RackTop Hub Local Guide

Version 23.6

Terms of Use and Copyright and Trademark Notices

The copyright in the Documentation is owned by RackTop Systems and is protected by copyright and other intellectual property laws of the United States and other countries. Without limiting the rights of this copyright, no part of the Documentation may be modified, used in a compilation or otherwise incorporated into another work, or with or into any other documentation or user manuals, or be used to create derivative works, without the express prior written permission of RackTop Systems. RackTop Systems reserves the right to change the terms at any time, and your continued use of the Documentation shall be deemed an acceptance of those terms. RackTop Systems, the RackTop Systems logo, BrickStor, CyberConverged, and certain other trademarks and logos are trademarks or registered trademarks of RackTop Systems, Inc. in the United States and other countries. Other company, product and service names may be trademarks or service marks of others.

Disclaimers

The Documentation and any information available from it may include inaccuracies or typographical errors. RackTop Systems may change the documentation from time to time. RackTop Systems makes no representations or warranties about the accuracy or suitability of any RackTop Systems-controlled website, the Documentation and/or any product information. RackTop Systems-controlled websites, the Documentation and all product information are provided "as is" and RackTop Systems disclaims any and all express and implied warranties, including but not limited to warranties of title and the implied warranties of merchantability and/or fitness for a particular purpose. In no event shall RackTop Systems be liable to you for any direct, indirect, incidental, special, exemplary, punitive, or consequential damages (including but not limited to procurement of substitute goods or services, loss of data, loss of profits, and/or business interruptions), arising out of or in any way related to RackTop Systems-controlled websites or the documentation, no matter how caused and/or whether based on contract, strict liability, negligence or other tortuous activity, or any other theory of liability, even if RackTop Systems is advised of the possibility of such damages. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitations may not apply to you.

Table of Contents

Hub Local Overview

What is Hub?

Hub is a horizontally-scalable unified architecture providing command, control, and configuration for RackTop's Cyberstorage.

The Hub functions as a versatile platform for processing, transforming, analyzing, and sharing both system and user-generated data, while also facilitating third-party integration.

Hub is single pane of glass management platform for BrickStor SP devices and is managed with web-based user-interface (UI).

Hub Versions

Hub-Central provides the full functionality of the Hub platform. It runs on a standalone server and is capable of managing a fleet of appliances.

Hub Local is a version of the platform that runs directly from a BrickStor SP appliance and is capable of managing a single node.

Vault management and configuration is housed within the RackTop Hub interface.

NOTE Hub Local provides abridged functionality of the full platform.

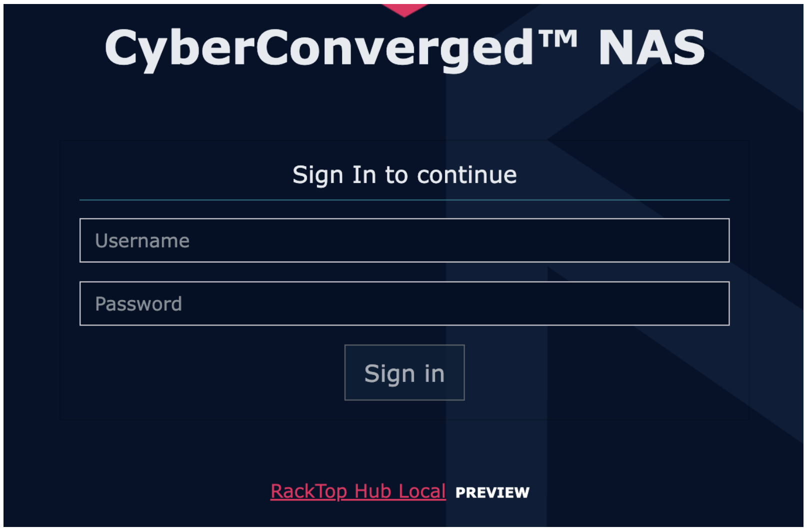
This guide will introduce you to the Hub user interface, outlining each of the sections and available functions, as well as describing general conventions and options.

Logging in to The RackTop Hub Interface

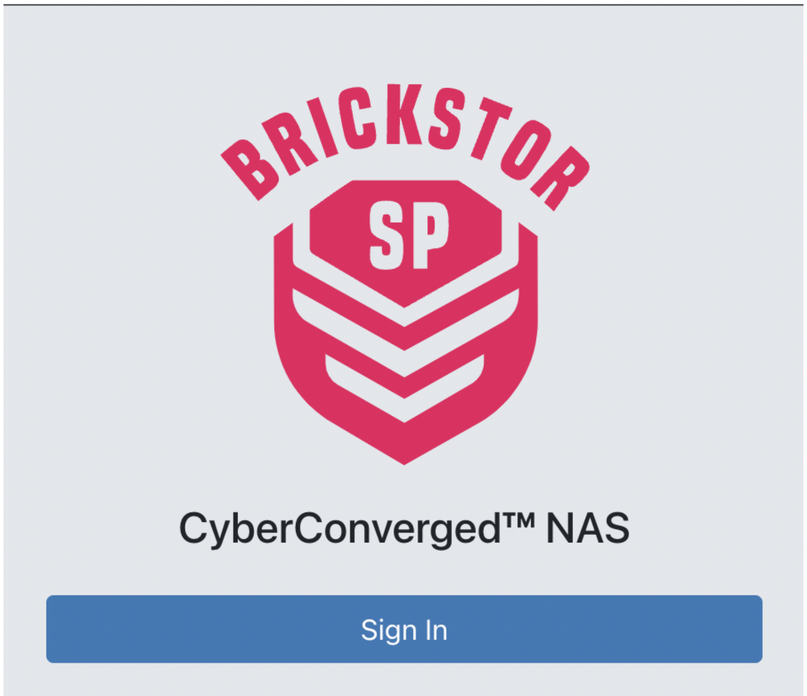
- To access the Hub, begin by opening up an internet browser, and entering the IP of your BrickStor SP into the search bar.

NOTE The browser may present a warning about untrusted self-signed SSL certificate for Hub web user interface. To proceed, accept the warning or add the certificate to your computer's trust store.

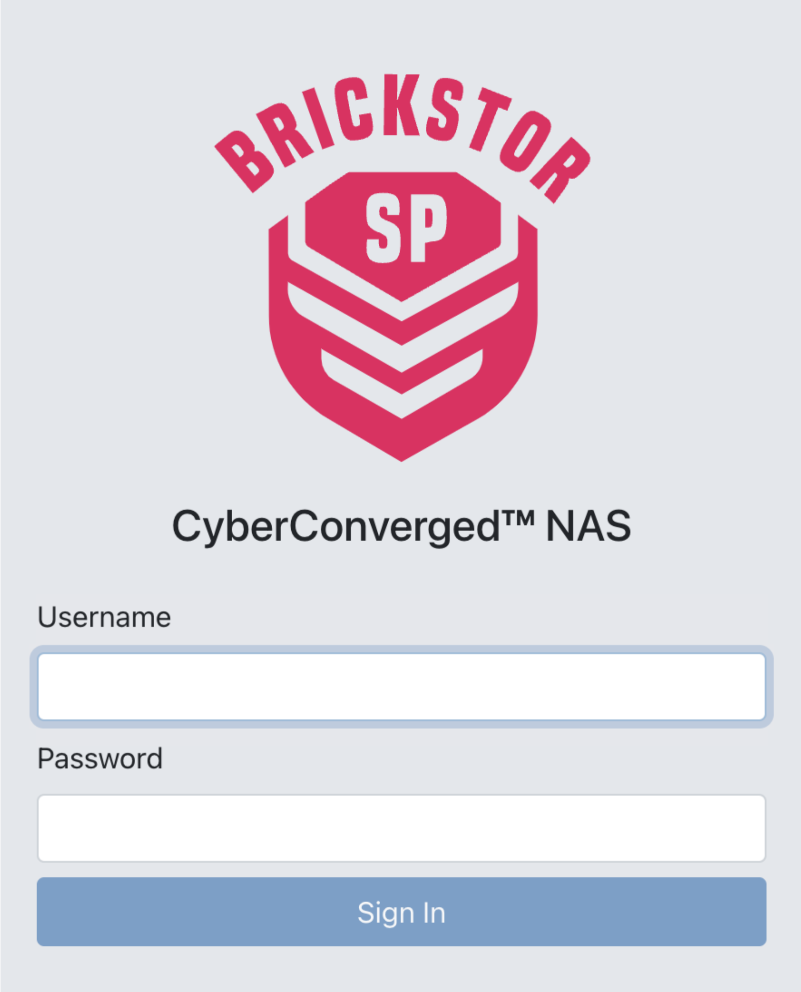
- At the bottom of the login page, click **RackTop Hub Local PREVIEW**.



- This will redirect the browser to the Hub Interface.



- Click **Sign In**.



CyberConverged™ NAS

Username

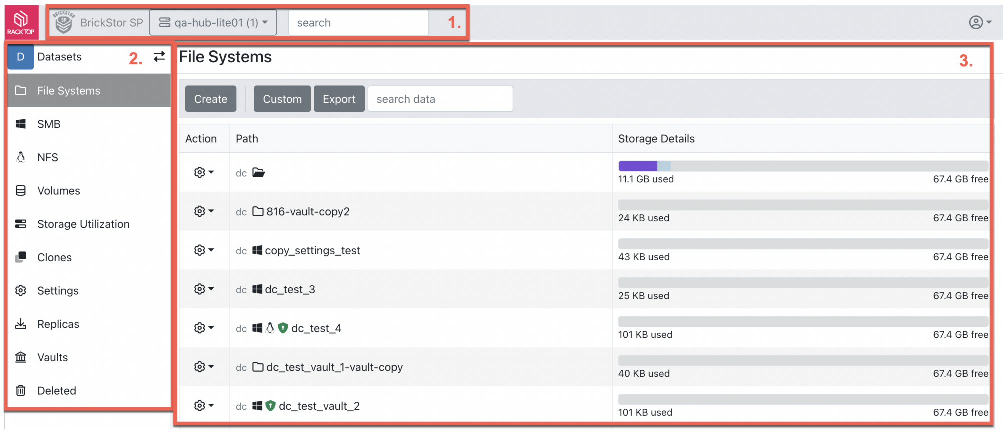
Password

- Log in with the credentials to your BrickStor SP.

Hub Local User Interface

The following is a brief overview of the Hub User Interface (UI).

NOTE For the purposes of the 23.6 Release, Hub functionality is limited to the management of the new Vault interface. Instruction for the Hub interface will as such be limited to Vault creation, configuration, and management.



File Systems

Action	Path	Storage Details
⚙	dc	11.1 GB used 67.4 GB free
⚙	dc 816-vault-copy2	24 KB used 67.4 GB free
⚙	dc copy_settings_test	43 KB used 67.4 GB free
⚙	dc dc_test_3	25 KB used 67.4 GB free
⚙	dc dc_test_4	101 KB used 67.4 GB free
⚙	dc dc_test_vault_1-vault-copy	40 KB used 67.4 GB free
⚙	dc dc_test_vault_2	101 KB used 67.4 GB free

The Hub UI can be split into three parts Banner, Sidebar, and Main Content:

1. The Banner - Allows for the selection of the specific BrickStor SP that is to be managed. This is selectable by **Clicking** the downward arrow next to the name of the BrickStor SP.
2. The Sidebar - The Sidebar allows for easy navigation of Hub features dependant on the currently selection Main Content page.
3. Main Content - The Main Content section displays system contents through a modifiable lens. To change the field of the Main Content section, simply click (default) **Datasets** to reveal a list of three Main Content sections. These sections are Datasets, Hardware, and Data Protection.
   - Datasets - This page will default to the Datasets section, which shows a list of present File Systems available on the system. The sidebar options follow:
     - File Systems - This File Systems Page also allows for the curation of the File Systems list, as well as the creation and export of a File System. To manage any specific file system, simply **click** the cog to the left of the desired file system. The option to Open Dataset, open Snapshots, and Add Child will present.
     - SMB - Shows a list of present SMB shares on the system. Allows for the curation of the presented list, as well as the creation, edit, and export of an SMB share.
     - NFS - Shows a list of present NFS shares on the system. Allows for the curation of the presented list, as well as the creation, edit, and export of an NFS share.
     - Volumes - Shows a list of present Volumes on the system. Allows for the curation of the presented list, as well as the creation and export of a Volume.
     - Storage Utilization - This section shows a circle graph displaying the current storage status of the system on a per-pool basis, with named sections viewable by highlighting each section with the cursor. Further, a comprehensive list of system data is present, with the ability to filter the list results and export datasets as well.
     - Clones - Shows a list of present Clones on the system. Allows for the curation of the presented list, as well as the creation and export of a Clone.
     - Settings - Shows a list of present Settings on the system. Provides a filtering option to show Non-Default settings. Allows for the curation of the presented list, as well as the creation, edit, and export of System Settings.
     - Replicas - Shows a list of present Replicas on the system. Allows for the curation of the presented list, as well as the creation, restoration and export of a Replica.
     - Vaults - Shows a list of present Vaults on the system. Provides a filtering option to the list. Allows for the curation of the presented list, as well as the creation, staging, sealing,

manifesting, and export of Vaults.

    - Deleted - Shows a comprehensive list of deleted files present on a system. Provides a filtering option to the list. Allows for the export of deleted files. Allows the ability to Restore, Destroy, and view information of the deleted file.

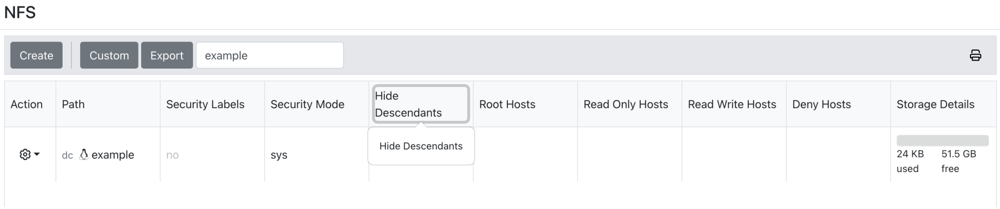
  - Hardware - This section allows for a view of the System Hardware, as well as sections to view Hardware Tasks, HA, Rack View, Drives, Pools, Enclosures, and iSCSI.
  - Data Protection - This section shows a list of Auto Snapshots on the system, as well as sections to view Auto Snapshot Policies, and Dataset Snapshots.

NFS

NFS is a file sharing mechanism that allows file and directories to be shared on different machines. It is typically used with Linux/Unix based machines. BrickStor SP supports versions NFSv3 and NFSv4.0/4.1/4.2 of NFS.

The NFS Home Page can be divided into two sections:

- Toolbar - Provides options to filter the list of current NFS shares. It features a Create button to create a new NFS enabled Dataset. A Custom button to customize visible grid fields. And Export button to export grid data to CSV, Excel, PDF or print.
- NFS Share List - Shows a vertically organized list of current Datasets with NFS sharing feature enabled. This list is managed through the toolbar, and updates in real-time dependent on filters selected.



Action	Path	Security Labels	Security Mode	Hide Descendants	Root Hosts	Read Only Hosts	Read Write Hosts	Deny Hosts	Storage Details
⚙ ▾	dc example	no	sys						24 KB used 51.5 GB free

Clicking the **Cog** wheel allows for the option to **Edit** the NFS Export. Clicking this option opens the NFS Export Configuration window.

Further options to Open Dataset, Open Snapshots, and Add Child are present when clicking the **Cog** wheel.

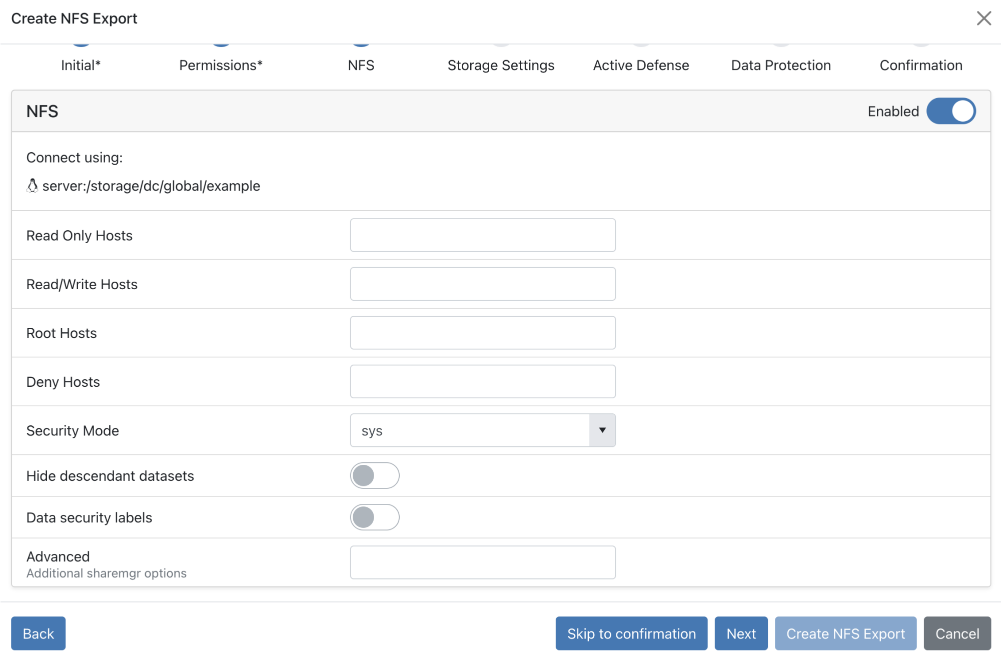
Create NFS Export

The option to create a new NFS Export is available by clicking the **Create** button in the Toolbar on the NFS home page:

- The NFS Export creation dialog will open.
- Add a Path in the provided field.
- Name the NFS Export in the provided path.
    - Optionally, add a description to the NFS Export.
- Click the **Next** button.
- Configure the [dataset-permissions].
- Click the **Next** button.
- The NFS Export Configuration window will present.
- Click the **Next** button.
- If further Dataset options are not required, click the **Skip to Confirmation** button. To view comprehensive instruction of Dataset configuration options, visit [creating-a-dataset].

NFS Export Configuration

- The NFS Export Configuration window will present.



NFS Enabled

Connect using:
server:/storage/dc/global/example

Read Only Hosts	
Read/Write Hosts	
Root Hosts	
Deny Hosts	
Security Mode	sys
Hide descendant datasets	○
Data security labels	○
Advanced Additional sharemgr options	

This dialog allows you to specify which hosts, IPv4 addresses, and subnets can access the NFS share, and how it can be accessed. This is known as "host based access control". In addition, individual users on the hosts/subnets can be specified (see the example below).

The following choices can be made:

- No choice - Anyone with network access can mount the file system. File names are visible but no content or metadata. This is the default setting, and one of the least secure choices.
- Read-Only - Hosts, subnets, and users that may mount the share as read-only, i.e., the share may only be read, not modified. Whether you can actually read individual file shares depends on permissions for the shared files themselves. If Everyone (i.e., '*') is specified, anyone can mount the share read-only.
- Read/Write - This allows the same choices as Read-Only. Here, the file share is mounted readable and writable, depending on the permissions on the underlying file. If "Everyone" is chosen for Read-Only, setting a host(s) and/or subnet(s) here will override the read-only setting for the hosts(s)/subnet(s) specified.
- Full Control (Root) - This allows you to run as root on the shares. Note that this does not imply that you can access the files for read/write or read-only, but you can read-only or read/write access the files if the host(s)/subnet(s) is specified in the read-only or read/write access list. Normally, the root user on the nfs client is mapped to an anon user on the server. The Full Control (Root) access list does not map the root user on the client to an anon user on the server. Instead, the root user on the client runs as the root user on the server.
- Deny - Hosts/subnets in this list may not mount shares from the server for read-only or for read-write. If Everyone ('*') is in this list, no one can use the nfs share.

TIP `Read-Only: Everyone`

> `Read/Write: @10.2.22.77; @10.2.22.102`
>
> `Full Control (Root): @10.2.22.77`
>
> `Deny: @20.2.22.75; maxb@10.1.29.0/23`
>
> Everyone not listed as **read-only** access.
>
> Host 10.2.22.77 and 10.2.22.102 has **read-write** access.
>
> 10.2.22.77 has **root** access.
>
> Any access from 20.2.22.75 is **not allowed**.
>
> Any access from user `maxb` on 20.1.29.0/23 subnet is **not allowed**.

- The security mode (defaulted to `sys`) can be configured by clicking the **downward arrow** and selecting the available options by **clicking** any displayed option.
- The option to enable/disable Hide descendant datasets, and Data security labels is configurable by clicking the provided **Sliders**.

ImmutaVault

Summary

The ImmutaVault feature uses the combination of a virtualization technology, data encryption, orchestration services, and an application program interface to electronically sever the network connection from the data such that the data, once ingested into the data system, cannot be accessed by any third parties either over the network or directly attached to the system itself.

What is ImmutaVault?

A Vaulted system is a single node, or collection of like nodes, that are not physically connected via a network connection to another system. Think of your PC before the advent of the Internet. The use case for an air gapped system is for critical data protection, whereby eliminating the network access creates a strong security boundary that can only be breached by direct, physical access.

Active Airgap

Through RackTop's patent pending technology, your data will be protected to the same level as a physical air-gap without the need for disconnecting network cables or separate systems.

Privileged User Protection

ImmutaVaults are protected from admin or operator abuse (insider threat, misuse of privilege to view data) and accidental destruction through a patent pending isolation system which ensures that vaulted data is only accessible to its owners.

Data Attestation

Data stored in ImmutaVault can be cryptographically verified to ensure the chain of custody from the time of ingest into the vault to any point in the future.

Chain of Custody

ImmutaVaults exclusively accept data from identified data owners, including users, applications, or source machines. This data ingestion process is thoroughly audited and verified, ensuring the establishment of a chain of custody proof essential for the highest security and most critical data environments.

Common Protocols

ImmutaVaults in the staging phase, prior to sealing, can ingest data from any source that can mount an NFS or SMB file share. Another unique benefit of RackTop's ImmutaVault is that data being used in production can be instantly converted into a vault without the need to copy it to a new system, which saves on time, money, and additional storage costs.

One Way & Permanent

ImmutaVaults are permanently protected with no mechanism to modify, add, or revert once sealed, validated, and cryptographically signed. This true immutability protects from outsiders, insiders and advanced system (OS) oriented attacks.

Policy Driven

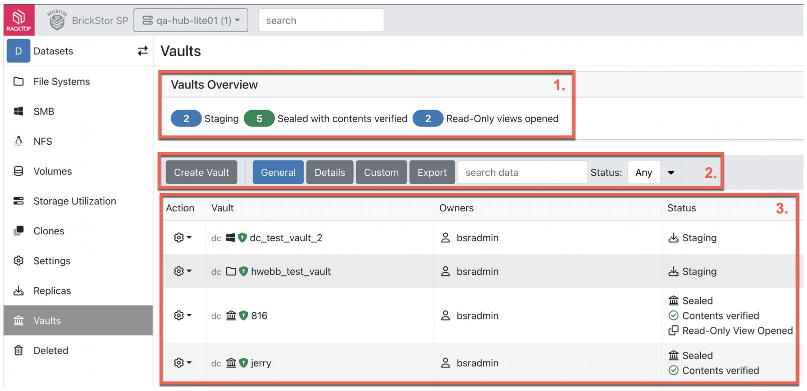
Each ImmutaVault implements its own policy which dictates the data owner (who can view and share vaulted data), as well as the retention and protection settings required to meet any type of regulatory or security compliance requirement.

Digital Views

After sealing an ImmutaVault, access to its contents becomes exclusive to RackTop Digital View technology. Data owners and system operators have the capability to create a Digital View of an existing ImmutaVault, sharing it through common network protocols such as NFS and SMB with specific users, groups, or systems. Importantly, the original ImmutaVault data remains untouched; only the Digital View, an instantaneous zero-copy clone of the vault's data, is accessible. These Digital View ImmutaVaults are subject to governance policies, allowing vaulted data to be exposed for any desired duration and solely to users, hosts, and networks associated with that Digital View's perspective.

Vault Home Page

- The Vault Home Page will present:



Vaults Overview

2 Staging 5 Sealed with contents verified 2 Read-Only views opened

Action	Vault	Owners	Status
⚙	dc dc_test_vault_2	bsradmin	Staging
⚙	dc hwebb_test_vault	bsradmin	Staging
⚙	dc 816	bsradmin	Sealed Contents verified Read-Only View Opened
⚙	dc jerry	bsradmin	Sealed Contents verified

- The Vault Home Page can be divided into three parts:

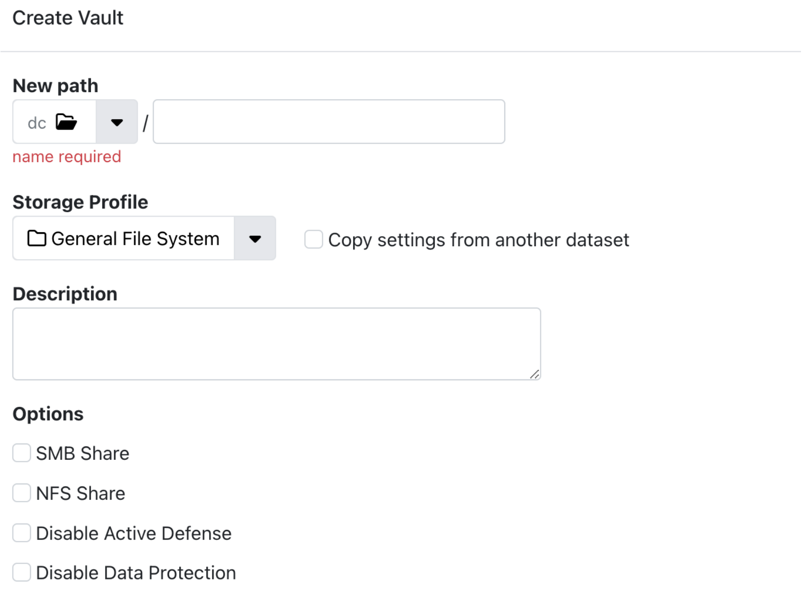
  1. Vault Overview - The Vault Overview displays a quick representation of the Vault's status at any given time. This display shows the number of Vaults currently in the Staging, Sealed With Contents Verified, and Read-Only Views Opened statuses.
  2. The Vault Banner - The Vault Banner allows for the creation of new Vaults, as well as buttons to see different information of the listed vaults below the banner. The buttons are customizable via clicking the **Custom** button. Inherently, the navigation buttons will show the **General** and **Details** options. Further, the banner allows for the export of a Vault by clicking the **Export** button, selecting a desired file format and name, then clicking **Export**. Finally, the Banner allows for the search of any vault by name in the list below.

3. Vault List - The Vault list shows all of the Vaults on a BrickStor SP at any given time. The List is divided into four columns:
   - Actions - Contains the options to Generate Manifest, Finish Staging/Seal, Configure, and Destroy a Vault.
   - Vault - Displays the name of any existing Vault.
   - Owners - Displays the name of the creator of any Vault.
   - Status - Displays the current status of any Vault.

Creating a Vault

Beginning on the Vault Home Page, the steps to create a Vault are as follows:

- Click **Create Vault** in the banner section of the Vault Home Page.
- The Create Vault Page will present:



Create Vault

New path

dc ▾ /

name required

Storage Profile

General File System ▾ □ Copy settings from another dataset

Description

Options

□ SMB Share

□ NFS Share

□ Disable Active Defense

□ Disable Data Protection

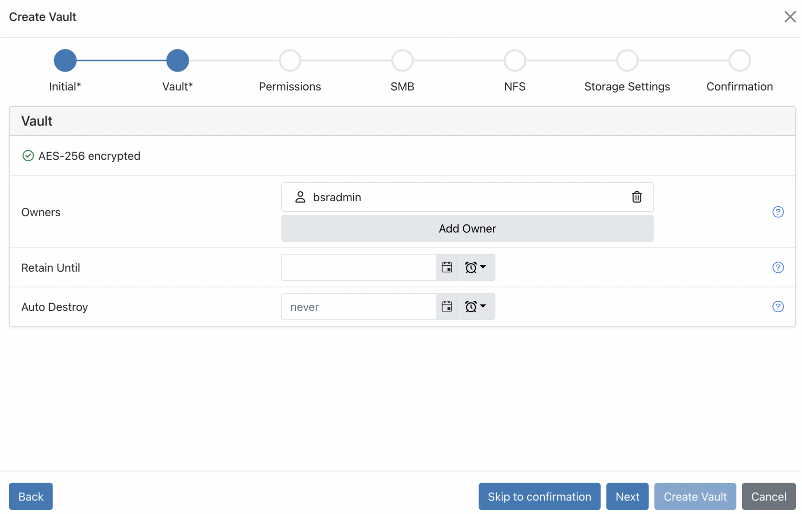
- This page allows for the customization of a Vault that is to be created.
- Select the desired Path for the Vault by clicking the **Downward Arrow** located beneath the New Path Header.
- Enter the desired name of the Vault by Clicking the empty field to the right of the path selection, and entering the desired name of the Vault.
- Select the desired Storage Profile by clicking the **Downward Arrow** located beneath the Storage Profile Header.

NOTE If the creator of the Vault intends to use the Storage Profile settings from another dataset, simply click the **Checkbox** to the right of the Storage Profile selection.

- Optionally, enter a description for the Vault by clicking the empty field beneath the Description header, and typing the desired content.

- Under the Options section, select any arrangement of configurations for the vault.
- Once finished, click **Next** at the bottom of the Create Vault Page.
- The Vault page will present:

Vault Page

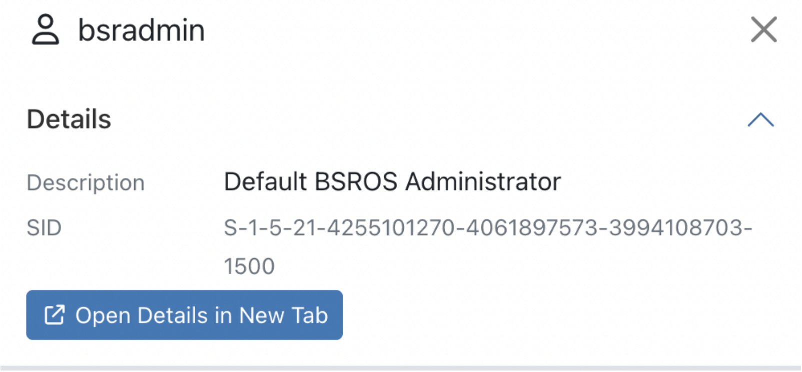


Vault

AES-256 encrypted

Owners	bsradmin
Retain Until	
Auto Destroy	never

- This page provides an overview of the Vault that is being created.
- Under the Owners section, the default owner will be listed. To see details of their ownership, simply **Click** the owner name.



bsradmin

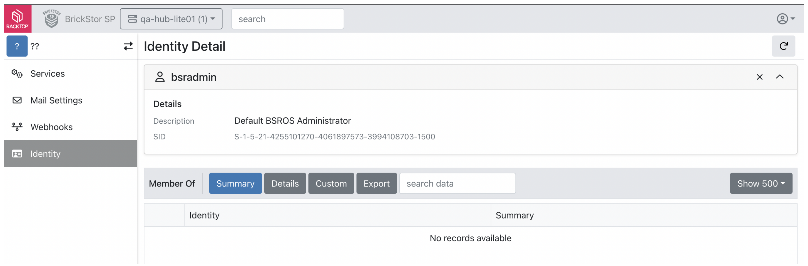
Details

Description	Default BSROS Administrator
SID	S-1-5-21-4255101270-4061897573-3994108703-1500

- The owner name, SID, and option to view in advanced detail will present.

NOTE

- To view more details, click to view in a **New Page**.



Identity Detail

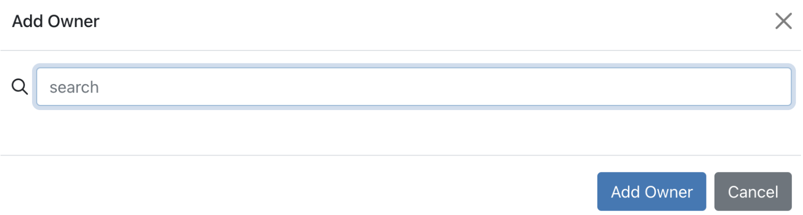
bsradmin

Details

Description	Default BSROS Administrator
SID	S-1-5-21-4255101270-4061897573-3994108703-1500

Identity	Summary
No records available	

- To exit the owner details screen, click the **X** at the top-right of the sidebar.
- To add an owner, click the **Add Owner** button.



Add Owner

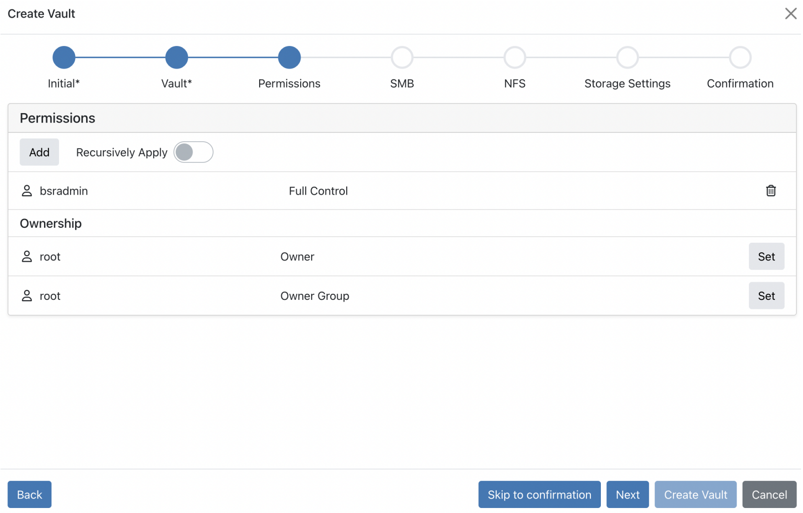
- The ability to search for and add an existing owner is available by searching for the owner name, and clicking **Add Owner**.
- To designate a holding period for the Vault, enter a holding date following M/d/y h:mm AM format under the Retain Until Section.
- To designate a Auto Destroy date for the Vault, enter a destroy date following M/d/y h:mm AM format under the Auto-Destroy Section.

CAUTION Once the Auto-Destroy date is passed, the Vault will be destroyed, and the data within will no longer be accessible.

- Once the desired settings have been configured, click **Next** at the bottom of the page.

Vault Permissions

- The Permissions section will present:



Create Vault

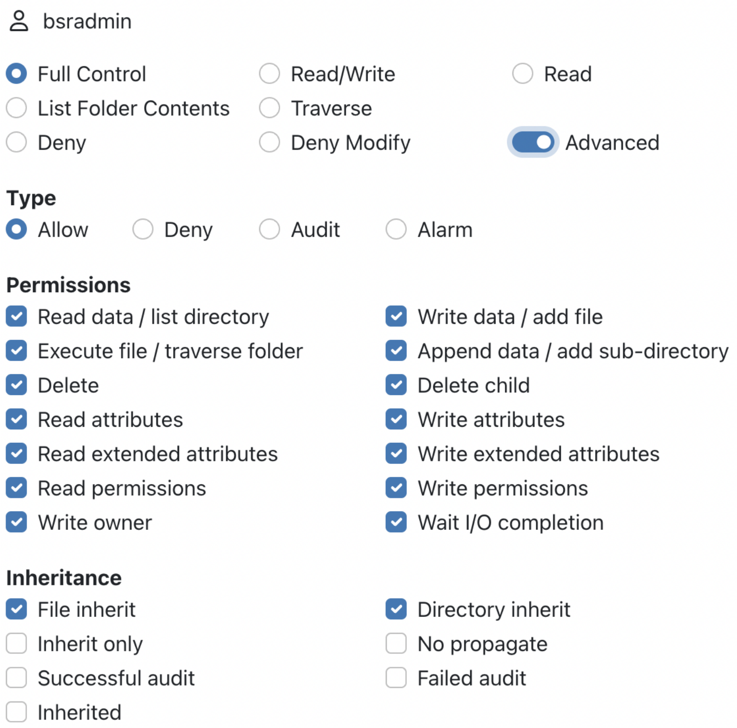
Permissions

bsradmin	Full Control

Ownership

root	Owner	Set
root	Owner Group	Set

- To add permissions to a Vault, click the **Add** button and search for permissions within the provided search bar. Once located, click the **Select** button to add the located permissions.
- To Recursively Apply the selected permissions to any previously created vaults, simply click the **Slider** beside Recursively Apply.
- Permission configuration on a by-user basis is completed by clicking the button that defaults to **Full Control** and selecting from the provided options.



bsradmin

● Full Control ○ Read/Write ○ Read
○ List Folder Contents ○ Traverse
○ Deny ○ Deny Modify ● Advanced

Type

● Allow ○ Deny ○ Audit ○ Alarm

Permissions

☑ Read data / list directory ☑ Write data / add file
☑ Execute file / traverse folder ☑ Append data / add sub-directory
☑ Delete ☑ Delete child
☑ Read attributes ☑ Write attributes
☑ Read extended attributes ☑ Write extended attributes
☑ Read permissions ☑ Write permissions
☑ Write owner ☑ Wait I/O completion

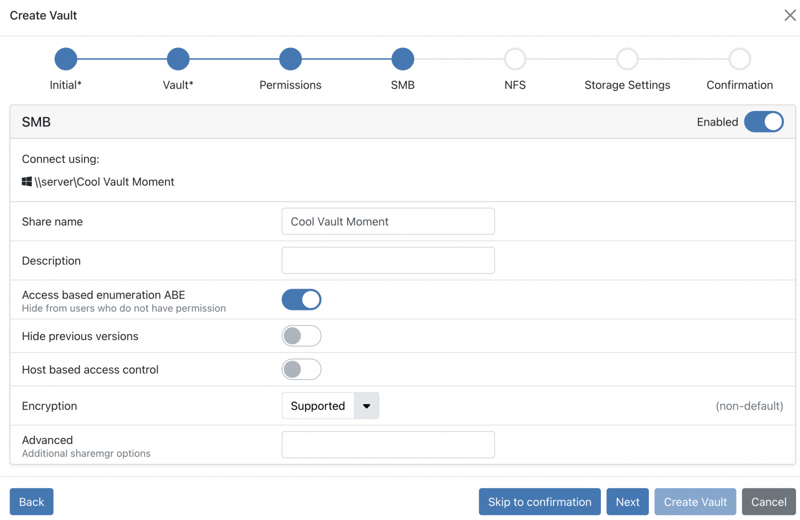
Inheritance

☑ File inherit ☑ Directory inherit
☐ Inherit only ☐ No propagate
☐ Successful audit ☐ Failed audit
☐ Inherited

- The option to select any arrangement of available permissions is possible. Once selected, click the **Add** button.
- The ability to set any added owner is available below by clicking the **Set** button, and searching for the desired owner. Once finished, click the **Select** button.
- Once finished, click the **Next** button at the bottom of the page.

Vault SMB

- The SMB Screen will present:



SMB Enabled ●

Connect using:
\\server\Cool Vault Moment

Share name	Cool Vault Moment
Description	
Access based enumeration ABE Hide from users who do not have permission	●
Hide previous versions	○
Host based access control	○
Encryption	Supported ▾ (non-default)
Advanced Additional sharemgr options	

- Here, the option to enable/disable SMB on the Vault is present by toggling the **Slider** at the top-right of the page.

- The Share name will default to the Vault name, but is editable by clicking the open field where the default name is present, and typing the desired name.
- Optionally, enter a description for the Vault by clicking the empty field beneath the Description header, and typing the desired content.
- The option to enable/disable Access based enumeration ABE, Hide Previous Versions, and Host based access control is configurable by clicking the **Sliders**.
- SMB Encryption is a feature that provides end-to-end privacy and integrity assurance between the file server and the client. It can be disabled or enabled on the share level by setting Encryption property to Supported, Required or Disabled.

NOTE

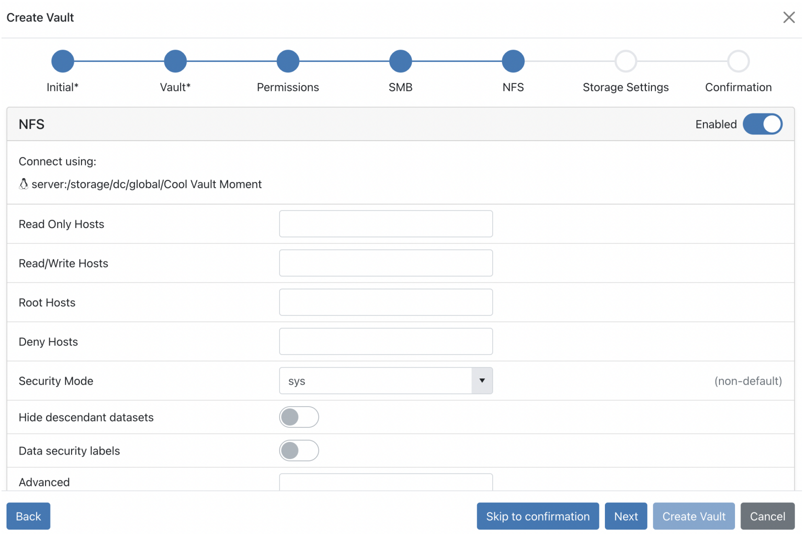
These selection augment the following:

Disabled → Encryption is disabled. **Supported** → Encryption is enabled but not enforced. The SMB client will negotiate whether to use encryption or not. **Required** → SMB 3+ feature. Encryption is enabled and required in order to establish the connection.

- If advanced options are desired, enter any desired `sharemgr` commands in the empty field located beside the Advanced section.
- Once finished, click the **Next** button at the bottom of the page.

Vault NFS

- The NFS section will present:



Enabled

Connect using:
server:/storage/dc/global/Cool Vault Moment

Read Only Hosts

Read/Write Hosts

Root Hosts

Deny Hosts

Security Mode: sys (non-default)

Hide descendant datasets

Data security labels

Advanced

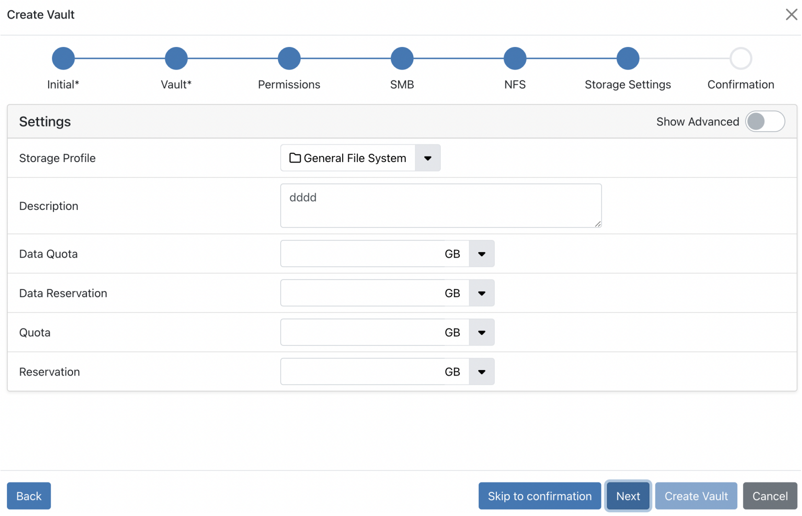
- The option to add Read-Only Hosts, Read/Write Hosts, Root Hosts, and Deny Host, is configurable by searching for the host name via the empty fields beside each respective section.
- The security mode (defaulted to `sys`) can be configured by clicking the **downward arrow** and selecting the available options by **clicking** any displayed option.
- The option to enable/disable Hide descendant datasets, and Data security labels is configurable by clicking the provided **Sliders**.
- If advanced options are desired, enter any desired commands in the empty field located beside

the Advanced section.

- Once finished, click the **Next** button at the bottom of the page.

Vault Settings

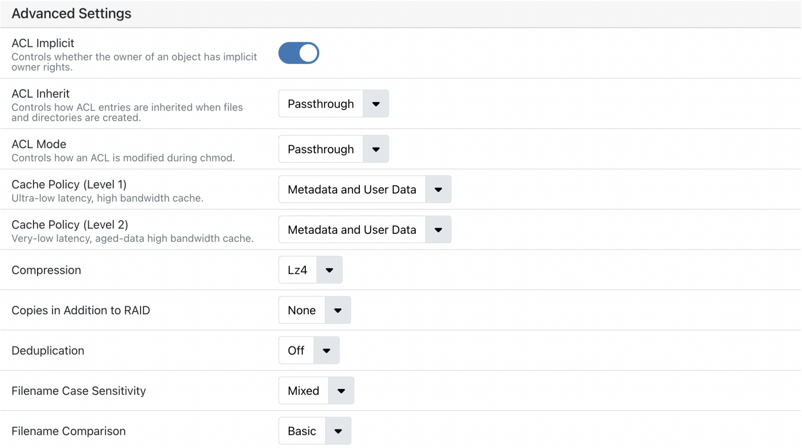
- The Vault Settings screen will present:



Settings

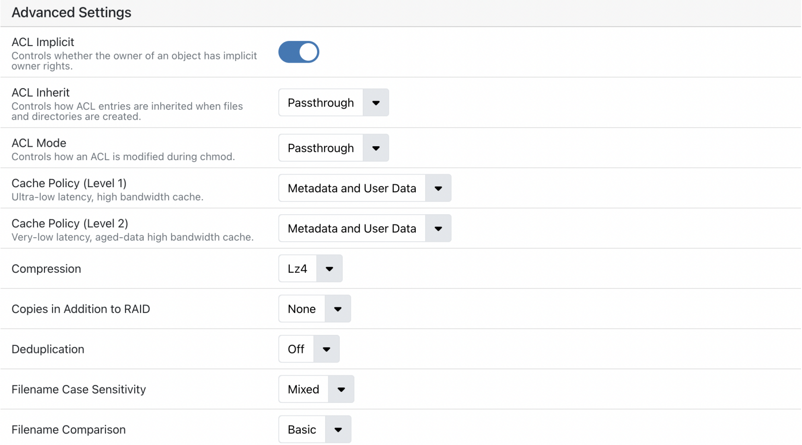
Storage Profile	General File System
Description	dddd
Data Quota	GB
Data Reservation	GB
Quota	GB
Reservation	GB

- The option to select the storage profile location is located by **clicking** the defaulted location name.
- To add a description, **click** the empty field to the right of the Description header.
- Data Quota, Data Reservation, Quota, and Reservation data limits may be set to a configurable memory unit.
    - Enter the desired numerical value by **clicking** the open field to the right of the respective headers.
    - Select the desired memory unit by **clicking** the downward arrow next to the defaulted memory value, and selecting the desired memory value.
- To view the advanced list of settings, toggle the **slider** at the top-right of the page:



Advanced Settings

ACL Implicit Controls whether the owner of an object has implicit owner rights.	●
ACL Inherit Controls how ACL entries are inherited when files and directories are created.	Passthrough
ACL Mode Controls how an ACL is modified during chmod.	Passthrough
Cache Policy (Level 1) Ultra-low latency, high bandwidth cache.	Metadata and User Data
Cache Policy (Level 2) Very-low latency, aged-data high bandwidth cache.	Metadata and User Data
Compression	Lz4
Copies in Addition to RAID	None
Deduplication	Off
Filename Case Sensitivity	Mixed
Filename Comparison	Basic



Advanced Settings	
ACL Implicit Controls whether the owner of an object has implicit owner rights.	●
ACL Inherit Controls how ACL entries are inherited when files and directories are created.	Passthrough ▾
ACL Mode Controls how an ACL is modified during chmod.	Passthrough ▾
Cache Policy (Level 1) Ultra-low latency, high bandwidth cache.	Metadata and User Data ▾
Cache Policy (Level 2) Very-low latency, aged-data high bandwidth cache.	Metadata and User Data ▾
Compression	Lz4 ▾
Copies in Addition to RAID	None ▾
Deduplication	Off ▾
Filename Case Sensitivity	Mixed ▾
Filename Comparison	Basic ▾

- The following is a list of configurable advanced settings:
  - **ACL Implicit** - Controls whether the owner of an object has implicit owner rights.
  - **ACL Inherit** - Controls how ACL entries are inherited when files and directories are created.
  - **ACL Mode** - Controls how an ACL is modified during chmod.
  - **Cache Policy (Level 1)** - Ultra-low latency, high bandwidth cache.
  - **Cache Policy (Level 2)** - Very-low latency, aged-data high bandwidth cache.
  - **Compression** - Select which compression algorithm to run on the dataset.
  - **Copies in addition to RAID** - Select the (max 2) number of vault copies.
  - **Deduplication** - Select the value and granularity of Deduplication checks within the Vault.
  - **Filename Case Sensitivity** - Manage the Vault’s sensitivity to upper/lowercase lettering.
  - **Filename Comparison** - Select from a basic comparison level, or from a variety of Unicode form levels.
  - **Filename UTF-8 Only** - Toggle adherence to UTF-8 Filename formatting.
  - **Flush Data to Stable Storage** - Defaults to Synchronous (POSIX Standard), but may be changed to All or Periodic.

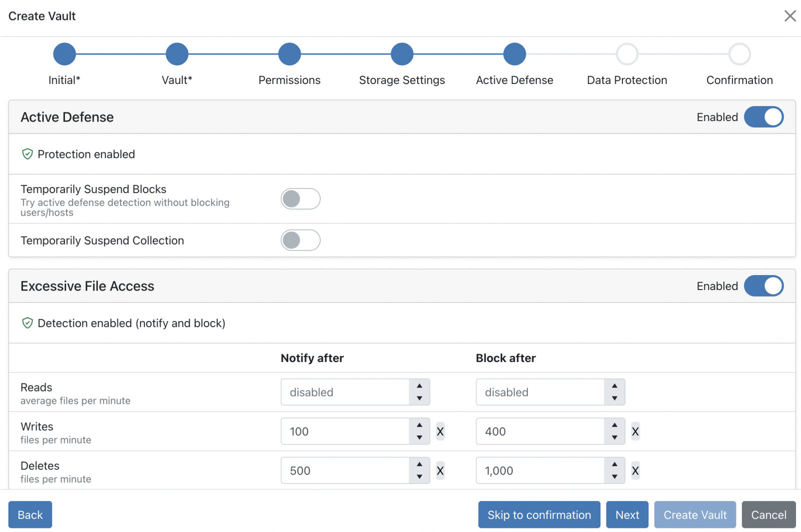
NOTE When configuring Data Flush, the choice of **All** will heavily impact system performance. Periodic will yield quick performance, but puts the data at the highest available risk.

- **Indexing** - Toggle the Indexing utility.
- **Integrity** Checksum Algorithm - Configure the Integrity checking on user data.
- **Log Bias** - Defaulted to Latency, can be changed to Throughput if streaming large files.
- **Metadata Redundancy** - Configure the amount of metadata redundancy in addition to RAID.
- **Mount** - Configure whether or not to allow the Vault to be mounted, or only allow mounting of the Vault via explicit action.
- **Non-Blocking Mandatory Locks** - NBMAND lock coordination across SMB, NFS and local processes.
- **Read Only** - Configure the Vault to be editable or read-only.

- **Record Size** - Determine the desired Record size at the byte level.
- **Smart Folders** - Automatically create sub-dataset when client creates top-level directory.
- **Update Access Time on Read** - Changes the date last accessed when a user reads the Vault.
    - Any/all of the Advanced settings may be configured in any orientation to achieve the desired Vault settings.
    - Once finished, click the **Next** button at the bottom of the page.

Vault Active Defense

- The Active Defense screen will present:



Create Vault

Active Defense — Enabled

Protection enabled

Temporarily Suspend Blocks
Try active defense detection without blocking users/hosts

Temporarily Suspend Collection

Excessive File Access — Enabled

Detection enabled (notify and block)

	Notify after	Block after
Reads average files per minute	disabled	disabled
Writes files per minute	100 X	400 X
Deletes files per minute	500 X	1,000 X

- The option to toggle Active Defense on/off is present at the top-right of the Active Defense section.

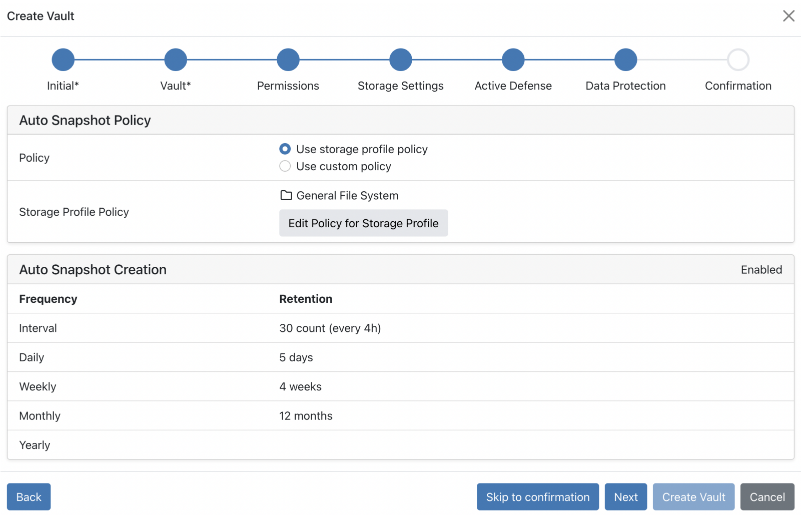
NOTE If the decision is made to toggle Active Defense off, the further section options will hide, click the **Next** button to continue.

- The option to Temporarily Suspend Blocks, or to try active defense detection without blocking users/hosts, is configurable on/off by clicking the **Slider** beside the header.
- The option to Temporarily Suspend Collection is configurable on/off by clicking the **Slider** beside the header.
- The option to enable/disable Excessive File Access protocol is present the top-right of the Excessive File Access section.
- The Excessive File Access Section allows for the configuration of a file range that notifies administrators after a set amount of file Reads, Writes, and Deletes. The option to configure the blocking of these abilities after a numerical limit is reached is also present, along with the ability to disable the notification limits at each level.
    - To configure the Excessive File Access values, click to select the desired empty field and enter the desired numerical value to set the limit of files before/after notification and blocking of File Access. To remove a specific notify or block parameter, simply click the **X** beside the parameter that is to be disabled.

- Once finished, click the **Next** button at the bottom of the page.

Vault Auto Snapshots

- The Vault Auto Snapshots screen will present:



Create Vault

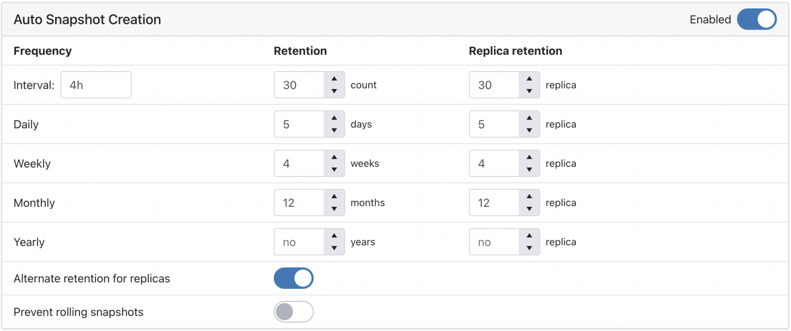
Auto Snapshot Policy

Policy	● Use storage profile policy ○ Use custom policy
Storage Profile Policy	General File System Edit Policy for Storage Profile

Auto Snapshot Creation — Enabled

Frequency	Retention
Interval	30 count (every 4h)
Daily	5 days
Weekly	4 weeks
Monthly	12 months
Yearly	

- The option to select between a storage profile or custom Auto Snapshot policy is present. To configure this selection, **click** to highlight the button beside the desired Auto Snapshot policy.
- If a custom Auto Snapshot policy is selected, the Auto Snapshot Creation section will change from listed, to configurable values pictured below (Shown with Alternate retention set to **On**):



Auto Snapshot Creation — Enabled

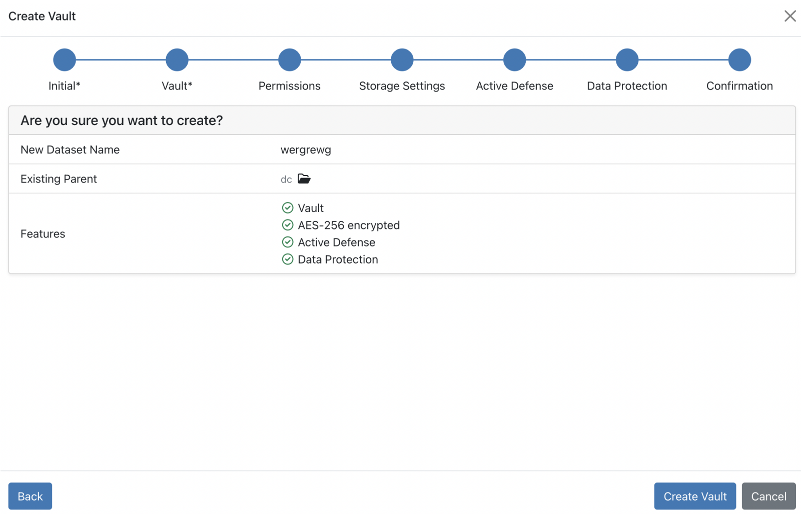
Frequency	Retention		Replica retention	
Interval: 4h	30	count	30	replica
Daily	5	days	5	replica
Weekly	4	weeks	4	replica
Monthly	12	months	12	replica
Yearly	no	years	no	replica
Alternate retention for replicas	On			
Prevent rolling snapshots	Off			

- Auto Snapshot configuration is completed by first selecting the interval that Snapshots will be taken on the system. The default value is every four hours, but may be changed by **clicking** the default field, and entering a desired numerical value, as well as a time signature (ex: 6h, 1d, 30s).
- The Snapshot Retention value will augment the amount of saved Snapshots on a Vault at any given time. This value operates on a rolling basis, when the maximum value is reached, the oldest Snapshot is deleted to make room for a newer Snapshot (The option to prevent the Rolling nature of Snapshots is configurable via the **Slider** at the bottom of the Auto Snapshot Creation section). To configure this, click the (default 30) value, and enter the desired numerical amount of Snapshots to hold at a given time.
- Additionally, the option to retain Snapshots on a per-day/week/month/year basis is configurable by **clicking** the field to the right of the desired retention time, and entering the desired numerical retention value.

- Optionally, the ability to select Alternate retention for replicas will present the Replica Retention section of the Snapshot settings. This allows for similar configuration as discussed above, allowing selection of retention amount by a numerical amount as well as Replica retention on a per-day/week/month/year basis.
- Once finished, click the **Next** button at the bottom of the page.

Vault Confirmation

- The Vault Confirmation screen will present:



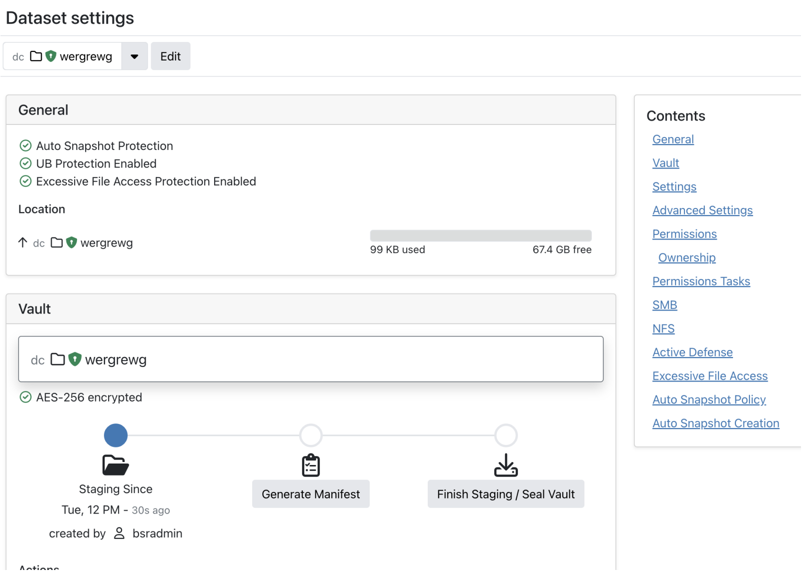
Are you sure you want to create?

New Dataset Name	wergrewg
Existing Parent	dc
Features	✓ Vault ✓ AES-256 encrypted ✓ Active Defense ✓ Data Protection

- Here, an overview of the vault that is being created will be shown.
- If the settings contained in the Vault Overview appear correct, click the **Create Vault** button at the bottom right of the screen to create the Vault with the configured parameters.

The Vault Details Page

Once a Vault is created, or when **clicking** a Vault's name from the Vault Home Page, a Vault Details page will present:



Dataset settings

dc wergrewg ▾ Edit

General

✓ Auto Snapshot Protection
✓ UB Protection Enabled
✓ Excessive File Access Protection Enabled

Location

↑ dc wergrewg — 99 KB used, 67.4 GB free

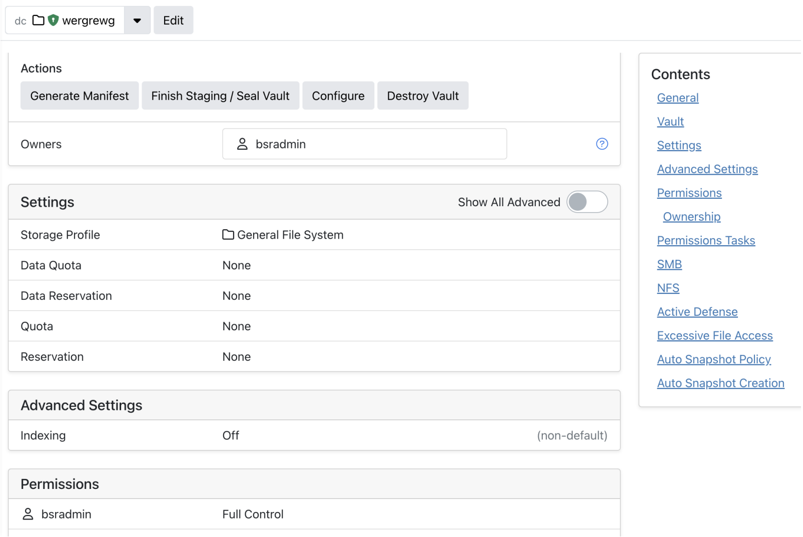
Vault

dc wergrewg

✓ AES-256 encrypted

● Staging Since Tue, 12 PM - 30s ago, created by bsradmin — ○ Generate Manifest — ○ Finish Staging / Seal Vault

Contents
General
Vault
Settings
Advanced Settings
Permissions
Ownership
Permissions Tasks
SMB
NFS
Active Defense
Excessive File Access
Auto Snapshot Policy
Auto Snapshot Creation



dc wergrewg ▾ Edit

Actions

Generate Manifest | Finish Staging / Seal Vault | Configure | Destroy Vault

Owners: bsradmin

Settings — Show All Advanced ○

Storage Profile	General File System
Data Quota	None
Data Reservation	None
Quota	None
Reservation	None

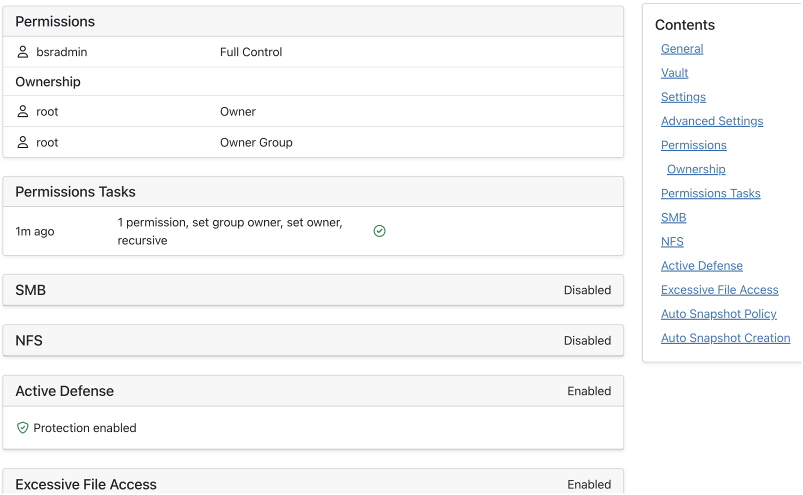
Advanced Settings

Indexing	Off	(non-default)

Permissions

bsradmin	Full Control

Contents
General
Vault
Settings
Advanced Settings
Permissions
Ownership
Permissions Tasks
SMB
NFS
Active Defense
Excessive File Access
Auto Snapshot Policy
Auto Snapshot Creation



Permissions

bsradmin	Full Control

Ownership

root	Owner
root	Owner Group

Permissions Tasks

1m ago	1 permission, set group owner, set owner, recursive	✓

SMB — Disabled

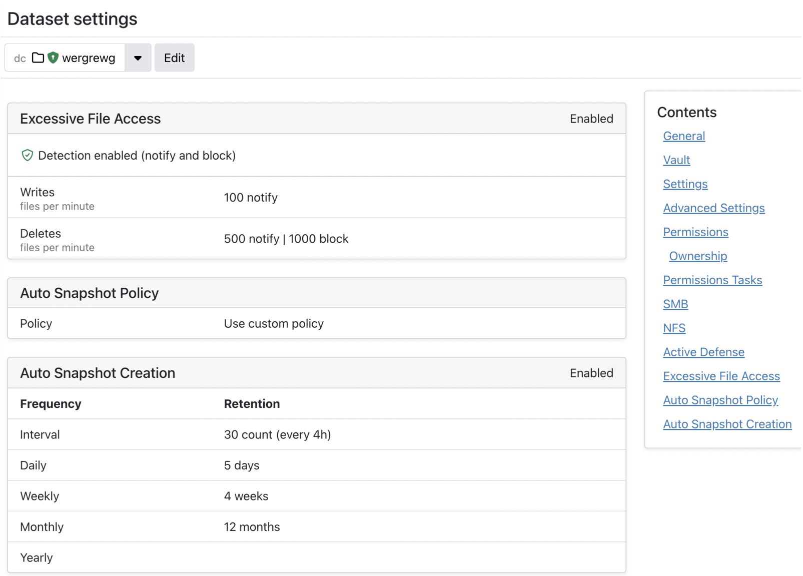
NFS — Disabled

Active Defense — Enabled

✓ Protection enabled

Excessive File Access — Enabled

Contents
General
Vault
Settings
Advanced Settings
Permissions
Ownership
Permissions Tasks
SMB
NFS
Active Defense
Excessive File Access
Auto Snapshot Policy
Auto Snapshot Creation



Dataset settings

dc wergrewg Edit

Excessive File Access	Enabled
Detection enabled (notify and block)	
Writes files per minute	100 notify
Deletes files per minute	500 notify | 1000 block

Auto Snapshot Policy	
Policy	Use custom policy

Auto Snapshot Creation	Enabled
Frequency	**Retention**
Interval	30 count (every 4h)
Daily	5 days
Weekly	4 weeks
Monthly	12 months
Yearly	

Contents

- General
- Vault
- Settings
- Advanced Settings
- Permissions
  - Ownership
- Permissions Tasks
- SMB
- NFS
- Active Defense
- Excessive File Access
- Auto Snapshot Policy
- Auto Snapshot Creation

The Vault Details Page begins with a General overview of the Vault status. It will denote the current status of SMB and NFS on the Vault, and show the location/current storage amount on the Vault.

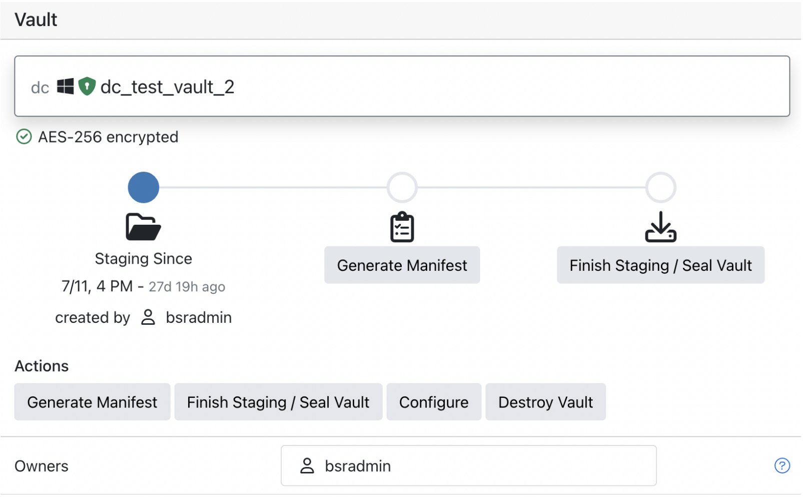
Further, the Vault Details Page will show the Vault's configuration settings selected when Creating a Vault by section.

Most importantly, the Vault Details Page shows the current status of the Vault in its Manifest/Staging/Sealing Process.

Staging, Manifesting, and Sealing a Vault

Vaults, when created default to the **Staging** phase. In this phase, the Vault's settings and ownership are configurable via The Vault Details Page.

To begin the Manifest Generation, Staging and Sealing of a Vault, begin at the **Vault** Section of The Vault Details Page.



Vault

dc dc_test_vault_2

AES-256 encrypted

Staging Since
7/11, 4 PM - 27d 19h ago
created by bsradmin

Actions

Owners bsradmin

Vault Manifest

The Vault Manifest functions as a thorough documentation of the present Vault data and its configuration parameters. It serves as an authenticated catalogue of all vault contents by recording file details and their respective hashes. The Manifest undergoes hashing and subsequent signing, establishing a fully verifiable chain of trust, ensuring the integrity of the vault files. Consequently, these files can be extracted from the vault and stored elsewhere, offering a permanent, standalone record of the vault's contents, independent of the vault system.

- The Manifest records a list of all files within the vault and their checksums.
- The system generates a Manifest automatically during the sealing process.
- Creating a Manifest independent of sealing allows for content validation before initiating the sealing process.

Accessing Manifest File(s)

- **Sharing Options:** Manifest file(s) are accessible for download by sharing the Vault via SMB/NFS.

Manifest output consists of the following:

`.rtvault_manifest.txt` - Vault manifest.

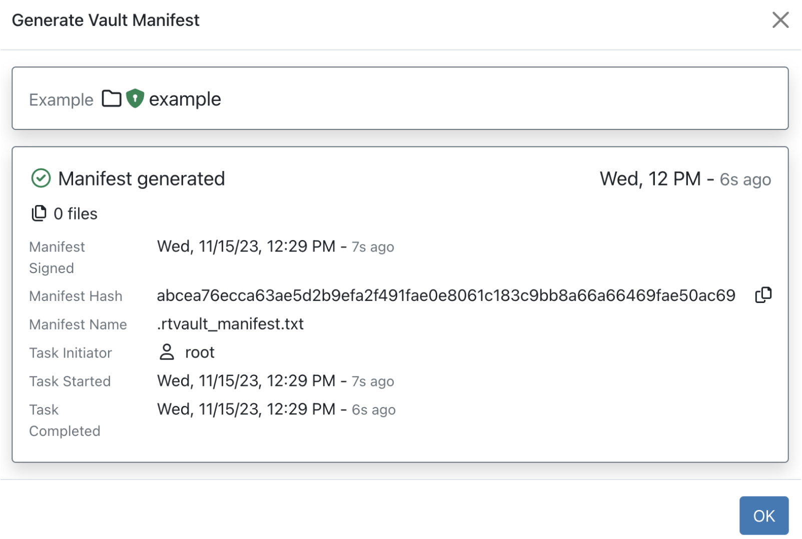
`.rtvault_manifest.sha256` - Checksum of the .rtvault_manifest.txt file.

`.rtvault_manifest.sig` - Vault signature.

Manual Manifest Generation

- To begin the Manifest Generation, click the **Generate Manifest** button in the Vault Section of The Vault Details Page.

NOTE Clicking the Generate Manifest button in either the Vault Road Map or Actions section will yield the same result.



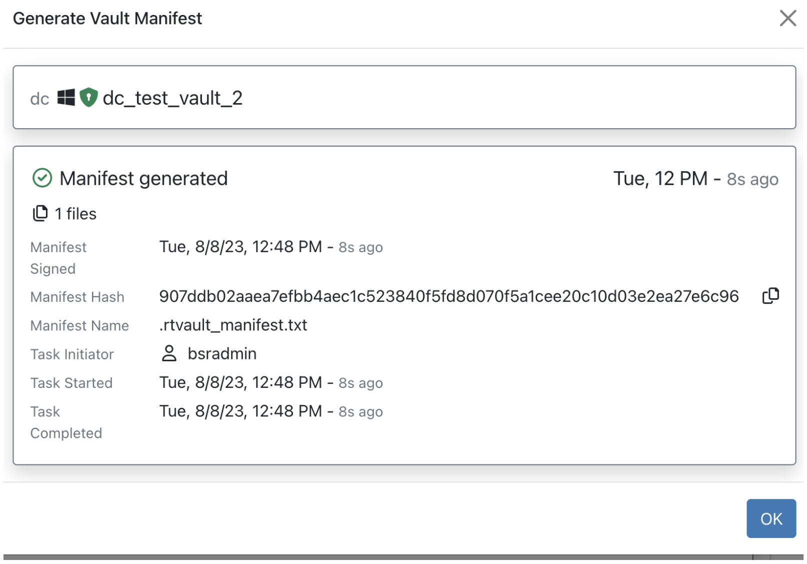
Example example

Manifest generated Wed, 12 PM - 6s ago

0 files

Manifest Signed	Wed, 11/15/23, 12:29 PM - 7s ago
Manifest Hash	abcea76ecca63ae5d2b9efa2f491fae0e8061c183c9bb8a66a66469fae50ac69
Manifest Name	.rtvault_manifest.txt
Task Initiator	root
Task Started	Wed, 11/15/23, 12:29 PM - 7s ago
Task Completed	Wed, 11/15/23, 12:29 PM - 6s ago

- Ensuring the Vault name is correct and the Manifest Generation is desired, click the **Generate** button.
- The following will present:



dc dc_test_vault_2

Manifest generated Tue, 12 PM - 8s ago

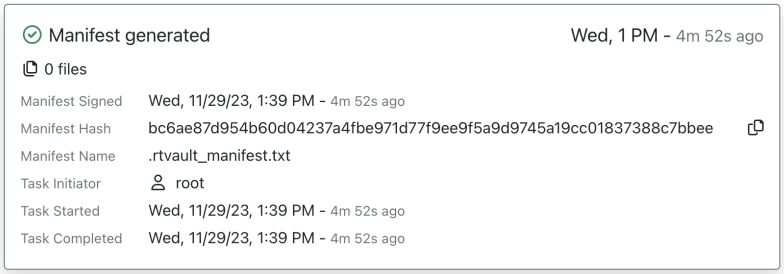
1 files

Manifest Signed	Tue, 8/8/23, 12:48 PM - 8s ago
Manifest Hash	907ddb02aaea7efbb4aec1c523840f5fd8d070f5a1cee20c10d03e2ea27e6c96
Manifest Name	.rtvault_manifest.txt
Task Initiator	bsradmin
Task Started	Tue, 8/8/23, 12:48 PM - 8s ago
Task Completed	Tue, 8/8/23, 12:48 PM - 8s ago

- Here, a confirmation of the completed Manifest Generation will appear, as well as a listing of metadata regarding the Vault and what was manifested on it.
  - It is recommended to copy and save the Manifest Hash of the Vault. To copy the Hash to the system clipboard, simply click the **File** button to the right of the listed Manifest Hash.
- Once reviewed, click the **OK** button.
- To reopen and check the Vault contents at any time. Click the **Verify Contents** button in the Actions section. This will present the same screen that is reached after Generating a Manifest.
- The option to Regenerate the Manifest is available at any time before sealing the Vault by clicking the **Regenerate Manifest** button and following the above steps again.

Accessing Manifest

- Manifest information may be accessed at any time by beginning at the Vault Home Page and clicking the **Vault Name** in the Vault List.



Manifest generated Wed, 1 PM - 4m 52s ago

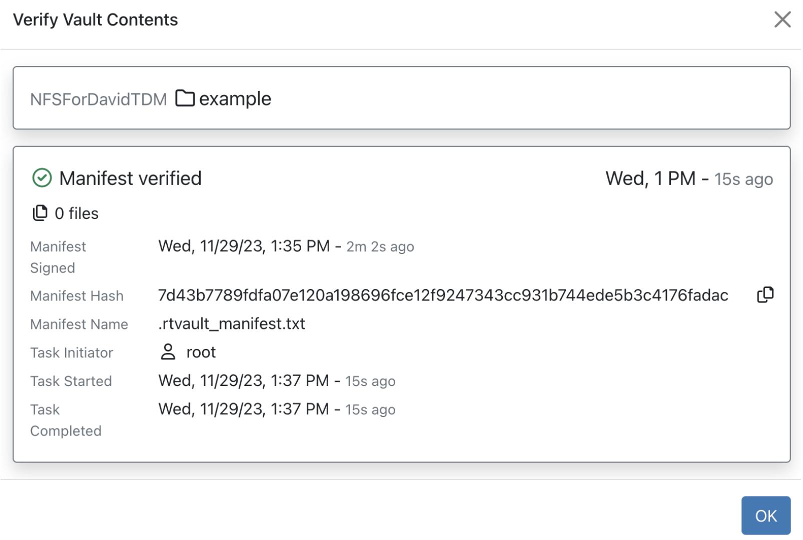
0 files

Manifest Signed	Wed, 11/29/23, 1:39 PM - 4m 52s ago
Manifest Hash	bc6ae87d954b60d04237a4fbe971d77f9ee9f5a9d9745a19cc01837388c7bbee
Manifest Name	.rtvault_manifest.txt
Task Initiator	root
Task Started	Wed, 11/29/23, 1:39 PM - 4m 52s ago
Task Completed	Wed, 11/29/23, 1:39 PM - 4m 52s ago

- The following overview is present:
    - Manifest Signed - Shows the date of the Manifest's last signing.
    - Manifest Hash - Displays the Hash string for the Manifest, this can be copied to the system clipboard by clicking the **Copy** icon immediately to the right of the Hash.
    - Manifest Name - Displays the named .txt file of the Manifest.
    - Task Initiator - Displays the Username of the user who initiated the Manifest Generation. Details of the user can be displayed in further detail by clicking the displayed **Username**.
    - Task Started - Displays the date/time of the Manifest Generation's initiation.
    - Task Completed - Displays the date/time of the Manifest Generation's completion.

Verifying Manifest Contents

- Clicking the **Verify Contents** button will begin verification of Manifest contents against the Vault.
- A window to confirm verification will present, click the **Verify** button.



Verify Vault Contents

NFSForDavidTDM example

Manifest verified Wed, 1 PM - 15s ago

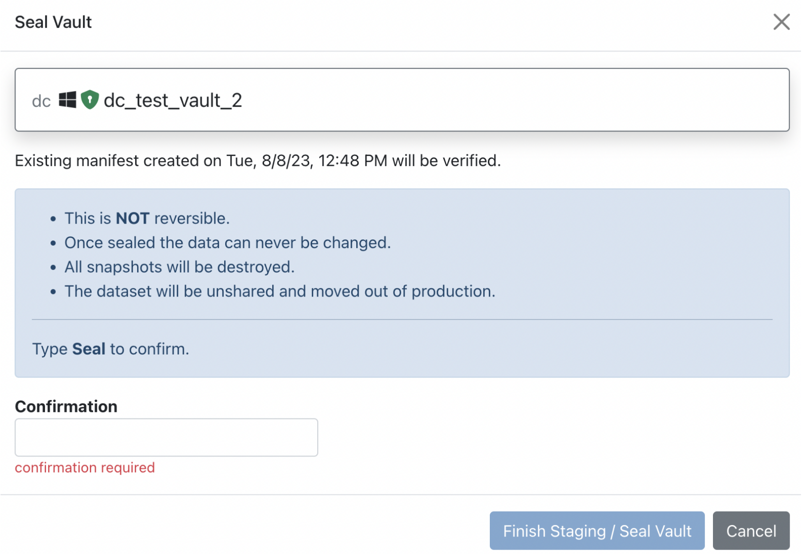
0 files

Manifest Signed	Wed, 11/29/23, 1:35 PM - 2m 2s ago
Manifest Hash	7d43b7789fdfa07e120a198696fce12f9247343cc931b744ede5b3c4176fadac
Manifest Name	.rtvault_manifest.txt
Task Initiator	root
Task Started	Wed, 11/29/23, 1:37 PM - 15s ago
Task Completed	Wed, 11/29/23, 1:37 PM - 15s ago

- An overview of the verification will present, as well as a time stamp denoting the most recent Manifest verification.

Finish Staging/Seal Vault

- Begin the Vault sealing process by **clicking** the **Finish Staging/Seal Vault** button in The Vault Details Page.



Seal Vault

dc dc_test_vault_2

Existing manifest created on Tue, 8/8/23, 12:48 PM will be verified.

- This is **NOT** reversible.
- Once sealed the data can never be changed.
- All snapshots will be destroyed.
- The dataset will be unshared and moved out of production.

Type **Seal** to confirm.

Confirmation

confirmation required

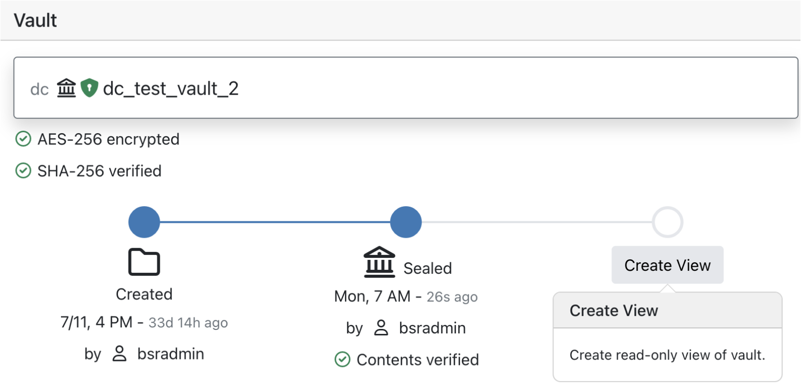
NOTE Sealing a Vault is an irreversible process. Once data is sealed in a Vault it no longer may be changed. All Snapshots will be destroyed when the Vault is sealed. The dataset will be unshared and moved out of production when sealed.

- Once ready, **click** the empty text field and type **Seal** to confirm the sealing process.
- Click the **Finish Staging/Seal Vault** button.
- The vault has now been sealed.

Managing a Sealed Vault

Once a Vault has been sealed, there are a few new options present to manage the vault.

After successfully sealing a vault, or when clicking on an already sealed vault from the Vault Home Page, the sealed Vault details will present.



Vault

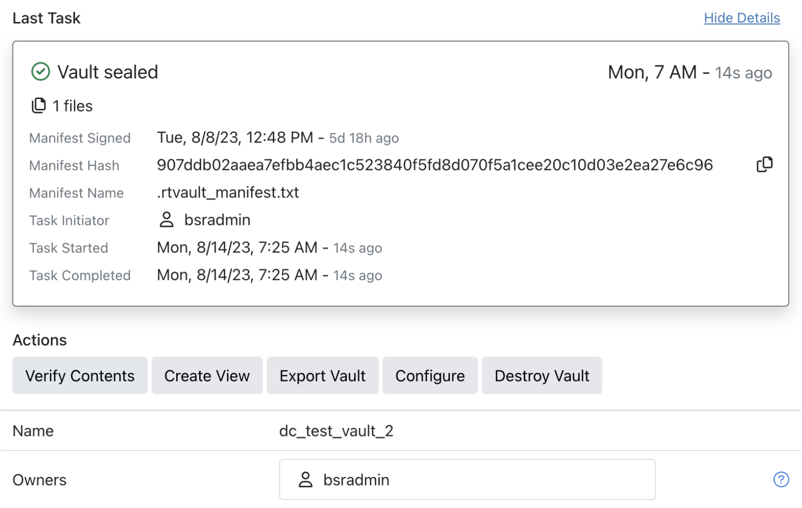
dc dc_test_vault_2

✓ AES-256 encrypted

✓ SHA-256 verified

Created
7/11, 4 PM - 33d 14h ago
by bsradmin

Sealed
Mon, 7 AM - 26s ago
by bsradmin
✓ Contents verified



Last Task

Vault sealed Mon, 7 AM - 14s ago

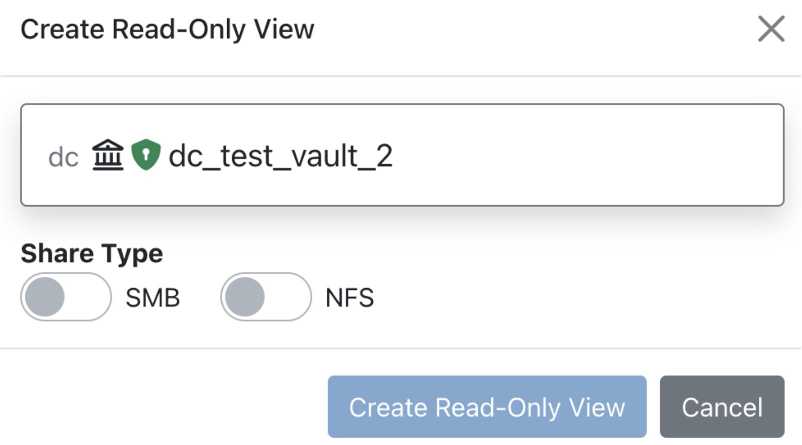
1 files

Manifest Signed	Tue, 8/8/23, 12:48 PM - 5d 18h ago
Manifest Hash	907ddb02aaea7efbb4aec1c523840f5fd8d070f5a1cee20c10d03e2ea27e6c96
Manifest Name	.rtvault_manifest.txt
Task Initiator	bsradmin
Task Started	Mon, 8/14/23, 7:25 AM - 14s ago
Task Completed	Mon, 8/14/23, 7:25 AM - 14s ago

Name	dc_test_vault_2
Owners	bsradmin

Here, the choice can be made to create a **Read-Only View** of the Vault.

- To do so, begin by clicking the **Create View** button on the Vault Road Map.

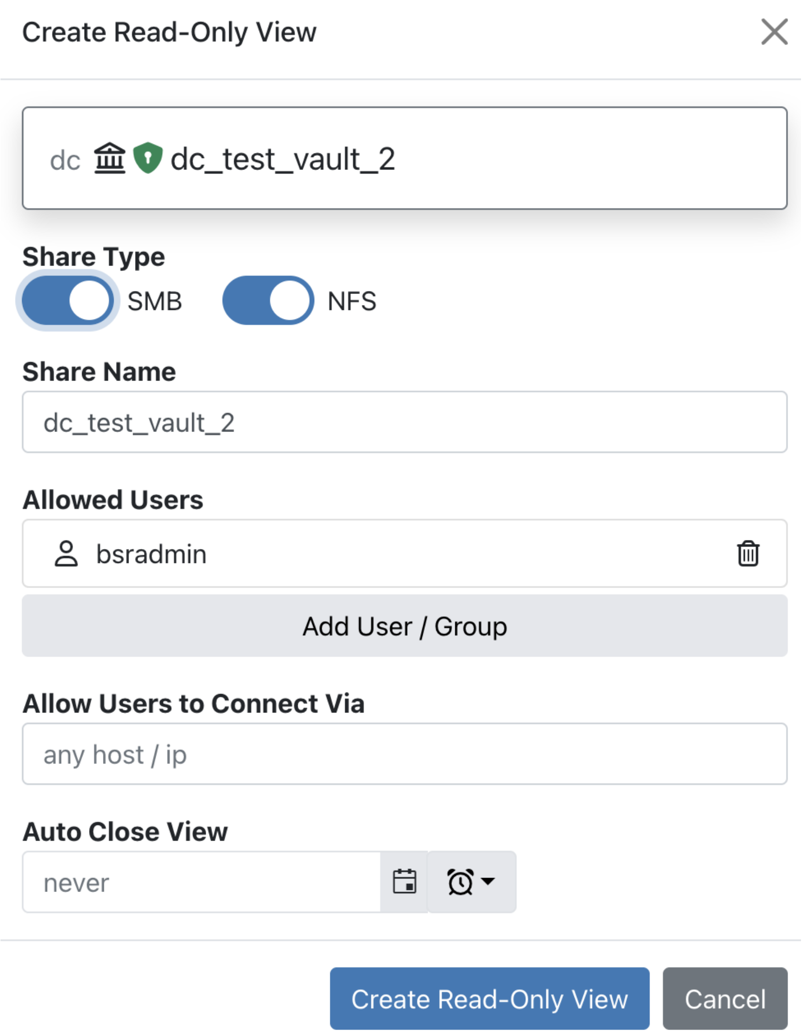


Create Read-Only View

dc dc_test_vault_2

Share Type

- To enable NFS or SMB on the View, click their respective **Sliders**.



Create Read-Only View

dc dc_test_vault_2

Share Type

SMB ● NFS ●

Share Name

dc_test_vault_2

Allowed Users

bsradmin

Add User / Group

Allow Users to Connect Via

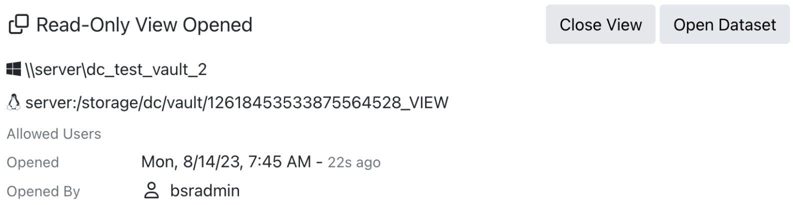
any host / ip

Auto Close View

never

Create Read-Only View Cancel

- Here, the option to change the share name, allowed users, connectivity by configurable IP, and auto-close timing (Defaulted to never auto-close).
- Once the desired settings are configured, click the **Create Read-Only View** button.
- The read-only view will be created, and shown on the sealed Vault details page:



Read-Only View Opened

Close View Open Dataset

\\server\dc_test_vault_2

server:/storage/dc/vault/12618453533875564528_VIEW

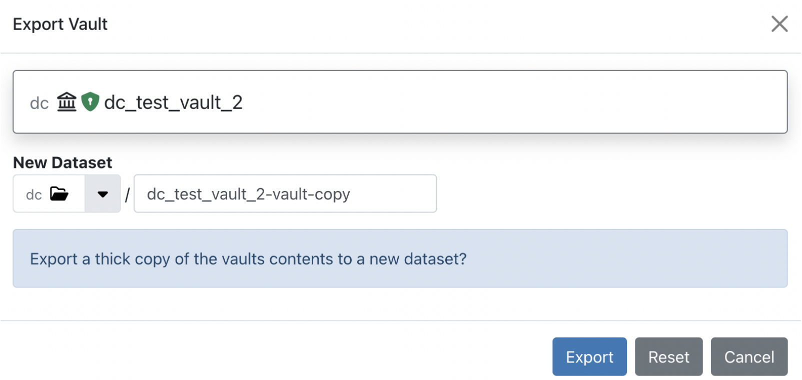
Allowed Users

Opened Mon, 8/14/23, 7:45 AM - 22s ago

Opened By bsradmin

- To view the read-only Vault dataset, click the **Open Dataset** button.
- The Sealed Vault settings will now display showing the Vault’s configuration.
- To close the read-only view of the sealed Vault, click the **Close View** button.
- At the bottom of the screen, a list of buttons that allow further management of the sealed Vault are present:

  - Verify Contents - To verify Vault contents, simply click the **Verify Contents** button, click **Verify**, then click **OK**.
  - Create View - Follows the same operative use-case as explained above.
  - Export Vault - Allows for Vault content export to a new dataset:
    - To export the Vault, click the **Export Vault** button.



Export Vault

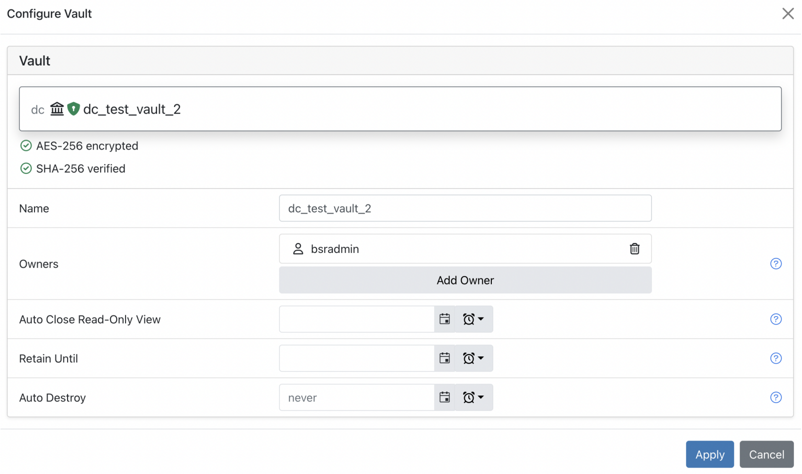
dc dc_test_vault_2

New Dataset

dc / dc_test_vault_2-vault-copy

Export a thick copy of the vaults contents to a new dataset?

- Configure the exported dataset name, then click **Export**.
- A prompt denoting success will present.
  - Configure - Allows for administrative configuration of the sealed Vault.
- To configure the sealed Vault, click the **Configure** button.



Configure Vault

Vault

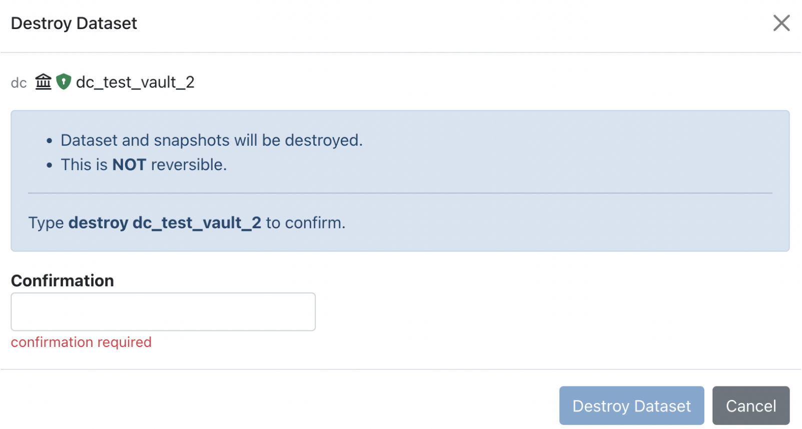
dc dc_test_vault_2

AES-256 encrypted

SHA-256 verified

Name	dc_test_vault_2
Owners	bsradmin
Auto Close Read-Only View	
Retain Until	
Auto Destroy	never

- The option to change the Vault name and ownership are available, as well as the option to set Retain Until/Auto-Destroy dates.
- Once configured, click the **Apply** button.
  - Destroy Vault - Completely destroy the Vault and all of its data.
- To destroy the sealed Vault, click the **Destroy Vault** button.



Destroy Dataset

dc 🏛 dc_test_vault_2

- Dataset and snapshots will be destroyed.
- This is **NOT** reversible.

Type **destroy dc_test_vault_2** to confirm.

Confirmation

confirmation required

NOTE Destroying a vault is an **irreversible** action. The dataset and all snapshots will be irrecoverably destroyed.

- Once ready, click the empty text field and type `destroy VAULT NAME`.
- Finally, click the **Destroy Dataset** button.