COHESITY

Archive Data to Tape with Cohesity Platform & QStar

Use QStar Archive Storage Manager with Cohesity Platform for Long-Term Data Retention

Version 2.0

July 2025

ABSTRACT

While many organizations are increasingly adopting cloud solutions for data archiving, tape remains a cost-effective and widely used medium for long-term data retention. In some regions, tape archival is also mandated for compliance and legal purposes. To address these needs, the Cohesity Platform offers a comprehensive, cloud-agnostic archival solution that now integrates with QStar. This integration simplifies the process of archiving data to tape, helping organizations meet regulatory requirements while optimizing storage costs.

Table of Contents

Figures

Tables

The Need for Archival to Tape

Rapid advances in technology demand that organizations implement long-term data retention strategies for streamlining the influx of new data. In addition to using the data for internal audits and analytics, in many countries, long-term data retention is mandatory for fulfilling a host of compliance, regulatory, and legal requirements. You can safely move the sensitive data that you want to retain for future reference or regulatory compliance to an archive environment. This serves as an air-gap strategy to secure your data from threats and also as a way to reduce primary storage consumption and costs.

Tapes are the go-to medium for long-term data retention, and the incremental costs of backing up to tapes are negligible in most environments. The key advantages of using tape for archiving are its low cost of ownership and its long-term durability and robustness.

When choosing a tape archival solution, you should consider many factors, including:

- Security
- Recovery window
- Write speed
- Reliability
- Interoperability

Factoring in all major requirements, Cohesity partnered with QStar, a leading enterprise-class tape archival solutions provider, to provide an all-inclusive, data- and tape-agnostic archival solution. Achieving your long-term data retention and archival objectives is now made simpler with Cohesity.

This solution guide details the steps and best practices for backup administrators to set up, schedule, and manage archives on a QStar tape library using Cohesity Platform.

> **NOTE**: In addition to tape-based archival, Cohesity provides a comprehensive, cloud-agnostic archival solution for long-term data retention in AWS, Azure, Google Cloud Platform, S3-compatible storage, and NAS.

Integrate with QStar for Long-Term Data Retention

Cohesity Platform integration with QStar Archive Storage Manager (ASM) for tape enables organizations to:

- **Improve efficiency**. Use advanced Cohesity algorithms for compression to optimize capacity efficiency and lower the cost of archival.
- **Secure data**. Both inflight and at-rest encryption based on the strong AES-256 CBC (Cipher Block Chaining) encryption standard.
- **Derive greater value from data**. Faster access and retrieval of data to make data more useful to business teams seeking to uncover meaningful insights from previously untapped data.

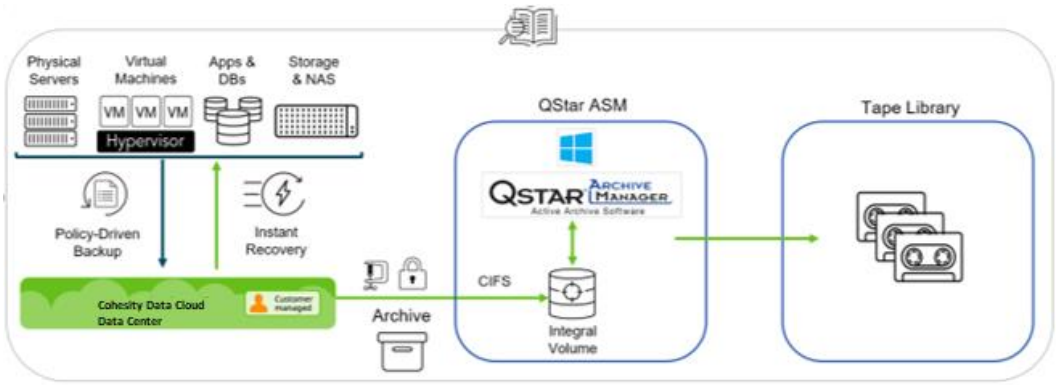
QStar has an in-house high-performance Tape Disk Object (TDO) file system to manage tape libraries with File Spanning capability. This delivers improved data consistency and integrity across tape libraries. TDO offers several advantages over the Linear Tape File System (LTFS) format.

The QStar server handles a qualified list of tape drives and exposes them as media. The interaction between these media and Cohesity Platform is facilitated by logical volumes in QStar, which are termed as QStar Integral Volumes (IVs). Each IV consists of a disk cache and the media associated with it. QStar IVs are exposed as CIFS Shares to Cohesity Platform.

QStar ASM is a Windows Server application configured to interface with clients for ingesting data and to integrate the QStar server for writing to tape. Cohesity Platform leverages QStar ASM as the media manager for tape libraries and provides a ‘single pane of glass’ approach to data management. When integrated with QStar ASM, Protection Policies in Cohesity Platform determine which backup images need to be archived to tape.

Cohesity ensures fast and secure archival with swift recovery options, without compromising data integrity. Before writing the data to the QStar IVs, Cohesity Platform first encrypts the data in the Cohesity cluster, eliminating the risk of data breaches due to loss of tapes. The data is also indexed and compressed before being pushed to QStar IVs and consequently flushed to tapes without delay. You can find information about these tape archives at any time on Cohesity Platform. This solution also boasts a fast and convenient workflow to recover data without losses or hiccups.

Figure 1: Cohesity Platform for Long-term Tape-based Data Retention

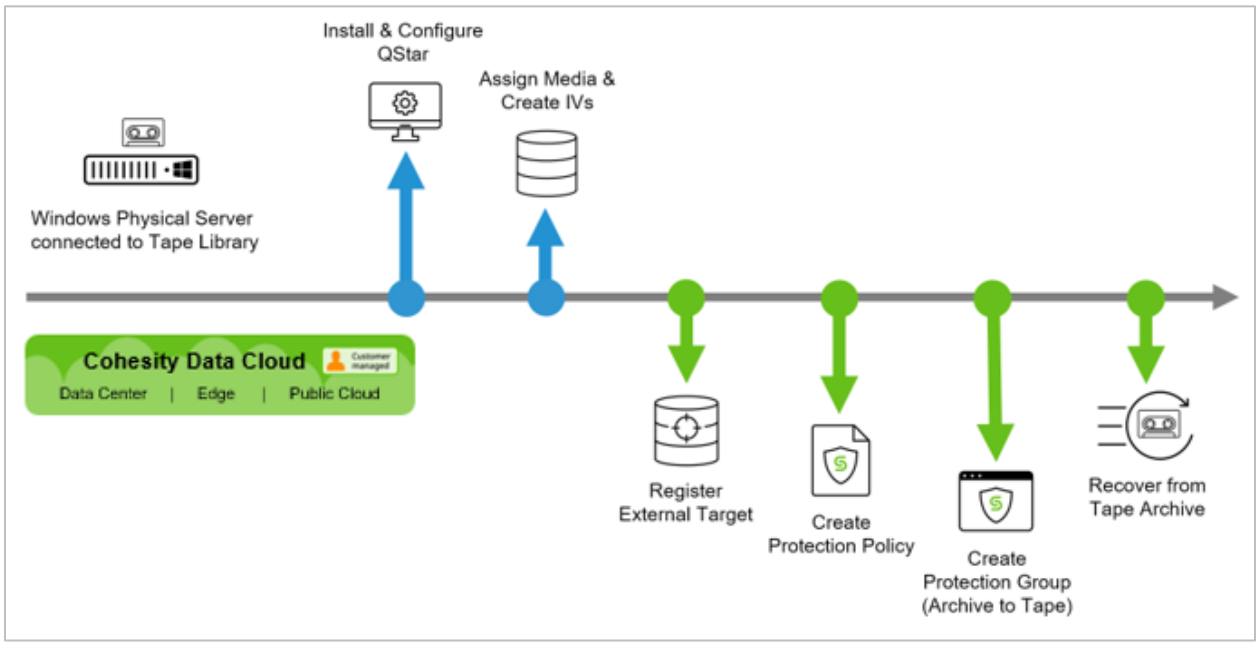


Tape Archive Using QStar Archive Storage Manager (ASM) and Cohesity Platform

To set up and start using QStar with Cohesity Platform, complete the following setup tasks:

1. Install and configure QStar on the Windows server.
2. Assign media and create Integral Volumes.
3. Register QStar Integral Volumes as External Targets on Cohesity Platform.
4. Create Cohesity Protection Policies and Protection Groups to archive your sources.
5. Recover from tape archive.

Figure 2: Cohesity Platform with QStar Solution Workflow



NOTE: Before you begin configuring archival to tape, see the list of supported workflows.

Configure QStar for Tape Archive

QStar ASM is a software solution that enables you to use tapes as a NAS interface for applications that need a simple way to store data for long-term retention purposes.

A QStar server installed on a Windows server acts as the primary External Target for the Cohesity cluster.

> **IMPORTANT**: The Backup Administrator is responsible for configuring the required tape library and connecting the Windows server that runs QStar to the physical tape libraries by means of standard interfaces such as NIC or FC.

For best results in archiving your data to QStar tape:

- Because this integration requires a fiber channel connection, Cohesity recommends you use a physical server running Windows Server connected to a supported tape library.
- See QStar's list of supported OS versions.
- Download QStar's Currently Shipping Supported Hardware List for tape libraries.

To configure QStar for tape archives on Cohesity Platform:

1. Install QStar Archive Storage Manager (ASM).
2. License the QStar Software.
3. Configure the tape storage library.
4. Create and mount Integral Volumes.
5. Assign slots to the media to use with QStar.

Install QStar ASM

To Install the QStar ASM on your QStar server, make sure that the following conditions are satisfied:

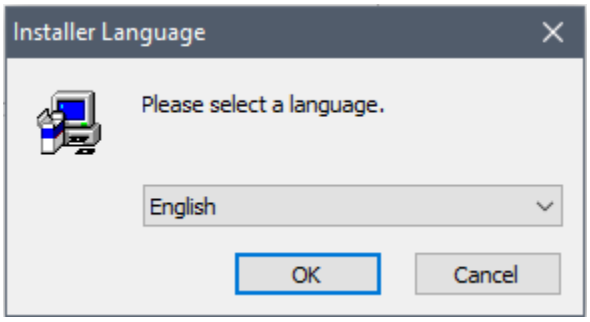
- Tape library is properly configured and is detected by the Windows server on which QStar software will be installed.
- Microsoft Removable Storage Services are disabled.
- Antivirus software is disabled. You can (and should) enable it again after you complete the installation.
- Exclude the following folders from the antivirus check:
  - QStar Cache Folders
  - QStar Installation Directory
  - QStar mounted directory and/or resulting SMB shares.

> **NOTE**: For the supported version of QStar ASM, see **QStar Archive Storage Manager** in the Supported Software list in the Online Help.

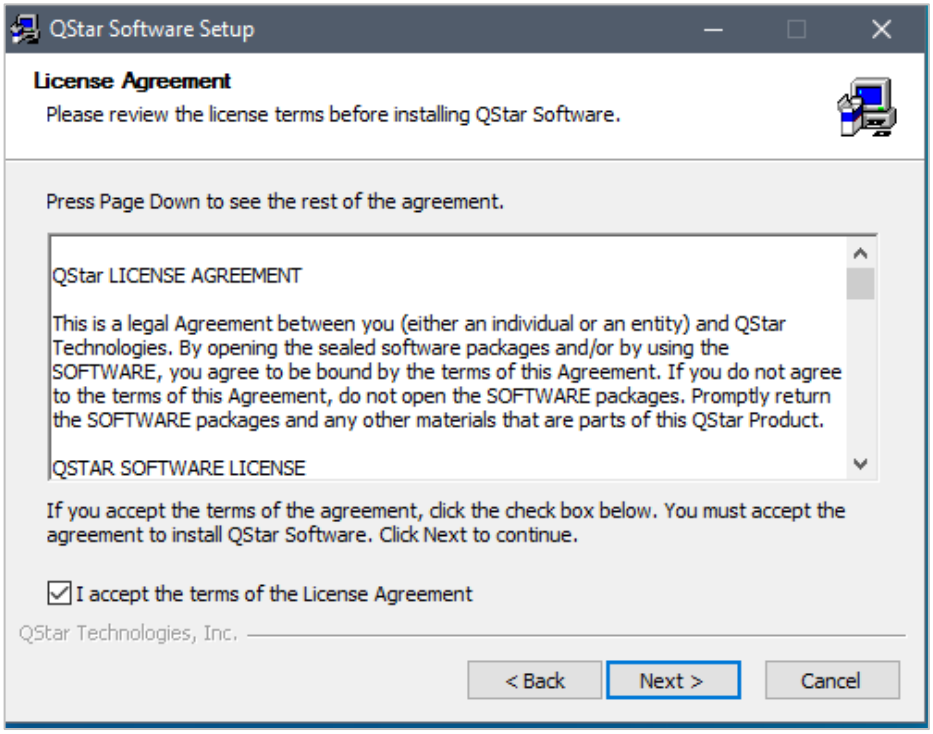
To install the latest QStar ASM 7.x:

1. Run the installation binary, as an administrator.

2. Select your preferred **Installer Language** and click 'Next' to continue the installation.

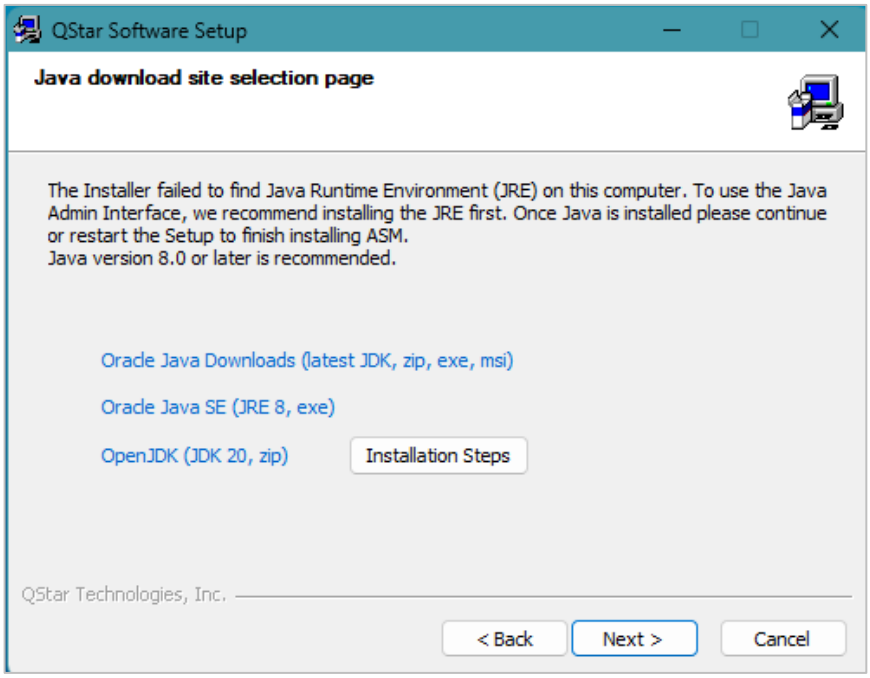


3. Accept the **License Agreement** and click **Next**.

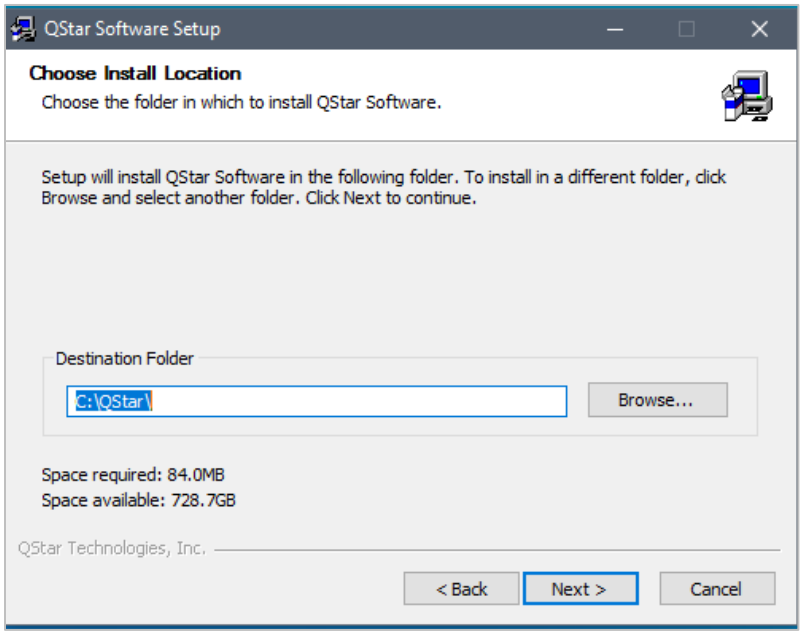


4. Java or OpenJDK is required for the QStar GUI. This can be installed later if needed, click Next to continue.

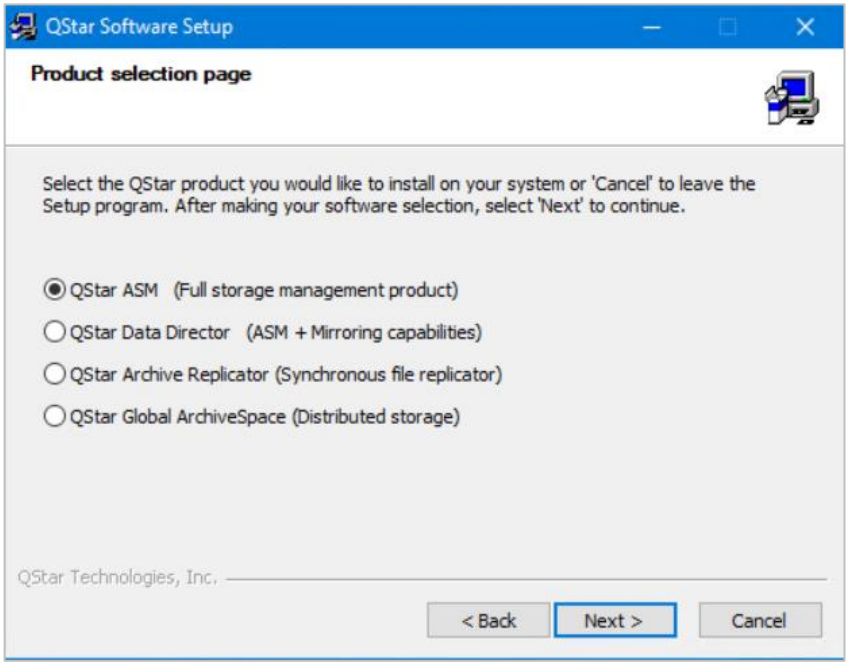
> **NOTE**: QStar recommends Microsoft OpenJDK to be installed.



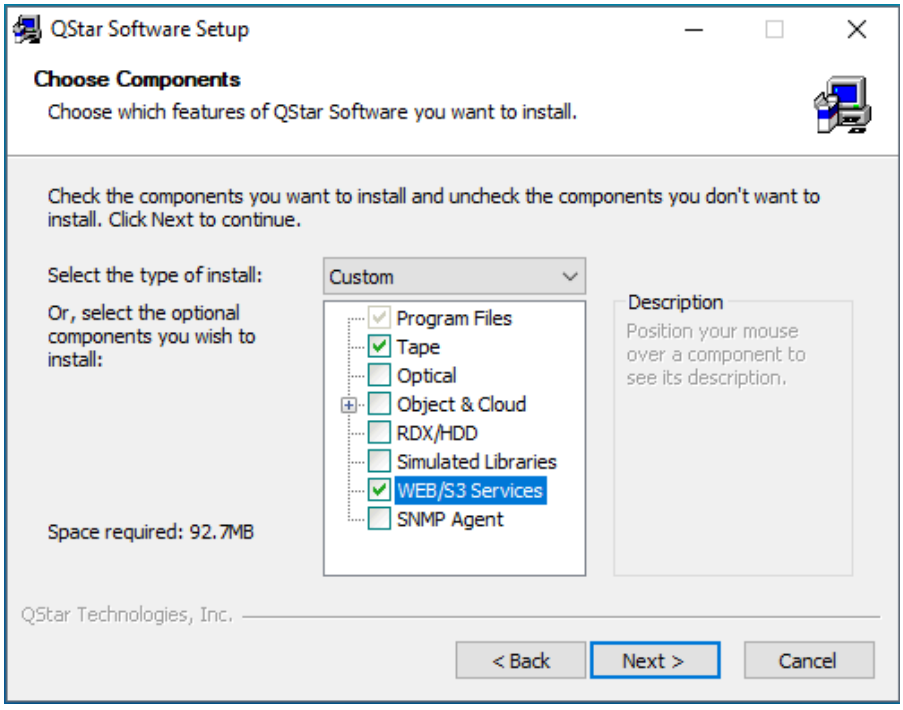
5. Enter the End User and Company Info.
6. Select a Destination folder for the installation and click **Next**.



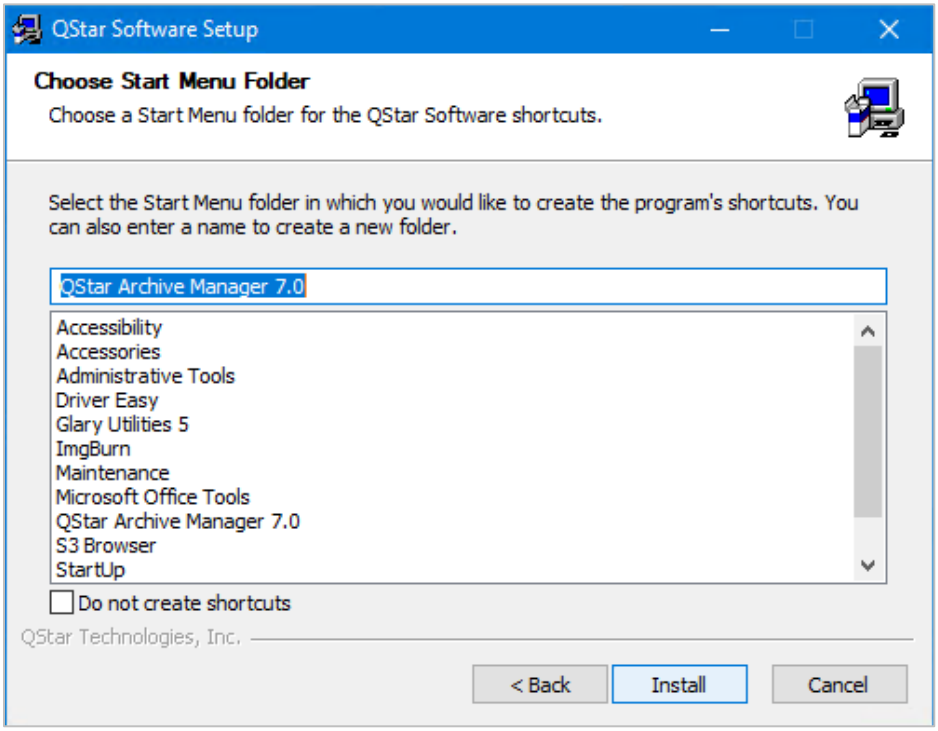
7. Select **QStar ASM** as the product and click **Next**.



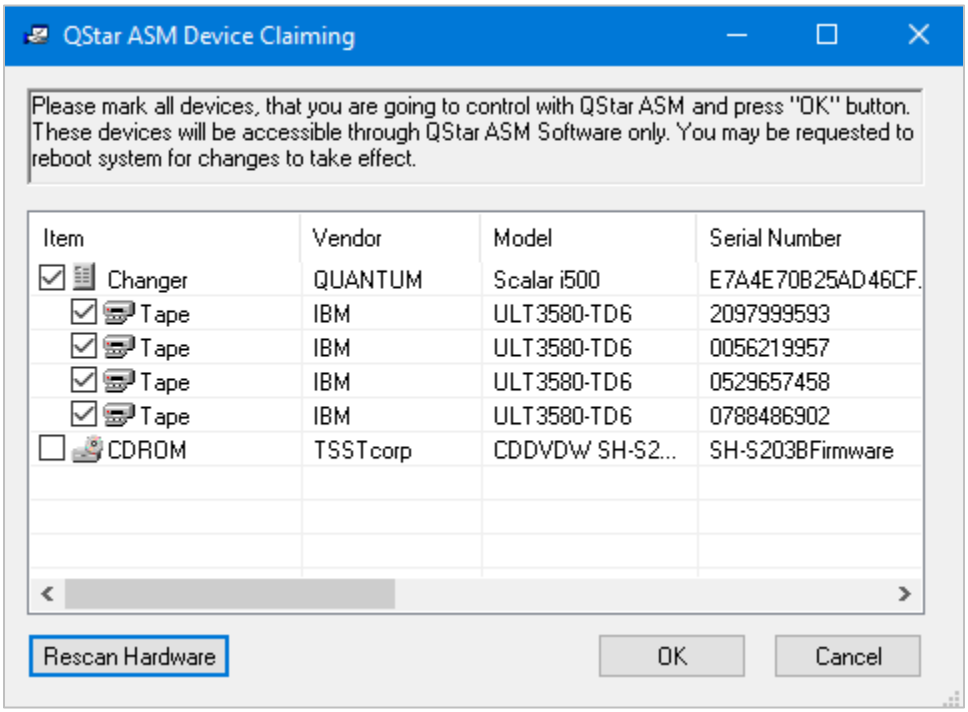
8. Select type of install as Custom and select the components to install as **Tape** and **Web/S3 Services**. Click **Next**.



9. Click **Install** to begin the installation and wait for the installation to be completed.



10. In the **QStar ASM Device Claiming** screen, select all the tape drives and libraries for use by Qstar and click **OK** (It's ok to click cancel and revisit this later if needed).



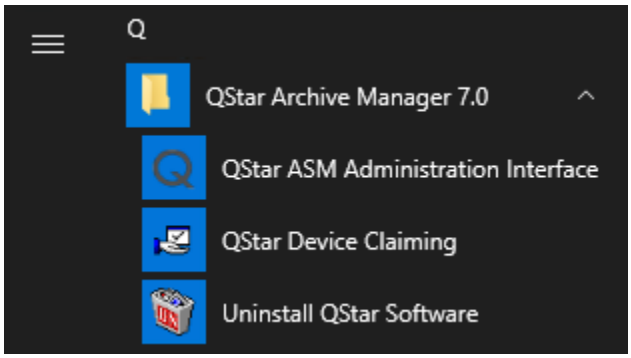
11. Click **Finish** and reboot the server to complete the installation.

License your QStar Software

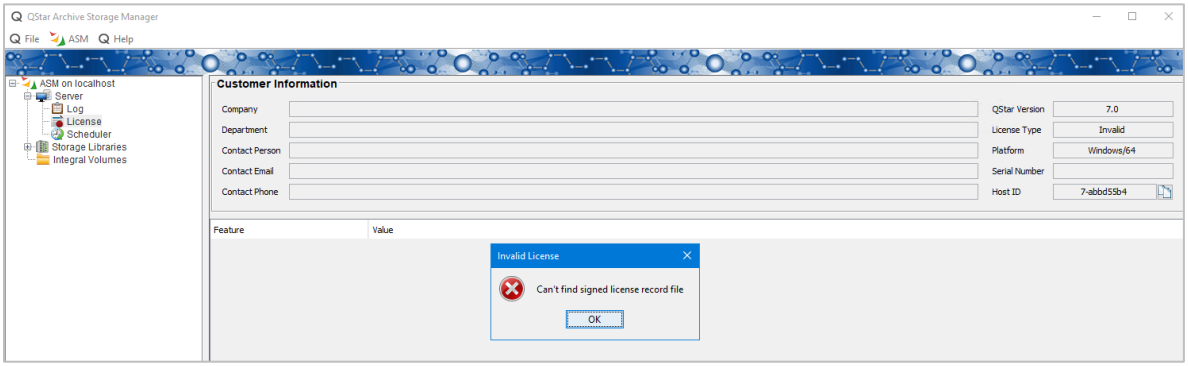
A key-based licensing mechanism protects your QStar software from unauthorized usage. License keys are directly and exclusively tied to the unique HOST ID of the CPU where the software is installed and provides access to the QStar software platform applications and features.

To install your QStar license:

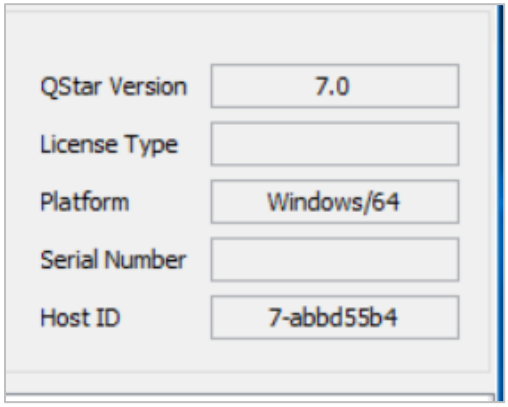
1. Launch the QStar ASM Administration Interface.



2. Browse to the **License** on the left. (‘OK’ the missing license warning).

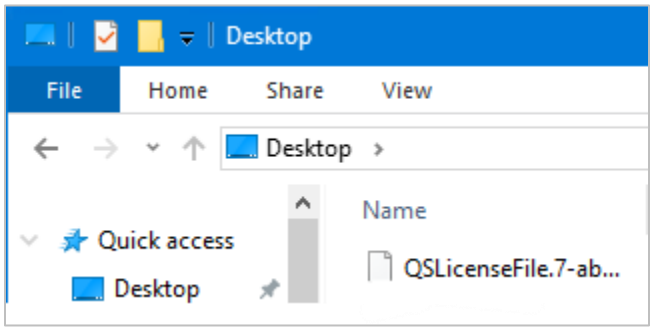


3. Get the **Host ID on** the right side of the screen.



4. Provide the **Host ID** information with your Cohesity representative and request a license key.
5. When the license key is received, copy it to the server and load it on the same screen.

6. Browse to where the file was saved and open it.



7. With the ASM application licensed, we can now finish the configuration.

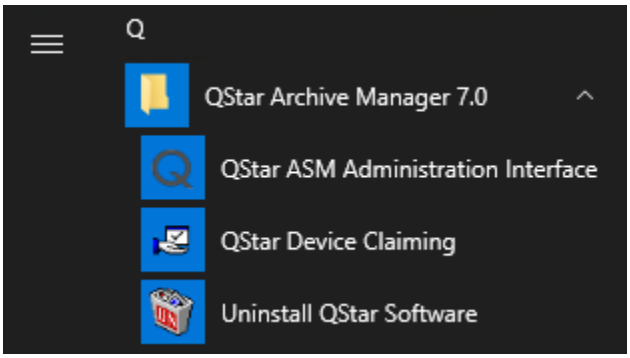
Configure Your Tape Storage Library

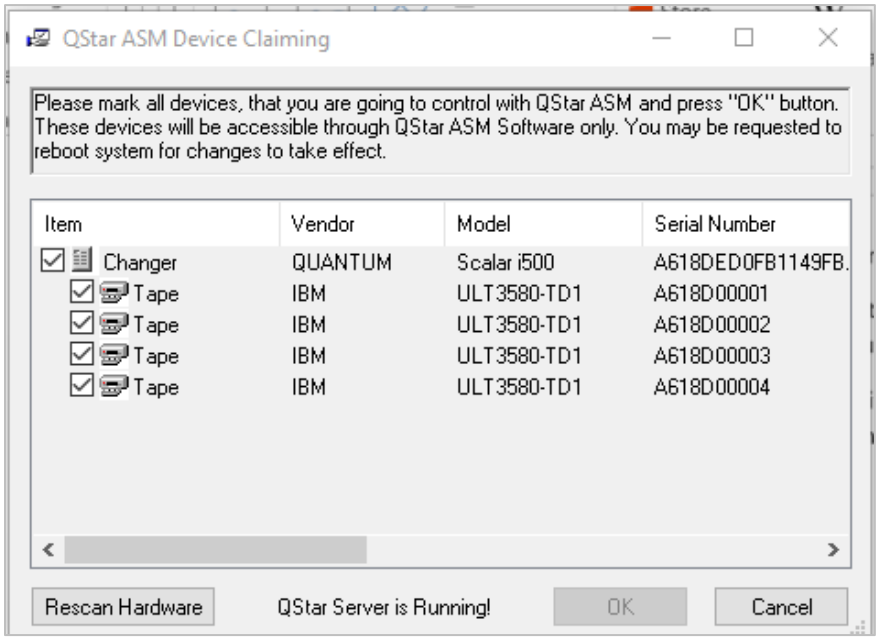
A tape server has multiple tapes to which the archived data is written. A drive changer monitors the tape usage and orchestrates data archival. Configuring storage libraries in turn brings the tapes under a drive changer and these tapes are made available under the library in the QStar Administration Interface.

First, storage will need to be configured. For Cohesity, this will be a tape library.

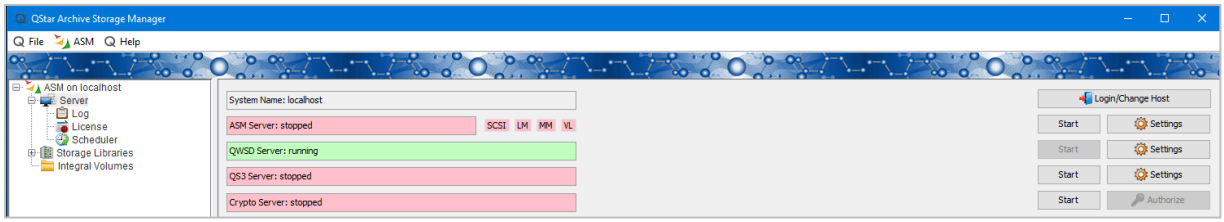
Check Windows Device Manager to verify that the tape library changer and drives are appearing properly. If QStar Device claiming was run during the installation, they will appear as “QStar Passthrough Driver” devices.

Otherwise, they will appear as the standard “Unknown Media Changer” and tape drives. If the latter is the case, before proceeding, run the “QStar Device Claiming application” and select the appropriate changer and drives.

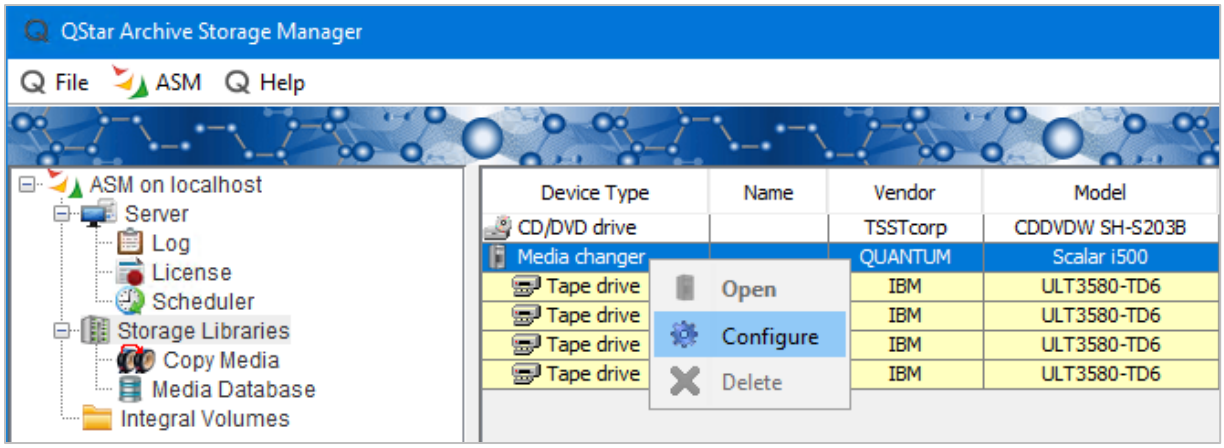




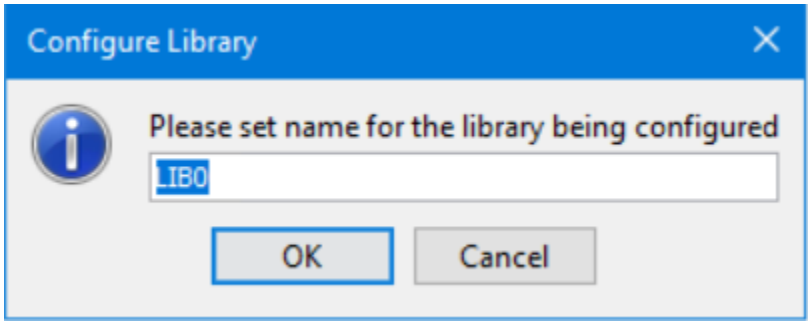
1. Before configuring tape devices, the ASM services need to be stopped. In the left-hand menu, click Server and then in the upper right, click the **Stop** button. Wait for the services to stop. Note: The QWSD service will remain running. That is OK.

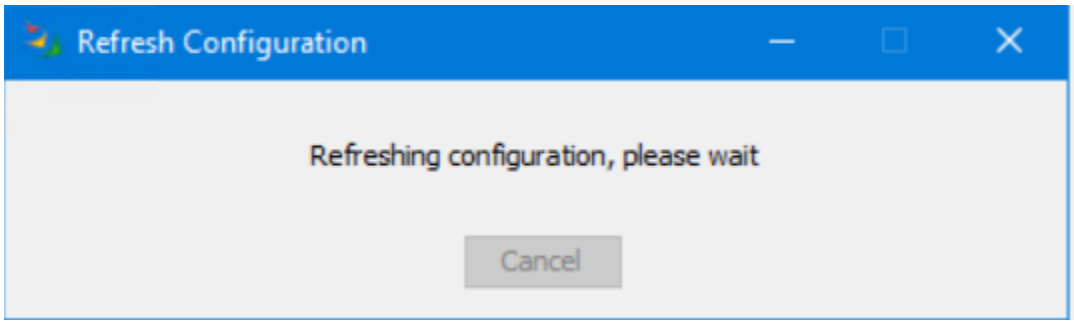


2. Now the tape library can be added, in the left-hand menu, select **Storage Libraries** then right-click the “Media Changer” row and select “Configure”.

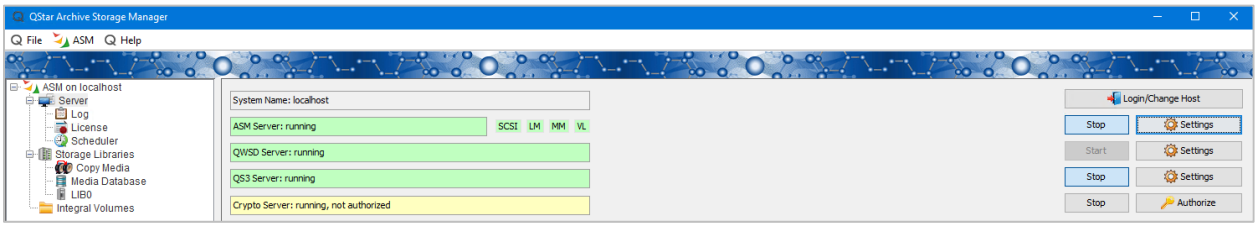


3. Name the library, or use the default, and click OK.



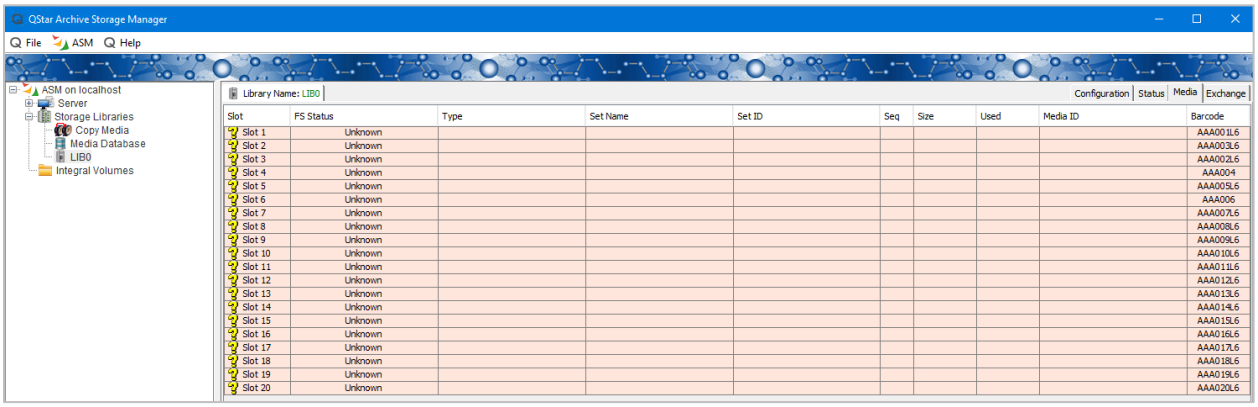


4. Once the libraries are configured, click **Server** on the left and Start the ASM Services, ensure ASM Server, QS3 (Web API), QWSD Services (UI) are running.



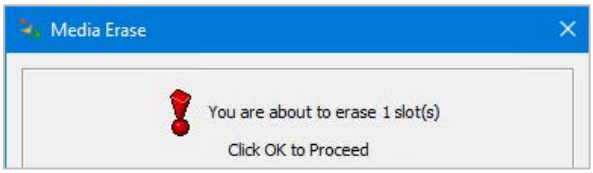
With the tape library attached, the next step is to prepare the media for use to configure your tape storage library:

1. In the left-hand menu, expand the Storage Libraries section and select LIB0 (or whatever it was named in step 3) If needed, in the upper right, select the “Media” tab.



2. Select one or more slots and then click the **Refresh** button. Media previously used by QStar will show detailed info. Erased media will show as such, and media written to by another application will still show Unknown. Unknown media will need to be erased. Please ensure that you are erasing the correct unknown media. Select one or more media and click Erase, then click OK for the default options. “**DO NOT use Full Erase unless directed to do so by QStar support”**

> **Note:** LTO9 has introduced a new process called “tape calibration” which can be very time consuming.
> Work with the tape vendor to enable auto-calibrate, or factor in the required time in this step. Generally, it requires about one hour per piece of media.



Create and Mount Integral Volumes

QStar exposes Integral Volumes using a web API for external users to perform read and write operations on the volumes. In short, IVs are the external interfaces for QStar .

Once the IVs are created, we assign a specific slot (or tape) to each of them. The sequence of tapes to be used is set during this step. (See Add Media to Integral Volume section for details.)

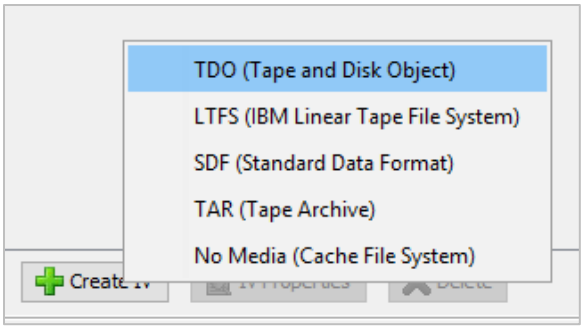
Once a tape is assigned to an IV, you must mount the volume for the tapes to make them ready for use. The Web services then expose the IV to be consumed by Cohesity Platform.

Create an Integral Volume

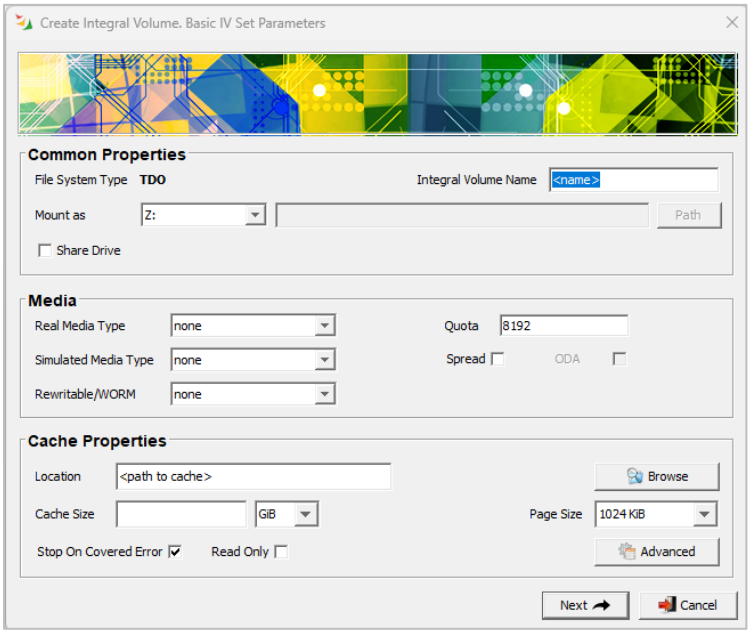
To create an IV:

With the library and media prepared, an Integral Volume (IV) can be created. The IV is what creates the link between the SMB file system and backend tape devices and media.

1. In the Qstar Administration Interface, click on the **Integral Volumes** section, and then click the **Create IV** button. Choose the desired type as TDO.



2. The Integral Volume dialog will open.

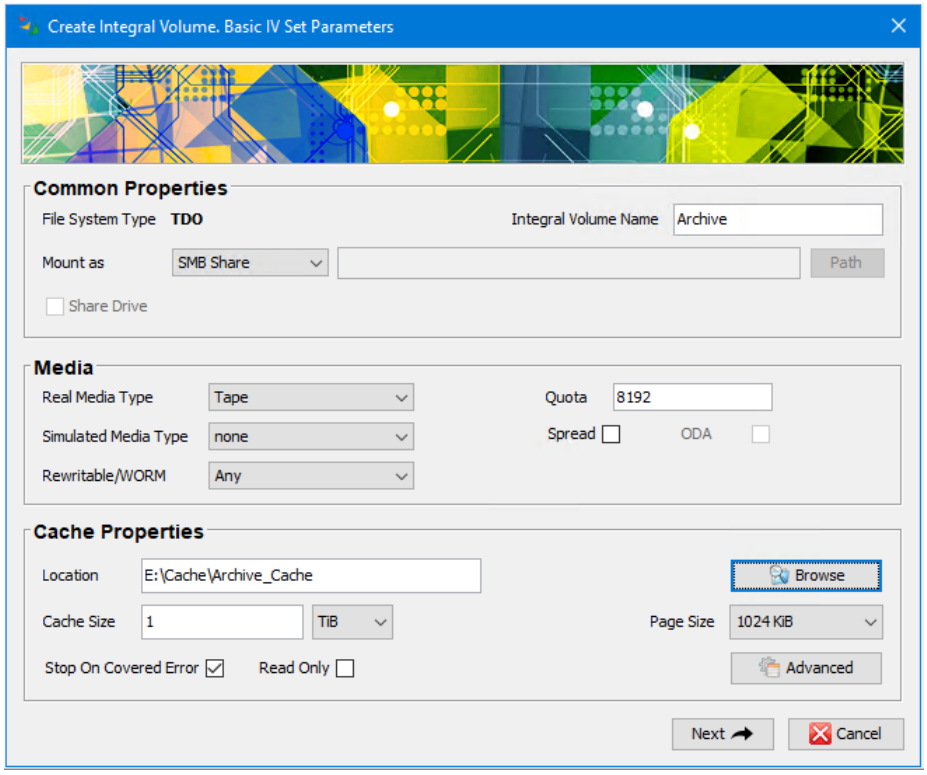


- The **Integral Volume Name** will also be the name of the Windows mount point and/or SMB share.
- Check “Share Drive” for mounting the volume.
- In the Real Media dropdown, select tape. Select all **Media Types** and then click OK.
- In the rewritable/worm dropdown, select **Any**.
- For the cache location, browse to a dedicated drive volume and create a new folder for the cache.
- Set **Cache Size** to 1TB NVMe or higher.
- Set **Page Size** to 1024 KiB
- Check **Stop on covered error.**

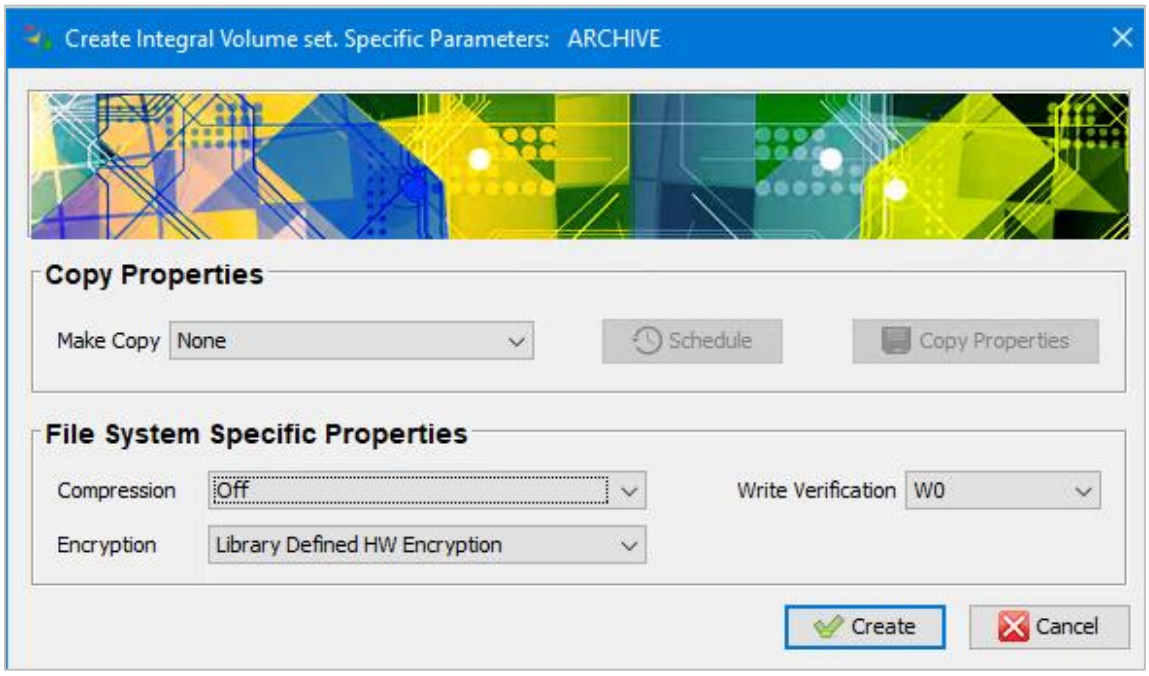
*The cache drive volume should be formatted with a 64k Allocation Unit Size
**Best Practice is to name this folder <IV-Name>_cache.

> **Note**: **Do not** store the cache on the OS drive, or any network attached drive. Use local or SAN attached disk only. For LTO7, 8, or 9 NVMe drives are required to fully utilize the speed of the tape drives. For sizing, 1TB is the minimum recommended size. Also, there is some data written to the volume separate from the cache, so leave at least 100GB free space on the drive, in addition to the cache size.

3. Click **Next.**



4. Set Compression to “Off” (as the data is already compressed by Cohesity) and Encryption to “Library Defined HW Encryption.” Use defaults for the rest and click **Create**.

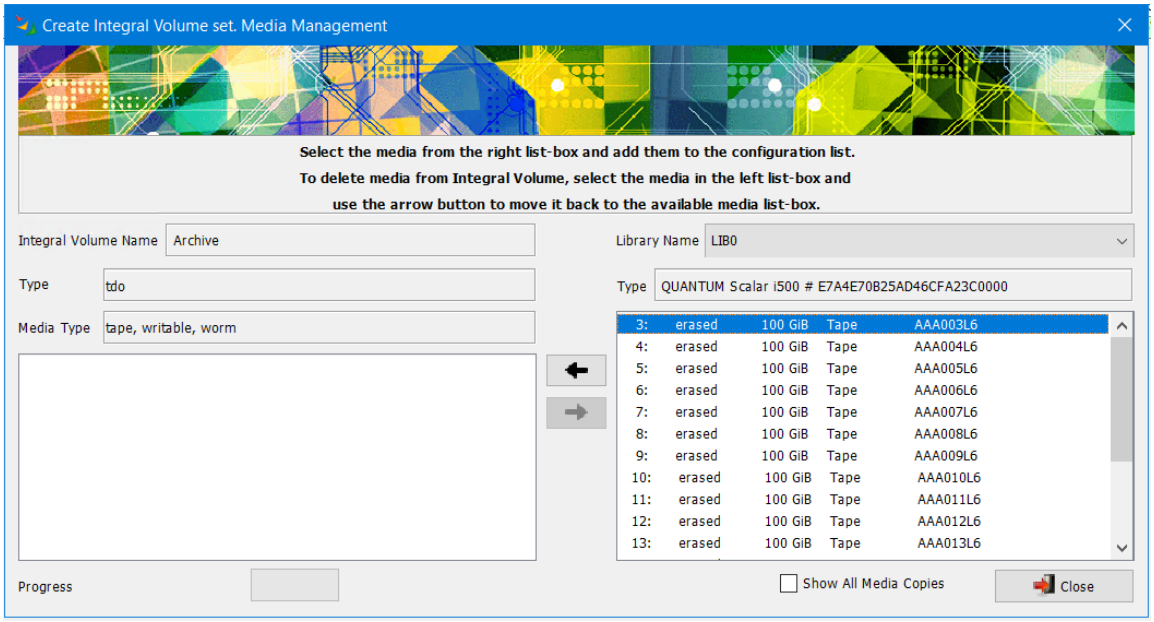


Add Media to your Integral Volume

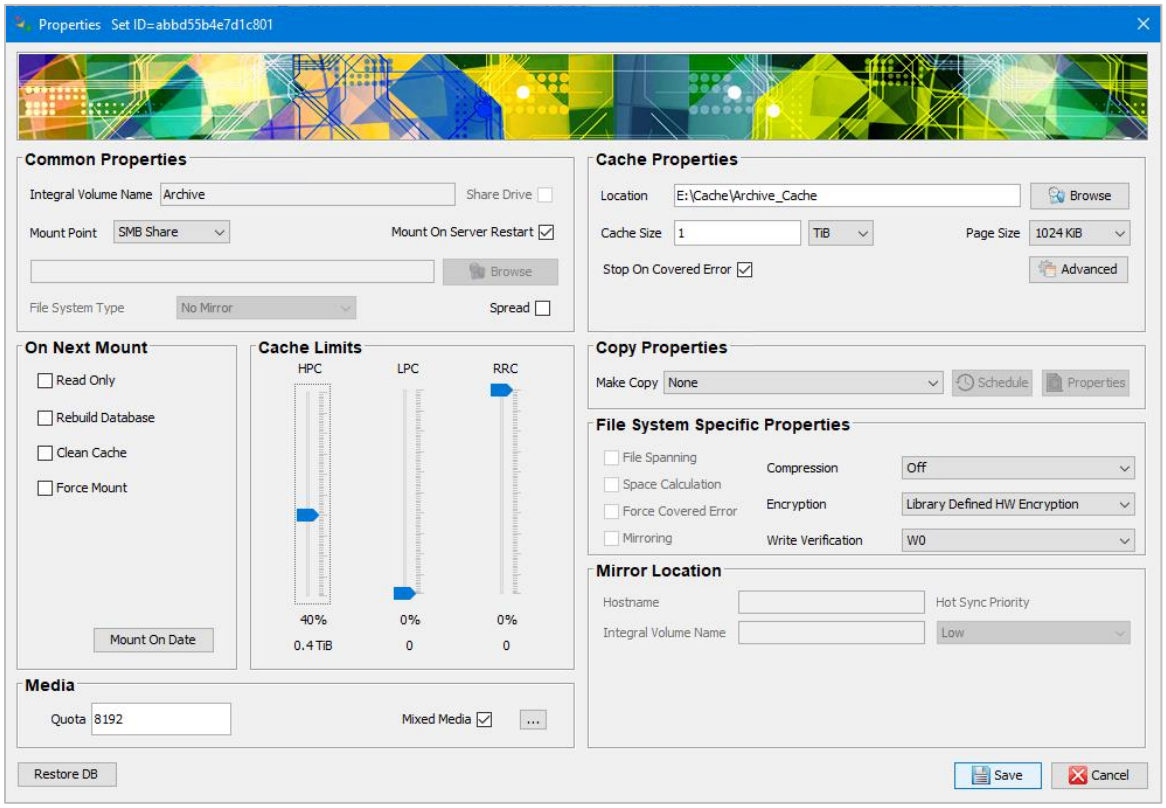
Once an IV has been created, you’re ready to add media to it.

To add media to your IV:

1. On the next screen, select **one** piece of Erased media to be initialized and assigned to the Integral Volume. Click the arrow to move it from Available to Assigned.



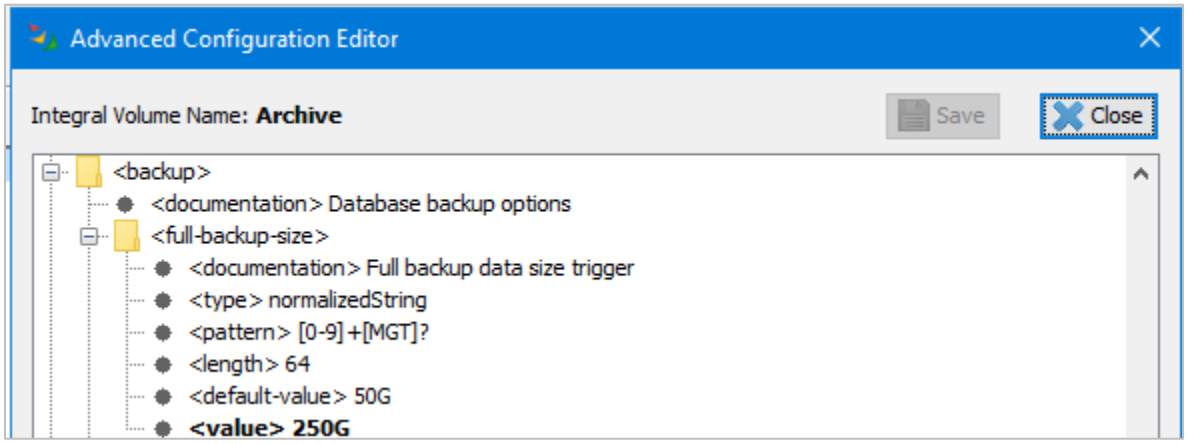
2. Next, two additional settings need to be changed that are not available in the initial creation dialog. Select the newly created Integral Volume in the left side menu, and then click on the **Properties** button.



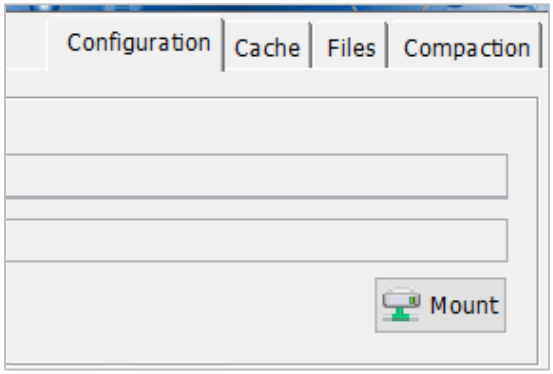
- Check the box for **Mount On Server Restart.**
- Drag the **HPC** slider down to 40%. (Keyboard Page Up/Down keys can be used to make it exact).
- Click **Save**.

3. Next to the **Properties** button, click the **Tuning** button. Scroll about ¾ of the way to the bottom and find the section titled <backup>.

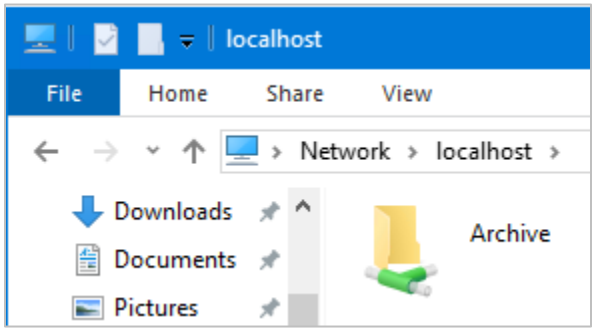
   In the line that is **bold**, change 50G to 250G. Hit Enter, then click **Save** and **Exit**.



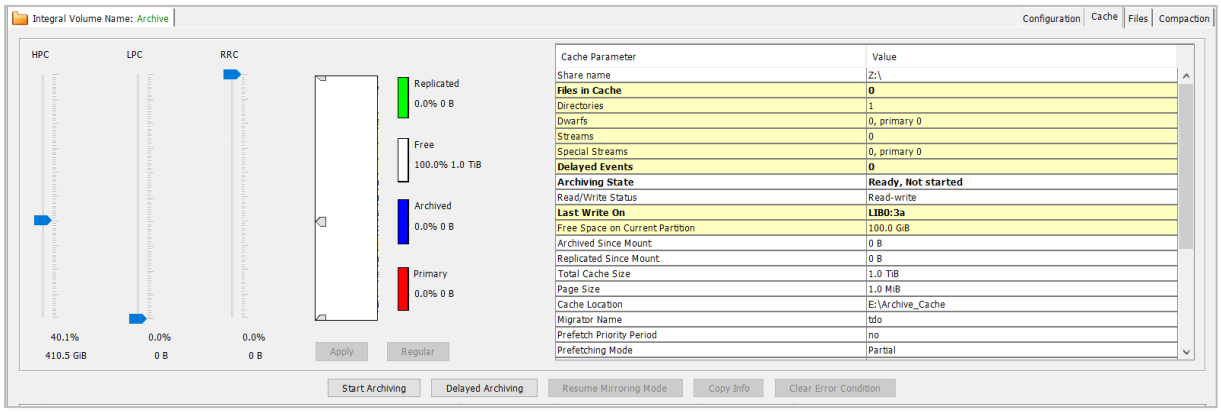
4. Finally, with the newly created Integral Volume selected, click the **Mount** button.



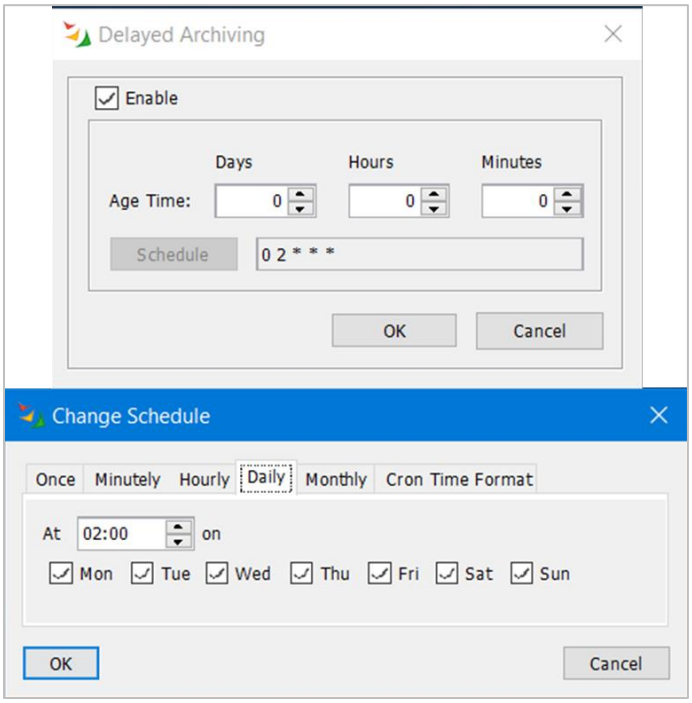
5. Once the mount completes, the SMB share will be available, however it will not appear by default in Windows Explorer. To access it, in the address bar, type \\localhost and hit enter.



6. Any data that lands here, when it hits the 40% HPC watermark, will then get written to tape. To view the status of the data archiving, with the Integral Volume selected, click the Cache tab in the upper right.



7. Lastly, if the 40% watermark isn't reached in a timely fashion, ASM has the ability to schedule archiving to take place. This can be as frequent as desired. To set the schedule, click **Delayed Archiving**. Check **Enabled** and then click **Schedule**. Set the desired schedule, then click OK and OK.

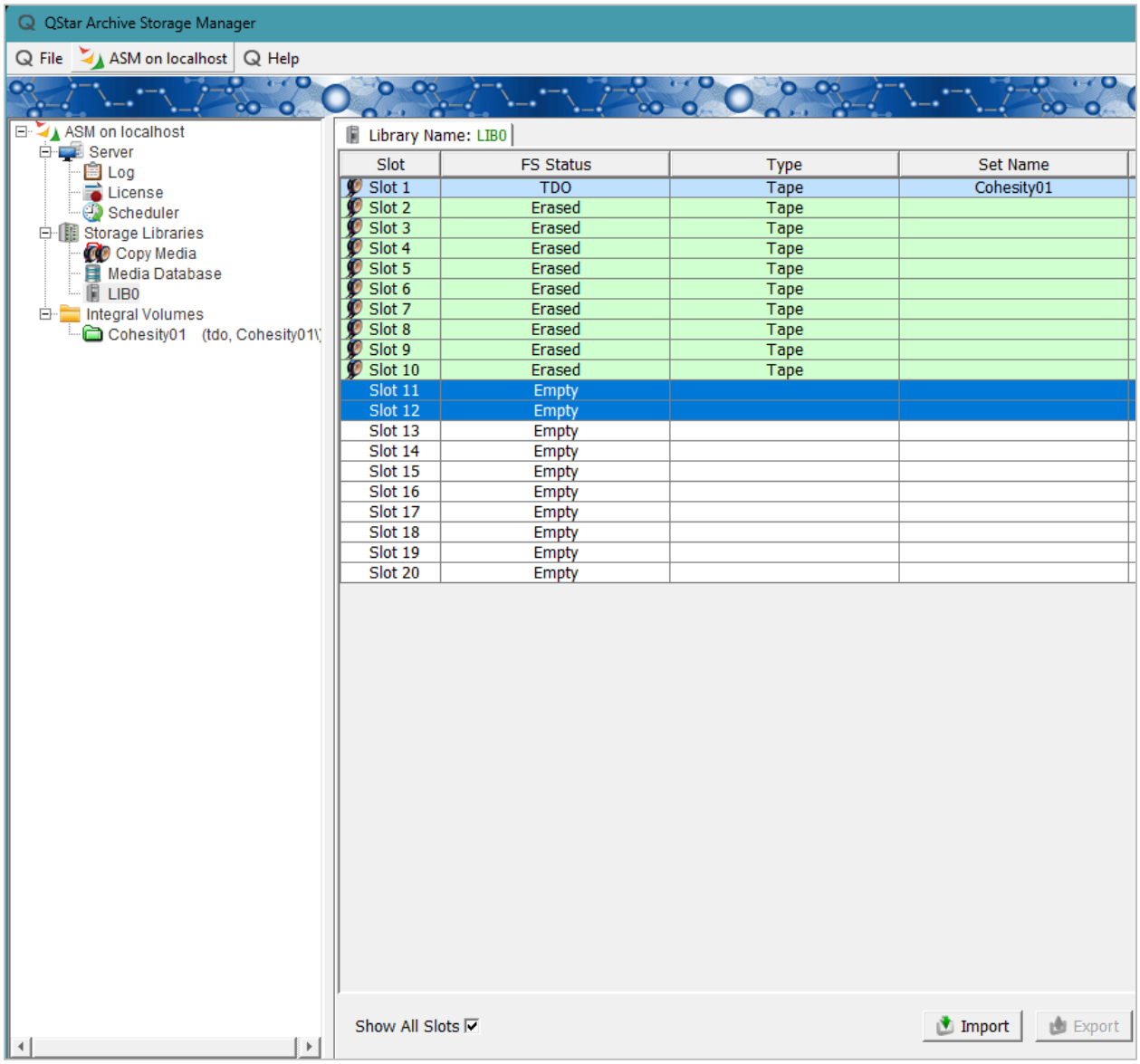


8. Launch the QStar Administration Interface, click Storage Libraries on the left, and select Configuration.

Add Media to the Tape Library

The end user will need to have inserted some media into the I/O or Mail Slots of their tape library.

Then with the "Show All Slots" checkbox checked, select one or more 'Empty' slots and then click 'Import'.



This will move the tape media from the Mailslots to the regular storage slots that were selected, refreshing them in the process.

Once they are imported, just like with a newly attached library, the tapes will show as 'Erased', 'Unknown', or with QStar information, and the end user can act on them accordingly.

Save the QStar ASM Configuration

Once you complete the configuration on the original server, it is a good practice to save the information to protect for situations where it becomes unavailable.

To view the configuration information, in the **QStar Administration Interface**, select **Media > Online Media.** Under **Online Media**, make note of and save the values for **Set Identifier**, **Set Name**, **Device Name**, **Barcode**, etc. This information is crucial during the recovery process.

To save the QStar Configuration:

1. Log in to the server running the QStar Archive Storage Manager.
2. Next, you need to reconfigure the new QStar server. To do so, you need to know which tape belongs to which volume set, and also which *Set ID*s (tapes) belong to which IV.

   To view the configuration, issue the following command from the command prompt:

   ```
   C:\QStar\bin>vlcmd lsset -va
   ```

   For example:

   ```
   C:\QStar\bin>vlcmd lsset -va >lsset.txt
   ```

   In our example, the command displays the current QStar server configuration:

   - **First Volume**: CohesityIV
   - **Integral Volume created with tapes**: lto3, lto4, lto5
   - **Mounted point**: M:\
   - **Cache Location**: E:\IntegralVolume\CohesityIVCache
   - **Cache root size**: 1 TiB
   - **Compression**: on
   - **Set type**: TDO (Tape Disk Object file system)
   - The **Set ID**, **Sequence number**, and **Barcode** are displayed.

```
C:\QStar\bin>vlcmd lsset -ua w
CohesityIV
   Use_media=tape<lto3,lto4„lto5),writable Spread=no Quota=4096 Media=13
   Restore_fsdb=no Read_only=no Real_sin_nix=no
   Make_copy=no
   Mount_on_server_restart
   Default_mount_point="M:\"
   Set_type=tdo <Tape and Disk Object file system)
   Compression=On
   Uerify_write=default <Device may enforce hardware verification)
   Set Id=5dd0e486f8fb2eee
   Cache:     Cache_root =E:\IntegralUolumes\CohesitylUCache
              Max_number_of_pages=1048576 <1.000 TiB)
              Page_size=1024 Kbytes
              Low_primary_capacity=0 <)
              High_primary_capacity=738198 <720 GiB)
   Published as M:\
   95:  Online=JB0:18 Sequence_number=133 Published=a   Barcode=[000018]
   96:  Online=JB0:3  Sequence_number=134 Published=a   Barcode=[000004]
   97:  Online=JB0:4  Sequence_number=135 Published=a   Barcode=[0000021
   98:  Online=JB0:19 Sequence_number=136 Published=a   Barcode=[000020]
   99:  Online=JB0:20 Sequence_number=137 Published=a   Barcode=[000016]
   100: Online=JB0:23 Sequence_number=138 Published=a   Barcode=[000008]
   101: Online=JB0:l  Sequence_number=139 Published=a   Barcode=[000001]
   102: Online=JB0:2  Sequence_number=140 Published=a   Barcode=[000005]
   103: Online=JB0:5  Sequence_number=141 Published=a   Barcode=[000015]
   104: Online=JB0:8  Sequence_number=142 Published=a   Barcode=[0000031
   105: Online=JB0:10 Sequence_number=143 Published=a   Barcode=[000010]
   106: Online=JB0:12 Sequence_number=144 Published=a   Barcode=[000009]
   107: Online=JB0:ll Sequence_number=145 Published=a   Barcode=[000011J

IV0
   Use_media=tape,writable Spread=no Quota=4096 Media=3
   Restore_fsdb=no Read_only=no Real_sim_mix=no
   Make_copy=no
   Mount_on_server_restart
   Default_mount_point="U:\"
   Set_type=tdo <Tape and Disk Object file system)
   Compression=0n
   Verify_write=default <Device may enforce hardware verification)
   Set Id=bdcll4afc8636f48
   Cache:     Cache_root=E:\IntegralUolumes\New folder
              Max number of pages=512000 (500 GiB)
```

3. To save the data, redirect the output of the command to a file.

```
C:QStar\bin>vlcmd lsset -va > <file_path>\<file_name>
```

IMPORTANT: Whenever you make a configuration change to QStar ASM, save it in a safe location.

Archive Your Data Using Tape

Cohesity Platform allows archiving of data to various targets, including public cloud, private clouds, S3-compatible storage, and QStar-managed tape libraries. You can register all supported targets in the Cohesity Platform as External Targets.

This chapter covers the steps to integrate QStar with Cohesity

1. Register the QStar server.
2. Create a Protection Policy.
3. Create a Protection Group to archive your data.
4. Recover data from tape archives.

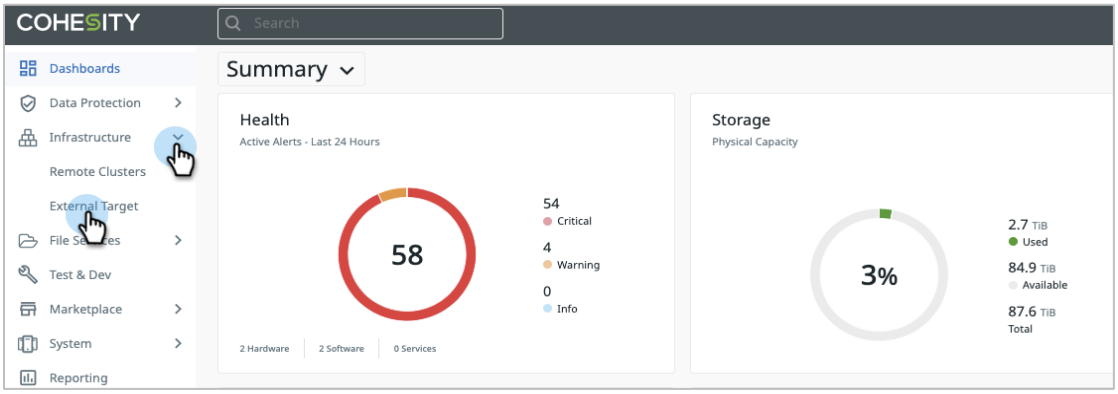
NOTE: Before you begin, see the list of supported workflows.

Register the QStar Server

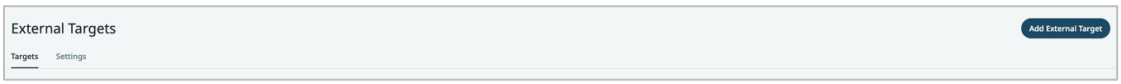
To copy the snapshots located in a Cohesity cluster to a QStar server using the Cohesity Platform, you first need to register QStar as an External Target.

To register the QStar Server as an External Target:

1. Log in to the Cohesity Platform and navigate to **Infrastructure > External Target**.

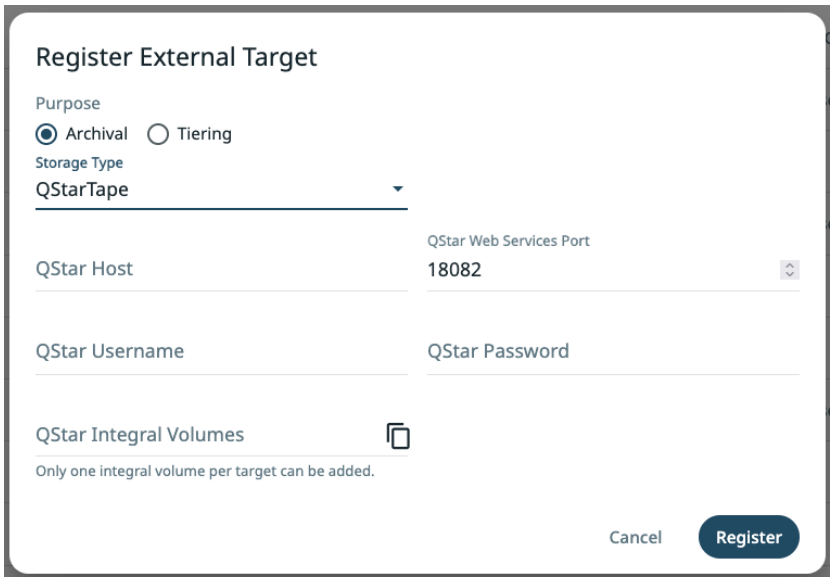


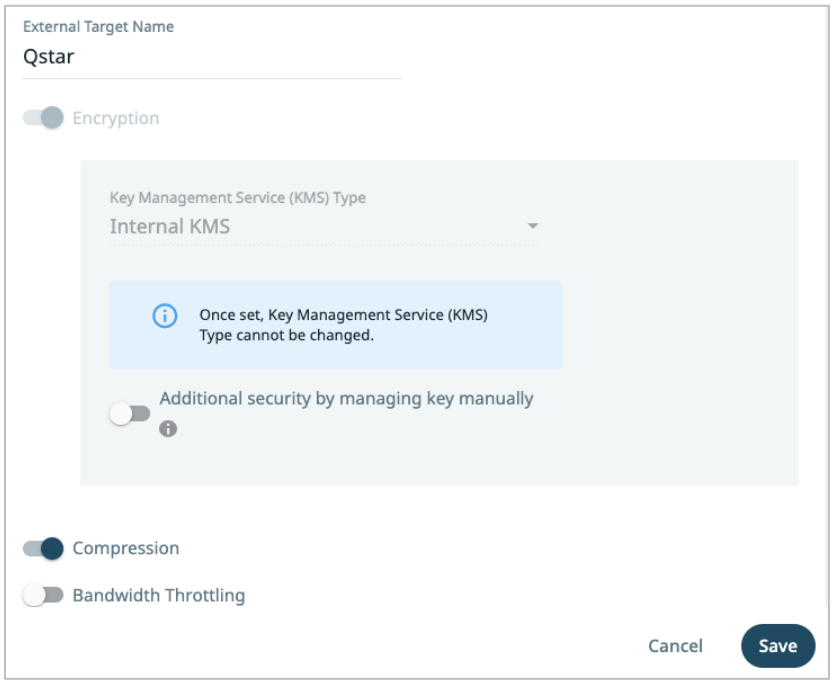
2. Click Add External Target.



3. In the External Target form that opens, enter the parameters as specified, and click **Save**.
   a. **Purpose**: Archival
   b. **Storage Type**: QStarTape
   c. **QStar Host**: *<name of the QStar server host>*
   d. **QStar Web Services** Port: 18082 (default)
   e. **QStar Username**: *<QStar account username>*
   f. **QStar Password**: *<QStar account password>*

g. **QStar Integral Volumes**: *<name(s) of the QStar Integral Volume(s)>*
h. **Qstar Target Name**: <Provide a name for the External Target>
i. **Encryption** is enabled by default.
j. **Enable Compression**





NOTE: QStar communicates on port 18082 by default. Do not change this port unless it is changed on the QStar server.

Once the QStar server is successfully registered as an External Target in Cohesity Platform, you can use it to create tape archives.

For more, see Register or Edit an External Target in the Online Help.

Create a Protection Policy

In the Cohesity Platform, Protection Groups use Protection Policies. Protection Policies reflect business needs, such as backup and archival frequency, retention requirements for each, as well as Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs). A Protection Group defines operational requirements, such as which source objects to protect, the Protection Policy to use, and operational considerations like indexing, exclusions and inclusions, alerts, app consistency, and more. This process of combining business needs (Policy) with the objects to protect (source data) and the operational requirements (Job) provides rich flexibility to customers.

A Protection Policy defines:

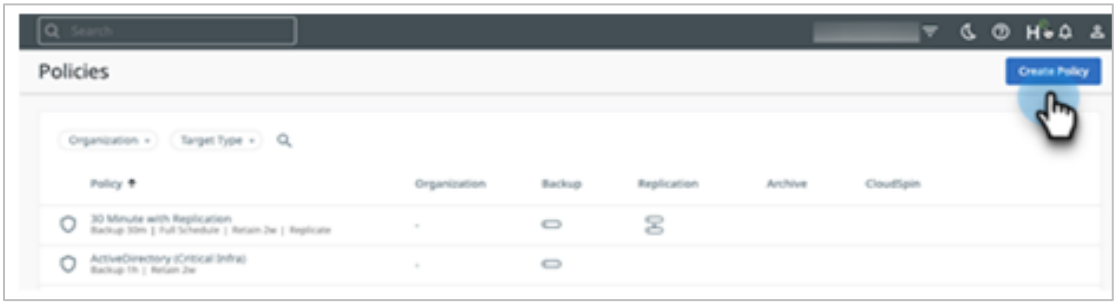
- How source data (like virtual and physical servers, databases, unstructured data, etc.) will be backed up and then archived.
- Where and how frequently they will be archived.
- How long the archives will be retained.

In the Protection Policy, you can select the tape-based External Target you have just registered.

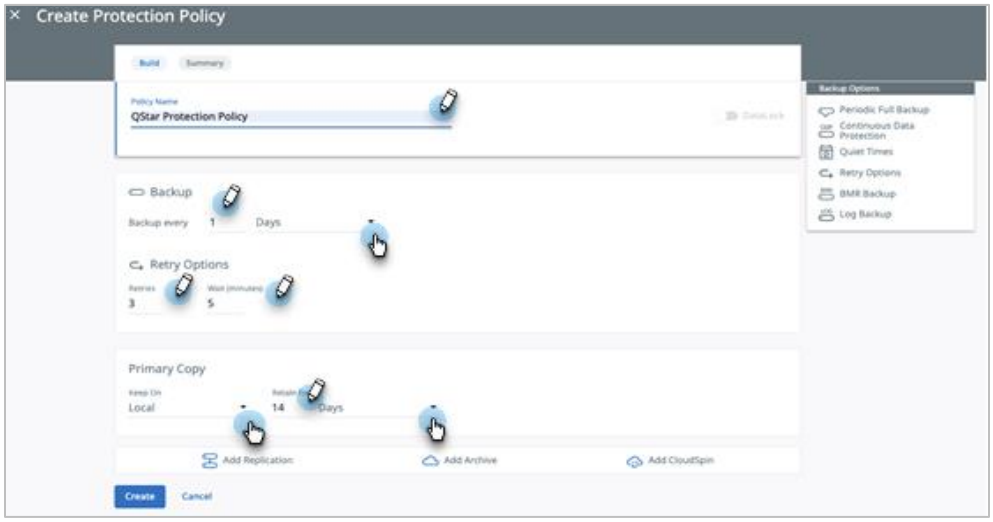
To create a Protection Policy:

1. Log in to the Cohesity Platform and navigate to **Data Protection > Policies**.

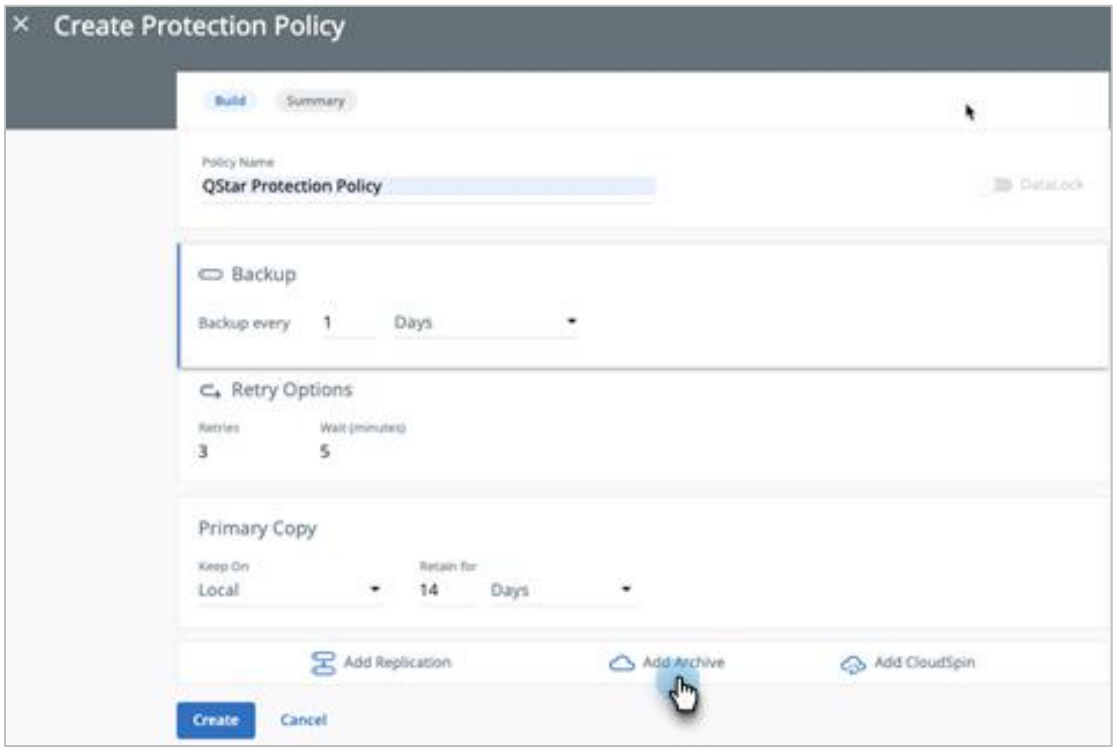
2. Click **Create Policy**.



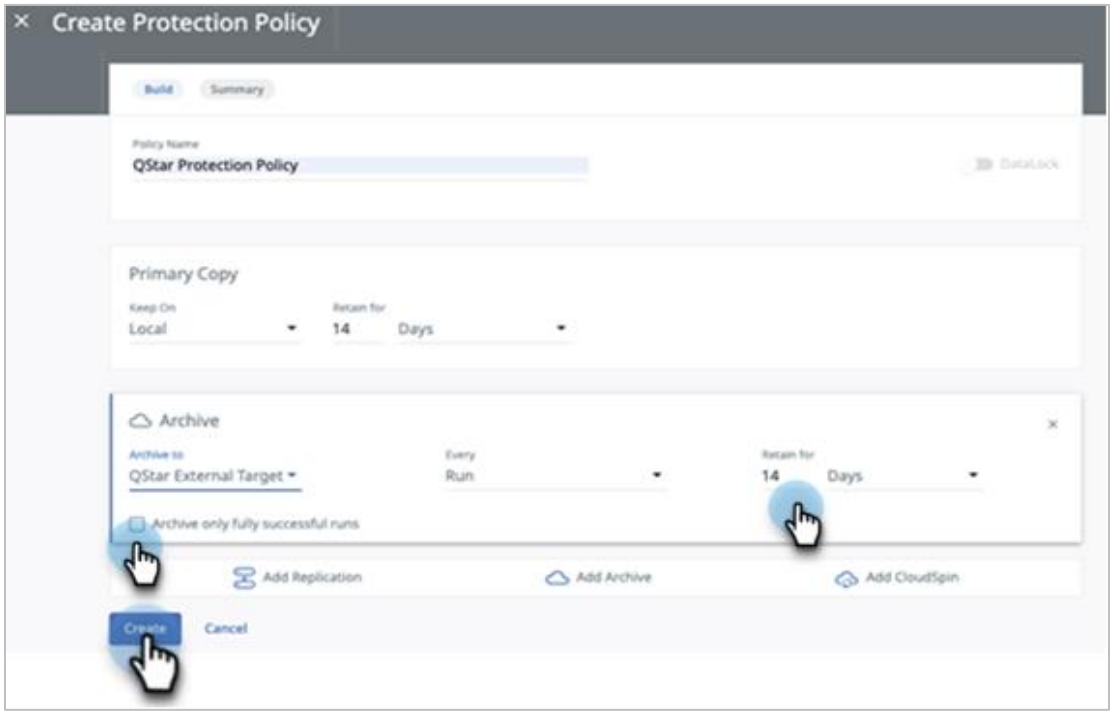
3. In the **Create Policy** form, enter a **Policy Name**, select the interval and retention times for the **Backup** of the data (volumes) on your server. You can edit the **Retry Options** and specify the location (Local) to store the Primary Copy.



4. Click **Add Archive** to add an Archive to the policy.



5. Under **Archive**, select the External Target you have just created. Under **Every**, set the archival frequency and the **Retain for** period (90 days, by default). You can also enable **Archive only fully successful runs** in the checkbox at the bottom. Then click **Create**.



NOTE: Cohesity Protection Groups to Tape archive full backup images to tape. Cohesity recommends you schedule tape-based Protection Groups to run once a month, once a quarter, or even less frequently.

For the complete list of Protection Policy parameters, see Create or Edit a Standard Policy in the Online Help.

Create a Protection Group to Archive Your Data

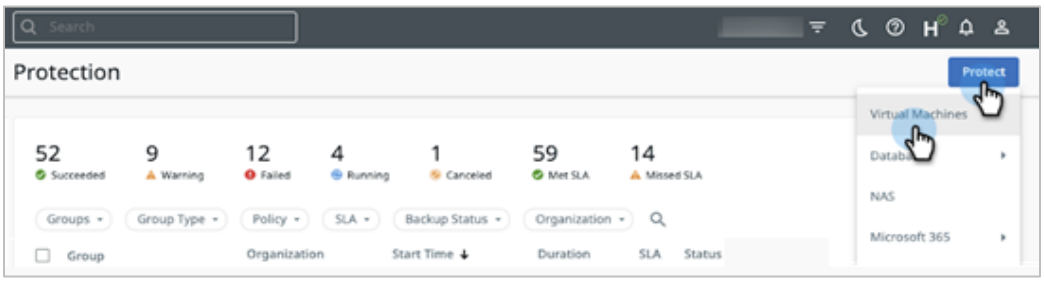
Protection Groups combine operational requirements with the business requirements defined in a Protection Policy. Multiple Protection Groups can use the same Protection Policy, but each Group can have only one Policy. Protection Groups protect specific source objects, such as virtual servers, physical servers, Views, SQL servers, Oracle databases, remote adapters, Pure Storage Volumes, or network-attached storage (NAS).

For this example, we look at the steps to create a Protection Group for a virtual server, but the steps to protect other source objects are very similar too.

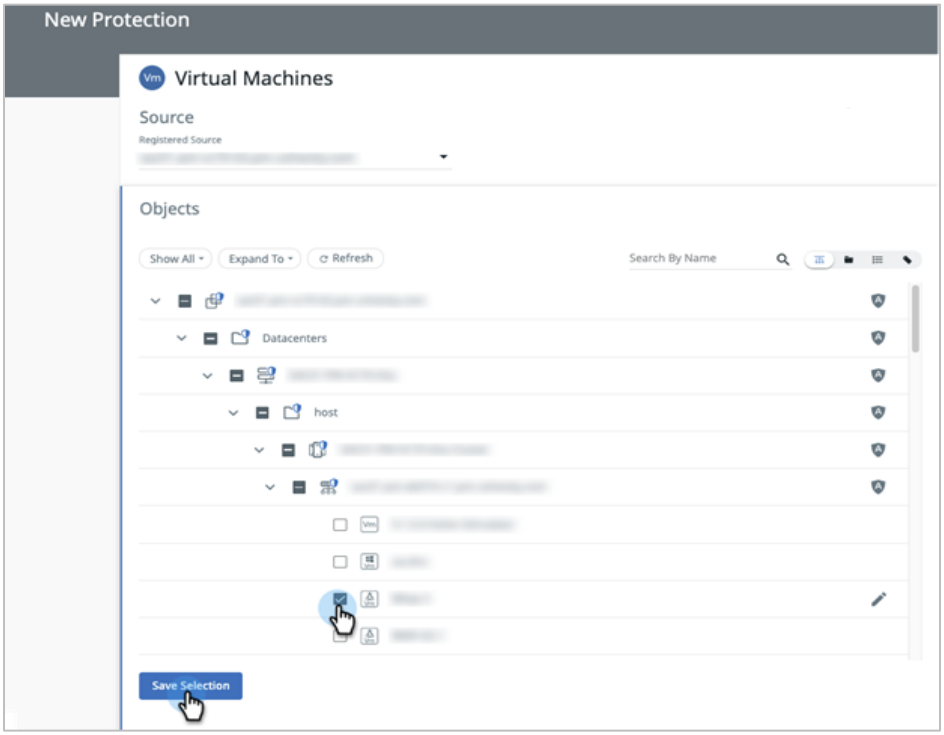
To create a Protection Group:

1. Log in to Cohesity Platform and navigate to **Data Protection** > **Protection**.

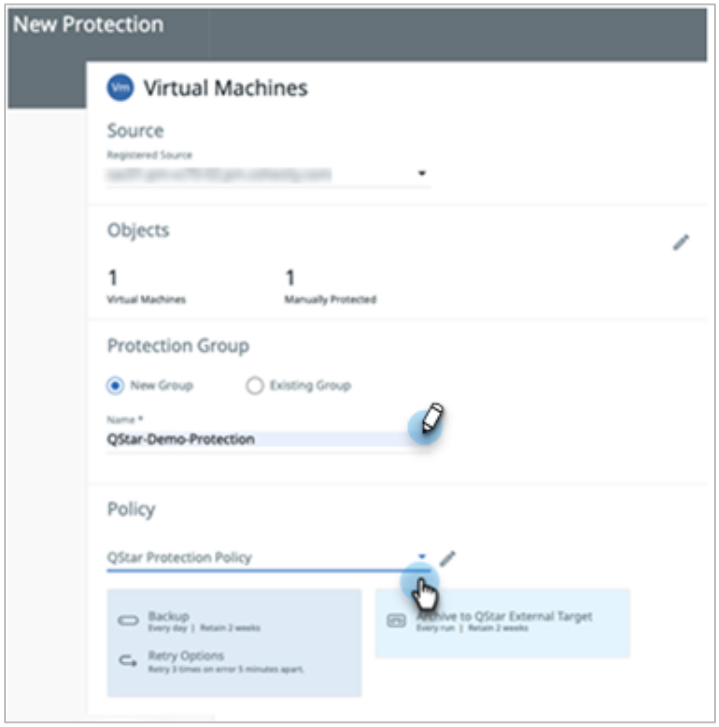
2. Click **Protect** and choose the type of data to protect.



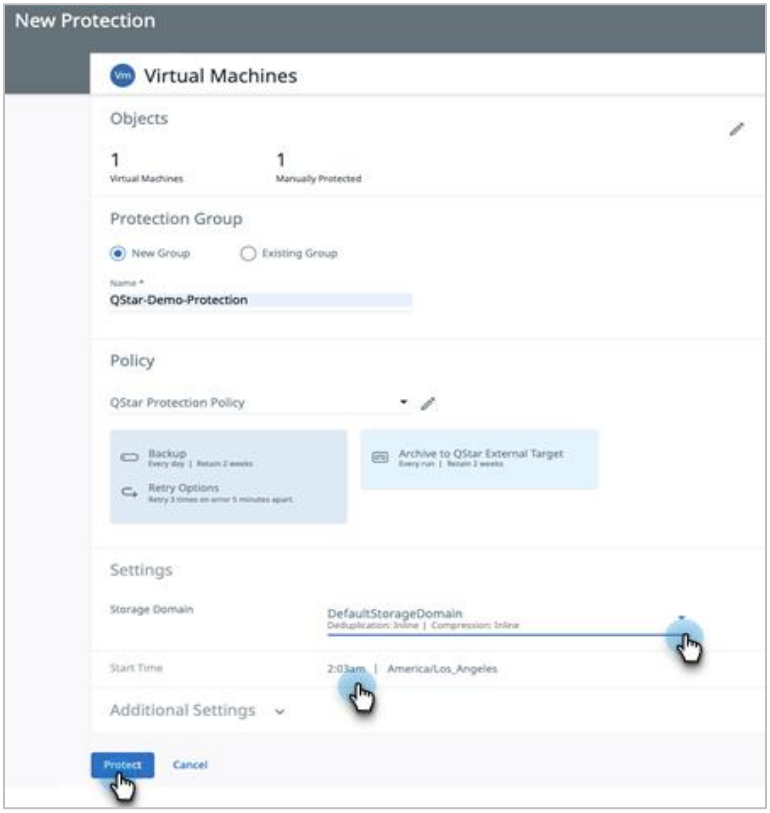
3. In the **New Protection** form, select **vCenter** as **Source** and choose the specific VMs you wish to protect. Click **Save Selection**.



4. Enter a **Name** for your Protection Group and select the **Policy** that you created earlier.

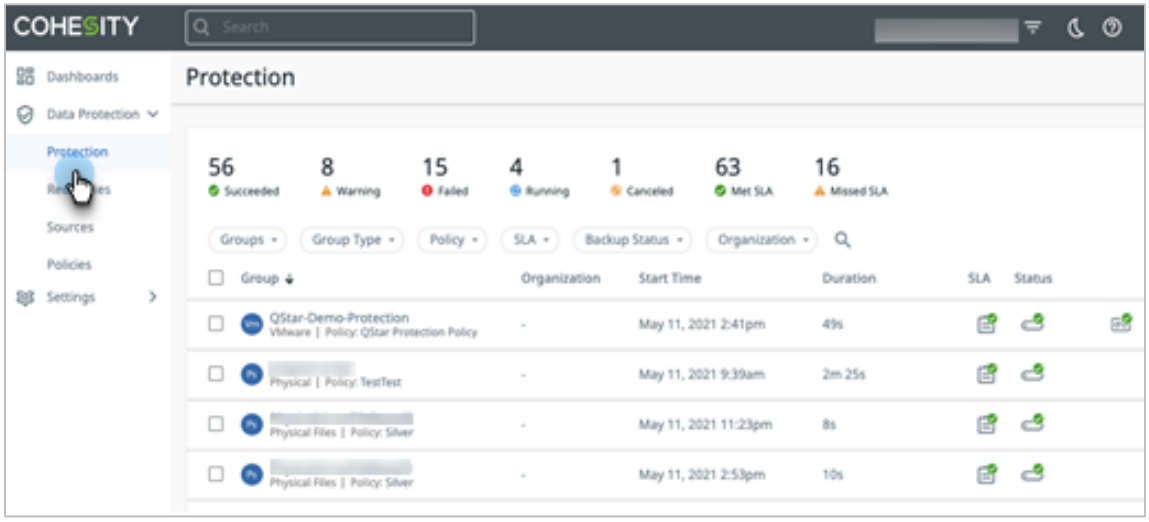


5. Select a **Storage Domain**, edit the **Start Time** if necessary, and click **Protect**.

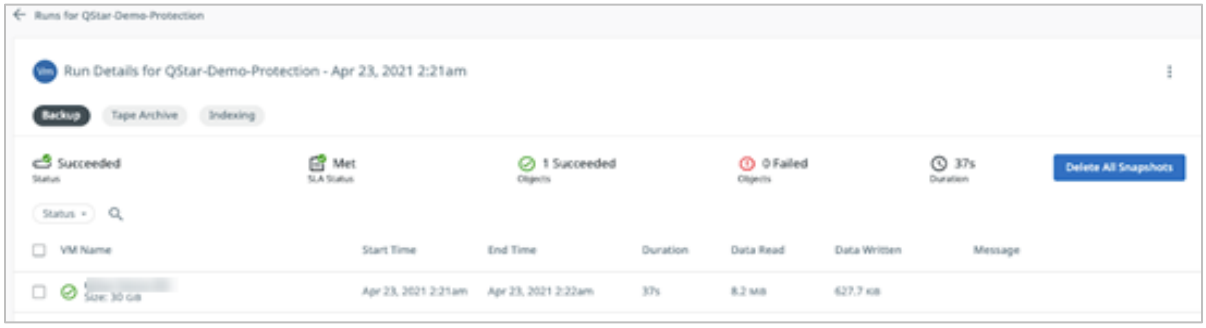


For more details, including the **Additional Settings** in a Protection Group, see Add or Edit a Protection Group for Virtual Servers in the Online Help.

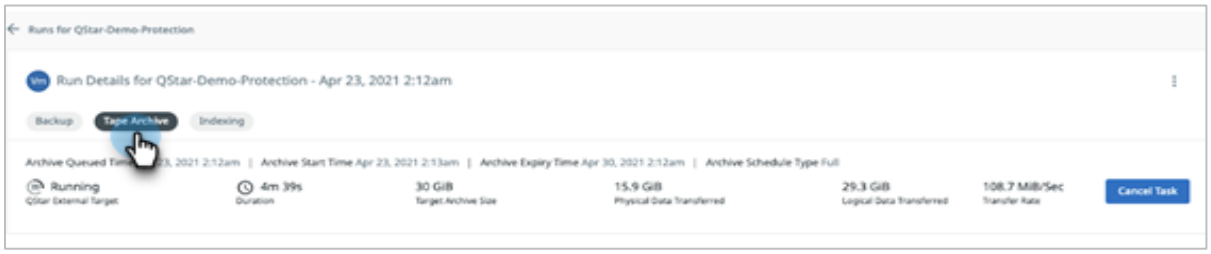
1. Click **Protection** to view the list of Protection Groups.



2. Click the Protection Group name to check the detailed status of the Protection Runs.



3. Click **Tape Archive** tab to check its status.



> **NOTE**: If the QStar server runs out of tape media, QStar sends the message to Cohesity Platform, which will trigger an alert to advise the administrator to load additional blank media for the operation to continue.

4. On successful archival, the status is updated with the details on the amount of data transferred.

Recover Data from Tape

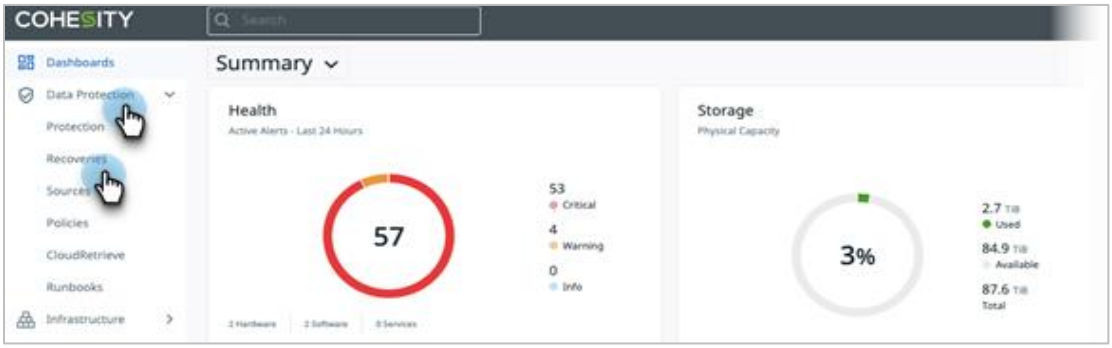
In the Recovery workflow, you can recover archived objects (such as VMs, databases, NAS, etc.) using the Cohesity cluster that archived them. Whether you are recovering data from a local Cohesity cluster or tapes, the recovery experience and workflow are the same.

> **NOTE**: Before you begin recovering from tape, see the list of supported workflows.

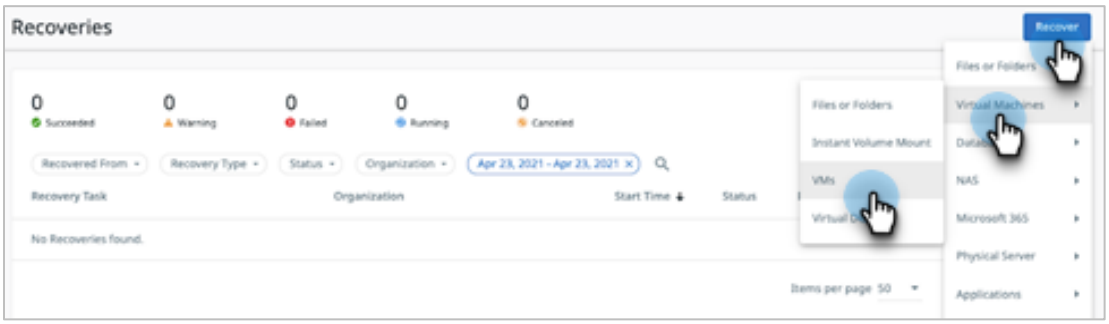
Recover Using Original Cohesity Cluster

To recover data onto your original Cohesity cluster from your tape library:

1. Log in to Cohesity Platform and navigate to **Data Protection > Recoveries**.

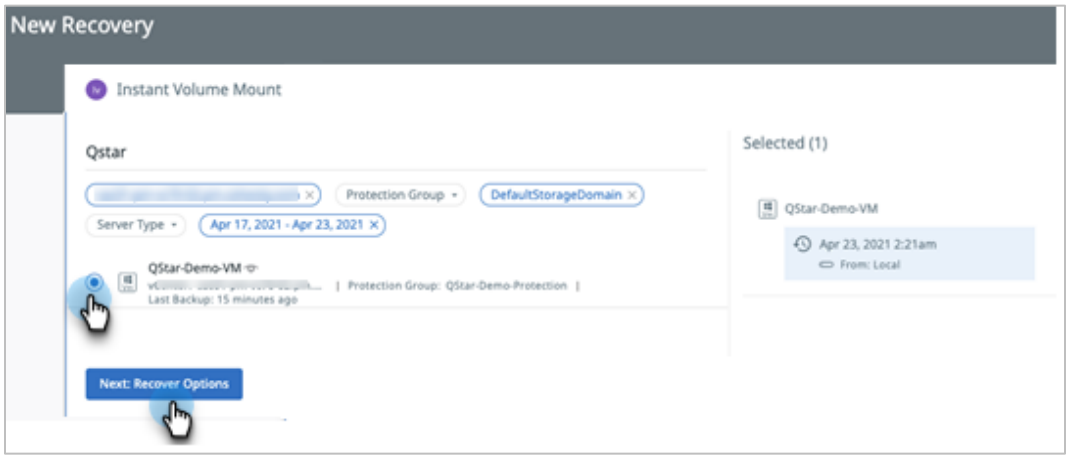


2. Select **Recover** > **Virtual Machines** > **VMs**.

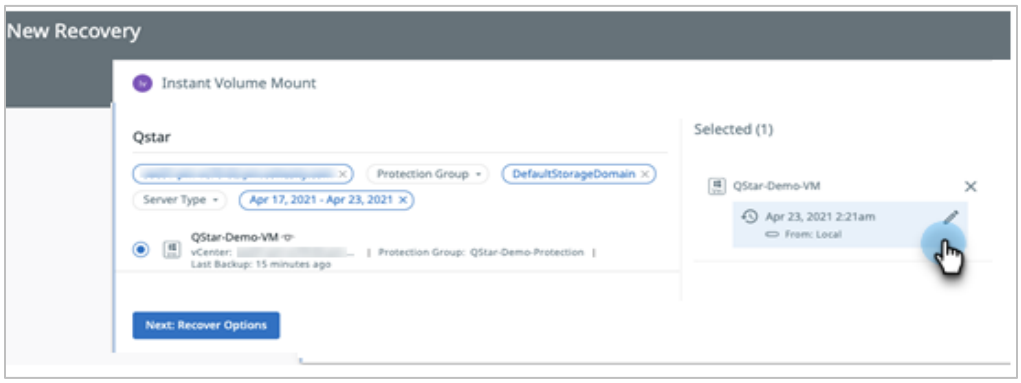


> **NOTE**: The steps that follow show the example of seeking out and recovering a VM, but the recovery process is very similar for all supported recovery types in the **Recover** menu above.

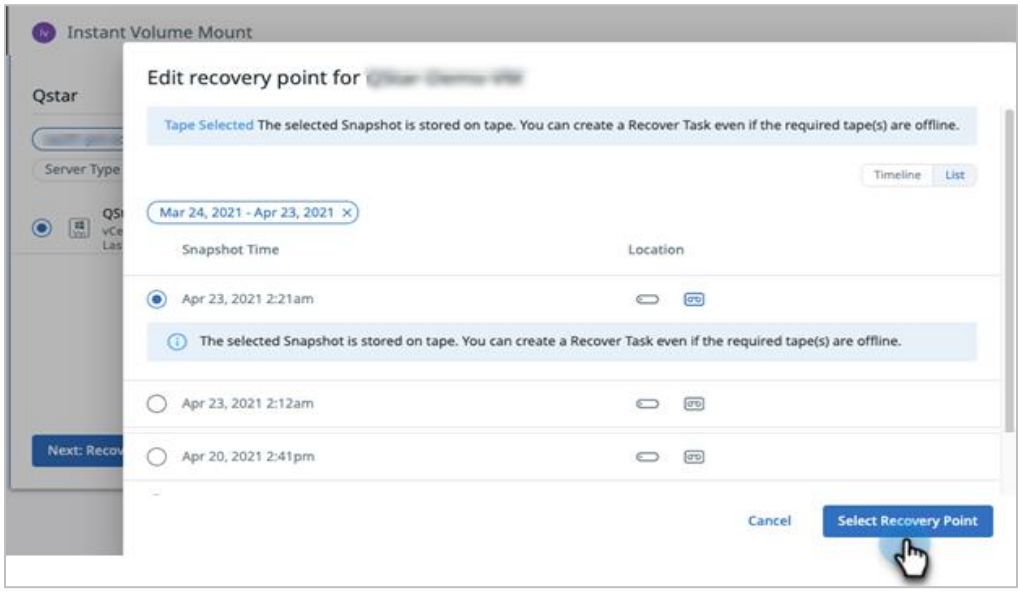
3. Enter a term to search by **VM name or Protection Group Name**. In the search results, click the VM you wish to recover.



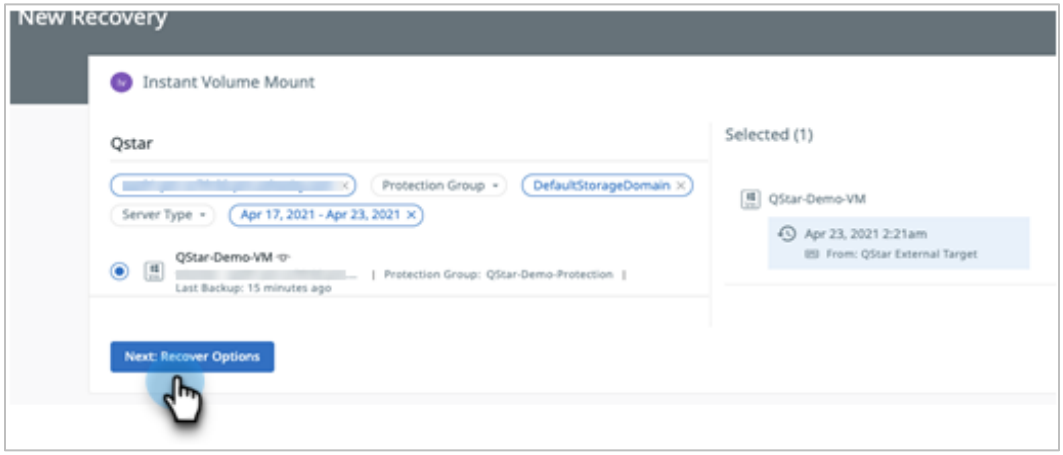
4. Select the **Tape Recover Point** and click the **Edit** (pencil) icon.



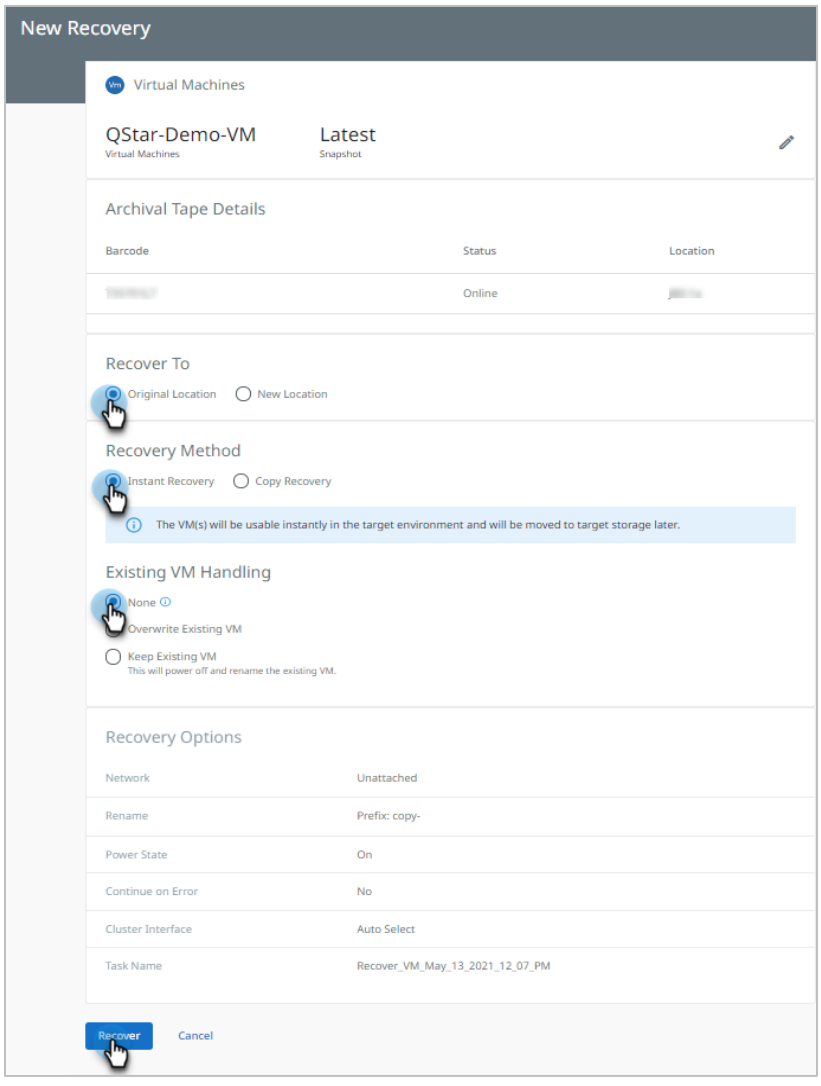
5. Choose a recovery point, select **Tape** as **Location**, and click **Select Recovery Point**.



6. Click Recovery Options.

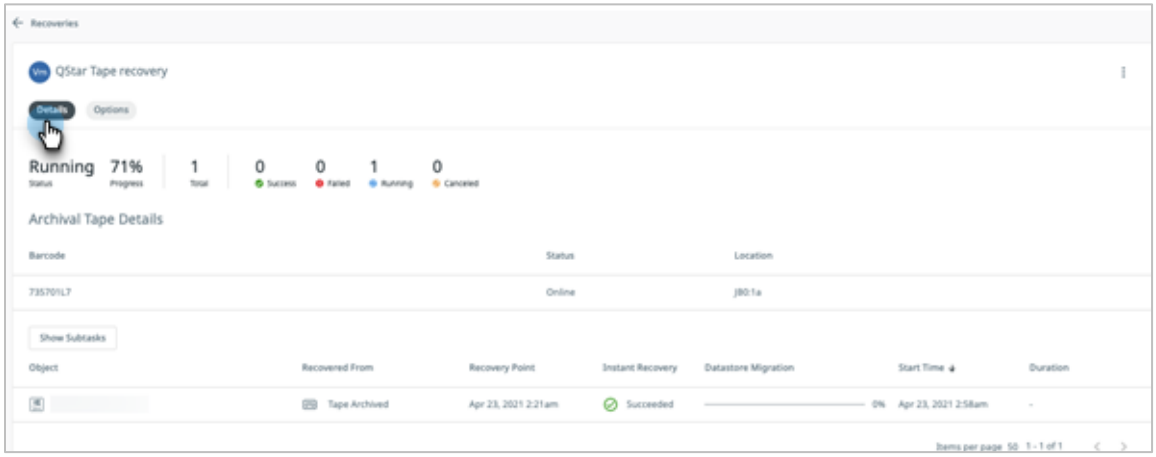


7. Choose the **Recovery To** location, select the **Recovery Method**, set the **Recovery Options**, and click **Recover** to start the recovery process.



NOTE: This example is for recovering a VM. The recovery options vary by Protection Group type.

8. Click **Finish** to start the recovery process and monitor the progress of the recovery.



NOTE: If one or more of the required tapes are offline, Cohesity Platform highlights the required tapes and prompts you to load them to the tape library attached to the QStar server. Once the tapes are brought online, the recovery task continues.

For more on the many capabilities and choices in our recovery process, see the Recovery section in the Online Help.

Appendix: Review Recovery Point Objectives

Cohesity Platform employs an adaptive throttling mechanism when archiving to tape, by monitoring the IV cache utilization. If cache utilization exceeds the threshold, Cohesity Platform waits until cache utilization level returns below the threshold before archiving more data to tape. This approach mitigates the risk of data loss to the data stored in the cache.

The amount of data at risk is an important metric to consider while planning ape archival. In this Appendix, we discuss the monitoring options in QStar ASM and how Cohesity Platform provides a complete and reliable archival solution.

Strategies for Mitigating Data Loss in the Event of Failure

Three main triggers prompt the QStar ASM to initiate writes to the tape:

- **High-Primary Capacity (HPC):** The point at which QStar ASM will start to request archiving, based on the percentage of the allocated cache size.
- **Manual archiving**: Initiated using explicit commands, or using the **Migration View > Start Archiving** command.
- **Scheduled**: The archiving process can be scheduled to occur at specific times, such as *10.00 PM every night*, for example.

Cohesity Platform uses only the HPC trigger to determine when to initiate the archival process and does not wait for the HPC acceptance limit to be reached. Instead, it proactively ensures that primary data on the server is periodically archived to the tapes, thereby mitigating data loss in the event of failure.

Monitor Archival Status Using Migration View

Migration View is an essential tool to check the status of your archive at any point. It shows you how much of the data is in danger of being lost. To access the tool, open the QStar Administration Interface, and select **Integral Volumes** > **Migration View**.

Figure 3: Migration View on QStar ASM

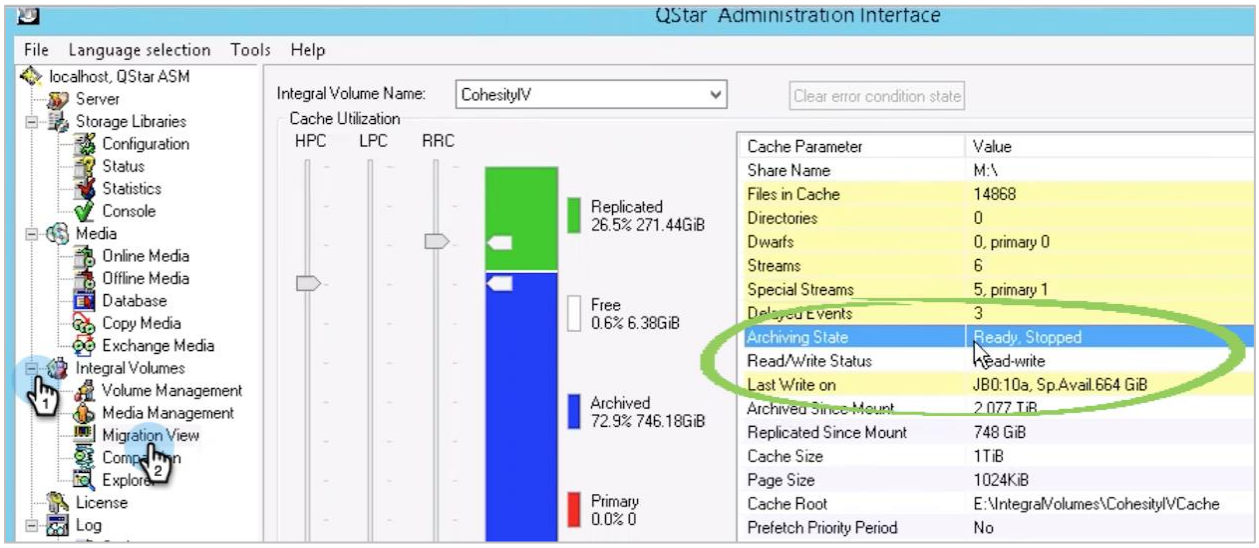


Table 1 below describes the different states of data.

Table 1: Data Archival Status

DATA RANGE	LABEL	DESCRIPTION
Primary	**Red**	Data is on the server (‘primary data’) but hasn’t been archived to tape yet.
Archive	**Blue**	Data is on the tape but is not immediately available from the server.
Replicated	**Green**	Data is both available on the server and archived to tape.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Jedidiah Sonavane is a Solutions Architect at Cohesity. In his role, he focuses on Cloud Archival, Multi-tenancy, Service Provider, Tape Archival and so on.

Other essential contributors include:

- Surya Swaminathan, Principal Solutions Architect
- Siddhesh Rumde, Quality Assurance
- Gautam Bhasin, Product Manager
- Adaikkappan Arumugam, Sr. Director, Solution Architect
- Bart Abicht, Staff Technology Writer and Editor

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.0	Nov 2019	First release
1.1	Feb 2020	Content update
1.2	Apr 2021	Updated workflows
1.3	May 2021	Updated for Cohesity v6.6
1.4	Feb 2022	Minor updates
2.0	July 2025	Updated for Qstar ASM 7.x

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 42 of the Fortune 100.

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