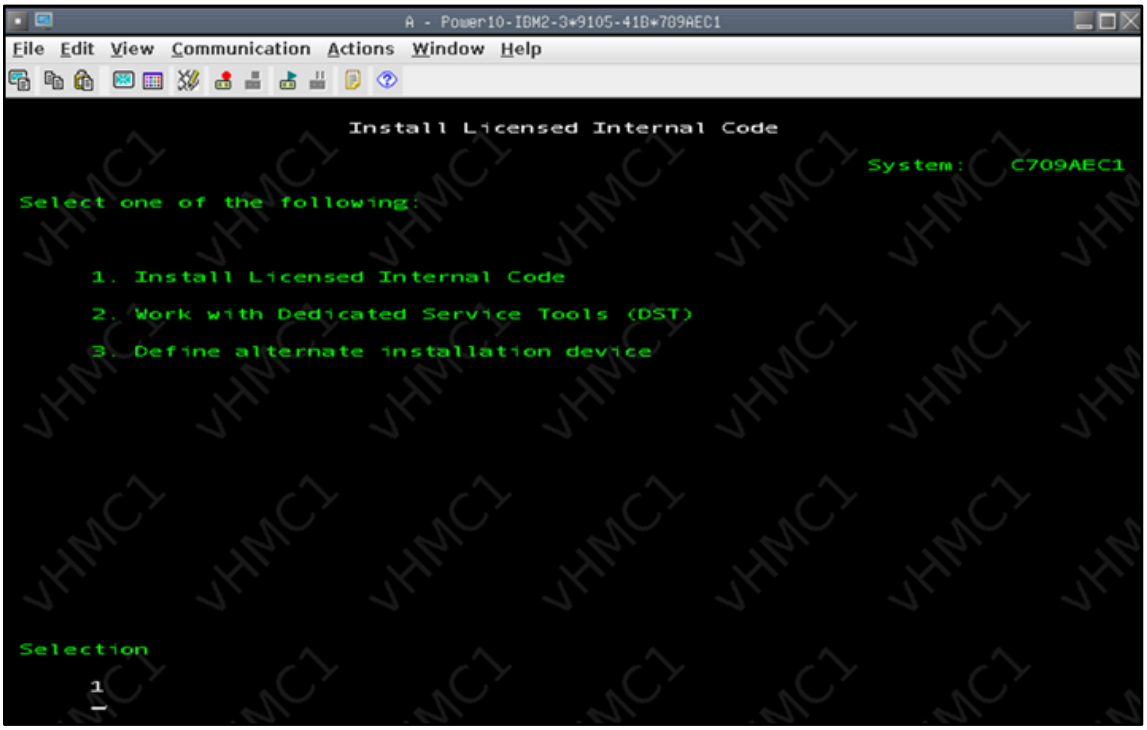
Volume containing the SAVSYS is loaded in tape drive 1. No other tapes loaded in any other drives.



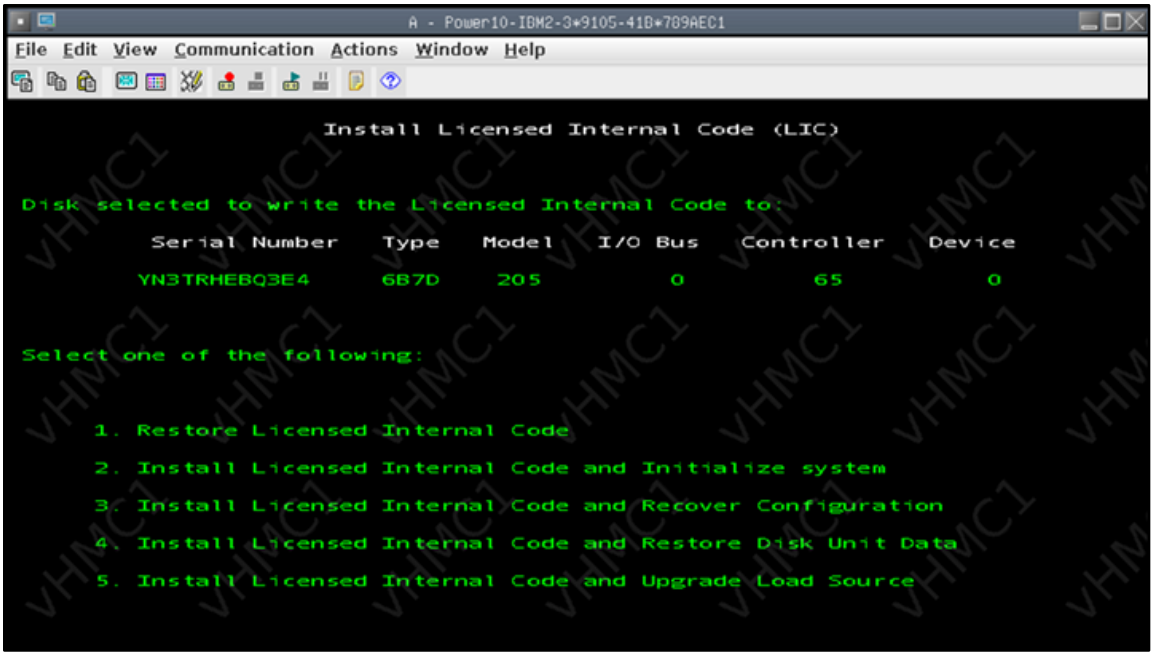
Initial Program Load (IPL) the LPAR:



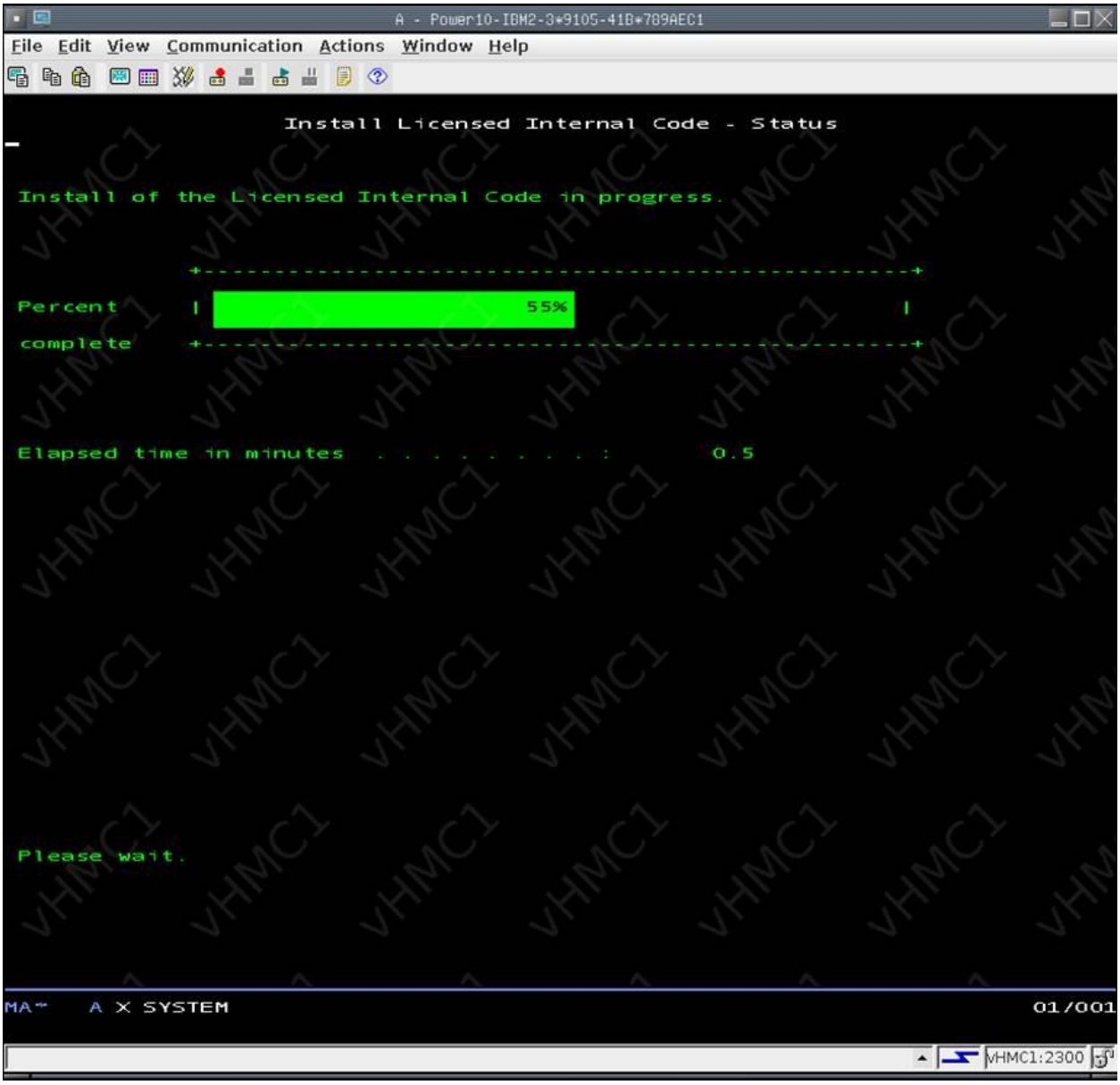
After the LPAR has IPL'ed the DST sign on screen is displayed and you sign on. Then, take option 1 to install the LIC (Licensed Internal Code)



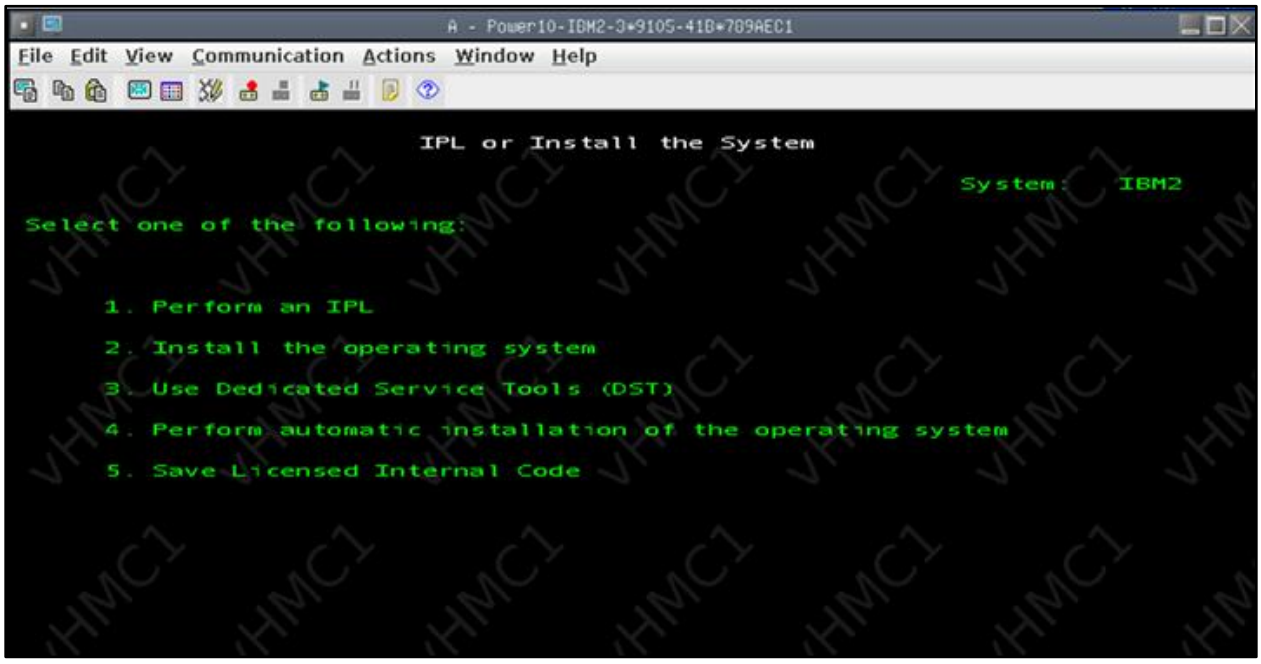
From the next screen you can select various options depending on what you wish to accomplish. In this test, option 1 was chosen to restore the Licensed Internal Code (LIC).



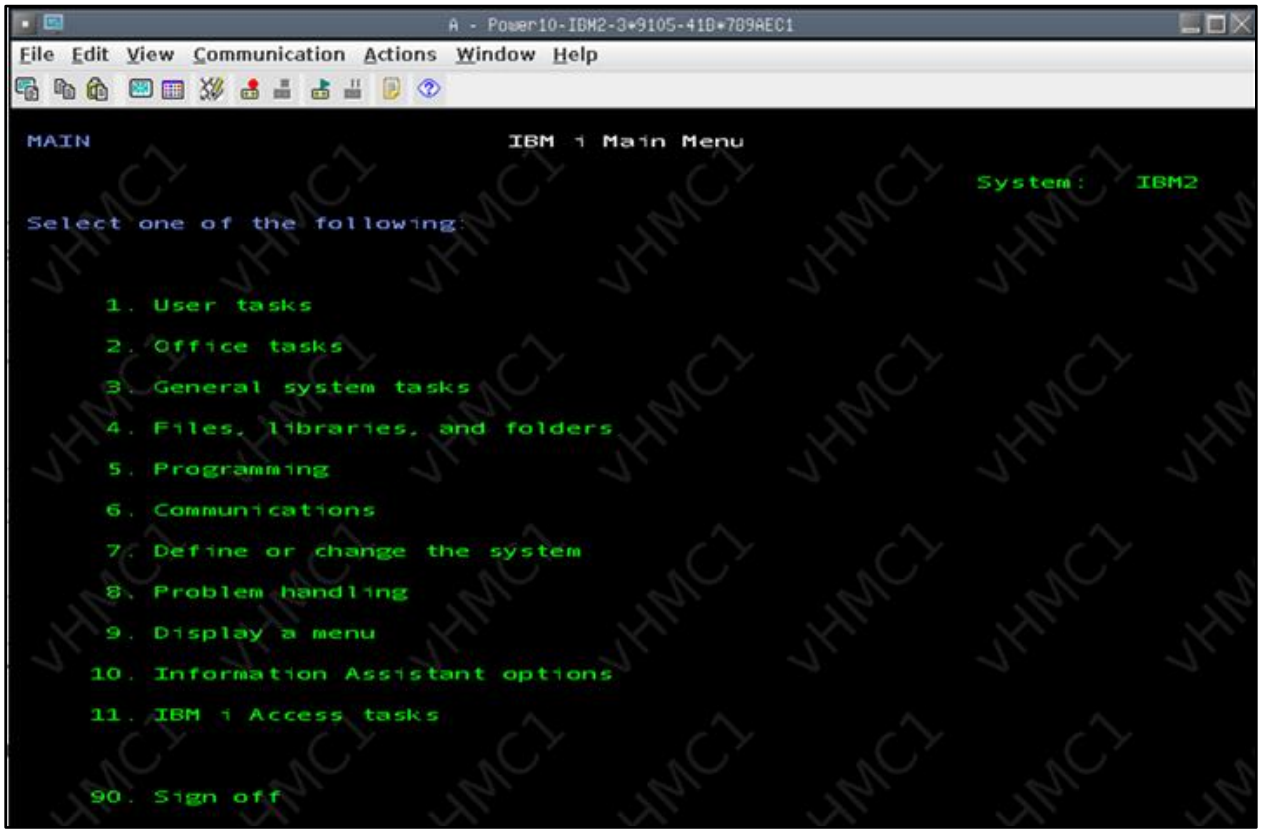
Licensed Internal Code (LIC) is being restored.



After LIC is restored and the LPAR reboots, you can sign on and take the next step to restore the rest of the operating system and user data. In this example option 1 was provided to perform IPL.

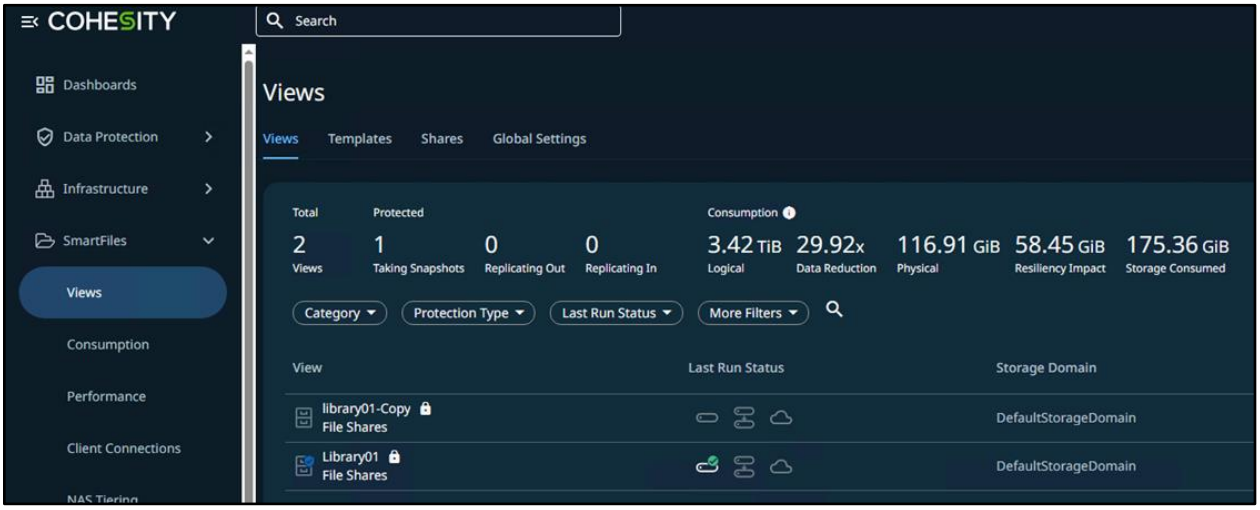


Now the partition is up.



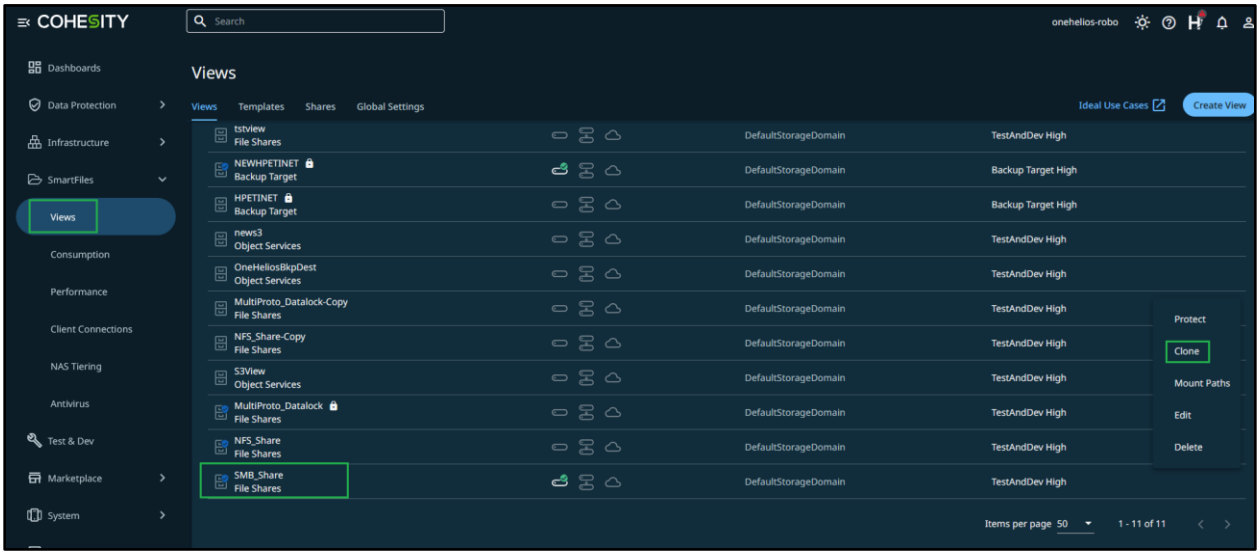
Recovery using SMB View Clone Option

Recovery from the Virtual Tape Library can be accomplished by using SMB View Clone from Backup. The Clone View can be mapped to LaserVault as Clone/Copy of Library from Backup and Data can be restored/copied from the Clone View.

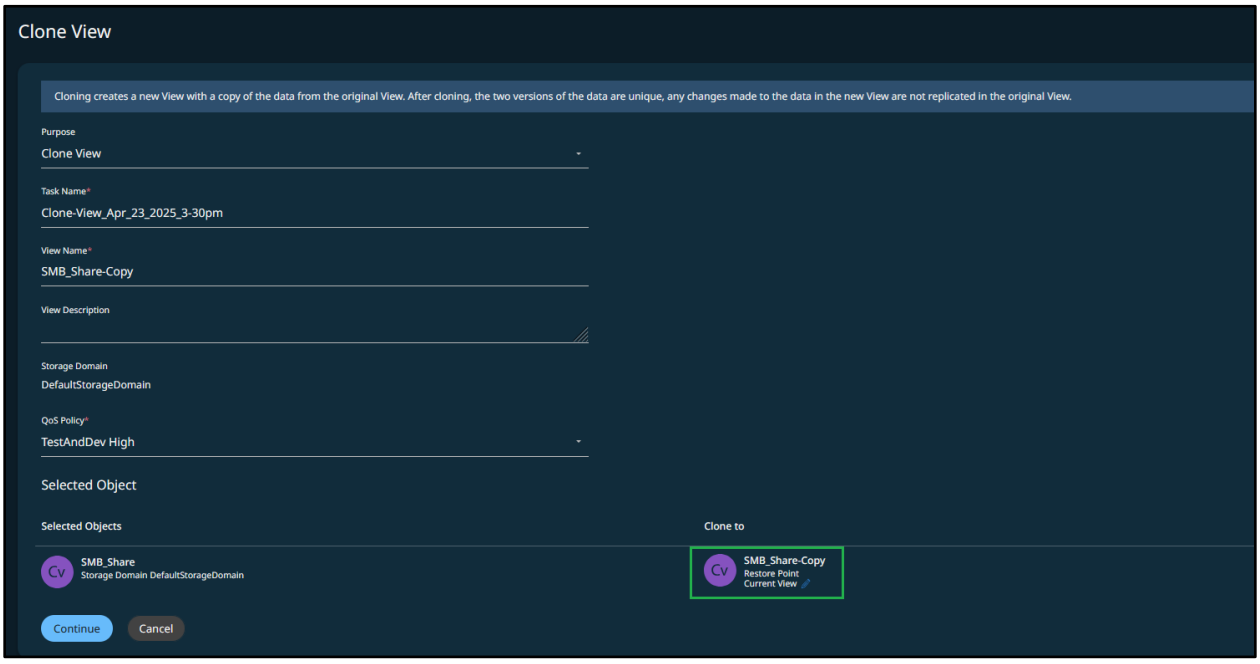


To clone a library from SMB View, follow the steps below:

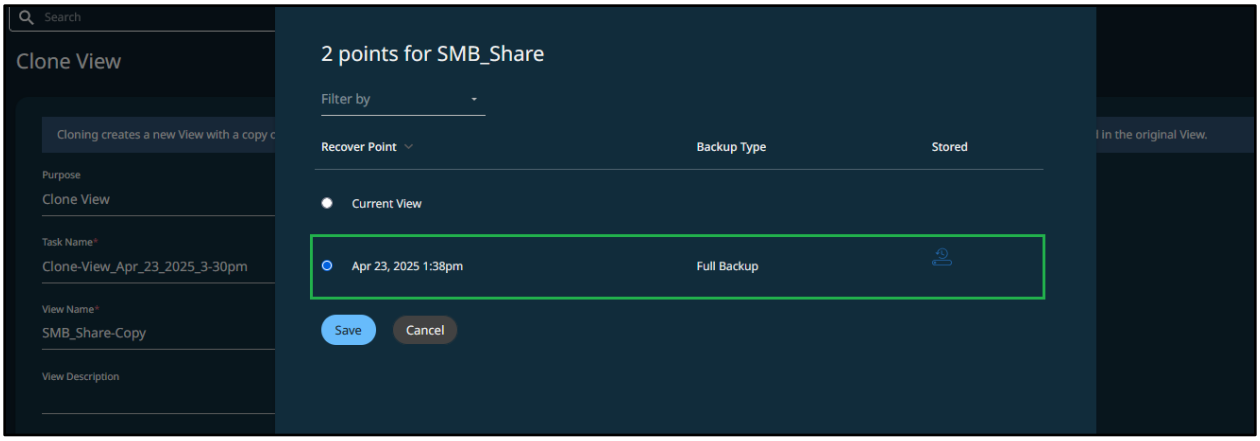
1. For example, SMB_Share is the view, click on ellipses (3 dots) icon, choose ‘Clone’.



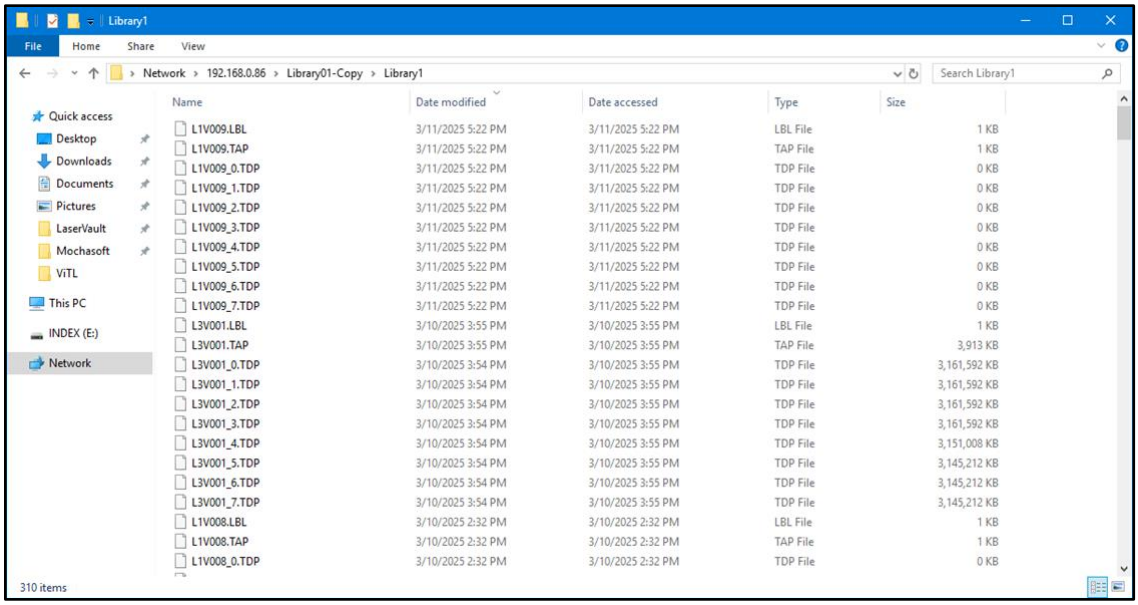
2. ‘Clone View’ wizard comes up, edit the clone ‘View Name’ appropriately as required. Select the ‘Pencil’ icon on the Clone view name.



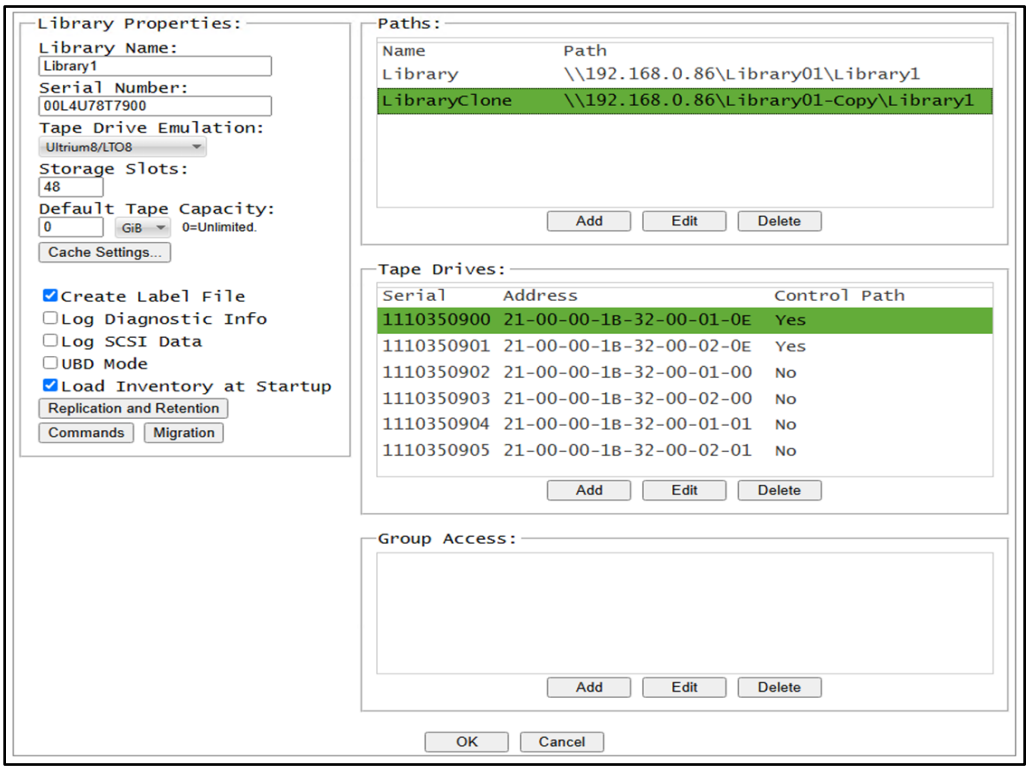
3. Wizard to choose either ‘Current View’ of ‘Backup’ from which View has to be created shows up. Choose the appropriate Backup.



4. The Clone View can be mapped to see the contents on the LaserVault hosted Windows Server.



5. Update the LaserVault to point to Cloned View.

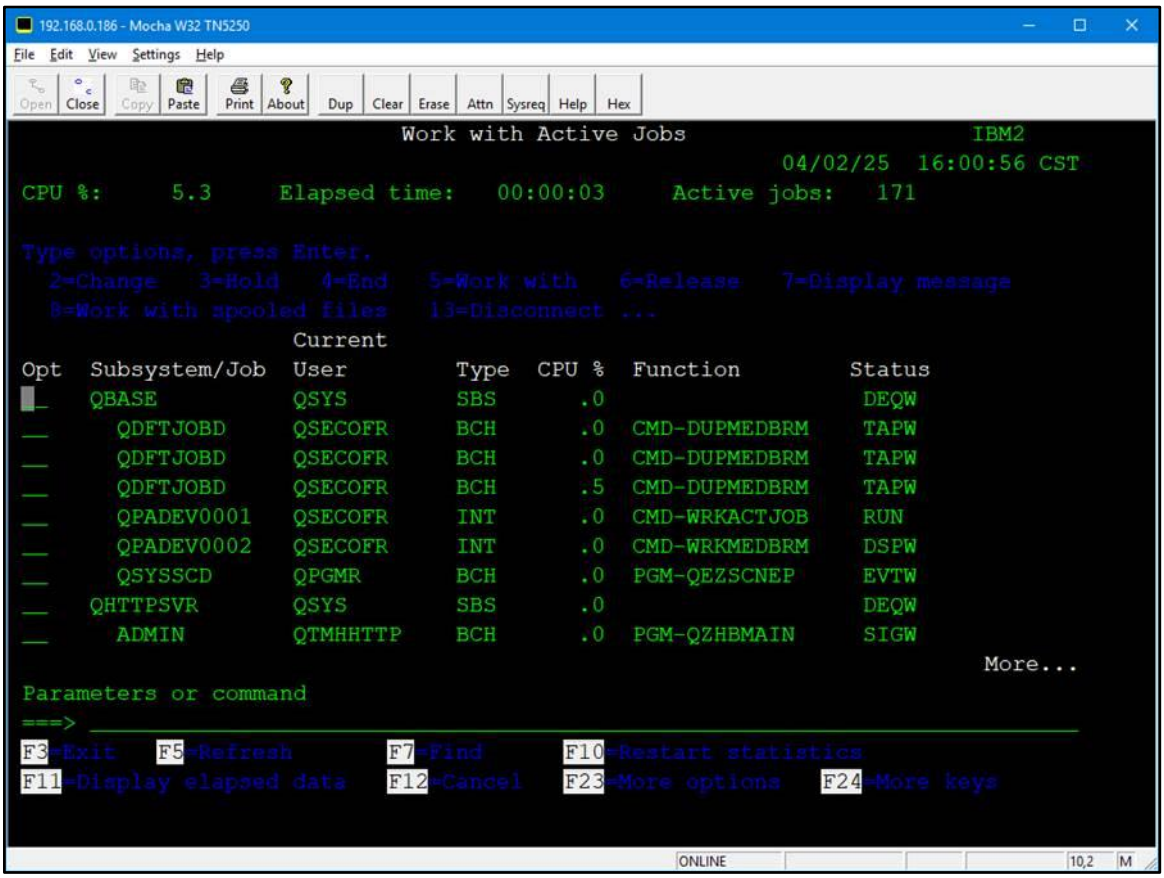


At the IBM i end, the Clone View of Backup from which DATA needs to be recovered is available. Restore the Data from Cloned View and overwrite to the source/original view or delete the DATA from source and restore from Cloned View.

Migration

Migration of data from different vendor storage to Cohesity Data Protect Cluster is the Use Case which is supported by Cohesity. The Source Storage systems could be any that IBM i-Series has been keeping Data on.

Here is an example of how migration is achieved using the DUPMEDBRM (Duplicate Media using BRMS) command. In this example, DUPMEDBRM will be used to duplicate 3 tapes (e.g., it could be DataDomain) in parallel. The jobs will be submitted to run in batch (background process).



The following are a few considerations during Migration:

As migration jobs tend to run longer, it is obvious to expect performance impact on scheduled backups and occasional restore. However, that can be mitigated by proper tuning.

- On the IBM i Server, BRMS tool has options to set **Priority** to the jobs ensuring QoS to Backup and Restore over migration jobs. For e.g., Backup jobs can have priority no. 60 and a migration job as 40.
- On the IBM i Server, BRMS tool also provides an option to **Pause/Resume** migration job which can be leveraged to ensure Backup jobs are completed on time
- CPU load during migration is in the range of 5-6% leaving enough computing power to cater to priority jobs.

Summary

Cohesity's NAS delivers the best performance using web-scale architecture. Using SMB NAS as a target for IBM iSeries Servers via LaserVault ViTL, delivers a comprehensive data protection solution to any organization. Cohesity delivers a proven backup solution that is infinitely scalable, highly available and provides unparalleled performance.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Shivananda K N is a Senior Solutions Architect at Cohesity. In his role, Shivananda focuses on enterprise data protection, solution validation, solution testing, solution qualification, and software usability.

Other essential contributors included:

- **Mahesh Pulipati**, Principal Solutions Architect at Cohesity
- **Asim Aleem**, Senior Lead Architect at Cohesity

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.0	April 2025	Protect IBM Power Systems iSeries with Cohesity using LaserVault ViTL

ABOUT COHESITY

Cohesity is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including six of the Fortune 10 and 44 of the Fortune 100.

Visit our website and blog, follow us on Twitter and LinkedIn and like us on Facebook.