BACKBOX

BackBox® E4.11 User Guide

ETINET

Legal Notice

Table of Contents

PREFACE

This User Manual contains a product presentation and reference information for the configuration and operation of a BackBox subsystem connected to a NonStop server.

BackBox is part of the BackPak product family that also contains BackLib, a library management for NonStop attached tape libraries.

BackBox and BackLib share the software components running on the NonStop host and the user interface.

This present manual is dedicated to the BackBox version E4.11 .

The BackBox end user documentation consists of the following:

BackBox Upgrade Procedure – Updating NonStop and MS-Windows Platforms.

BackBox User Manual – BackBox Product. Configuring and operating BackBox subsystems.

BackBox Tape Encryption Option – Tape Volumes Encryption Guide

BackBox VTC Scripting Option – Guide for implementing Windows scripts archiving tape volumes to an Enterprise Backup Infrastructure.

BackPak UI Installation – Installation of the UI component of a BackPak domain.

BackPak Catalog Sync Option – Configuration and operation for replicating DSM/TC and BackPak catalogs.

BackPak Messages Manual and Troubleshooting – List of EMS error messages generated by the BackPak products.

BackPak Third Party Components – List of third-party software included in BackPak.

PRODUCT DESCRIPTION

ETI-NET BackBox is a virtual tape solution to connect the NonStop Guardian tape subsystem to external storage facilities.

BackBox related products

- BackBox – provides NonStop virtual tape capability to store virtual volumes in various (enterprise) storage infrastructures.

Data Store is the storage system for virtual volumes.

BackBox currently supports three Data Store types:

1. Windows (compatible) disk file system:

- Any internal disk or SAN LUNs, configured under the Windows file system, or
- Any file server (SMB/CIFS) that is compatible with the Windows operating system. This includes specialized de-duplication appliances such as EMC Data Domain, HPE StoreOnce or Quest QoreStor.

2. Embedded QoreStor storage for data deduplication and replication
3. The IBM Spectrum Protect™ (TSM) Storage infrastructure implemented via the IBM Spectrum Protect™ TSM/API.

BACKBOX COMPONENTS
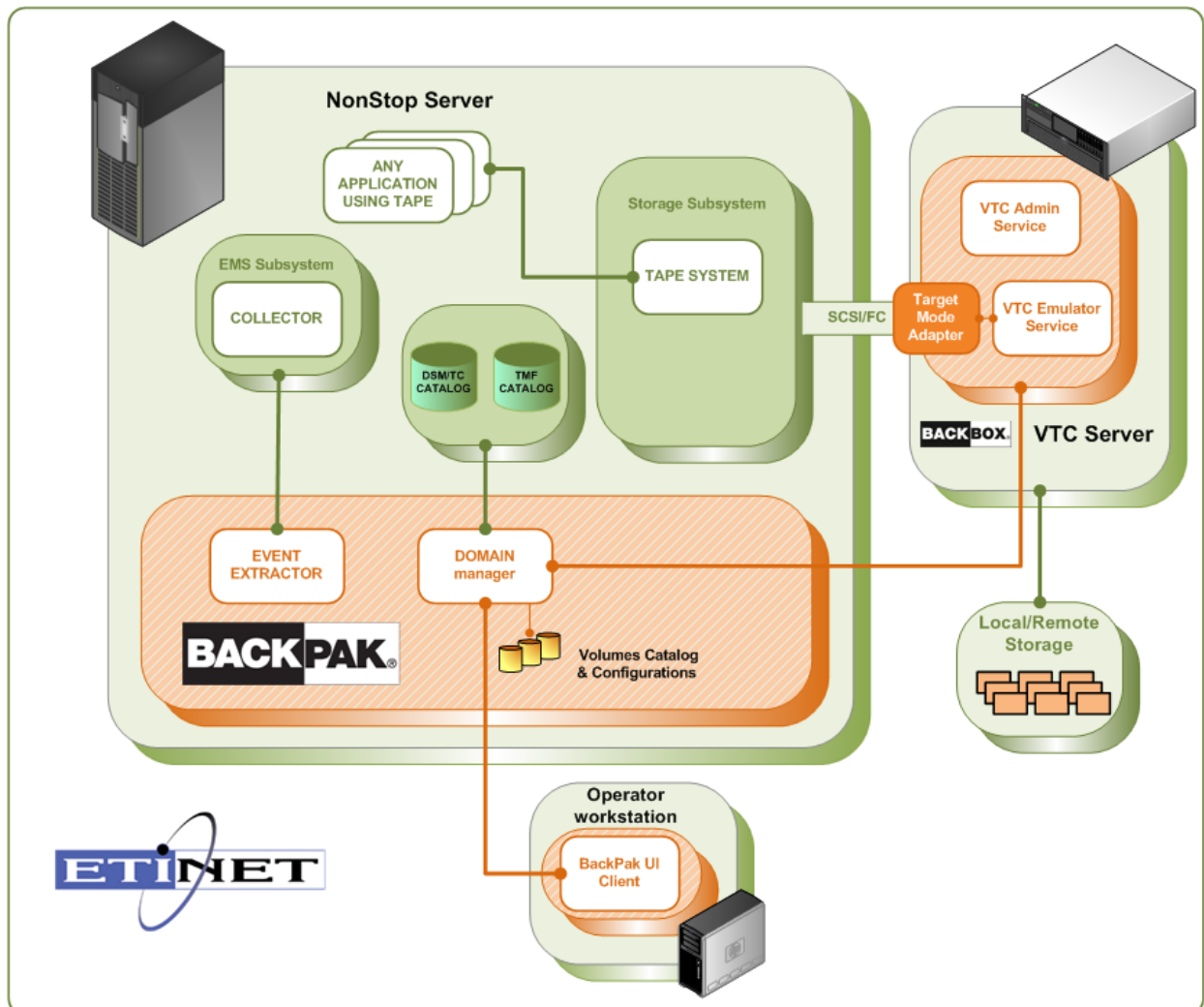
BackBox components:

- Virtual Tape Controller (VTC) unit
- BackPak User Interface Client
- Domain Manager
- Event Extractor

A graphical user interface (UI) to BackBox runs on the operator workstation.

The Domain Manager, Event Extractor and User Interface are BackPak components.

BackBox virtual tapes and BackLib library tapes can be managed in the same BackPak Domain. In a consolidated configuration, BackBox tape drives and BackLib tape drives appear on the same Client User Interface status page and they are operated by the same BackPak processes on the NonStop platform.

Virtual Tape Controller (VTC)

VT Controllers are Windows-based servers connected to a NonStop server via Fiber Channels and via iSCSI for Virtual NonStop. Several VTCs can be connected to the same NonStop system and several NonStop systems can be connected to the same VTC. VTC functions are controlled through TCP/IP.
The VTC is built on a dedicated Windows Server 2012 R2, Windows Server 2016 or Windows Server 2019 server platform. It stores virtual tape images through the Windows file system. Any Windows compatible disk subsystem can be used for storage. The number of possible physical connections per VTC depends on the model.

For more info see Product Requirements section below.

BackPak User Interface Client

The BackPak graphical user interface is a web-based client application that runs on the operator's workstation. The User Interface is used for configuration, virtual volume creation and manual exception operations.
Standard VTC operations are automated. The usual NonStop tape-related utilities and user interfaces are used for daily operations.
The BackPak User Interface Client can be installed in any Windows-based workstation. An instance must also be installed on each VTC. The User Interface Client installed on the VTC can be accessed through Windows Remote Desktop client.

Domain Manager

A BackPak domain is a group of VTCs and Guardian nodes whose virtual tapes are managed in a single environment. In a Domain, a unique label is given to each tape volume. If the virtual tapes of several NonStop nodes are managed by the same Domain Manager, the volume label must be unique across all nodes.
The user logs in to a Domain using the User Interface Client. The user can configure the virtual devices, the virtual volume characteristics and their storage, can create virtual volumes and query the operational status.
The main task of the Domain Manager running on the NonStop platform is to reply to the User Interface requests. It maintains a Domain configuration and a catalog of virtual volumes, including the real data location of each virtual volume. It also manages mount requests for virtual volumes.

Event Extractor

Each Guardian node set with virtual drives runs a BackPak Event Extractor. The Event Extractor essentially automates the mounting of the virtual volumes requested by $ZSVR, by forwarding them to the Domain Manager.
The Event Extractor also assumes secondary roles, such as maintaining the status of tape drives in the NSK OPER file for quicker display in the User Interface.

PRODUCT REQUIREMENTS

VTCs

The VTCs are delivered with the required hardware and software:

Data Rate	Celerity FC HBA type	NonStop connectivity type
8Gbits	FC-8, FC-16	G6 Storage CLIM with optional 8 Gbps HBA
16Gbits	FC-16	G10 Storage CLIM with FC-16

> ⚠️ HPE recommends installing Microsoft patches manually rather than configuring Windows for automatic updates. Automatic updates may impact VTC usage if the update causes services to be restarted or the VTC to be rebooted. If you have two VTCs, the best practice is to choose a time when none of the tape devices connected to an individual VTC are in use, stop those devices, perform the update and then restart the devices. Repeat this procedure for the other VTC at a time when its devices are not in use.

NonStop Host System

Hardware Requirements

- NonStop Integrity, NonStop Blade system, NonStop X system or vNonstop system.
- TCP/IP connection to the VTC unit(s) and to the operator workstation.
- FC connection (FCSA or CLIM) for NS Integrity & NS Blade Series.
- iSCSI connection (FCSA or CLIM) for vNonStop

Software Requirements

- Guardian versions: L15.02, H06.06 or J06.06, or later in each series.
- IPV4 TCP/IP or compatible.
- Support of labeled tapes.

> ⚠️ Expand connectivity between all NSK nodes of the BackPak domain

The Expand security must allow the Domain Manager to start Guardian utilities on the peripheral nodes. For BackPak UI sessions, the account to authorize the access is the one entered to log in to the UI, and the utilities are TACL, SCF, MEDIACOM, MEDIASRV, TMFSERVE and CLIMCMD.

For automatic sessions such as the processing of mount requests, the account to authorize the access is SUPER.SUPER, and the utilities are MEDIACOM, MEDIASRV and TMFSERVE.

This basic security schema can be slightly adjusted. See <u>NonStop Access Authorizations</u>.

Additional Software

Tape catalog: DSM/TC recommended with optimal BackPak integration.

⚠	Partial integration is provided for QTOS.

For DSM/TC replication (Catalog Sync option), an HP license for the SQL run-time is required on the NonStop running the BackBox BBDBM program.
Required product: x5810 TSQLRUN.

Operator Workstation

Hardware Requirements

Microsoft Windows x64 computer system with TCP/IP connection to the NonStop system.
TCP/IP connection for remote VTC server(s).

Software Requirements

Windows 10, Windows Server 2012 R2, Windows server 2016 or Windows server 2019 operating system with latest Service Pack
Microsoft .NET Framework 4.5

Key Manager for Tape Encryption

Tape Encryption requires a Key Manager. Key Manager Servers currently supported are:

- HP Enterprise Security Key Manager (ESKM)
- ESKM through NonStop Volume Level Encryption (VLE)
- Any Key Manager Server compatible with the OASIS Key Management Interoperability Protocol (KMIP) standard

⚠	For KMIP compatible key manager server requirements and licenses, refer to specific KMIP vendor documentation.

Supported products

BackBox supports different storage appliances, including deduplication units, and various storage add-ons:

Supported Storage Software	Version
BackBox Dedupe Software Powered by QoreStor™	4.09, 4.10, 4.11
HPE StoreOnce	3.18.17 or earlier
DDos 7.9.0.0-1011258 and eralier (for BackBox E4.08 or later)	with BoostFS – client 7.9.0.0-1010595 and earlier

BACKBOX FUNCTIONALITIES

Basic BackBox functionalities are:

- Creation of virtual volumes.
- Automatic tape mounts.
- Emulation of a tape drive connected to a NonStop host.
- Access control to virtual volumes and their data.
- Import/export of virtual volumes through a physical tape drive attached to the VTC (virtualization / materialization).
- Encryption of virtual volumes (see *BackBox Tape Encryption Option* manual).
- Replication of catalog entries (BackPak catalog and DSM/TC catalog) to a secondary site (see *BackPak Catalog Sync* option manual).
- Primary storage pool Synchronization with the Copy Pool, available through the Windows Advanced Pool Management (see [Copy Pool Sync] in [Windows Advanced Pool Management] section).

> ⚠️ Some BackBox optional functionalities are controlled by the license key. For example, the use of specific storage types, such as a deduplication appliance, is controlled by the license key.

Virtual Volume Creation

Before using virtual volumes, they must be created through the BackBox user interface.

Volumes are created through the BackPak user interface:

- When a volume is created, it generates an entry in the Guardian tape catalog (DSM/TC or TMF), if the Volume Group is associated with such a catalog.
- The catalog stores the virtual media label to enable the Domain Manager to process the mount request (no separate labeling step is required under Guardian).
- BackBox does not allow the manual deletion of a virtual volume that contains non-expired data.
- For certain configurations, the volume has to be set up as a scratch volume in the chosen Data Store.

> ⚠️ Volumes associated with the NonStop tape catalog (such as DSM/TC) configured for auto-scratch are not created in the Data Store until they contain data.

Tape Drive Emulation

To the NonStop host, a BackBox virtual tape drive appears as a physical drive connected by SCSI or Fiber Channel. The tape drive appears as LTO3 (i.e. using LTO3 or LTO2 media type) by default, unless

otherwise specified in the VTC Management Console.

- 3480 media type can also be supported for Guardian nodes with older tape system (G06.31 or SPR T0021G05^ABW, H06.13 or SPR T0021H01^ABZ).
- LTO4 can be used for HP VLE Encryption with ESKM.
- LTO6 can be used on CLIM base NonStop host supporting LTO6 tape drive. LTO6 cannot be used for VLE Encryption with ESKM.
- BackBox supports all NonStop tape I/O commands that affect the data content on tape and the current position on the media.
- Data is stored and controlled by the BackBox configuration and the Data Store software/hardware, and it is transparent to the Guardian.

Virtual Volume Storage

Virtual volumes can be stored on a variety of storage, such as Windows Data Store, Embedded QoreStore Data Store, or IBM Spectrum Protect™ (TSM) Data Store. See the description of different types of data stores in Windows Data Store and IBM Spectrum Protect (TSM) Data Store.

In all types of Data Stores, the size of the storage space allocated to a virtual volume is equal to the size of data actually written plus a marginal amount of metadata, regardless of the maximum size specified in the Volume Group.

The image of each virtual volume is kept indefinitely in the Data Store until:

- The virtual volume is rewritten by the Guardian tape application,

   or
- The BB017_FREE_EXPIRED batch TACL macro frees the storage of volumes declared expired by DSM/TC and TMF,

   or
- The virtual volume is deleted manually through the Web user interface.

Compression

Software compression is available for Windows file system Data Stores. Two types of compression are available:

- HIGH – better compression, more CPU usage for the VTC.
- LIGHT – Less compression, less CPU usage for the VTC.

When the size of the compressed data reaches the maximum volume size defined in the Volume Group, an EOT (End-Of-Tape) indication is sent to the Guardian tape process.

VTCs add metadata to the User data received from SCSI commands. This metadata is included in the computed storage size, displayed in the web application and used to compute the compression ratio. Consequently, the reported ratio is marginally lower than the ratio computed only on the user data.

Before choosing the final compression setting, it is recommended to determine which is the most appropriate compression type for your data.

To determine if compression is advantageous for your environment, check the following:

- The effective compression for different backup types and different compression algorithms on the Web UI Volume list page.
- The global effective compression per Volume Group in the Volume Summary page.
- The CPU usage in the VTC server using the Windows performance monitoring tools.
  Important: VTC CPU saturation should be avoided.
- The impact on throughput as reported by the BackBox statistical report (OBB018 OBEY file).
- Virtual tape should be compressed only once, either by the VTC or by the enterprise backup software.

⚠️	The compression setting can be changed any time. The change will affect all subsequent volume mounts in that Volume Group.

Important: When sending the virtual volumes to a data de-duplication appliance (such as Data Domain), BackBox VTC compression should be disabled. Failure to do so results in poor de-duplication ratios.

Encryption of Virtual Volumes

Tape volumes can be encrypted by the BackBox VTC software or by the storage subsystem where the media is written by BackBox.

Encryption by BackBox Software

Software encryption is available for Windows File System Data Stores and for all NonStop systems H06.xx and J06.xx.
The data is encrypted using IEEE 1619.1 (tape) industry standard algorithms before it is sent to the Data Store. The encryption algorithm uses a 256-bit encryption key stored in an external Key Management Server.
Encryption by BackBox software can be used with an HP Enterprise Security Key Manager (ESKM) and can optionally be fully integrated with the NonStop Volume Level Encryption (VLE) product. The backups created from Blade systems with LTO4 and VLE can be restored by older systems with LTO3 or CART3480 emulations and vice-versa. When emulating LTO3 or CART3480, the BackBox VTC creates and retrieves the same encryption keys as would a CLIM with VLE.

⚠️**Important:** For storage subsystems that implement data deduplication, BackBox data encryption **MUST NOT BE USED**. Encryption or compression prevents deduplication algorithms from matching

recurring data blocks, making deduplication ineffective. For these subsystems, the encryption should be performed by the storage subsystems themselves.

Further detail about BackBox Encryption can be found in the Compression / Encryption section.

Encryption by the Storage Subsystem

Encryption provided by the storage or operating system itself is not described in this manual.
For example, EMC offers optional capabilities for "data at rest" and "data in motion" encryption on their Data Domain products, HPE StoreOnce or Quest QoreStor.
IBM Spectrum Protect™ (TSM) API Data Stores and WINDISK Data Stores backed-up to a IBM Spectrum Protect™ (TSM) server offers various encryption functionalities, as do other similar enterprise backup products.

LARGEBLOCKS Support

From L17.08 onwards, both BackBox and Virtualized BackBox support BLOCKSIZE of 224, 448, 672, and 896. To use this option, the LARGEBLOCKS attribute must be ON for the tape device in SCF (for more information, see *SCF Reference Manual for the Storage Subsystem* on the HPE support website.

By default, on the VTC, LARGEBLOCKS mode is set to ON and it works whether the device on the NonStop is enabled for it or not. To turn this feature OFF see VTC Management Console section of this manual.

WINDOWS FILES DATA STORE

Under Windows Files Data Store, the virtual volume is implemented as a package of two Windows disk files:

- An .IND file - a small index file containing metadata (filename.IND).
- A .DAT file - a variable length data file, whose size is based on the current content of the volume (filename.DAT).

A Windows File Data Store is defined as a pool of disk paths following the UNC syntax (\\server-\path\directory\). Although drive letters (d:\directory) are supported for single VTC, it is strongly recommended to use UNC for all Data Stores.

If the disk units are presented as a single logical disk, the emulator manages to provide:

- Space balancing across disks.
- Load balancing across disks.
- On the fly scratch volume creation (Data Store fault tolerance).

While writing and reading these Windows disk files:

- The VTC reserves the configured maximum volume size plus a margin of 10 MB when loading a volume in write mode. Unused space is freed at volume unload.

⚠	Compression affects the file size but not the amount of NonStop data contained in the volume.

- Virtual volume may be moved from one disk to another in order to balance the space utilization or the work load when the Data Store is configured across a pool of disks.

A file can be moved when:

- A SCRATCH volume loaded for output with auto-scratch on, is deleted and recreated at the optimal location.
- A restore script is executed and the virtual tape is restored in the optimal location.

By using a parameter in the Data Store configuration, and independent of any other consideration, the user can change the load balancing algorithm to force use of the local disk.

Creation of Virtual Volumes

The virtual volumes in each set are spread evenly across the data paths on disks, creating sufficient free space for at least one volume on each data path. For a Volume Group configured as AUTOSCRATCH and

associated with a NonStop tape catalog such as DSM/TC or TMF, no files are created by default.

However, when creating virtual volumes, both disk pool configuration and security settings are checked. Volumes are registered in BackPak and in DSM/TC or TMF.

Free Space on Remote Paths

When the size of the free space on a disk cannot be known, the VTC always considers that there is enough space for the current volume.

File Access Security

The files holding the virtual volumes are protected by Windows security. The Windows credentials entered in the Data Store configuration are used also for file creation and system access.

The account must successfully log in to all VTCs that are routes for the Data Store. The same account must have full access to all paths specified in Data Store configuration.

The account can be a workgroup account. In this case, the account must be defined with the same password in all file servers providing a share to the Data Store.

The account may also be defined in Windows Active Directory and can be a non-interactive account.

For **Work Group** - in case of user password change, user must log on in each VTC server to manually update with the respective account password.

For **Active Directory** - in case of system password change, it's not necessary to update the account password on each VTC server.

However, for each Data Store a specific user has access to, the new password has to be re-entered via BackBox UI. The same password update can be performed from the Nonstop using BB004 macro script.

Scripting/Background Migration on Tapes

For convenience and performance purposes, BackBox is most often configured to write the tape image files to disk. Once the configuration is done, BackBox copies or moves (migrates) the image to a physical tape or to other storage for long-term retention.

To migrate virtual tapes, either install a general HSM client in Windows or use the BackBox scripting facility to trigger a backup by an enterprise backup client (such as Networker, NetBackup or IBM Spectrum Protect™ TSM).

- HSM solutions are transparent to BackBox.
- Script files are user written command files to call the enterprise backup client in order to save or restore a given virtual tape image.

The user can also:

Schedule regular backups by the enterprise backup client.

Configure BackBox to trigger scripts when:

- A virtual volume needs to be copied or moved as soon as it is unloaded from the tape drive. Unavailable when the Copy Pool Sync option is activated.
- A virtual volume must be loaded in read mode and must be restored by the enterprise backup client.

Scripting Facilities

Scripts are configured in the **Data Store Advanced** configuration page. Script parameters can also be defined and their values set on the same page.

There are two script types: Implicit (IBM Spectrum Protect™ TSM and Manual Restore) and explicit (Generic). For implicit script, the user cannot specify a script name, as they are already predefined.

If IBM Spectrum Protect™ (TSM) or Generic type scripts are selected, the backup method must be specified (BackBox script or other methods – triggered by an enterprise backup software). IBM Spectrum Protect™ (TSM) and Generic type scripts can also be submitted via the Script Controller.

Without the Script Controller, scripts are executed for each virtual volume.

> ⚠ With the Script Controller, the scripts named in the Data Store advanced configuration, forward the backup or restore request to the VTC Script Controller. The Script Controller manages queues of backups or restores requests and submits actual backup or restore scripts that can process several virtual volumes at the same time.

The Script Controller is a batch sub-system and is used for:

- *Retries:* When the user wants another layer of error recovery on top of the one implemented by the enterprise backup client. By default, the Script Controller will retry for 24 hours, with a delay of 5 minutes before each retry.

- *Serialization:* A VTC typically implements several virtual tape drives and might trigger several concurrent scripts. The number of concurrent script executions might be limited by the enterprise backup software, or just because the enterprise backup client writes directly to a physical tape library. The Script Controller queues the backup or restore requests, consolidates similar requests, and submits them in a number of queues and threads per queue, as set by the user.

For detailed information on scripting in the BackBox, refer to the *BackBox VTC Scripting Option* manual.

Disk Space Management Tools

The UI Storage Admin page shows a summary of the Windows Data Store disks.

The user can either:

- Resubmit the backup script for all Windows files that have not been backed up or,
- Manually start the synchronization of the storage and copy pool, if the Copy Pool Sync option is activated.

BackBox provides TACL macros that can be scheduled in NetBatch to:

- Delete files corresponding to volumes expired in TMF or DSM/TC catalogs. If a delete script is configured, it will be executed to also delete the backup of the expired file. (BB017_FREE_EXPIRED).

- Delete backed-up files after a certain number of days have elapsed since their backup. This allows the immediate retrieval of recent backups and the freeing of disk space associated with old backups (BB023_DEL_BACKEDUP).

- Delete restored files after a certain number of days have elapsed following their restore. This allows several executions of the NonStop RESTORE program after a single execution of the restore script (BB023_DEL_BACKEDUP).

- Check the available free space against a warning threshold set in the Data Store configuration and the maximum volume size configured in Volume Groups (BB022_CHECK_SPACE).

Windows Disk Path Reservation

For Windows Data Stores, in certain cases, different kinds of virtual volumes need to be set apart on different disks. For example, when only part of the available Windows disks is mirrored and should be assigned to the TMF AUDIT dumps or to the backups of a specific DSMTC pool.

The disk path reservation allows for specifying that certain disk paths will be used exclusively for a specific Volume class.

Volumes in a volume class with reserved paths will use only these paths.

The configuration of disk path reservation can be set through the Data Store configuration page in the UI.

Windows Advanced Pool Management

With this option, a user can define **Spare pool** and **Copy pool** in addition to **Storage pool**.

The **Spare pool** is an emergency disk pool. This is the location the VTC will use only if all the Storage pools (all disk paths) are unavailable or full. In this case:

- The new backups will be written to the Spare pool. They are available only for Volume Groups defined as Auto Scratch.

- If an enterprise backup restore needs to be done through a script to satisfy a mount from the NonStop, the **Spare pool** will be used as an alternative staging area.

The content of a **Spare pool** is not automatically moved back to the **Storage pool** when it becomes available. However, it can be initiated manually through the UI in the **Storage Admin** page> **Data Store** name >**Move Files from Spare pool**.

The **Copy pool** is a path to a copy of the **Storage pool**, in case the **Storage pool** is not available for Restore. In general, it uses a path to a replicated copy on a remote site. The VTC will search in the **Copy**

pool only when a NonStop restore is executed and the virtual volume is not found in the regular **Storage pool**.

Copy Pool Sync

When the **Windows Advanced Pool Management** is available, it allows volume copying from the primary storage pool to the copy pool of the same Data Store by the CopySync program. Copying is done via the regular backup script and it is automatically submitted after a backup or on demand through the UI (for a single volume or the entire Data Store). The script execution is reported in EMS as a regular backup script, although it is not configured as a script.

When activated, this option is incompatible with the backup script of an Enterprise Backup taking additional copies. However, an Enterprise Backup Server that pulls files from the storage pool is compatible.

The CopySync program chooses an available remote path (copies are only done on remote paths) in the Copy Pool. If the only available path is local, the copy will not be executed. Please take note that:

- Any pre-existing instance in the Copy Pool is deleted.
- The source volume is opened with write protect, but allows concurrent readings.
- The volume is not declared "IN USE" in the domain, but it is available to a load on the NonStop restores.
- After a successful copy, the target file modification time is set equal to the source file copying time.

If the **Windows Advanced Pool Management** option is not selected, the Copy Pool Sync option is not available. The storage pool replication does not depend on the product and it is provided with the customer installation.

⚠	The copy pool sync scenarios work only without ENCRYPTION.
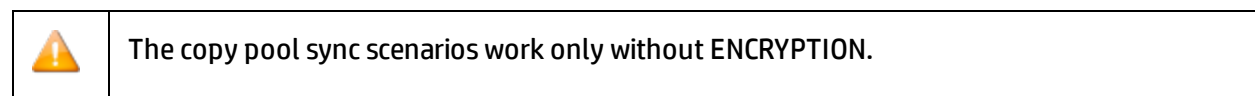
Use the following example for Copy Pool Sync set up:

Before setting up the Copy Pool Sync, choose the paths that you want to store the files into:

\\ASTERIX\DATASTOREQC\ on the **local** storage pool

\\OBELIX\COPY_QC\ on a different VTC Copy Pool

1. To set up the **Storage Pool**:
    a. Log in as user with Configuration Editable permissions, go to **Configuration** > **Data Store** > click on the **Data Store ID** where your storage pool has been created and click**Switch to Edit Mode.**

b. Scroll down to **Windows Pool** section and select **Storage Pool**. In the **Path*** field put the name of the path that you defined for the local storage pool (e.g. \\ASTERIX\DATASTOREQC\).

c. Scroll down to **Storage Route** section and add one storage route for the local machine (e.g. ASTERIX) and one storage route for the remote machine (e.g. OBELIX).

2. To set up the **Copy Pool**:
   a. In the **Windows Pool** section, click on **Copy Pool** and in the **Path*** field put the name of the path that you defined for the copy pool (e.g. \\OBELIX\COPY_QC\).

   b. Scroll down to **Storage Route** section and add one storage route for the local machine (e.g. ASTERIX) and one storage route for the remote machine (e.g. OBELIX).

3. To set up the **Advanced** options:
   a. Go to **Advanced** option of the data store and select **Copy Pool Sync Without Script Controller** option for the **Copy Pool Sync** feature, then click **Update**.

Data Store ID	Store Type	Status	Domain Access	Description		
DATASTORE-QC	WINDISK	Active	PRIMARY		Catalog Sync Export	Advanced

Advanced

Restore On Same VTC ☐

Disk Block Size (KBytes) 128 ▾

Copy Pool Sync Copy Pool Sync Without Script Controller ▾

Force Local Path ☑

[Update]

Enterprise Backup Software Scripting

Script Type No scripts ▾

[Update Script Information]

Script Parameters   [Add]

		Name	Value
Edit	Delete	BBOX_COPY_IOPACING	0
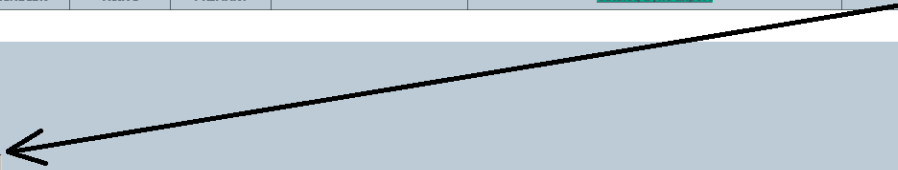
b. **Save** the configuration

⚠	Make sure to set the shared file(s) permissions according to your data storage type.

QORESTOR

BackBox with Windows file Data Store can use different kinds of NAS Storage with deduplication engine (such as, ETI-NET certified EMC Data Domain, HPE StoreOnce , Quantum, Cohesity).

With BackBox 4.09 and above, the Quest QoreStor server can now be used as a NAS Storage featuring deduplication.

BackBox provides for QoreStor I/O optimization with Quest Rapid CIFS source deduplication Client.

In most cases, a dedicated NAS storage is shared by a pair of VTC connected by FC or iSCSI to a NonStop host (see the diagram below).
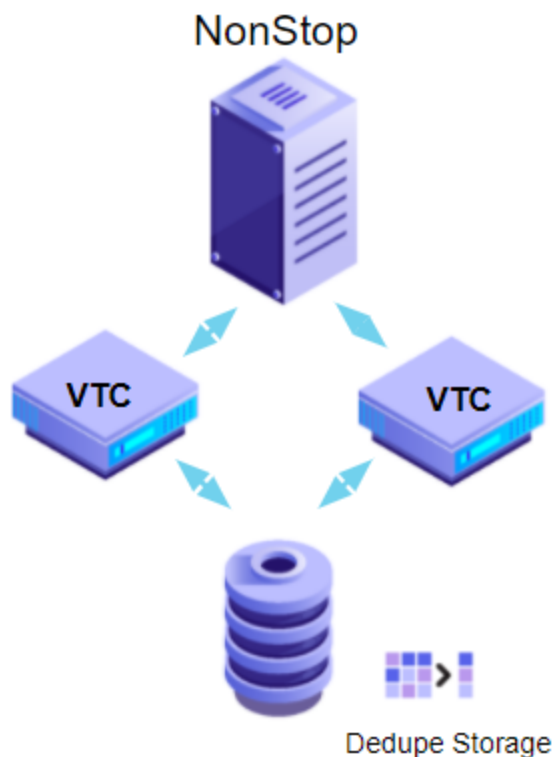
QoreStor Embedded DataStore

What makes QoreStor solution even more efficient is the possibility to run QoreStor on the VTC hardware as an isolated virtual machine. This solution reduces complexity and hardware footprint.

When a pair of VTC is used (see the diagram below), one of the VTCs can be used to run the QoreStor VM, which will act as a regular NAS for both VTCs.

NonStop

VTC

VTC

VM

Non
Dedupe
Storage

Dedupe Storage
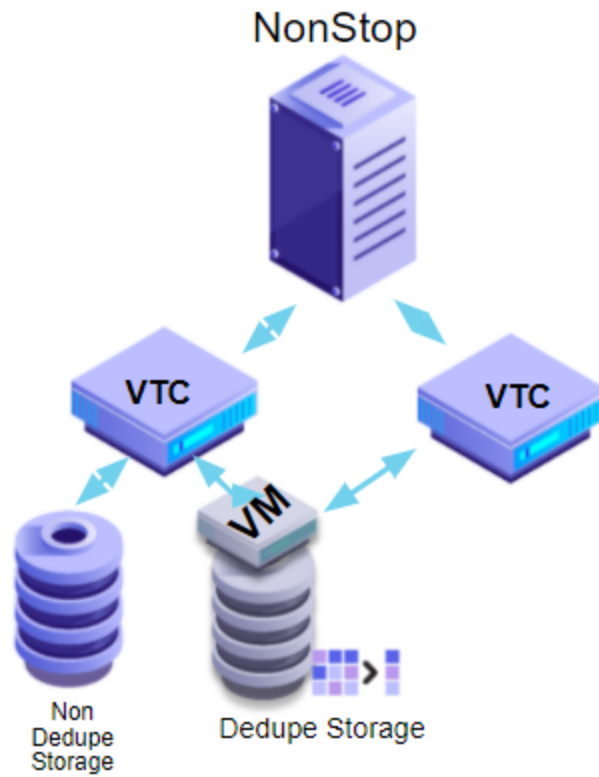
To scale out the above-mentioned solution, use an embedded QoreStor on each VTC (see the diagram below) to create a datastore distributed across all VTCs in order to increase storage and throughput.
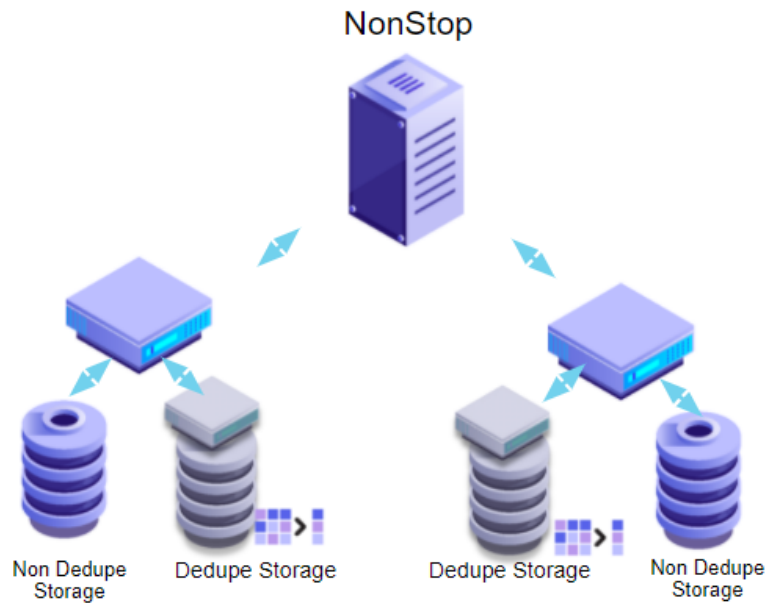
QoreStor overview

Each embedded QoroStor can replicate data to a single QoreStor target (for data to be replicated). A QoreStor target can be:

- an embedded QoreStor
- a corporate QoreStor.

A QoreStor can be used as replication target by multiple sources.

Each QoreStor can expand its storage capacity by 4x using Cloud Tier Storage.

Policies define :

- if data can use Cloud Storage or not
- how long data is stored on premise only, in the Cloud only, or on both
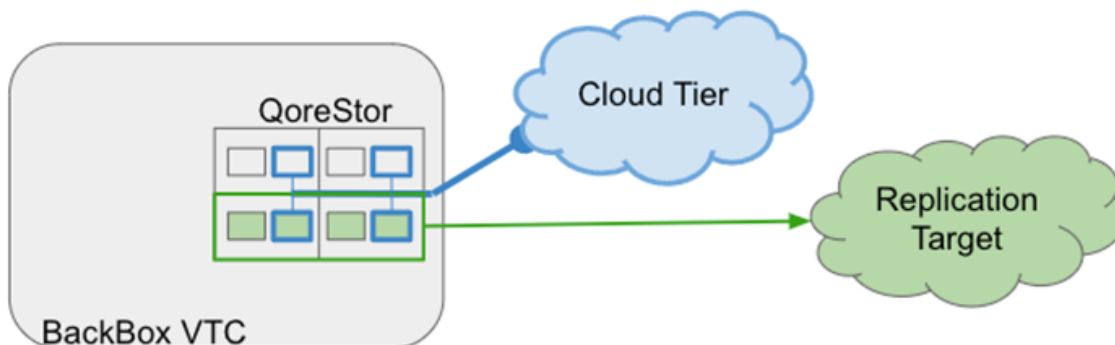
Datastore managed by Policies

When creating a QoreStor Data Store, different levels of configuration have to be set up (with or without encryption, with or without cloud tiering) in order to establish which QoreStor pre-configured container will be used.

To use Cloud **storage expansion**, open VTC Management Console to choose the storage Cloud service: AWS S3 or Microsoft AZURE.

Set up the following:

- **connection string**
- **idle time**
- **retention criteria** (on-premises) to identify which files are most suited for replication to the cloud (how long the files are retained locally, when they are migrated to the cloud and when they are stored on the cloud only).

⚠️ You can define a QoreStor Data Store with cloud policies, even if the cloud storage settings haven't been initially configured. That specific Data Store will be available for cloud tiering anytime afterwards.

If you enable cloud policies, the Data Store will use WORM (Write Once and Read Many) media type, as any file in the Cloud Tier containers will be read only. Therefore, NonStop tape pool should always be used with **append off** if the files are to be used in a Cloud Tier container.

WORM characteristics are available even before the cloud setup.

Policies vs QS containers
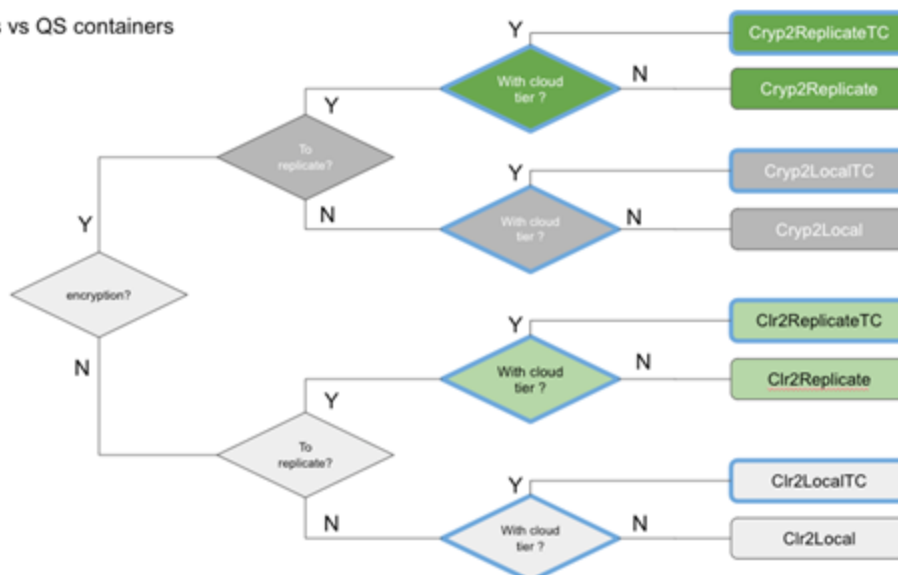
Collocation by volume group

A Windows Data Store uses a set of storage paths: **copy pool path** and **spare pool path** to store virtual volumes. Even if those volumes are organized in volume groups (which correspond to NonStop tape pool), they are indiscriminately stored in same storage folders. In the new DataStore type, volumes from a volume group XYZ are stored in a sub-folder XYZ.

This feature helps identifying tapes below a volume group and setting selective backup policies.

QoreStor containers and advanced pool management

When more than one VTC with embedded Storage is used, in addition to storage replication (used to create off-site copies) a local second copy can be created by BackBox copy pool sync. That local second copy improves the restore time when the original VTC/QoreStor becomes unavailable, in case a restore is needed.

> ⚠️ QoreStor fast replication speeds up the write replication, but it doesn't speed up the read from replication storage.

The Copy Pool storage contains 2 copies that the VTC will use in the most efficient way to restore.
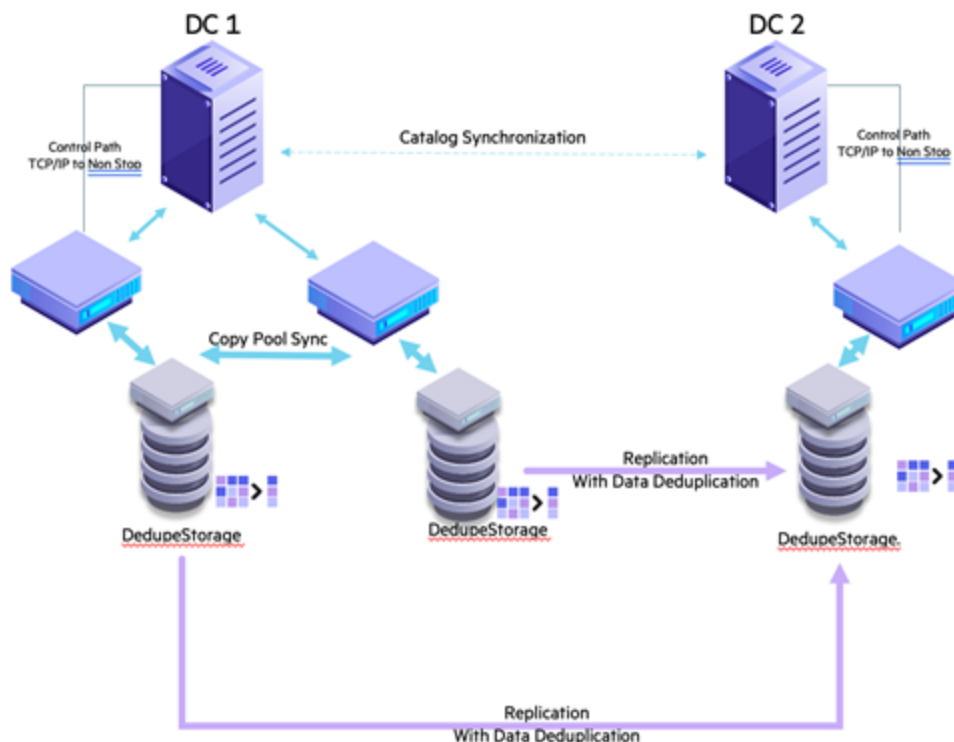
Interfaces used with QoreStor

VTCMC

For Embedded QoreStor licensed systems, the QoreStore can be configured via VTCMC interface.

For VTCs with Embedded QoreStor, the following settings can be configured through VTCMC:

- Define **QS Hostname**
- Set **IP config** of Embedded QoreStor corporate NIC and fast NIC (the internal NIC is pre-configured and shouldn't be modified by the user)
- **Join/Leave** Active Directory Domain
- Define **QS target replication**
- Get **replication Status**
- Generate and download **diagnostic package**
- Update **Licenses**
- Update **Users**
- Access **Event Forwarder**

QoreStor UI

QoreStor offers a web-based user interface to **monitor** your QoreStor system.

> ⚠️ Because the Embedded QoreStor is managed by VTC, a monitor user can access only **Configuration Information** and **Status** panels.

To access QoreStor UI from any supported browser:

1. Navigate to **https://<hostname:5233>**

> ⚠️ Use either the host IP or hostname.

2. Log in with the default credentials: username: **monitor**/password: **BackBoxQS**

Support

QoreStor UI Overview

The QoreStor UI consists of different sections structured as follows:

- Header pane
- Navigation pane
- Status pane
- Operations pane

Header pane gives access to the following features:

- *QoreStor Alerts* – list of Alerts on the QoreStor system.
- *Current User* – displays *current user account* details, *log out* option, and switch the UI to the *Light theme*.

Status pane with access to the following items:

- *Version* – displays the version of QoreStor
- *System Status* – displays the status of the QoreStor

Navigation pane with navigation options for the following action items:

- *Dashboard*
- *Containers*
- *Local Storage*
- *Cloud Storage*
- *Replications*
- *System*
- *Diagnostics*

- *Users*
- *Events*
- *Management*

Operations pane that displays data and various appropriate dialogs related to the chosen navigation option.

Supported software browser versions:

- **Mozilla Firefox** 67 or later
- **Microsoft Internet Explorer** 11.01
- **Microsoft Edge** 44 or later
- **Google Chrome** 75 or later

Port configuration

Component/Function	Required Ports
UI/Cloud Tier	- 80 - 5233
Replication	- 9904 - 9915 - 9916
CIFS	- 139 - 445
Secure Connect2	- 9443

BackBox Storage Administration

QoreStor can be monitored as Windows File Data Store on the BackBox **Storage Administration** page.

QoreStor message forwarding

Messages from the embedded QoreStor are read by VTC and forwarded to NonStop EMS log.

Examples:

```
20- 12- 21  20:57:35  \ETINIUM.$Y463  ETINET.100.100  030000
SHE409-BBOX2019-3-I30000 290-QoreStor Repository Cleaner pro-
cess stopped as per schedule,

20- 12- 21  20:57:35  \ETINIUM.$Y465  ETINET.100.100  030000
QCH409-BBOX2019-3-I30000 290-QoreStor Repository Cleaner pro-
cess stopped as per schedule,

20- 12- 21  20:57:35  \ETINIUM.$Y45X  *ETINET.100.100  010208
SHE409-BBOX2019-3-W10208 VTC license has expired on 2020-12-
16
```

QoreStor Updates

With software version 4.09 and later the component license may replace BackBox site license. The component license gives a more granular control over the expiration date and simplifies component license management (in case of new component licenses or component license renewals).

Component license management is not mandatory for version 4.09 or later, except when using QoreStor embedded features or for Windows 2019 OS (or later).

When a component license is used for one component, that component license needs to be used on all VTCs and all Hosts.

Customized bundles of component and site licenses are not supported.

- It is not possible to upgrade only VTC or only the NonStop when running a BackBox upgrade to 4.09 or later.

To run QoreStor updates, go to [VTC Management Console](#) and run the updates (if any available): **Embedded QoreStor** > **System** > **Update**.

Replication

Data replication creates multiple copies of data and stores them at different locations to improve their overall accessibility across a network. In general, data replication applies to both servers and computers. The data replicates can be stored within the same system, on-site and off-site hosts, and cloud-based hosts.

Although data replication is a complex process (requiring extra-storage, compliance policies, etc.) there are considerable advantages of using it:

- Improve data availability
- Increase data access speed
- Enhance general performance
- Cover a wide range of disaster recovery scenarios

To use data replication with Embedded QoreStor, go to VTC Management Console ([Replication](#)) and perform the required steps under the node **Replication**.

Cloud Tiering

QoreStor's cloud tier feature enables QoreStor storage to be expanded to the cloud tier for better dedupe management. Using your existing BackBox and CIFS protocol, files can be written to a QoreStor container and transparently replicated to your cloud tier according to easily defined policies.

QoreStor provides a policy engine that allows you to set idle time and on-premises retention criteria to be used in identifying when files are replicated to the cloud. Policies are defined at the container level and are applied to all files within that container. Using the QoreStor Cloud Policy, you can replicate files based on:

- Idle time - replicate stable files idle for more than the selected number of hours.

- On-Premise Retention Age policy - allows you to specify how long a file copy is kept on the QoreStor local storage after having been replicated to the cloud.

Once the retention age passes, the file on the QoreStor server becomes a stub, meaning that the file resides in the namespace, but the data resides only in the cloud. Files are always read-only in the cloud tier folder (WORM).

⚠	If you are using QoreStor DataStore, the WORM will make the Cloud Tier data store contents read-only before setting it up for cloud tiering.

To set up and configure Cloud Tiering, go to VTC Management Console (VTC Management Console) and follow the steps to enable the option and set it up.

⚠	Make sure you have a cloud service provider (such as Microsoft Azure or Amazon S3) and access to all relevant information.

IBM SPECTRUM PROTECT™ (TIVOLI STORAGE MANAGER) DATA STORE

In a IBM Spectrum Protect™ (Tivoli Storage Manager) server, a virtual volume is made of a series of IBM Spectrum Protect™ (TSM) objects of a certain size.
When the BackBox is set up as a storage appliance, its server can be a IBM Spectrum Protect™ (TSM) client and/or a host dedicated IBM Spectrum Protect™ (TSM) server.

IBM Spectrum Protect™ (Tivoli Storage Manager) Software

The IBM Spectrum Protect™ (TSM) Windows client API runtime module is required by all VTCs accessing IBM Spectrum Protect™ (TSM).

This software must be bought from an authorized distributor and installed according to user requirements.

IBM Spectrum Protect™ (TSM) Features

BackBox is a IBM Spectrum Protect™ (TSM) API client and all IBM Spectrum Protect™ (TSM) functionalities offered to API clients are available.

- Rule-based storage management, with automatic migration and duplication.
- Support of several server platforms.
- A choice of connectivity between the BackBox and the IBM Spectrum Protect™ (TSM) server, including LAN-free connections.
- A wide choice of storage media, drives and libraries.

Please refer to the IBM Spectrum Protect™ (Tivoli) documentation for more information about IBM Spectrum Protect™ (TSM).

IBM Spectrum Protect™ (TSM) Activity Log

Each time a new session is activated from the VTC to the IBM Spectrum Protect™ (TMS) Server a message will be issued to the TSM Activity Log. This message states the virtual tape labels for which the session was started.

```
4/27/2016 11:17:25 ANE4991I (Session: 1639, Node: QCMONT)

ANE4991 BackBox: Starting session for the virtual volume PBCT04 in WRITE
mode. (SESSION: 1639)
```

Integrity Check when a Volume is Written

When a recently re-written volume is unloaded, the IBM Spectrum Protect™ (TSM) data base is queried to verify the list of IBM Spectrum Protect™ (TSM) objects containing the virtual volume.

If an anomaly is detected, message **#6005** or **#6006** is issued to the EMS. The backup should be re-executed and ETI-NET support contacted.

⚠	• The backup or TMF dump finishes without any error.
	• The number of IBM Spectrum Protect™ (TSM) objects can be seen in the Volume detail web page.

ADDITIONAL FUNCTIONALITIES

Auto-Scratch Mechanism

When auto-scratch is enabled in the **Volume Group** configuration, the VT Controller does not access the image of a virtual volume that is mounted for output, but it recreates the image of that volume.

This mechanism makes it possible to:

- Avoid restoring the archived image of the expired virtual volume
- Instantly move the Windows files from an unavailable path (disconnected or full) to an available path, or to the most efficient path.

> ⚠️ The volume content is deleted by this operation before any tape data is read by the NonStop. When Auto-scratch is not enabled, the last image of the tape volume is presented to the NonStop host.

Auto-scratch is incompatible with POOL set to APPEND ON.

The auto-scratch mechanism is active for automatic mounts and for manual loads initiated through the **Pending Mounts** section of the User Interface.

When processing these mount requests, the Domain Manager knows the characteristics of the Guardian DEFINE CLASS TAPECATALOG that initiated the mount request and can determine if the volume is scratch or not. For a DEFINE CLASS TAPE, the scratch status is determined by the tape header expiry date saved in the BackPak catalog.

The auto-scratch mechanism is never active for manual loads initiated through the UI **Volume Detail** page. Manual loads should be executed in the **Status Node** page.

The conditions to determine a volume scratch status depend on the type of label and catalog processing settings:

TMF tapes

The media must be SCRATCH in the TMF catalog.

The label processing must be enabled.

The define attribute USE must be OUT.

DSM/TC cataloged tapes

The tape define must be TAPECATALOG class.

The tape volume must be SCRATCH in the DSM/TC catalog.

The label processing must be enabled.

The define attribute USE must be OUT.

The tape volume must be recognized and known by DSM/TC.

The status of the tape volume must be PENDING or SCRATCH.

No tape file is cataloged on the required tape volume.

The DSM/TC pool associated with the tape mount must be set to APPEND OFF.

CA cataloged tapes

The tape define must be TAPECATALOG class.

The label processing must be enabled.

The define attribute USE must be OUT.

QTOS cataloged tapes

There must be a tape define of TAPE class

The label processing must be enabled.

The define attribute USE must be OUT.

Un-cataloged tapes

There must be a tape define of class TAPE

The label processing must be enabled.

The define attribute USE must be OUT.

The expiry date in the 1st file tape header (HDR1) recorded in the BackPak catalog must have been reached.

Delete Expired Volumes

To be able to free expired volume occupied storage, the Delete Expired Volumes in the Volume Group configuration must be checked.

The cleanup is triggered by the TACL macro BB017_FREE_EXPIRED in the daily batch OBB017.

The automatic cleanup is available only for DSM/TC, TMF and QTOS catalogs.

If a Delete script is configured for the Data Store, it is submitted to have the enterprise backup solution free its own storage.

Virtual Volumes Access Control

Access to virtual volumes can be secured at the volume level.

The VT Controller access control is similar to the basic security of the Guardian file-system. It works better when the Volume Group is set as auto-scratch, because the ownership of a volume is reset each time the volume is rewritten for a new backup.

Security attributes are stored in the BackPak catalog for each virtual volume:

The Guardian owner (Guardian node and Guardian user ID)

Three access authorizations: Read, Write and Control.

Read: to read the volume data

Write: to read, write and delete the volume data

Control: to change the volume security through the Web interface.

The security attributes are checked against the user at each volume operation; unless it is a load of a volume known as SCRATCH by DSM/TC or TMF and the auto-scratch is enabled.

Security attributes are reset each time the volume is loaded for output:

- The Guardian user becomes the owner.
- The access authorizations are initialized by the default values configured for the Volume Group, then overridden if the Guardian TAPE/TAPECATALOG DEFINE contains the special keyword BBOX-SECURE=rwc (Read, Write and Control authorizations).

User/Owner Identity

- To get the user identity, the Domain Manager queries the mount request detail from MEDIASRV.
- For operations initiated through the UI, the Guardian login information (Domain Manager node and user ID) is used.

Authorization Specification

Each of the three authorizations, Read, Write and Control, specifies how the user accessing the volume should be compared to the volume owner. Access can be:

N Any node, any user-id

C Any node, same group number

U Any node, same user-id

A Same node, any user-id

G Same node, same group number

O Same node, same user-id

? Use authorizations that were set at backup time

. Disabled access

'**?**' is a special value that cannot be entered, but is displayed by the BackPak UI for volumes that were created in a RESTRICTED Data Store.

For such volumes, the domain does not hold the RW authorizations; the access control is done by the VTC against the authorization specifications that were set at backup time and copied as metadata in the Data Store.

'**.**' is another special value that cannot be entered or removed. This is the value displayed for WRITE access when a volume is in a RESTRICTED or SECONDARY Data Store. Such volumes can never be written for a new backup.

bbox -Secure Specification

"**bbox-secure=rwc**" can be added to the MOUNTMSG DEFINE attribute. The keyword and authorizations are not case sensitive.

Example of specification through a TAPE DEFINE:

```
RESET DEFINE *

DELETE DEFINE =TAPE1

SET DEFINE CLASS TAPECATALOG

SET DEFINE FILEID FULL-BACKUP

SET DEFINE POOL BBOX_BACKUP

SET DEFINE LABELS BACKUP

SET DEFINE MOUNTMSG "Full backup bbox-secure=GGO"

SET DEFINE USE OUT

ADD DEFINE =TAPE1
```

Un-Cataloged Volumes

Restricting the access to un-cataloged volumes is conditional.

There is no volume status in Guardian that allows recognizing a SCRATCH volume before accessing it. This way, the authorization check cannot be bypassed.

Updating the Security Attributes of a Volume

The Security attributes of a volume can be changed through the UI: **Volume** > **Volume Details** > **Edit**. To change the volume ownership or access authorizations, the user must have CONTROL access to the volume or be SUPER.SUPER on the node running the Domain Manager. In addition, the volume must be created in a PRIMARY Data Store.

Device Reservation

Some tape devices can be reserved for specific usage: for example, if six devices are defined for a NonStop node, one of these drives can be reserved for TMF AUDIT DUMP activity.

Tape devices are reserved for volume class(es) that are defined in the Volume Group configuration.

Reservations can also be modified by the TACL macro BB020_RESERVE that allows automatic reservation changes in scheduled batch.

The default is set for a device to mount volume(s) of any class.

Reserved drives are preferred, in general, for volume(s) of a specified class.

Pre-load

When a multi-volume backup set has been moved from a Windows disk Data Store to an enterprise backup server, a RESTORE operation may last for a long period because of the time needed for each volume switch to execute the restore script.

Pre-load applies only to the restore of multi-volume backup sets. It anticipates the next volume load by executing its restore script, while the previous volume is being read by the NonStop.

To use pre-load with multi-volume backup set:

- Be sure there are two virtual devices available for each NonStop restore tape process.
- Enable Pre-load in the Volume Group configuration.

BackBox detects and registers multi-volumes backup sets (BACKUP, BRCOM or TMF dumps).

When a load for input is executed and the volume is part of a multi-volume set:

1. The restore script for the first volume is run.
2. As soon as the first volume has been mounted and is in use by the tape application, the restore script for the second volume is started.
3. When the restore script ends, the volume is loaded and recognized by the NonStop tape system as an "Unrequested load".
4. When the tape application requests the next volume, it is already mounted.

⚠	When the next volume has less than 1MB of data, the pre-load is not executed.

Restricted Data Stores

A Restricted Data Store is a view of a Data Store owned by another domain. Restricted Data Store provides read access to virtual volumes owned by another BackPak Domain, most often running on different NSK nodes.

Restricted Data Stores are also a way to manually repopulate the BackPak catalog when the catalog has been lost, and:

- No backup is available to restore VOLUME*
- No DSM/TC or TMF Catalog can be used as a source of re-registration in the BackPak domain (Import from tape catalogue)
- Actual volume images are still available in the Data Stores

The Data Store is created RESTRICTED to manually register the volumes in the domain. Once volumes are registered, the Domain access of the Data Store is changed to PRIMARY to allow backup and restore.

Restricted Data Store
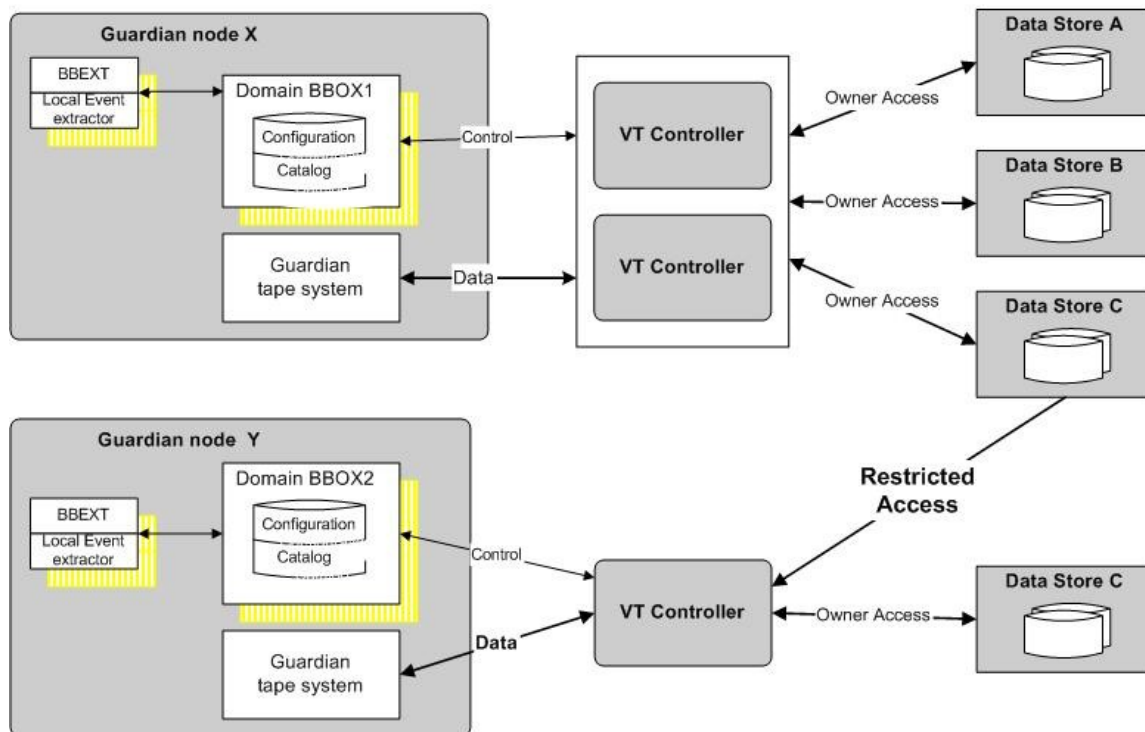
To Set-up a Restricted Data Store in a Domain:

In the Domain configuration, a Data Store is defined with RESTRICTED domain access. The Data Store ID and Volume Group IDs are ideally the same as in the original domain. If different, the original ids must be specified in Primary Data Store ID and Primary Volume Group ID. These primary IDs become visible in the configuration pages only when the Data Store access is set to RESTRICTED.

The volume images in the Data Store must have been created with these same primary Data Store IDs and Volume Group IDs.

Once this is completed:

The Volumes Creation page is used to register the volumes in the domain catalog. The volumes creation in a RESTRICTED Data Store only registers the volume labels in the domain catalog. The image of volumes in Data Stores and TMF/DSMTC catalogs are not accessed.

The deletion of volumes removes only the volume entries from the domain catalog.

Tape application running on the nodes of the alternate domain can access the restricted volumes in Read only (SET DEFINE USE IN) mode.

For WINDISK Data Stores:

- Only Restore and Post restore scripts are available.
- The volume timestamp check is not available.

The access control to volume data is different from a PRIMARY Data Store:

In PRIMARY Data Stores, access to a volume is controlled by the security settings (volume owner and access authorizations) stored in the domain catalog.

In RESTRICTED Data Stores, Read is the only access option. The Read access is controlled by the security settings (owner and authorizations) that have been set in the original domain when the volume was written for a backup.

In the volume details displayed by the UI, access rights are shown as"?" or ".".

The "?" indicates the domain does not know the authorization and the owner for READ access.

The "." indicates the WRITE access is disabled.

Notes about access authorizations:

- If volume security settings are modified through the UI in the PRIMARY Data Store domain, these changes will not be forwarded to any other RESTRICTED Data Store domains.
- READ and WRITE authorizations can be updated only in PRIMARY Data Stores.

The user must manually coordinate the sharing of Data Stores between domains.

A data store can be configured for simultaneous access by:

- A single PRIMARY domain.
- One or several RESTRICTED domains.

With some NAS storage types, BackBox cannot open files in exclusive mode in order to avoid many program updating the same virtual volume at the same time and preserve data integrity. If DSM/TC Catalog is correctly configured it is possible to avoid selection of the same tape volume by multiple host.

In IBM Spectrum Protect™ (TSM) API Data Stores, simultaneous access on the same volume by several domains is also technically possible and can be avoided in the same way.

The **Domain access to Data Store** can be modified at any time:

- In a site or recovery environment, a RESTRICTED Data Store promoted to PRIMARY replaces the original owner.
- When a RESTRICTED Data Store is promoted to PRIMARY domain access, the volumes of the Data Store will progressively migrate to the full Primary domain access state, as they are rewritten for backup by the new Owner domain.

> ⚠️ When a PRIMARY Data Store is changed to RESTRICTED, then changed back to PRIMARY less than 24 hours after, there is no progressive migration: all volumes are considered immediately migrated.

After a volume is migrated:

- The next load will be controlled by the volume timestamp (if the timestamp is enabled by the Data Store configuration).
- The next access will be authorized by the security setting registered in the domain catalog.

When volumes are not migrated, they are managed as Restricted.

There is no control of volume timestamp.

The authorizations displayed in the BackPak UI look like: "**??N**".

The two '**?**' indicate that READ and WRITE access will be checked according to the settings saved at backup time as metadata in the tape volume image.

The user can override the security settings by specifying regular authorizations (such as N, O, G…) for READ and WRITE access and for reviewing the ownership (displayed in the same volume detail page).

Secondary Data Stores and Catalog Replication

To prepare for disaster recovery, virtual tape volumes must be backed up or replicated. The tape catalogs on NonStop (BackPak catalog, DSM/TC catalog, etc.) must also be saved.

The virtual tape volumes are saved by specific storage means: HPE StoreOnce, IBM Spectrum Protect™ (Tivoli Storage Manager - TSM), Data Domain, and disk arrays. All these have their own methods of duplicating the objects representing a tape volume. BackPak is not involved in this data replication, except when the replication is obtained by triggering backup scripts (when virtual volumes are written).

With Catalog Sync option, BackPak replicates the entries in the BackPak and DSM/TC catalogs immediately after each backup.

QTOS, CA and TMF catalogs cannot be duplicated. For environments using these catalogs, only the BackPak catalog will be replicated from the primary to the secondary side.

The BackPak catalog replication brings several benefits:

- The timestamp of the last backup on the volume is written and will be verified against the volume in storage at restore time, securing the identification of the version of the volume data.
- When the virtual volumes are written on Windows disk and then saved to an enterprise backup server, the BackPak catalog contains the name of the original Windows file. At restore time, this name must be specified in the command to the enterprise backup software.
- The replicated volume may inherit owner and access restrictions.

To receive the replicated catalog entries on the secondary site, a Data Store must be configured with SECONDARY domain access in the BackPak Domain on the secondary site.

Refer to the *BackPak Catalog Sync Option* manual for more information.

Cloning Physical Tapes

Use OBEY file OBB055 to clone a set of physical tapes to a set of virtual media. The OBEY file receives two tape drive inputs: one physical and one virtual.

The new virtual tape has the same label as the physical one and it is automatically added in the BackBox catalog once created.

> ⚠️ This option is not available on the Virtualized BackBox.

CONFIGURATION

The chapter is organized as follows:

Entities Configured in a Domain - presents the main entities defined for a domain configuration.

Special Considerations at Installation – notes on installation procedure

WINDISK Data Stores and IBM Spectrum Protect™ (TSM) Data Stores- characteristics of WINDISK and IBM Spectrum Protect™ (TSM) Data Store types

The two last sections provide info on the ESM extractor and on the recovery procedure:

EMS Extractor Configuration is a reference set for the BBEXT program that automates the tape load.

Procedures for Recovery describes the backup procedures.

Entities Configured in a Domain

The BackPak Domain configuration defines the VTC(s) and their virtual devices, where the volumes and virtual volume images are stored.

This configuration is kept in the **BBSVCFG** NonStop file located in the same disk sub-volume as the Domain Manager program BBSV.

This configuration is updated through the BackPak User Interface.

From the main Configuration tab of the UI, a sub-tab allows the user to configure each entity:

- **Domain** contains global data such as the license key and the trace settings.
- **NSK Nodes** includes operational details and parameters about the NonStop systems.
- **VT Controller** defines the virtual devices and the TCP/IP or iSCSI/FC connections to the NonStop.
- **Tape Library** communicates with the physical tape library.
- **Key Manager** manages the secondary encryption method.
- **DataStore** describes where the virtual volume images are stored.
- **Volume Groups** sets volume attributes, such as maximum volume size, volume type, and matching NonStop catalog and pool.

Domain

A domain is an operational environment for tape applications. It is a set of one or more NonStop systems connected to one or more VTCs. The domain is defined by a catalog of virtual tape volumes and a set of configurations for the VTCs, the storage, and the tape.

NSK Nodes and NSK Profiles

The NSK nodes make up the system where the VTC(s) presents the tape drives. The VTC(s) presents their tape drives to the NSK node systems.

The NSK profile configuration includes operational details, such as timeouts on the EMS Extractor running on each node.

The actual values are stored in NSK profiles. Usually, the NSK profile created by default does not need adjustment and can be shared by all NSK nodes of the domain.

VTCs and Virtual Devices

The VTC configuration defines the VTC servers and associates some or all of the available iSCSI/FC connections to virtual tape drives on the NonStop systems.

Each available physical iSCSI/FC connection to the VTC is presented as a port in the VTC configuration page.

Configuring several virtual devices on the same port:

- Allows more tape applications to run concurrently.
- Maximizes the usage of the available bandwidth.

With the virtual NonStop, the iSCSI port is a virtual device that establishes connections between the VTC and the virtual NonStop. There is a total of 12 iSCSI ports allowed per network adapter connection.

DataStores

A data store is a data repository for a set of volume groups.

To configure a data store in a domain you must define an area of storage and the routes to the storage. The routes establish through which VTCs a given storage area can be reached. The data storage area must be available to all routes of the data store. For a Window disk Data Store all paths configured in the disk pool must be reachable by all VTCs defined as routes.

Volume Groups

A volume group is a group of volumes that share the same set of attributes:

- Data store name.
- Tape maximum size.
- BackBox compression.
- Catalog type and name.

Once a volume group has been created, its name cannot be changed.

⚠	Maximum volume size, class, compression and encryption will take effect only on volumes loaded for output.

Special Considerations at Installation

Specifications for the Mount Request Message in EMS

The mount request message issued by $ZSVR in EMS must specify the volume label, in order for Back-Box to automatically mount the requested volume on a tape drive.

Tape catalogs like DSM/TC and TMF identify the volume to mount in the request.

Third party tape catalogs must be configured to generate mount requests that include the tape label.

OBEY files for uncataloged tape operation must not specify VOLUME SCRATCH in the TAPE DEFINE, but rather specify a volume label.

Recommendation for the TAPE DEFINE

The TAPE or TAPECATALOG DEFINE should not specify any tape drive. This will allow BackPak to choose a tape drive, providing:

- Fail-safe processing when some resources, such as a VTC server are down, but others are still up.
- Load balancing on the available resources.

BackPak will choose the appropriate drive if there is a mix of media types or if a VLE drive is required for tape Encryption.

Options for BACKUP, BRCOM and TMF

These options should be reviewed, given the differences between physical and virtual media. Some options apply to real media, but not necessarily to virtual media.

- Always use the maximum BLOCKSIZE supported.
- Use 52K in BACKUP and TMFCOM DUMP FILES commands.
- The block size of TMF Audit dump must be configured by TMFCOM
- With Backup/restore 2 BRCOM uses the maximum 56 K (by default). For Backup it is important to specify the BLOCKSIZE because the default value is only 4K.
- Avoid using NOUNLOAD.

Characteristics of Virtual Volumes

Size of Virtual Volumes

The maximum size of virtual volumes is configured by Volume Group. Note that the allocated size of a virtual volume is limited to the size effectively used for the data after compression (if applicable), in both Windows files and IBM Spectrum Protect™ (TSM) Data Stores.

This size should be consistent with the media capacity expected by the software (such as DSM/TC and TMF). For example, a very small size such as 5 MB should be generally avoided. For more info, see section [Number of Virtual Volumes](#).

If virtual volumes are to be exported to physical media, the amount of uncompressed data must fit on a single physical media. Similarly, physical media content must fit in a single virtual volume when imported.

The maximum volume size must be supported by the Data Store.

In Windows files Data Stores, the maximum volume size plus 10% must fit on a single disk.

In IBM Spectrum Protect™ (TSM) Data Stores, the Volume Group configuration allows the split of a single virtual volume into several IBM Spectrum Protect™ (TSM) objects, allowing a very large virtual volume size. See details in the Volume Group section.

Note: Smaller volumes can reduce the time for a partial restore in a multi-volume backup, when BACKUP was executed with the CATALOGFILES option, or when the user keeps the backup output report and chooses the required volumes in this report for the partial restore. The benefit is especially important if the Data Store is Windows files with archive scripting, and if the Windows files must be restored on Windows disks before the virtual volume load can be completed.

Because each volume load introduces a delay, very small virtual volumes will significantly increase the time to complete a multi-volumes restore operation.

The maximum volume size is usually set from 10 to 50 GB.

Number of Virtual Volumes

Smaller catalogs are easier to manage. Therefore, it is recommended to avoid defining more volumes than needed. In some environments expired storage freeing is not possible, either because the tape catalog is not supported by BackPak or because it was not possible to write a delete script to remove the volume copy from the enterprise backup storage.

In such environments, the only way to limit the storage occupied by volumes is to speed up volume re-use by keeping the number of media as close as possible to the actual number needed.

Media Type of Virtual Volumes

Media types, such as LTO3 or LTO4, are not associated with each volume in the BackPak catalog. Each volume is considered being of the type currently defined in its volume group.

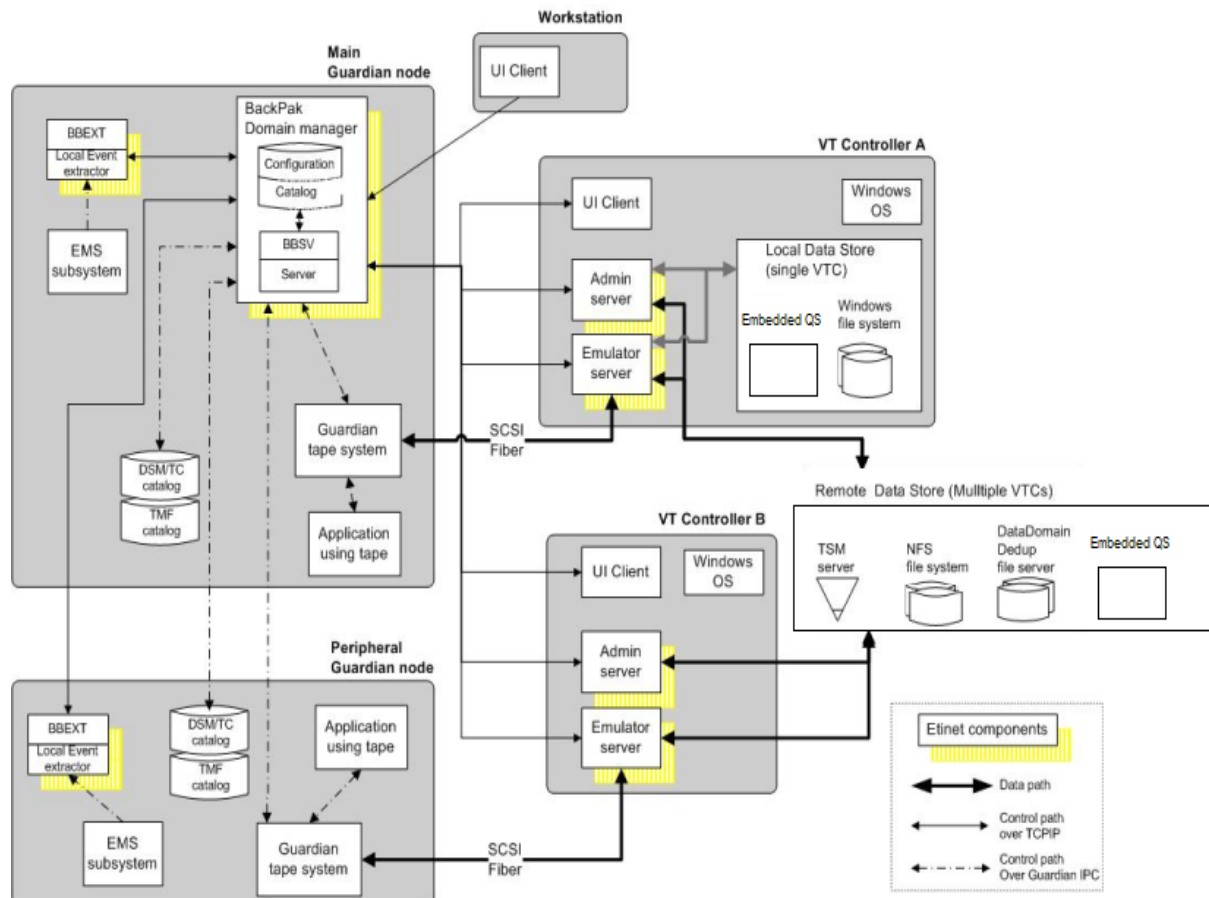Consider the following when define virtual volumes:

- Each tape drive reports a media type to NonStop host queries.

- DSM/TC (but not TMF) associates a media type with each catalogued volume. When a DSM/TC volume is requested, it will load only on media compatible tape drives.

- Some features are available only on specific tape drive types. For example, when the volume encryption is implemented through HP VLE, only LTO4 tape drives are supported.

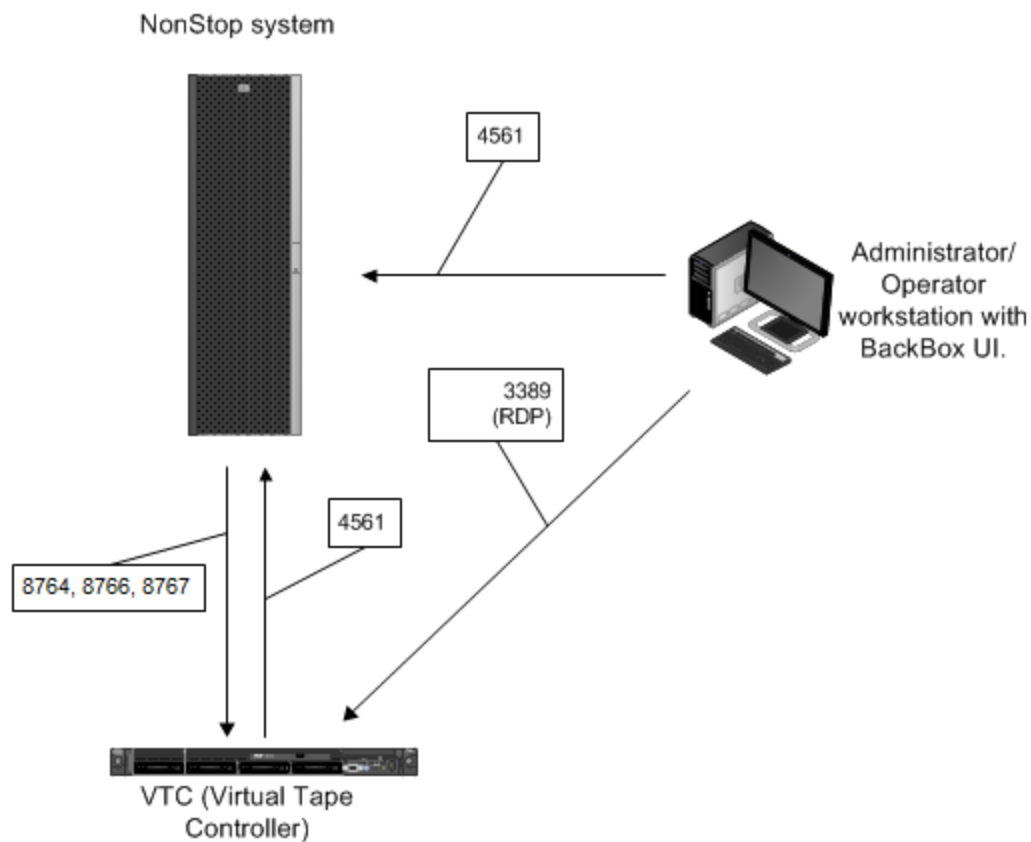BackBox VTC can emulate these media types:

- CART3480

- LTO2 (on LTO3 tape drives)

- LTO3 (also on LTO4 tape drives)

- LTO4 (also on LTO6 tape drives)

- LTO6

- V0505 for virtualized BackBox on the Virtualized NonStop

Domain Network

BackBox Network Topology

BackBox TCP/IP Ports

NonStop system

4561

Administrator/
Operator
workstation with
BackBox UI.

3389
(RDP)

4561

8764, 8766, 8767

VTC (Virtual Tape
Controller)

For BackBox TCP/IP, the firewall must have the correct ports opened to allow the connection to be established in the direction shown in the diagram

Domain Scope Considerations

Number of NonStop Nodes per BackPak Domain

A domain is defined by:

1. A main node that hosts the Domain Manager and a catalog of virtual volumes. This node runs the daily cleanup job OBB017.

2. Optional peripheral nodes that host only the EMS Extractor.

The UI requires a distinct login to each domain. UI instance shows only the configuration and operation of one domain at a time.

A multi-nodes domain consolidates the configuration and the operation of multiple systems, but it creates dependencies. The Domain Manager needs to be available to mount a tape on any of these systems.

There is no limit to the number of nodes in a domain, but the response time might become an issue with more than six nodes.

It is possible to concurrently operate several BackPak domains on the same NonStop node, but each domain must have its own separate:

- Domain Manager (distinct TCP/IP port).

- Domain installation sub-volume (programs, catalog and configuration).

- EMS Extractors (BBEXT processes).

- Data Stores (Disk for Windows data store, storage pool for IBM Spectrum Protect™ TSM Data Store).

Number of VTCs per Domain

For fault tolerance reasons we recommend that two or more VTCs be attached to each NonStop node (s). Several BackPak Domains can share a single VT Controller.

Although it is possible to share a device between domains, the load balancing across VTCs and virtual devices may not be optimum.

Network Configuration

All the control commands between the BackBox components (including Guardian BackBox components) are carried over TCP/IP sockets.

When there are several NSK nodes in the same BackPak domain, the Domain Manager accesses Guardian services on remote nodes through Guardian IPC over Expand. TMFSERVE and MEDIASRV processes are started in a remote node to access the tape catalogs.

Beside the requirement for Expand connectivity, the security settings must allow remote queries and catalog update commands to DSM/TC and TMF.

For further information on security, refer to NonStop Access Authorizations.

When the DSM/TC or TMF catalogs are not on the same node as the Domain Manager, the security parameters for remote access must be reviewed.

Assign to each VTC a permanent TCP/IP address.

Check all TCP/IP traffic for local network routing and firewalls.

For default port configurations, see *TCP/IP Traffic Port Configurations* in table below.

SSL can be implemented on the BackBox TCP/IP control paths through HPE NonStop SSL, thus providing an SSL tunnel through proxy processes on NonStop and Windows servers.

Client	Server (Inbound Rule)	Standard Port	Protocol	Protection
Product Mandatory Firewall Rules				
Workstation (UI Client)	NonStop (Domain Manager)	4561 (Note 1)	TCP	TLS (Note 2)
Workstation (Windows Desktop Client)	VTC (Windows Remote Desktop Server)	3389 (Note 7)	TCP (RDP)	SYSTEM (Note 3)
Nonstop (Domain Manager)	VTC (FC Emulator Services)	8764	TCP	TLS (Note 2)
Nonstop (Domain Manager)	VTC (Administrative Services)	8766	TCP	TLS (Note 2)
Nonstop (Domain Manager)	VTC (iSCSI Emulator Services)	8767	TCP	TLS (Note 2)
Only if Windows Disk Data Store with IBM Spectrum Protect™ (TSM) scripts is used:				
VTC (Windows scripts fetching the IBM Spectrum Protect™ TSM client command line)	IBM Spectrum Protect™ TSM Server, Data Service	1501	TCP	TLS (Note 5)
VTC (Script Manager Service)	IBM Spectrum Protect™ TSM Server, Administrative Service	1580	TCP	TLS (Note 5)
Only if Windows Disk Data Store is used				
VTC (Emulator and Administrative Services)	VTC (Network Share)	139	TCP (CIFS/SMB)	SYSTEM (Note 4)
VTC (Emulator and Administrative Services)	VTC (Network Share)	445	TCP (CIFS/SMB)	SYSTEM (Note 4)
Only if QoreStor Data Store is used				
Workstation (Web Browser)	QoreStor Log-in	80	TCP	SYSTEM (Note 6)
Workstation (Web Browser)	Cloud Tier	5233	TCP	AES 256

VTC (QS Source Replication)	VTC (QS Target Replication)	9904	TCP	AES 256
VTC (QS Source Replication)	VTC (QS Target Replication)	9915	TCP	AES 256
VTC (QS Source Replication)	VTC (QS Target Replication)	9916	TCP	AES 256
VTC (Emulator and Administrative Services)	VTC (QS Network Share)	139	TCP (CIFS/SMB)	SYSTEM (Note 4)
VTC (Emulator and Administrative Services)	VTC (QS Network Share)	445	TCP (CIFS/SMB)	SYSTEM (Note 4)
VTC (Emulator and Administrative Services using RapidCIFS)	VTC (QS Secure Connect2)	9443	TCP	TLS
Only if TSM API Data Store is used				
VTC (Emulator and Administrative Services)	IBM Spectrum Protect™ TSM Server (Data Service)	1501	TCP	TLS (Note 5)
Workstation (Web Browser)	IBM Spectrum Protect™ TSM Server (Administrative Service)	1580	TCP	TLS (Note 5)
Only if iSCSI connectivity is used				
NonStop Storage CLIM (iSCSI Initiator)	VTC (iSCSI Target)	3260	TCP	SYSTEM (Note 4)

Note	Description
Note 1	Default BackBox application port or assigned port number.
Note 2	TLS need to be enforced in the BackBox configuration. See BackBox product documentation BackBox SSL Setup for more information.
Note 3	Port protections depend on the Windows server and/or Active Directory Remote Desktop security policies.
Note 4	We recommend point-to-point Network connection for data path protection.
Note 5	TLS need to be enforced in the Spectrum Protect configuration. See IBM Spectrum Protect™ documentation on how to enable TLS communication.
Note 6	Port protections depend on certificate and browser policies.
Note 7	RDP port need to be open if Remote Desktop application will be used to manage the server remotely.

Tape Catalogs in the NonStop System

A tape catalog simplifies many operations and the user doesn't have to manage separately each volume.

BackBox works with any tape catalog. BackBox is fully integrated with DSM/TC and TMF and partially with QTOS. Special processing is also associated with CA catalogs. Other catalogs and not-catalogued volumes must be associated with the "No catalog" processing in the Volume Group.

Installation with DSM/TC, TMF and QTOS

When virtual volumes are cataloged in DSM/TC, TMF or QTOS, BackBox knows whether a volume is set as SCRATCH or not, and consequently optimizes storage occupancy and operation. A SCRATCH volume does not contain valuable data, and if the Volume Group is configured for Auto-scratch, SCRATCH Volumes are removed from storage. They are artificially regenerated as empty volumes, when requested again by a tape application.

Installation with QTOS

The virtual volumes are defined in both QTOS and BackBox. To register the volumes in the BackPak Domain:

- They are first created in the QTOS database.
- To populate BackPak catalog from the QTOS database, go to the BackPak UI, **Volume** > **Import from Tape Catalog**.

QTOS must be set for SILO.

QTOS vault must be set for Vault location "V" and Silo "S".

A BackBox Volume Group must be configured for each QTOS vault. They will contain the same set of media.

Auto-scratch should be enabled only on non-appended BACKUP.

It is assumed no backup will run in APPEND mode.

⚠️	Any volume requested for output will be deleted first, whatever the status of the volume in QTOS.

Installation with CA

The virtual volumes must be defined in both CA and BackBox. For BackBox, go to BackPak UI > **Volume tab** > **Create Volume**.

Auto-scratch should be enabled only on non-appended BACKUP.

It is assumed no backup will run in APPEND mode.

⚠	Any volume requested for output will be deleted first, whatever the status of the volume in QTOS.

If the BackBox Data Store contains Windows files and these files are archived (on IBM Tivoli Storage Manager, for example), and then deleted, the index file of each volume (.IND) along with .DAT file, should be deleted as well.

CA verifies the tape header HDR1 of each loaded volume to check that it matches the information recorded in its catalog. To allow auto-scratch, BackBox stores the HDR1 image in its catalog and uses it when auto-scratch must be executed.

For the auto-scratch feature with the CA catalog, BackBox VTC recreates an assigned but empty volume with the tape headers expected by CA.

NonStop Access Authorizations

This section describes the default and recommended setup that controls the access to NonStop resources.

BackPak installation:

- An account in the SUPER group (ex: SUPER.BACKBOX represents the installation user), but not SUPER.SUPER, is used to install the BackPak sub-volume (see more in the *BackPak NonStop Installation* manual).
- This user ID will own all files and, therefore, the Domain Manager BBSV will be PROGID.
- The installation INSTALL macro allows the SUPER group to get access to all the files.

How BackPak Actions Are Initiated

Except for statistics and reports, all BackPak actions are executed by the Domain Manager, which is an instance of the BBSV program started by the NonStop TCP/IP LISTNER.

Because BBSV's PROGID file attribute is set, BBSV does not run under SUPER.SUPER, but under the user ID that has installed the package.

Introduction

With 4.09 version, original BackBox access control from UI has been replaced by a more granular and explicit access control feature managed by the new **User Management** tab.

4.09 version allows access to UI only to defined users. SUPER.BACKBOX and SUPER.SUPER users are automatically defined for initial configuration and user manager setup.

4.09 version and later doesn't allow any longer full NonStop log-on (impersonalization). BBSVs run always under the security of SUPER.BACKBOX user and simply authenticate the

user/password (and PIN if multi-factor authentication is used) during the UI Sign-on. Once signed in, the user has permission-based access only to certain UI functions. Therefore, the domain option **Run interactive processes under the NonStop user ID** affects the NonStop actions.

The new BackBox user management feature gives all users (including existing customers using security with safeguard ACL and all other NonStop users) access to UI functions based on permissions. When a user without the right permission tries to perform a certain action without permission to it, the action will fail, being blocked by Safeguard ACL.

The legacy paradigm is the equivalent of 4.09 security with user *.* with a profile set to Administrator and with reintroduction of the domain option **Run interactive processes under the NonStop user ID** (BBSV's impersonalization).

User Name	Profile
.	Administrator

Since version 4.10 the following have been reintroduced:

- BBSV's impersonalization
- user profile with *.* as administrator (to have the same behavior as pre-4.09 version) for customers preferring control based only on NonStop Safeguard.

However, domain option **Run interactive processes under the NonStop user ID** gives the user access to certain functions based on the user's permissions.

> ⚠️ If you upgrade from version 4.09 and want to keep your current User Management configuration, unchecke the **Run interactive processes under the NonStop user ID** box on the **Configuration Domain** page. SUPER.SUPER user may be required to update the configuration.

Version 4.10 also introduces a hybrid access feature that combines the User Management UI functionalities profile control within the access rules reinforced by NonStop Safeguard ACL.

4.10 specific security modes:

1. Legacy security mode : *.* as administrator, BBSV's use impersonalization to control access using Safeguard
2. Security controlled only by BackBox manager: with the possibility to use MFA for UI sign-on (and no BBSV's impersonalization) .

3. Security controlled by BackBox manager and reinforced by Safeguard ACL: without the possibility to use MFA.

For Security controlled only by BackBox manager (with no impersonalization)

When the connection comes from the UI, the UI sign-on authenticates the user/password. Once signed in, the user has access only to the UI functions defined under the user's profile. BBSVs will run under SUPER.BACKBOX and allow access to users with permissions to certain features (assigned under their profile).

The new **User Management** page is designed to define access levels and permissions in such a way that non-Super User has access to all available functions (even to the functions usually restricted to super-group).

Two-factor Authentication method with third-party products, such as XYGATE, is also supported. The two factor authentication method requires that users authenticate with username, password AND PIN number through BackBox UI Client. The access control is now defined using the **User Management** section.

For Hybrid Mode

Only defined NonStop users have access rights to the UI functions.

Based on assigned permissions, users have access to certain UI functions defined under their profile. However, if a new user has been granted permission(s) to functions usually restricted to super-group, a non-Super User will NOT have access to those functions. The same applies to a user who doesn't have access to the Nonstop configuration file: that specific user cannot modify the configuration file even if their profile grants them the permission to do so.

UI sign-on Multi-Factor-Authentication (PIN) is not supported.

For Legacy security mode with longer full NonStop log-on (impersonalization)

Any NonStop user has access to all UI functions, given that they belong to the super-group with access permissions usually restricted to other super-groups.

The user needs to have write access to modify configuration files.

UI sign-on Multi-Factor-Authetication (PIN) is not supported.

When upgrading from a pre-4.09 version to 4.10 version the legacy security mode is the default mode, keeping the user permissions the same as in the pre-4.09 version.

When upgrading from 4.09 version to 4.10 version, the security is controlled only by Back-Box manager mode. Users permissions will be kept as in the 4.09 version.

When the connection comes from a VTC server or from another NonStop process (such as the EMS Extractor or a TACL BackPak macro), the BBSV continues to run under SUPER.BACKBOX. In this case, only the actions pre-defined in the configuration are executed.

Examples of pre-defined actions:

- Cleanup of expired storage initiated by BB017_FREE_EXPIRED macro.

- Log message coming from a VTC server forwarded to EMS.

Access to the NSK Files in the BackPak Installation Sub-Volume

The basic Guardian security (set by the INSTALL configuration macro) allows remote access and updates the SUPER group.

File	Content	Access
BBSVCFG	Domain Configuration	All BBSV processes (UI and AUTOMATION) need to read it. The update might be reserved to specific users .
VOLUME and VOLUME0	Catalog of Virtual Volumes	All BBSV processes must be allowed to modify it. Local and remote EMS Extractors BBEXT must be allowed to read it.
STATE	Automatically Renewed IBM Spectrum Protect™ (TSM) Passwords	All BBSV processes must be allowed to read and modify it.
OPER	Operational States	All BBSV processes must be allowed to modify it. Local and remote EMS Extractors BBEXT must be allowed to read and modify it.
All other files		All BBSV processes must be allowed to read and modify them. All users executing a TACL BackPak macro or OBEY file must be authorized to read and execute.
MEDIASRV, TMFSERVE, MEDIACOM	Guardian Utilities	All BBSV processes need to run these programs. They are started by BBSV in peripheral nodes included in the BackPak domain.
SCF, TACL, CLIMCMD	Guardian Utilities	BBSV processes for UI need to run these programs during the tape drives configuration of the VTCs in the domain.

Access to the NSK Utilities

BackPak starts SPI processes with MEDIASRV, TMFSERVE and MEDIACOM to access the Guardian tape system and catalogs during configuration and during normal operations. The MEDIASRV & TMFSERVE action commands are reserved for the SUPER group.

During the configuration through the BackPak UI, the programs TACL, CLIMCMD, SCF are also run.

In a domain that covers several NSK nodes, these programs are started on the peripheral nodes by BBSV running in the main node. The BBSV PROGID is important for non-interactive activities not requiring a login.

SUPER Group Not Available to Operators

For some systems, the Guardian security pattern for the tape system is not directly applicable; especially when operators cannot be given a Guardian user ID in the SUPER group. In these cases, the PROGID attribute given to BBSV by the installation can be bypassed.

By default, the result of the PROGID attribute on interactive processes running for the UI will be overwritten by the logon initiated by the UI.

If the PROGID attribute must be applied to these interactive processes, a special item must be reset in the BackPak domain configuration in order to still verify the Guardian's user ID/password at UI login; it will not execute the full Guardian sign on procedure.

1. Log on to the BackPak UI with SUPER.SUPER or with the owner of the BBSV file.
2. Modify the configuration at the domain page: uncheck **Run interactive processes under the NonStop user ID**

To limit this wide-ranging access, the page updating the domain configuration executes a real full logon before applying any modification. As a consequence, the user ID that modifies the configuration must be authorized in the NonStop operating system to update all data files: BBSVCFG, BBSVCFGO, VOLUME*, OPER, STATE.

Even though the modifications made outside the UI are not recommended, they are effective. The special setting **Run interactive processes under the NonStop user ID** is disabled and full log-on is executed for any new UI session.

The following message is also issued: **W3391 BBSV was running SUPER.SUPER**.

Full sign-on for user <login user-id> is executed even if **Run interactive processes under NonStop user ID** is un-checked.

Data Stores - Windows Files

A virtual volume is implemented in two disk files stored on a Windows compatible file system.

Supported storage technologies: any SAN, EMC Data Domain, HPE StoreOnce.

File Servers - NAS Considerations

Hardware Requirements

Write/read virtual tape images on a remote file server requires high performance network.

It is recommended to use gigabit Ethernet and dedicated network.

NAS Deduplication vs. BackBox Compression

For normal configuration with a deduplication appliance, such as StoreOnce or Data Domain, the Back-Box internal compression should be deactivated for the associated volume groups, except for the TMF AUDIT dumps (where local compression is suggested).

> ⚠️ The optional BackBox tape encryption avoids deduplication. As the encryption is enabled per BackBox volume group, the encryption can be enabled only for a dedicated volume group and associated DSM/TC pool.

Details on the Disk File-System Usage

The complete image of a tape volume is stored in two files:

- An index file containing META-DATA information. The file name has the form:

LB<volume–name>**.IND** for labeled virtual volumes

NL<volume-name>**.IND** for non-labeled virtual volumes

- A variable length data file containing the NonStop tape application output. The file name has the form:

LB<volume–name>**.DAT** for labeled virtual volumes

NL<volume-name>**.DAT** for non-labeled virtual volumes.

These files will be created in one of the paths defined in the data store's pool(s):

- *Storage Pool*
- *Spare Pool*

Copy Pool

A path is a fully qualified directory that can be specified in two formats: the UNC format based on share name (\\SERVER\SHARE\DIR\) or the legacy DOS format based on drive letter (d:\DIR\SUBDIR\). The path gives access to a local or a remote storage disk.

Paths on different disks can be added in a pool to increase storage space and to optimize parallel operations. If needed, multiple paths can point to the same disk in the same pool.

⚠️	The DOS syntax based on a drive letter prohibits the sharing of virtual volumes by several VTC's. To allow several VTCs to access the same virtual volumes for fail-over and scalability purposes, all paths must be specified in the UNC format.
	Even if it's in UNC format or not, a path is considered local for a VTC when the underlying disk is configured as a local disk in the host Windows system. The same path is considered remote by other VTCs sharing the same data store. Any path pointing to a storage managed by an external file server (or a NAS), is considered remote by all VTCs.

File Access Authorizations

For all file operations in the Data Store, the VTC does a non-interactive Windows log-in with the user account and password configured at the data store level.

This account can be a local user present in each VTC, but it should preferably be an account managed by a Windows Active Directory. The account should be a "non-interactive account" with the password set to never expire.

For **Active Directory** - in case of user password change, each VTC server has to be manually updated with the respective password.

For **Work Group** -in case of system password change, it's not necessary to update the VTC server password.

Full access authorization must be given to the configured Windows account for all paths of the data store.

Without a configured Windows account, the files are accessed through the Local System account.

Data Store pool(s) changes

The Data Store path(s) configuration can be dynamically modified.

When a path is removed from the pool:

- The VTC software will stop accessing this path and any valid files in this path must be moved to a path still present in the pool.

- The last known files location in this path is still preserved in the BackPak catalog. This location will be used in script to access a virtual media copy on an enterprise backup manager in order to restore the copy to a path still configured in the pool.

To manually move all files from an obsolete path to a newly defined path:

- Stop the Guardian tape activity.
- Move the files to a valid path in the disk pool.
- Make sure the moved files allow full access to the account specified in the data store configuration.

When a path is added to the pool:

- This path is immediately active and is considered as a candidate for the next file creation, as well for any move/restore operation.

Distribution of Files Among the Paths of a Pool

When a file is re-created to satisfy a mount for output (for example, when executing a NonStop backup), a selection algorithm is applied to choose one path from the Data Store pool(s) as follows:

1. Paths from the storage pool are always selected over paths from the spare pool. A path in a spare pool can be selected only if no paths in the storage pool are available or can satisfy the volume space requirement.

2. Under the same pool, all paths are considered part of the same group and selection criteria are applied among them.

Exception: Spare pools under Storage Optimization for StoreOnce NAS consider all paths of the pool as an individual group and select the first path available in the order they have been configured.

3. Under the same group of paths, the following selection criteria are applied, in order:
    a. Between two disks, a local disk is always preferred over a remote disk.

    b. Between two disks, the disk with the less writing activity is always the preferred disk.

    c. Between two disks, the disk with more free space is always the preferred disk.

    d. Between two paths of the same disk, the path with the less writing activity is always the preferred path.

    e. Between two paths of the same disk, the path with the lesser number of DAT files on it is always the preferred path (or the path with the lower DAT file size, when the Storage Optimization is for StoreOnce NAS.)

It is possible to change the behavior of some criteria by configuration:

- When the **Force local path** is checked in the data store advanced properties, only the path pointing to the local disk will be considered as a candidate. If the local path enforcement is

activated, the load request may be rejected if there is not enough space on any local disk – even if there is enough space on a remote one.

Data Stores - IBM Spectrum Protect™ (TSM)

This chapter assumes that at least the following requirements are met:

- The IBM Spectrum Protect™ (TSM) client has been installed in each VTC.
- The API run-time is present.
- The command-line backup client is installed.
- The UI backup client is installed.
- The connectivity between the VTC and the IBM Spectrum Protect™ (TSM) environment has been tested using:

  1. A IBM Spectrum Protect™ (TSM) backup client
  2. The IBM Spectrum Protect™ (TSM) client node ID / password that will be used by the VTC.

- The IBM Spectrum Protect™ (TSM) management class to be used by the VTC meets the BackBox requirements.

IBM Spectrum Protect™ (TSM) Server Configuration

For a typical IBM Spectrum Protect™ (TSM) configuration, three objects should be defined on the IBM Spectrum Protect™ (TSM) server:

- [Storage Pool](#)
- [Management Class](#)
- [Client Node](#)

Storage Pool

Disk Storage Pools are strongly recommended for BackBox.

When tape media is required, it is recommended to back up to a disk pool and to let IBM Spectrum Protect™ (TSM) migration move the data to tape.

It is also recommended to carefully plan restore operations, especially when the execution of several concurrent restore jobs may be expected. IBM Spectrum Protect™ (TSM) may consolidate several virtual NonStop volumes on the same physical media, limiting its ability to run several concurrent NonStop RESTORE operations.

The number of concurrent NonStop backup tasks is limited to the number of physical tape drives available to the BackBox client (mount points).

An emulated NonStop tape drive has response time limitations that are more sensitive to long delays and which are more likely to occur when a physical media must be loaded inside IBM Spectrum Protect™ (TSM).

Refer to the IBM Spectrum Protect™ documentation to configure storage pools for the VTCs.

Management Class

The VT Controller stores only "Archive" objects. One or more management classes in the archive copy group must be defined specifically for BackBox.

A Management Class defines the backup data retention and the names of the Storage Pool.

The expiration of the tape volumes is managed by the Guardian tape catalogs. The storage corresponding to expired volumes is explicitly released by the BB017_FREE_EXPIRED macro.

> ⚠️ The IBM Spectrum Protect™ (TSM) server should keep the BackBox archives forever and the **Archive Copy Group** must be set accordingly.

When defining an **Archive Copy Group** for the VT Controller, set the following parameters:

DESTINATION = storage-pool

RETVER = NOLIMIT

RETINIT = CREATION (default value)

Other parameters usually do not apply to BackBox.

The IBM Spectrum Protect™ (TSM) Management Class for BackBox virtual volume can be specified in the BackBox **Configuration** > **Volume Group**.

IBM Spectrum Protect™ (TSM) provides a default Management Class for each IBM Spectrum Protect™ (TSM) Client node.

IBM Spectrum Protect™ (TSM) Client Node

IBM Spectrum Protect™ (TSM) API client nodes must be explicitly registered in the IBM Spectrum Protect™ (TSM) server by using a IBM Spectrum Protect™ (TSM) administrative client. To access a given IBM Spectrum Protect™ (TSM) Data Store, all VTCs of the domain log on to the IBM Spectrum Protect™ (TSM) server using the same IBM Spectrum Protect™ (TSM) node and password.

Alternatively, each VTC logs in with a different node name; the data is owned by a single target node. The access to the target node's data is authorized by the IBM Spectrum Protect™ (TSM) administrator.

This setup is mandatory in a LAN-free configuration. For more info see Specifying NODENAME and PASSWORD in LAN-free configuration.

The VTC supports the IBM Spectrum Protect™ (TSM) automatic renewal of the node password. Different data stores directed to the same IBM Spectrum Protect™ (TSM) server will be set with different node names.

The Client Node must be authorized to delete archives.

The IBM Spectrum Protect™ (TSM) Client Node for a BackBox virtual volume can be specified in the Back-Box configuration on the **Data Store** page or in the DSM.OPT file of each VTC. For more info see IBM Spectrum Protect™ (TSM) Client configuration.

Configuration of the IBM Spectrum Protect™ (TSM) client in each VTC

A DSM.OPT file must be prepared for each VTC.

DSM.OPT is a text file that must contain at least the IBM Spectrum Protect™ (TSM) server address. It can be located anywhere on the local disk.

To create a DSM.OPT file, either use the sample DSM.OPT with recommended options provided or copy the one used by the IBM Spectrum Protect™ (TSM) UI Backup client.

Creating the DSM.OPT with the IBM Spectrum Protect™ (TSM) Backup UI:

1. Start the IBM Spectrum Protect™ (TSM) UI backup-restore client application.
2. **Edit** > **Preference** > **General** > *Node Name*: specify the node name registered for the VTC.
3. **Edit** > **Preference** > **General** > **Authorization** > **Password Access**: choose **Password prompt**.
4. **Edit** > **Preference** > Communication: specify TCP/IP method and IBM Spectrum Protect™ (TSM) server address.
5. On the IBM Spectrum Protect™ (TSM) Backup UI, click on **File** > select **Connect** or **Logon** to logon to the server and then make an archive.

For each VTC:

- Create a folder with the same name as the VTC name and include the DSM.OPT file for the VTC.
- Copy the DSM.OPT created by the UI or by the BackBox installer to the directory created for the VT Controller:

(C:\Program Files\tivoli\tsm\baclient) or

(C:\Program Files\ETINET\Virtual Tape Controller\Config\Samples\dsm.opt)

- Use any text editor to finalize DSM.OPT.

Verify the value of these keywords:

COMMMETHOD TCP/IP (TCP/IP is the default value)

TCPServeraddress ip address

Tcpport 1500 (1500 is the default value)

TCPBUFFSIZE 32 TCPWINDOWSIZE 63

TCPNODELAY YES

PASSWORDACCESS PROMPT

Remove the following keyword:

NODENAME

PASSWORD

Specifying NODENAME and PASSWORD in LAN-free configuration

> ⚠️ This setting must be used when there are several VTCs accessing the same IBM Spectrum Protect™ (TSM) data storage in a LAN-free configuration.

- Each VTC must connect by using a distinct NODENAME/PASSWORD and must share access to the virtual volume data by specifying a distinct target node (ASNODENAME) that owns the IBM Spectrum Protect™ (TSM) data .
- Each VTC must specify a different NODENAME in its DSM.OPT file. The ASNODENAME must be the same in all VTC attached to the same domain.
- PASSWORD can be specified in the DSM.OPT file or set in the Windows registry by using PASSWORD ACCESS GENERATE (Refer to IBM Spectrum Protect™ TSM documentation for details).
- Only PASSWORD ACCESS GENERATE allows the TSM API (IBM Spectrum Protect™)to manage the automatic TSM password renewal when NODENAME/PASSWORD is specified in DSM.OPT file.
- In the configuration of the IBM Spectrum Protect™ (TSM) data store, the TSM user ID and password must be omitted when NODENAME/PASSWORD is specified in DSM.OPT.

Compression / Encryption

Compression and Encryption by the IBM Spectrum Protect™ (TSM) API are supported. However, the performance may be degraded if backup encounters a bad disk sector and must issue a back-space.

PARTIAL-RETRIEVE is a functionality that allows IBM Spectrum Protect™ (TSM) to position a media on the object being requested. It is however, not supported when using compression or Encryption.

If the performance is preferred, the TSM partial retrieve can be enabled in the VTC. Add the line below in the text file C:\Program Files\Etinet\Virtual Tape Controller\BBSL.OPT:

PARTIAL_OBJECT_RETRIEVE=1

⚠	BackBox is distributed with PARTIAL_OBJECT_RETRIEVE=0
⚠	PARTIAL_OBJECT_RETRIEVE=0 is required to restore from a tape image created with PARTIAL_OBJECT_RETRIEVE=0

Recap of TSM Client Configuration Settings

TSM Setting	TSM Client Configuration
Location of DSM.OPT file in the VTC	VTC Domain configuration, Data Store route. Field **TSM Client Option File**.
Server Address and Port	DSM.OPT file. Keywords **COMMMethod** , **TCPServeraddress**, **TCPPort**
Other IBM Spectrum Protect™ TSM Client Options	DSM.OPT file. Keywords **PASSWORDAccess** , **TCPBuffsize**, **TCPWindowsize**
Client Node and Password	VTC Domain configuration, Data Store. Fields **Node**, **Password**. Or (LAN-free case): DSM.OPT file. Keywords **PASSWORDAccess** , **NODEName**, **ASNODEName**, **PASSWord**
Maximum Object Size	VTC Domain configuration, Volume Group. Fields **Max Object Size**.
Management Classes	VTC Domain configuration, Volume Group. Field **Management Class**.
File Space Names	VTC Domain configuration, Data Store. Fields **File Space** .

EMS Extractors

Each Guardian node where a BackBox virtual device is operating must run the EMS Extractor program BBEXT as a permanent process.

BBEXT reads tape mount messages from EMS events and forwards them to the Domain Manager. It also retries pending mount requests according to parameters specified in the domain configuration NSK Node profile.

A default profile is automatically created and associated with all nodes of the domain, with default values that fit most system installations.

BBEXT regularly checks the MEDIACOM list of pending mounts to detect any new mount that may have been missed if BBEXT was not running. This periodic check is executed every *failsafe-retry-interval*.

When BBEXT receives a device busy reply (or a similar error requiring quick retry), it retries the load every *busycheck-retry-interval* seconds. The load is also attempted when an unload EMS event is received.

When the *max-busycheck-retries* value is reached, the retries are executed only at the failsafe timer.

When BBEXT receives a severe error, it retries the load every *failsafe-retry-interval* seconds.

The retries are executed at the failsafe timer stop when *max-failsafe-retries* is reached. A new load attempt can only be executed manually through the BackPak user interface. When restarting BBEXT, reset the retry loop for all pending mounts.

BBEXT Start-up samples:

- BBEXT must run under a Guardian user-ID in the SUPER group.
- The file OEXT to start BBEXT is available in the BackBox installation sub-volume.

RUN BBEXT / NOWAIT, NAME $BBEXT/

Start BBEXT Automatically

BBEXT can be started automatically by the Guardian system at each system boot. A sample SCF input file SCFIN1 is available.

```
ADD PROCESS $ZZKRN.#BBOXEXT, &
PROGRAM $DATA05.BBOX.BBEXT, &
NAME $BBEXT, &
AUTORESTART 3, &
CPU FIRST, &
HOMETERM $ZHOME, &
STARTMODE APPLICATION, &
USERID SUPER.OPER
START PROCESS $ZZKRN.#BBOXEXT
```

Procedures for Recovery

This section describes backup procedures for the BackBox environment. The recovery procedures are detailed in the Operations section.

When planning for recovery of the BackPak environment in the event of a site disaster or a simple file loss, three groups of BackBox data must be considered:

1. The metadata on NonStop server(s): the BackPak Domain Manager configuration, its catalog and one or more EMS Extractor configurations.
2. The configuration data kept in the BackBox VTC(s).
3. The images of virtual tape volumes kept in Data Store(s).

This related data must also be considered:

1. The tape catalog, such as DSM/TC.
2. The configuration of the storage for the Data Stores, such as NAS with de-duplication and replication.
3. The security settings for accessing the storage which could reside outside the storage appliance (in a Windows Active Directory, for example).

In a BackPak multi-domain environment, the data and metadata of each domain must be recovered separately. The BackPak Catalog Sync option handles the replication of the volumes metadata for the BackPak catalog (VOLUME* files) and the DSM/TC catalog. Please refer to the *BackPak Catalog Sync Option* manual.

With the **Catalog Sync Option**, the purpose of catalog recovery is to replicate that part of the catalog corresponding to a specific Data Store. The replication is an on-going replication of new/modified entries operated in a data store. The unit of recovery is not necessarily a BackPak domain.

Without the **Catalog Sync Option**, the BackPak VOLUME & VOLUME0 can only be backed up and restored globally using tools such as BACKUP/RESTORE or generic file replication tools.

⚠	It is not possible to recover information for only a volume group or a data store. Therefore, Backup/Restore functions work as a recovery tool only with a full BackPak.

Data on the NonStop Servers
Summary of operational files

Operational file	Description
BBSVCFG	Domain Configuration
BBSETUP	TACL parameters

OPER	Cache for temporary status information (no need to protect)
STATE IBM Spectrum Protect™ (TSM)	API passwords (not used for WINDISK / StoreOnce)
VOLUME	Catalog of virtual volumes
VOLUME0	Index for the previous file

BackBox Configuration

The BackBox configuration is stored on the NonStop server in the BackBox Domain Manager installation sub-volume. The configuration file name is BBSVCFG.

A supplementary configuration file, BBSETUP, is also kept in the installation sub-volume.

Catalog of Virtual Volumes

The BackBox virtual tape catalog is stored in two ENSCRIBE files: VOLUME and its alternate index VOLUME0.

For the automatic replication of the catalog, refer to the manual *BackPak Catalog Sync Option*.

A BackPak virtual tape must be registered in the catalog in order to be identified and used by the Domain Manager.

After the last tape load for output, VOLUME and VOLUME0 must be recovered at their last consistent state.

The catalog is updated each time a virtual tape is created, deleted, or loaded.

Each time a volume is loaded for output, the following information is updated:

- The volume **timestamp**.
- The **Last load for output time**. It is used at load time to check the virtual volume image version found in the Data Store. It is also used to select a file among several occurrences that might be present if a disk path went down and virtual volumes continue to be written on other disk paths. If the failed path is later recovered, a duplicate virtual tape might be found.
- The **volume owner** and **access authorizations**.

⚠	This data is also saved in the metadata part of the data store.

- For a Windows Data Store, the volume's **Last Update Index Path**.

This path is only used to retrieve Windows files from the enterprise backup software as the fully qualified original file name in the restore command.

The last time the volume was re-written by a NonStop tape application, but, at restore time, this location was not used to retrieve the virtual image in the disk pool(s). Instead, volume's last update index path was used.

The host name of the VTC is provided as script parameter BBOX_BACKUP_HOST (V31.0 and up). This parameter can be used as client original identifier to recognize the backup that has to be to restored from an enterprise backup server in case the files are restored by a VTC other than the original one.

Each time a volume is loaded for input or output, different statistics are saved in the catalog files.

Basic Protection for the BackPak Files

The files STATE, VOLUME and VOLUME0 are distributed with the AUDIT attribute. It is suggested to protect them with TMF.

The other data files, including OPER, cannot be audited by TMF.

- Each time the BackPak Domain configuration is changed:

  - BACKUP the whole BackPak Domain NonStop sub-volume to a specific volume (labeled "non-cataloged"), to be able to restore it without the help of DSMTC and TMF.

  Alternatively, save this sub-volume to a PAK file.

  - Also save the configuration BBSVCFG text file separately.
  - Keep the copy of BBSVCFG and the PAK file (created above) in a safe place.
  - Plan for the license key that is included in the BBSVCFG file. The production license keys specify node names, system numbers and VTC IP address or host name.

- If the BackPak Catalog Sync Option is not available, each time the list of virtual volumes is changed:

  BACKUP the whole BackPak Domain NonStop sub-volume to a specific volume (labeled "non-cataloged"), to be able to restore it without the help of DSMTC and TMF.

  Alternatively, save this sub-volume in a PAK file.

- Enable TMF protection on the VOLUME* files. Execute a TMF DUMP once per day.

Basic Protection of NonStop DSM/TC Catalogs

- This applies when the BackPak Catalog Sync Option is not available.

Refer to the HPE documentation, such as:

Disaster/Recovery of DSMTC catalogs (Id: gcsc10456)

How to move a VOLCAT or FILECAT to another system (Id: 1.0.1593289.2189680)

How to recover/restore the DSM/TC database to the original node using TMF (Id: 100.0.40060491.3470204)

⚠️	Some of these HPE documents include the following restriction: "*This solution only applies to single node DSM/TC configuration without third party tape processing integration*".

This restriction does not apply to BackPak since it is not "integrated" with the HPE tape systems, but it rather communicates with this system through standard and public interfaces.

Protection with the BackPak Catalog Sync Option

- Configure and operate the BackPak catalog exports to save the new/updated BackPak and DSM/TC catalog entries each time a volume is created or re-written for a new backup. Refer to the *BackPak Catalog Sync* manual.
- Protecting the configuration files (documented in Basic protection for the BackPak files) is still required. TMF is still useful for VOLUME* files.

Configuration Data on Each VT Controller

VTC is built to be easily replaced in case of a failure or of an update. VTC configuration is minimal and it must be done using the VTCMC.

If the VTC needs to be replaced, enter the NonStop Domain address and the configuration before the replacement/update will be applied to the new VTC or to the updated version. The configuration has to be redone only for the tape drive whose FC card has been changed.

Images of Virtual Volumes Kept in Data Store(s)

IBM Spectrum Protect™ (TSM) Data Stores

A IBM Spectrum Protect™ (TSM) server provides high-end data protection features.

Refer to the Tivoli Storage Manager documentation for securing the data.

⚠️	Backup Sets are not usable with the IBM Spectrum Protect™ (TSM) API client.

Windows File Data Stores

Protection tools for the Windows file system (such as the disk replication) are used independently of the BackBox software.

The BackBox VTC scripting integrates in the enterprise backup infrastructure.

OPERATIONS

Basic BackBox operational procedures are presented below:

VTC Startup

1. Stop the virtual tape devices emulated by the VTC with the Guardian SCF command:

   ```
   TACL> SCF STOP TAPE $vtname
   ```
2. Power on the VTC.

⚠️	If the VTC has an embedded QoreStor VM, the VM should start automatically. The QoreStor may take several minutes before becoming fully operational. Messages from VTC and from its embedded QoreStor are forwarded to NonStop EMS sub-system. Prompting messages will display when QoreStor Repository Service and the CIFS server are started. Once these services are started, the QoreStor is ready.

```
030000 QCH409-BBOX2019-2-I30000 345-Windows Active Directory client module started. Event time:2021-01-11 09:35:48
030000 QCH409-BBOX2019-2-I30000 346-Windows Server module started.          Event time:2021-01-11 09:35:49
030000 QCH409-BBOX2019-2-I30000 347-Configuration Service started.          Event time:2021-01-11 09:35:49
030000 QCH409-BBOX2019-2-I30000 348-QoreStor Repository Service started.    Event time:2021-01-11 09:35:49
030000 QCH409-BBOX2019-2-I30000 349-RDA server initialized successfully.    Event time:2021-01-11 09:35:52
030000 QCH409-BBOX2019-2-I30000 350-Optimization initialized on container "CrypLocal". Event time:2021-01-11 09:35:52
030000 QCH409-BBOX2019-2-I30000 351-Optimization initialized on container "Cryp2Replicate". Event time:2021-01-11 09:35:52
030000 QCH409-BBOX2019-2-I30000 352-Optimization initialized on container "ClrLocal". Event time:2021-01-11 09:35:53
030000 QCH409-BBOX2019-2-I30000 353-Optimization initialized on container "Clr2Replicate". Event time:2021-01-11 09:35:53
030000 QCH409-BBOX2019-2-I30000 354-RDA server started successfully.        Event time:2021-01-11 09:37:23
030000 QCH409-BBOX2019-2-I30000 355-NFS server started successfully.        Event time:2021-01-11 09:37:23
030000 QCH409-BBOX2019-2-I30000 356-CIFS server started successfully.       Event time:2021-01-11 09:37:23
```

3. Wait for the following two EMS messages to be displayed on the Guardian node where the Domain Manager is installed:

   BBOX-I103 Service started (VTC Admin)
   BBOX-I103 Service started (VTC Virtual Tape Devices)
4. Start the virtual tape devices with the Guardian SCF command:

   ```
   TACL> SCF START TAPE $vtname
   ```

VTC Shut Down

1. Stop the virtual tape devices with the Guardian SCF command:

   ```
   TACL> SCF STOP TAPE $vtname
   ```
2. Shutdown the VTC.

⚠️	If the VTC has an embedded QoreStor VM, the VM should stop automatically.

```
030000 QCH409-BBOX2019-2-I30000 334-Appliance Node Health Monitor Service is being shut down. Event time:2021-01-11 09:13:44
030000 QCH409-BBOX2019-2-I30000 335-Appliance Node Health Monitor Service normal termination. Event time:2021-01-11 09:13:44
030000 QCH409-BBOX2019-2-I30000 336-Appliance Node Health Monitor Service version 01.02.18-67188. Event time:2021-01-11 09:14:20
030000 QCH409-BBOX2019-2-I30000 338-Appliance Node Health Monitor Service is running. Event time:2021-01-11 09:14:21
030000 QCH409-BBOX2019-2-I30000 339-Appliance Node Health Monitor Service is stable. Event time:2021-01-11 09:14:51
030000 QCH409-BBOX2019-2-I30000 340-Appliance Node Health Monitor Service is being shut down. Event time:2021-01-11 09:15:44
030000 QCH409-BBOX2019-2-I30000 341-Appliance Node Health Monitor Service normal termination. Event time:2021-01-11 09:15:44
```

Disabling the Volume Automatic Mount

When the EMS Extractor process is stopped, volumes will stop being mounted automatically. The mount requests will stay pending until a manual load is done or BBEXT is restarted.

If the EMS Extractor is not registered in the Kernel subsystem, simply stop the process:

```
TACL> STOP $BBEXT
```

If the EMS Extractor is registered in the Kernel subsystem, stop it through SCF.

If #BBOXEXT was the registered name:

```
TACL> SCF ABORT PROCESS $ZZKRN.#BBOXEXT
```

Enabling the Volume Automatic Mount

When the EMS Extractor is restarted, it will process firstly the pending mount requests before listening for new ones.

If the EMS Extractor is not registered in the Kernel subsystem, use the provided OBEY file to start it:

```
TACL> OBEY OEXT
```

If the EMS Extractor is registered in the Kernel subsystem, restart through SCF.

If #BBOXEXT was the registered name:

```
TACL> SCF START PROCESS $ZZKRN.#BBOXEXT
```

Manual Load and Unload

⚠	The processing of a manual load requiring the Domain Manager be running. Stand Alone loads do not require a Domain Manager and should be reserved to restore operations (for emergency cases). For further information, see Stand Alone Load section in this manual.

Unless operational needs require the pre-mount of a tape volume, the preferred method of operation consists of:

Loading a volume:

1. Start the tape application.

2. Log into the **Domain Manager** through the BackBox User Interface using a Guardian user in the SUPER group.

For a labeled volume: wait until the EMS tape mount request appears in the **Status** page of the User Interface.

For an unlabeled volume: select a volume from the Volume List page and go to step 5.

3. Locate the **Load** button associated with the pending mount request.

4. Click **Load**. The configured devices are presented for manual device selection.

5. A page showing the configured Guardian nodes and virtual devices is presented to the user to choose the mount point. The virtual device can be left unspecified to enable auto-assign processing.

Loading a volume:

1. Locate the drive on the **Status** page of the BackBox user interface.
2. Navigate to the **Unload** button associated with the drive.
3. Click **Unload** to unload the tape volume.

> ⚠️ The unload will cancel any current operation on the tape device. If there is a NonStop tape application writing or reading to/from the tape device, this application will fail, giving an IO error.

Unlabeled Tapes

The BackBox environment supports unlabeled tapes. This allows the VT Controller to support existing tape software that expects unlabeled tapes.

> ⚠️ It is not possible to automate the mount of unlabeled virtual volumes. All loads must be done manually.

In the BackPak environment, the user must identify each unlabeled volume by a pseudo-label. This pseudo-label is then used by the BackBox software to catalog and locate the image of the unlabeled volume.

Creating an Unlabeled Volume

1. Create the virtual volumes with the label type **Unlabeled**.
2. Assign a six-character label, along with a descriptive comment, to each unlabeled volume.
3. Click **Add**. The unlabeled volume is created.

The labels assigned to unlabeled volumes are usually different from those of labeled volumes in manual operations. Technically, it is possible to have an unlabeled volume and labeled volume share the same label; the label type allows the software to distinguish between the two volumes.

At volume load, the user can browse the catalog of unlabeled virtual volumes and correctly identify the required volume.

Daily Cleanup (OBB017)

Cleanup tasks are collected in the OBB017 OBEY file.

`BB017_FREE_EXPIRED`: Free the storage allocated to newly expired TMF, DSM/TC or QTOS volumes.

`BB023_DEL_BACKEDUP`: Delete old Windows files tape images (Windows file Data Stores only) that have been backed up to a third party enterprise backup manager according to the Volume Group's settings.

`BB022_CHECK_SPACE`: Verify the available disk space for Windows Data Stores.

Scheduling

It is recommended to run OBB017 daily. Each individual task can also be submitted independently. Execution may be slow if scheduled during a time of high tape activity. When virtual volumes are cataloged in DSM/TC, `BB017_FREE_EXPIRED` should be run after the DSM/TC AUTOEXPIRE process to reflect the catalog status more accurately. The UI **Volume Detail** page is always up-to-date because DSM/TC, TMF and QTOS catalogs are always accessed before the display.

For a Daily Cleanup (OBB017) sample see [OBB017 List](#) in Appendix A.

As an additional safety measure, volumes cannot be deleted when not expired in accordance with their original retention specification, as stored in the HDR1 tape header.

⚠	If this safety validation needs to be bypassed, the OBB017 file has to be modified by changing the value of the parameter BB017IGNORECHECKHDR1 into "**1**". The default value of this parameter is "**0**". With this value set to "**1**", the HDR1 check will be bypassed.

BB017_FREE_EXPIRED

The BB017_FREE_EXPIRED command will free space for the volumes that have become SCRATCH since the last execution:

- By deleting the virtual volume image files in the Data Store.
- By running the Delete script in the enterprise backup server storage (if this script is configured in the Data Store)

The command will free storage space for the virtual tape volumes that:

- have a Volume Group configured with Auto-scratch.
- are configured as SCRATCH according the DSM/TC, TMF or QTOS catalog specified in their Volume Group.
- are not in use.
- are in a PRIMARY Data Store.
- have a data size larger than the parameter MIN_SIZE, according to the "Write bytes count" kept in the domain catalog.

This macro will also unload tape volumes that were abnormally left in LOAD state after the tape application using it ended. If the volume was actually already unloaded by the tape system, the LOAD state is simply reset in the BackBox catalog.

When the Copy Pool Sync is configured, the VTC will also delete all instances in the Copy pool.

Syntax:

```
BB017_FREE_EXPIRED [SCRIPT_TIMEOUT minutes]
[,PROCESS NEW | ALL],
[,MIN_SIZE size]
[,OUT filename]
```

Parameters	Description
`[SCRIPT_TIMEOUT minutes]` Default value: 5 minutes.	Maximum number of minutes allowed for the VTC to process the script deletion. **Delete script** is a process that cleans up the backup copy on the server. ⚠️ If Delete Script is not configured on the Data Store, the VTC will not run the script deletion, therefore it will not clean up the backup copy on the server.
`[PROCESS NEW	ALL]` Default value: NEW	`NEW`: checks up the status of any `NEW` scratch volumes inside the BackBox catalog since the last clean-up process, regardless of the volume type (not cleaned up and/or containing data). `ALL`: checks up the status (scratch/sync) of all volumes inside BackPak catalog, regardless of the type and then sends a message for each and every volume inside that catalog (covering all volumes) to the VTC to run the clean-up for `ALL` tapes.
`[MIN_SIZE size]` Default value: 0	Set up volume size (in KB) to be ignored and therefore not cleaned up during BB017 process.
`[OUT filename]` Default filename: BB017 spooler (**$S.#BBOX.BB017**)	Filename destination of the clean-up report. Default filename is BB017 spooler.

Delete script is a process that cleans up the backup copy on the server.

> ⚠️ If **Delete Script** option is not enabled on the **Data Store**, the `[SCRIPT_TIMEOUT minutes]` process will not delete the script, therefore it will not clean up the backup copy on the server.

DataStore w/o delete-script	Reasonable Timeout
DataStore **not** configured with **delete-script**	reasonable timeout = VT controller timeout for DataStore with no delete-script
DataStore configured with **delete-script**	reasonable timeout = **VT controller** and **SCRIPT_TIMEOUT** for DataStore with delete-script

> ⚠️ NonStop error 40 - on socket
>
> When running a **delete script** process, NonStop might issue an error 40 due to lack of response from VTC.
>
> If no response within a reasonable timeout (`SCRIPT_TIMEOUT` value plus 1 minute), check the VTC log. If no error is found in the log, address the issue with ETI-NET support team.

For a sample report see BB017 FREE EXPIRED in the Appendix A – Guardian Tools Samples.

BB023_DEL_BACKEDUP

The BB023_DEL_BACKEDUP command will initiate a Windows process that will scan all configured paths in PRIMARY Data Stores and, according to the Volume Group configuration associated with each volume, will delete the Windows files that have been saved to the enterprise backup server.

A file is considered archived if its archive bit is set. The special processing for StoreOnce to test if a file is backed up by restoring it, depends on a distinct configuration flag "Archive bit supported" (**Data Store Configuration** in the UI).

Deletion is possible only if the the Volume Group configuration associated with each volume allows the process. Additional criteria for the deletion may be specified in the Volume Group configuration.

- Number of days (number of full 24 hour periods) since the last modification of the .DAT file before deletion.
- Number of days (number of full 24 hour periods) since the last access of the .DAT file.
- A minimum file size.

> ⚠️ The .IND file of a volume is never deleted when the Volume Group is not associated with a NonStop tape catalog. The .IND file contains a copy of the tape headers. When there is no NonStop tape catalog, the tape headers in the .IND file are used to tell if the volume has

	expired. The presence of .IND files on Windows disks allows for the Auto-scratch procedure without having to read the data file.

When the Copy Pool Sync is configured, only files in the Storage and Spare Pools are tested. If a file is to be deleted, all other instances with the same or older timestamp are deleted in the Copy pool.

Syntax:

```
BB023_DEL_BACKEDUP STOREID {stored-id | ALL}
[, STOREID_ALIAS {0 | 1 | 2}]
[, START_TIME HH:MN],
[, END_TIME HH:MN]
[, MAX_DURATION minutes]
```

Parameters:

Parameters	Description
STOREID {stored-id | ALL}	Specify a Store Id or ALL, for all Data Stores.
[STOREID_ALIAS {0 | 1 | 2}]	Interpretation of the STOREID value 1: replace '_' characters by space value 2: replace '+' characters by space. Default value is 0.
[START_TIME HH:MN]	Specific to StoreOnce. See after the Sample regular report. Minimum start time in the day. If the macro is run before, nothing will be executed. From 00:00 to 23:59. Default value is 00:00.
START_TIME and END_TIME	Must be both specified or both omitted.
[END_TIME HH:MN]	Specific to StoreOnce. See after the Sample regular report. The macro will not execute anything if run after this time. If the job is still processing at this time, the VTC will complete the current volume and stop processing. From 00:00 to 23:59. Default value is 23:59.
START_TIME and END_TIME	Must be both specified or both omitted.
[MAX_DURATION HH:MN]	Specific to StoreOnce. See after the Sample regular report. Elapsed time after which the VTC will complete the current volume and stop processing. From 00:00 to 99:59. Default value has no limitation.

Sample regular report:

When a Data Store is not configured for StoreOnce, the macro waits for the result and displays a control report showing the deleted volumes.

```
LSD3-BB023 Delete backed up Windows files 2016-08-21 10:38:36
Store id to clean up: ALL
Data Store: WIN1
Label Last Update Last Accsss Size (MB)
----- --------------- --------------- -----------
Path: \\208.180.1.87\LSAL_on_D\LSD3\WIN1
LMW104 2016-07-30 16:45:07 2016-07-30 16:44:59 31
Path: \\BB1\LS_E\LSD3\WIN1
LMW103 2016-08-21 10:32:49 2016-07-30 16:31:33 31
LMW111 2016-08-21 10:37:16 2016-08-21 10:37:03 31
Path: \\happy\lsal\lsd3\win1
LMW106 2016-08-01 14:03:56 2016-07-30 17:08:15 31
LMW107 2016-08-07 18:20:48 2016-08-07 18:20:39 31
LMW112 2016-08-21 10:33:51 2016-08-21 10:33:40 31
Data Store total
6 volumes for which Windows files have been deleted
12 Windows files deleted
185 MB deleted
LSD3-BB023 Delete backed up Windows files 2016-08-21 10:38:36
Data Store: WIN2
Label Last Update Last Accsss Size (MB)
----- --------------- --------------- -----------
Path: D:\LSAL\LSD3\WIN2
This path is not available
Data Store total
0 volumes for which Windows files have been deleted
0 Windows files deleted
0 MB deleted
Grand total
6 volumes for which Windows files have been deleted
12 Windows files deleted
185 MB deleted
LSD3-BB023 ends at 2016-08-21 10:38
I3224 BB023: 12 backed up Windows files have been deleted. Deleted
size: 194,559,102 bytes.
```

START_TIME, END_TIME and MAX_DURATION parameters for StoreOnce.

These parameters apply only to Data Stores configured for StoreOnce NAS.

The VTC cannot tell if a file located in a StoreOnce NAS is backed up or not according to its Archive Bit. Therefore, the VTC actually restores the files that would be candidates for deletion to temporary files. Then it checks the restored file against the original one before deleting both the original file and its

restored copy. This process can be very long and can compete with regular NonStop backups for net-work and storage resources.

- The first precaution is to consider scheduling OBB017 outside of the backup windows, which may result in possibly splitting OBB017 into several jobs.

- The second possible precaution is to use these parameters to limit the duration of the processing and to limit the execution according to the time of the day.

Data Stores associated with StoreOnce NAS are processed in the background and the report produced by the macro indicates: **Submitted as a long-run background process for StoreOnce.** The report is empty and processed volumes will be logged in EMS.

All Data Stores associated with StoreOnce NAS in the domain are processed in parallel and one volume at a time per Data Store.

For a sample report for StoreOnce see [BB023 DEL BACKEDUP](#) in the Appendix.

BB022_CHECK_SPACE

The BB022_CHECK_SPACE produces two reports sorted by Data Store ID.

BB022-A Check disk space in Windows Data Stores.
BB022-B Volume Groups per BackBox Data Store.

- BB022-A shows the summary per disk path and checks the actual free disk space in Windows Data Stores for each disk path.
- BB022-B shows the summary per Volume Group for all Data Store types, including IBM Spectrum Protect™ (TSM) Data Stores.

Checks on space are done during execution. A warning message may be issued to EMS and may be included in the report.

- W3217 LSD3-W3217 nn% of Windows disk space used in store store. Store has reached warning level of nn%. nnnn MB are used. nnnn MB are free.

- W3219 Free space (nn MB) in store is not enough for writing a full volume (nnnn MB) in Volume Group group.W3218 Disk path \\server\share\folder:\LSAL\LSD3\WIN2 in Store store is not accessible.

- W3313 Only 30% of SCRATCH Volumes available in Volume Group DSMTC_???. Volume Group has reached the warning level of nn%. n volumes are SCRATCH out of nn volumes in the Volume Group.

- E2611 Socket error nn when connecting to address nnn.nnn.nnn.nnn port 8766. (Cannot reach a VTC).

- E3034 No available route to Data Store store.

Depending on the requirements of a particular installation, the macro BB022_CHECK_SPACE might be scheduled in NetBatch more than once a day and software monitoring EMS events can be configured to generate alarms when message W3217 or W3313 is issued.

Syntax:

```
BB022_CHECK_SPACE [OUT file-name]
```

Parameters:

[OUT filename] destination of the control report. Default value is the current home term.

For a sample report see [BB022 CHECK SPACE](#) in the Appendix.

Batch Submission of Backup Scripts by BB036_BACKUP_STORE

The backup script can be submitted for all non-backed up files of a WINDISK Data Store through the UI **Storage Admin** page, **Backup all non-backed-up files**. This can also be accomplished by the TACL macro BB036_BACKUP_STORE.

Macro syntax:

```
LOAD /KEEP 1/ BBOX.BBSETUP BBOX.MACROS
BB036_BACKUP_STORE STOREID data-store-id
     [, ROUTE vtc-id ]
```

STOREDID specifies the identifier of a WINDISK Data Store.

ROUTE specifies the identifier of a VTC that will execute all backup scripts. This overrides the default distribution of script submissions.

Batch Device Reservation by BB020_RESERVE

Device reservation can be modified dynamically by the macro BB020_RESERVE, where the device requirements change regularly. This allows scheduling changes in NetBatch.

Macro syntax:

```
LOAD /KEEP 1/ BBOX.BBSETUP BBOX.MACROS
BB020_RESERVE [DRIVE [\node.]$name-pattern,
     [, CLASS name | (name, name...) | NONE ]
     [, LIST ]
```
LIST shows all current reservations.
To modify reservations, the keywords DRIVE and CLASS must be entered.

> ⚠️ The modified reservations are always listed.

DRIVE specifies which drive whose reservation will be altered. Only a single specification is allowed, but wild-cards can be used in the device name. The current node is the default.

CLASS specifies the volume class reserved for the DRIVE. Specify NONE to remove reservation.

LIST generates the list of all reservations in the domain.

The macro ignores the drives of disabled VTCs.

Windows Data Store: Recovering a Disk Path

If one of the paths defined in a Data Store becomes unavailable, it can be recovered by modifying the path's settings in the **Domain Configuration**.

To recover a Disk Path, perform one of the following:

- Load virtual volumes stored in other available paths.
- Load a volume located in the lost path (not SCRATCH according to DSM/TC or TMF). The load will succeed if the volume timestamp check is enabled and a Restore script is configured and executed correctly, otherwise, the load will fail.
- Load a SCRATCH volume for output will be successful if at least one path remains available and the Volume Group is configured for auto-scratch.

Each time the path in error is accessed, an error message will be logged to EMS.

⚠	To recover the files if there is no scripting, the user must restore the backups of these volumes in other paths of the Data Store.

It is recommended to modify the Data Store Disk Pool configuration to remove a path in error and add new paths as necessary. Virtual volume files must be manually moved to the new path as necessary.

Recover the BackPak Catalog

For the replication provided by BackPak, refer to the manual *BackPak Catalog Sync Option*.

⚠	To recover the VOLUME* files, the Domain Manager should not be running. The EMS Extractor process BBEXT must be stopped.

To recover a version of VOLUME* from TMF dumps:

- Run TMF RECOVER. If the dumps have been saved on virtual tapes, use the Stand Alone Load panel in the user interface to mount the volume requested by TMF.

1. To restore a backup done with the PAK utility, simply UNPAK VOLUME and VOLUME0 and DSM/TC or TMF catalogs.

> ⚠️ VOLUME0 is an alternate index and the option MAP NAMES should be used in the UNPAK command as follows: UNPAK pak- file, $SYSTEM.BBOX.VOLUME*, MAP NAMES $*.*.* TO $SYSTEM.BBOX2.VOLUME*, AUDITED, MYID, OPEN

2. To restore from a backup on virtual tape:

RESTORE =tapedef1, $SYSTEM.BBOX.VOLUME*, MAP NAMES $*.*.* TO $SYSTEM.BBOX2.VOLUME*, AUDITED, MYID, OPEN

> ⚠️ Manually load the volume using the UI page to initiate the load and check the restore completion of the restore in EMS. If an EMS message states that the unload cannot be registered, go to the **Volume** tab, display the detail of the volume, click the **Edit** button, reset the current operation and click **Update**.

If it is impossible to load the volume manually, use the **Stand Alone Load** panel in the BackBox user interface. A typical case would be to cold-load the system from an SIT tape on a virtual volume.

After the recovery of a catalog on another system, the restore jobs may fail because the access to the virtual volumes was controlled by the Domain Manager. The volumes security settings may not have been done correctly for disaster recovery; therefore, the read access may be denied.

Use BackBox User Interface to edit volume settings that were written since the BackPak catalog was backed-up and which may need to be restored/fixed due to volume load issues:

1. Modify the volume owner and security settings, if necessary.
2. Disable the **Check Volume Timestamp** at volume level or Data Store level.

> ⚠️ When the timestamp check is disabled and the Windows INDEX file is present in several Disk Pool paths, the load will fail and the user will have to delete the obsolete versions.

To recover the catalog when there is no available catalog backup, but the actual data is available in the Data Store, the catalog has to be entered manually. To do so, perform the following steps:

1. Use configuration backups and notes to rebuild the configuration of a new domain.
2. In the **Domain Configuration**, modify the Data Store's domain access to RESTRICTED.
3. In **Windows file Data Stores**, restore all *.IND files, if they have been deleted after archive/backup to a back-end enterprise backup server.
4. Using the **Create Volume** page of the user interface, re-create all virtual volumes in the BackPak catalog. This does not access the actual Data Store.

5. If possible, modify the security settings at the volume level, as required.

6. Change the Data Store back to PRIMARY and, using your record, set the configuration back to its former state.

7. Until the volume is rewritten in the new environment, its access will be authorized according the access authorization set at backup time.

Recover the BackPak NonStop Environment

To recover the BackPak NonStop environment, four items must be re-installed:

1. The BackPak software.

2. The static BackPak Domain Configuration (**BBSVCFG**, **STATE** and **BBSETUP** files.)

> ⚠️ **BBSVCFG** includes a license key that is valid only for specific NonStop node(s).

3. The catalog of virtual volumes (**VOLUME** & **VOLUME0** files).

4. The OBEY files, such as OBB017, that were customized by the user.

> ⚠️ A virtual volume must be recognized by the Domain Manager to be automatically loaded by BackPak. An up-to-date catalog is required to make all BackPak features available.

TMF and DSM/TC catalogs are not required to run restores from virtual volumes.
These NonStop catalogs must be restored according to the procedure recommended by HPE.

Recovery from Backups on a New NonStop System

If the backup was set for recovery when it was installed:

1. Unpack the PAK file containing the BackPak installation sub-volume including the VOLUME* files.
2. Check that the BackPak environment is operational and has access to Data Stores containing the images of TMF and BACKUP virtual volumes.
3. RESTORE the VOLUME* files from the most recent installation sub-volume backup.

The BackPak environment is now ready to process all mount requests. If the DSM/TC catalogs must be restored, it should be done at this time.

If the backup was set for recovery when it was installed:

- Install the BackPak software from an ETI-NET distribution package.
- Initialize the BackPak configuration by replacing the default **BBSVCFG** file with the one previously saved or in accordance with notes taken.

- Enter the list of virtual volumes in RESTRICTED Data Stores, as presented in the [Recover the Back-Pak Catalog](#) section above.
- Recover the DSM/TC catalog.

Recovery on a Prepared DR System

Requirements for a recovery on a prepared DR system:

- The DR system already has a working BackPak environment.
- Backups or replications recommended in the Setup for recovery section of the Installation chapter are available.

To make the recovery:

1. Check that the whole BackPak environment is operational and has access to Data Stores containing the images of TMF and BACKUP virtual volumes.

2. If VOLUME* files were not replicated, RESTORE them from the latest backup of the BackPak installation sub-volume.

3. Recover the TMF and DSMTC catalogs using the procedures documented by HPE. Eventually, use the BackPak Catalog Sync option for the DSM/TC catalog.

The BackPak environment is now ready to process all mount requests.

Recovery Hints:

If tape load requests are rejected because TMF is not yet operational, change the BackPak audited VOLUME* files to NO AUDIT until the NonStop system is fully operational.

If load requests are rejected because the timestamps in the BackPak catalog and those in the volume timestamps do not match, use the UI to:

- Disable the timestamp checking on the volumes that cannot be loaded.
- Disable the timestamp checking at the Data Store level, if you have more volumes.

If the BackPak catalog does not contain entries for volumes requested by RESTORE or RECOVER and no backup of the catalog is available, do the following:

- Configure a RESTRICTED Data Store and a corresponding Volume Group. Use BackBox UI to create all the required virtual volumes in that Data Store.
- If only a few virtual tape volumes are involved, use the **Stand Alone Load** page of the UI.

TOOLS

Guardian Tools

The following TACL and OBEY file programs are provided as support tools for various reports, virtual drives performance testing, and trace tracking.

A reset procedure for the NonStop tape subsystem is documented in the *BackPak Messages Manual and Troubleshooting*.

BBREST – Restore Files Through MEDIACOM

BBREST is a TACL macro that helps users (not familiar with MEDIACOM) execute simple restores with pre-defined options.

BBREST prompts for parameters to generate the MEDIACOM commands INFO DISKFILE and RECOVER DISKFILE. Only backups executed with the CATALOGFILES option can be restored by BBREST.

The macro accepts a single file name or file name pattern, and asks for optional additional selection criteria to produce a list of tape files (i.e. backup executions) and a list of matching disk files.

This list of disk files can be browsed in Detail Report or in Summary Report. The Summary Report shows only the backup executions containing matching files.

Both the **Detailed Report** and **Summary Report** allow the selection of a backup execution for submitting a restore. The user can loop between the browsing of Summary and Detail Reports before submitting a restore.

When a restore is to be submitted, the macro asks for the target location of restore and initiates the RECOVER DISKFILE command.

When the RECOVER DISKFILE command is executed, MEDIACOM asks for confirmation and issues a mount request in EMS. The request will be answered by the BackPak EMS Extractor.

⚠️	- When a disk file pattern is entered, different subsets of disk files might be present in different tape files (different backups), but the RECOVER DISKFILE will execute only from a single tape file. - Predefined standard restore options are set in the macro. It is possible to change them by editing BBREST. Search for: `#SET restore^opt LISTALL, OPEN, TAPEDATE, AUDITED` and `#SET outfile $S.#DSMTC.RESTORE`

Syntax:

```
LOAD /KEEP 1/ MACROS BBSETUP
RUN BBREST
```

For scenarios using the detailed report see the BBREST Scenarios in the Appendix.

TMFC2 – Extensions to TMFCOM Commands on Media

TMFC2 is a TACL macro (not specially attached to virtual tapes) that simply provides two extensions to the TMFCOM commands on media: INFO, ALTER and DELETE:

- A generic label pattern can be entered as a media name, ex: TMFC2 INFO MEDIA P*100?
- An optional keyword SELECTSTATUS is added to these commands to select the media object of the action according to their status in TMF, ex: TMFC2 ALTER MEDIA *, SELECTSTATUS RELEASE, STATUS SCRATCH

TMFC2:

- Receives the TMFCOM command as a TMFC2 command parameter.
- Browses the TMF catalog.
- Selects media according to the pattern and the SELECSTATUS parameter.
- Generates (in a temporary file) a command for each selected media.
- Runs TMFCOM giving the generated file as an input file.
- Deletes the temporary file.
- Requires running in the BackPak environment as it uses BackPak macro and programs.

Syntax:

```
LOAD /KEEP 1/ MACROS BBSETUP
TMFC2 [PEEK | NOPEEK,] [FILE file-name,] TMFCOM-command
```

Parameters:

[PEEK | NOPEEK,] allows preview of the commands to execute. Default value is NOPEEK.
NOPEEK: TMFCOM is executed with the generated input file
PEEK: the generated input file is displayed only.

[FILE file-name,] Name the TMFCOM input file to save it.

TMFCOM-command

TMFCOM command syntax on TAPEMEDIA. The clause [SELECTSTATUS status,] can be added, with status being SCRATCH, ASSIGNED, RELEASED or BAD.
The media-name can be a media-name pattern.

For TMFCOM samples see [TMFC2 Samples](#) in the Appendix.

BB000_COLLECT – Gather Information for Support

BB000_COLLECT is a TACL macro that produces a file documenting a BackBox environment. It is used when issues arise and support needs the latest information.

The collected information, such as logs and configuration files, documents only the NonStop system where the macro is executed. The same macro must be executed in peripheral NonStop nodes and a Windows specific procedure must be executed in the VTCs.

BB000_COLLECT requires a working sub-volume (TARGET parameter) where intermediate files and two consolidated final files will be created. When completed, these two file names are displayed and available to product support.

Syntax

```
VOLUME <BackPak-installation-subvol>
LOAD /KEEP 1/ MACROS BBSETUP
BB000_COLLECT TARGET <target-subvol>
[, TIME <yyyy-mm-dd [hh:mn[:ss]]>]
[, COLLECTOR $process]
[, LISTALL yes|no]
```

Parameters:

```
TARGET subvol
```
Required the sub-volume where the files will be created. It is recommended to specify the Back-Pak trace for the sub-volume configured in the BackPak domain

[TIME <yyyy-mm-dd [hh:mn[:ss]]>]
Optional time of incident that will be used as base to extract EMS messages.
The extracted messages will be those produced from 24 hours before this time and up to one hour after.
The current time is used as the default value.
00:00:00 is the default when a date is specified without the time of day.

[COLLECTOR process]
Optional EMS collector process name from which the messages will be extracted.
"$0" is used as the default value.

[LISTALL yes|no]
LISTALL YES produces the list of the PAK content (i.e. sends the LISTALL parameter to the BACKUP program). **No** is used as the default value.

For a BB000_collect sample see BB000_COLLECT sample in the Appendix.

BB010 - Extracts Virtual Volume Records

BB010 extracts virtual volumes records to the VOLEXT file for further reporting by BB011 or BB012.

Syntax:

```
RUN BB010 label-pattern [REPORT]
```
[REPORT] will generate a simple report of volumes that match label-pattern.
The VOLEXT file will be created if missing and its content will be overwritten if it already exists.
BB010 must be run in the sub-volume where the Domain Manager is installed.

Example:

$DATA15 BFERHG19 43> run bb010 AA* report

```
BB010- Extraction of the BackPak catalog to file VOLEXT 2020/10/28
16:50
Selection of volumes matching the label pattern: AA*

Label: AA0001 BACKUP
Max volume size : 5 MB
Automatic mount : Y
Creation time : 2020/10/06 17:42
Last load time : 2020/10/06 17:43
Owner : \LEOMIRA 255,100
Volume Group : FERNDSK
Store id : WIN1
Store type : WINDISK
Index path : D:\FERN\WIN1
Number records read : 24
Number records extracted : 1
```

BB017 - Free expired volumes.

BB017 is a cleanup task macro recommended to be run daily. BB017 frees the storage allocated to newly expired TMF, DSM/TC or QTOS volumes. Additional parameters have to be set up based on the data store(s) configuration.

For more details on the process, see Operations. Refer to Appendix A – Guardian Tools Samples for OBB017 sample.

Syntax:

```
BB017_FREE_EXPIRED [SCRIPT_TIMEOUT minutes]
[,PROCESS NEW | ALL],
[,MIN_SIZE size]
[,OUT filename]
```

Parameters:

`[SCRIPT_TIMEOUT minutes]` maximum number of minutes allowed to the **Delete script**. Default value is 30 minutes.

> ⚠ If **Data Store** doesn not have the **Delete Script**, the `[SCRIPT_TIMEOUT minutes]` parameter has no effect.

`[PROCESS NEW | ALL]` NEW: process only the new SCRATCH Volumes / ALL : process all SCRATCH Volumes or backup software. Default value is NEW.

`[MIN_SIZE size]` minimum number of KB of data in the tape volume, to allow the free up executed. Default value is 0.

`[OUT filename]` destination of the control report. Default value is the current home term.

`[BB017IGNORECHECKHDR1]` parameter that allows users to instruct BackBox to ignore checking "BackUp header 1" during the cleanup.

Values: 0 (No), 1 (yes).

BB022 - Verifies the available Disk Space.

The BB022_CHECK_SPACE produces two reports sorted by Data Store ID.

BB022-A Check disk space in Windows Data Stores.
BB022-B Volume Groups per BackBox Data Store.

- BB022-A shows the summary per disk path and checks the actual free disk space in Windows Data Stores for each disk path.
- BB022-B shows the summary per Volume Group for all Data Store types, including IBM Spectrum Protect™ (TSM) Data Stores.

For more information on the macro, see BB022_CHECK_SPACE in Operations.

Depending on the requirements of a particular installation, the macro BB022_CHECK_SPACE might be scheduled in NetBatch more than once a day and software monitoring EMS events can be configured to generate alarms when message W3217 or W3313 is issued.

Syntax:

`BB022_CHECK_SPACE [OUT file-name]`

Parameters:

[OUT filename] destination of the control report. Default value is the current home term.

For a sample see BB022 CHECK SPACE in the Appendix A - Guardian Tools Samples.

BB023 - Delete old files tape images

The BB023_DEL_BACKEDUP command will initiate a Windows process that will scan all configured paths in PRIMARY Data Stores and, according to the Volume Group configuration associated with each volume, will delete the files that have been saved to the enterprise backup server.

For more information on the macro, see BB023_DEL_BACKEDUP in Operations.

Deletion is possible only if the the Volume Group configuration associated with each volume allows the process. Additional criteria for the deletion are specified in the Volume Group configuration.

For a macro sample, see BB023_DEL_BACKEDUP in the Appendix A - Guardian Tools Samples.

BB044 –Series of Tape Label Reports

BB044 shows a summary of the tapes known in the NonStop system, listing them by a series of consecutive tape labels.

BB044 must run in a BackPak domain. It searches for tape labels registered in:

- The BackPak domain (i.e. the virtual tape volumes).
- All DSM/TC volume catalogs in the local NonStop system.
- The local TMF catalog
- The remote DSM/TC and TMF catalogs referred by Volume groups configured in the BackPak domain.
- The QTOS catalogs referred by Volume groups configured in the BackPak domain.

Syntax:

RUN BB044 [BPAK_REPORT {y|n}] [, CATALOG_REPORT {y|n}] [, MERGED_REPORT {y|n}]

Parameters:

`BPAK_REPORT {y|n}` If **Y** or **Yes**, the report BB044-1 will be produced. This report lists the virtual volumes of BackPak and their Volume Group name. Default value is **No**.

`CATALOG_REPORT {y|n}` If **Y** or **Yes**, the report BB044-2 will be produced. This report lists the volumes found in the tape catalogs and their location (DSM/TC VOLCAT and pool names). Default value is **No**.

`MERGED_REPORT {y|n}` If **Y** or **Yes**, the report BB044-3 will be produced. This report lists all volumes, matching the BackPak volumes and the volumes found in tape catalogs. Default value is **Yes**.

For BB044 sample see [BB044 Tape Label Report](#) in the Appendix.

OBB011 - List of Volumes in Windows Files Data Stores

OBB011: Lists the virtual volumes stored in Data Stores of Windows files, sorted by Windows disk path.

Syntax:

```
RUN OBB011 label-pattern
```
Label-pattern will select volumes whose label matches the pattern.
OBB011 must run in the sub-volume where the Domain Manager is installed.

For a sample of OBB011 - List of Volumes in Windows Files Data Stores see [OBB011 - List of Volumes in Windows Files Data Stores](#) in the Appendix.

OBB012 - List of Virtual Volumes

OBB012: Lists the virtual volumes registered in the BackPak catalog.

Syntax:

```
RUN OBB012 label-pattern
```
Label-pattern will select volumes whose label matches the pattern.

OBB012 must run in the sub-volume where the Domain Manager is installed.

For a sample of OBB012 see OBB012 - List of Virtual Volumes in the Appendix.

OBB018 - Statistics Report

OBB018 lists the VTC activity-related info: data size and throughput per volume loaded.

This report shows the activity of scripts started by the VTC emulator, but does not list the activity of scripts started by the Script Controller. See OBB019 - Statistics Report – Script Controller for the report on scripts initiated by the VTC Script Controller.

Rates printed in BB018 exclude the initial wait time. This report excludes all starting activity timestamps until the tape application begins to write or read data blocks.

Syntax:

```
OBEY OBB018
```

For a sample of the OBB018 content see OBB018 Statistics Report in the Appendix.

Report output:

```
$DATA05 BPAK 14> OBEY OBB018
BPAK-BB030 - Extraction of statistics files 2020-04-07 16:12
Stats file names : $DATA05.BPAK.STAT%YY%%MM%
Extract file : STATEXT
Selection from: 2020-04-06 17:00:00 to: 2020-04-07 17:00:00
Existing statistics files Records read Records extracted
------------------------ ------------ ------------------
\MONT.$DATA05.BPAK.STAT1102 5526 0
\MONT.$DATA05.BPAK.STAT1103 3712 0
\MONT.$DATA05.BPAK.STAT1104 766 4
Total records written: 4
BAPK -BB018 BackBox activity by Data Store page 1
From: 2018-04-06 17:00:00 to: 2020-04-07 17:00:00
Data Store: WIN1
Start End R Volume Data size Rate Set
time time Oper. W label MB MB/s ve VTC

-------- -------- -------- - ------ ---------- ------ -- --------------------

Start date: 2020-04-07
14:38:20 14:38:25 LOAD W OBCD09 2 1.0 I MTLBBLAB1
14:38:25 14:38:35 BACKUP W OBCD09 2 0.2 I MTLBBLAB1
14:55:03 14:55:22 LOAD R OBCD09 2 0.5 I MTLBBLAB1
14:55:04 14:55:16 RESTORE R OBCD09 2 0.2 I MTLBBLAB1
      BackBox activity summary for WIN1
        2 volumes accessed
        5 MB of transfered data
```

Report elements:

Start date/time: Time when the load request was accepted by the BackPak Domain Manager.

End time: Time when the volume was unloaded by the VTC.

Volume label: Virtual volume label.

Oper: BackPak operation.

LOAD - Virtual volume loaded in a NSK tape drive.

BACKUP – Backup Windows script.

RESTORE – Restore Windows script.

MOVE – Move the volume from a storage location to another.

EXPORT – Export to physical media.

IMPORT – Import from a physical media.

R/W: Read or Write (USE parameter of the tape define).

Data size: Data size written or read by the NSK tape application.

Rate: Transfer rate computed from the time the 1st data block is written/read (excluding tape headers processing) to the unload time.

Severity: I - information, normal emulation.

W – warning, error occurred during execution or the volume was manually unloaded.

E – severe error.

VTC: VT Controller identification.

OBB019 - Statistics Report – Script Controller

OBB019 lists script activities related to Script Controller: data size and throughput per script execution.

By using Script Controllers you can serialize backups, restore script operations, optimize access to resources, and minimize delays.

The statistics file name is specified through the BackPak user interface on the **Domain Configuration** page.

Syntax:

```
OBEY OBB019
```

For a sample of the OBB019 content see OBB019 - Statistics Report – Script Controller in the Appendix.

Sample of a OBB019 - Statistics Report – Script Controller:

```
$DATA15 LSBBOX 14> OBEY OBB019
BPAK-BB030 - Extraction of statistics files 2020-03-16 13:12
Stats file names : $DATA05.BPAK.STAT%YY%%MM%
Extract file : STATEXT
Selection from: 2020-03-15 14:00:00 to: 2020-03-16 14:00:00
Existing statistic files Records read Records extracted
----------------------- ------------ ------------------
\MONT.$DATA21.LSBBOX.STAT0912 5526 0
\MONT.$DATA21.LSBBOX.STAT1001 3712 0
\MONT.$DATA21.LSBBOX.STAT1003 766 313
Total records written: 313
```

```
BPAK -BB019 Scripts submitted by script controllers page 3
From: 2020-03-15 14:00:00 to: 2020-03-16 14:00:00
Start Start End Data size Rate Se
VTC date time time Oper. MB MBs ve
-------------- ---------- -------- -------- ---------- -------
---- ------- --
AUSTNSBUPC101 2020-03-15 16:56:13 16:56:19 BACK-BATCH 0 0.0 I
AUSTNSBUPC101 16:56:15 16:56:22 BACK-BATCH 1 0.1 I
AUSTNSBUPC101 16:56:29 16:56:35 BACK-BATCH 0 0.0 I
AUSTNSBUPC101 16:56:31 16:56:38 BACK-BATCH 1 0.1 I
AUSTNSBUPC101 16:56:50 16:56:55 BACK-BATCH 1 0.2 I
AUSTNSBUPC101 16:56:53 16:56:59 BACK-BATCH 0 0.0 I
AUSTNSBUPC101 16:57:11 16:57:17 BACK-BATCH 1 0.2 I
AUSTNSBUPC101 16:57:17 BACK-BATCH 0 0.0 I
AUSTNSBUPC101 16:57:29 16:57:36 BACK-BATCH 0 0.0 I
AUSTNSBUPC101 16:57:30 16:57:36 BACK-BATCH 1 0.2 I
AUSTNSBUPC101 16:57:47 16:57:52 BACK-BATCH 0 0.0 I
AUSTNSBUPC101 16:57:52 16:57:58 BACK-BATCH 1 0.2 I
AUSTNSBUPC101 16:58:09 16:58:15 BACK-BATCH 0 0.0 I
AUSTNSBUPC101 16:58:11 16:58:18 BACK-BATCH 1 0.1 I
AUSTNSBUPC101 16:59:09 16:59:15 BACK-BATCH 0 0.0 I
*** BB019 end of report
```

Report elements:

> **VTC:** VT Controller identification.
> **Start date/time:** Script start time according to the VTC system time.
> **End time:** Script end time according to the VTC system time.
> **Data size:** Data size written or read by tape application.
> **Rate:** Transfer rate computed from the time the 1st data block is written/read (excluding tape headers) to unload time.

Severity:

> **I** - information, regular execution.
> **W** – warning, some error occurred for one or all the files processed by the script.
> **E** – severe error occurred for one or all the files processed by the script.

OBB021 – Emulation Statistics Report

OBB021 lists the tape emulation activity only (data size and throughput per volume loaded).

Throughput calculations exclude the initial wait time.

Syntax:

```
OBEY OBB021
```

For a content sample of OBB021 see OBB021 - Emulation Report in the Appendix.

Report output sample:

```
$DATA05 BPAK 14> OBEY OBB021
BPAK-BB030 - Extraction of statistic files 2020-04-07 16:17
Stats file names : $DATA05.BPAK.STAT%YY%%MM%
Extract file : STATEXT
Selection from: 2020-04-06 17:00:00 to: 2020-04-07 17:00:00
Existing statistics files Records read Records extracted
----------------------- ----------- -----------------
\MONT.$DATA05.BPAK.STAT1102 5526 0
\MONT.$DATA05.BPAK.STAT1103 3712 0
\MONT.$DATA05.BPAK.STAT1104 766 4
Total records written: 4
LSBBE -BB021 BackBox emulation activity by Data Store page 1
From: 2020-04-06 16:00:00 to: 2020-04-07 16:00:00
Data Store: WIN1
Start End R Volume Data size Rate Compr En- Se
time time W label MB MB/s ratio cryp ve VTC
-------- -------- - ------ ---------- ------ ------ ---- -- ---------
---------
Start date: 2020-04-07
14:38:20 14:38:25 W OBCD09 2 1.0 2.36 I MTLBBLAB1
14:55:03 14:55:22 R OBCD09 2 0.5 2.36 I MTLBBLAB1
Virtual tape emulation summary for WIN1
2 volumes loaded
5 MB of transfered data
```

Report elements:

> **Start date/time:** Time when the load request was accepted by the BackPak Domain Manager.
> **End time:** Time when the volume was unloaded by the BackBox.
> **R/W:** Read or Write (USE parameter of the tape define).
> **Volume label:** Virtual volume label.
> **Data size:** Data size written or read by the NSK tape application.
> **Rate:** Transfer rate computed from the time the 1st data block is written/read (excluding tape headers processing), up to the unload time.
> **Compr. Ratio:** Compression ratio = user data size / storage size.
> **En-cryp:** Encryption indication = space or "Encr".

Severity:

> **I** - information, regular emulation.
> **W** – warning, error occurred in the emulation, or the volume was manually unloaded.
> **E** – severe error.
> **VTC:** VT Controller identification.

OBB038 – List of Encrypted Volumes

OBB038 lists the Encrypted volumes whose label matches an entered volume label pattern.

Syntax:

```
RUN OBB038 label-pattern
```

Where label-pattern is a specific label or a simple pattern ending by *.

Samples:

```
RUN OBB038 *
RUN OBB038 PR*
```

For a sample of OBB038 content see [OBB038 List of Encrypted Volumes](#) in the Appendix.

Report sample:

```
BB038 Encrypted volumes with label matching * 2020-10-24 11:24
Last DSMTC
Volume write or TMF
label date status Encryption Key ID
------ ---------- ------- ----------------------------------------
--------
Key manager id : KM-ESKM
Client type : 1-VTC ONLY
VE1001  2020/10/27  ASSIGNED  BBOX_ 21F5BD27VE1001D68095D44B400008_
111027202410
VE1015  2020/10/27  ASSIGNED  BBOX_ 767FE574VE1015D5C6642F4B230008_
111024144520
2 printed volumes for Key manager KM-ESKM
End of report BB038
```

Report elements:

> **Volume label:** Label of the virtual tape volume.
> **Last write date:** Last date the volume was written by a tape application.
> **DSM/TC – TMF:** Volume status in DSM/TC or TMF.
> **Status:** (when applicable).
> **Encryption Key ID:** Encryption Key name instance.

OBB039 – List of Virtualizations / Materializations

OBB039 lists the virtualizations, i.e. copies of physical volumes to BackBox virtual volumes and materializations, i.e. the copy of virtual volumes to physical volumes.

Syntax:

```
OBBEY OBB039
```

For a content sample of OBB039 see [OBB039 - List of Virtualizations/Materializations](#) in the Appendix.

Report output sample:

```
QC314EA -BB039 BackBox virtualizations / materializations page 1
From: 2020-08-01 18:00:00 to: 2020-08-02 18:00:00
```

```
Operation: MATERIALIZE
Volume Start Start Data size Rate Compr En- Se
label date time MB MB/s ratio cryp ve VTC
------ ---------- -------- ---------- ------ ------ ---- -- --------
EVTS01 2020-08-02 10:38:35 0 0.0 0.99 Decr W TANK
EVTS01 2020-08-02 10:40:26 0 0.0 0.99 W TANK
EVTS01 2020-08-02 11:02:44 135 7.9 0.99 I TANK
EVTS02 2020-08-02 13:40:33 4,832 4.4 0.99 I TANK
EVTSN1 2020-08-02 14:15:53 135 11.3 0.99 I TANK
EVTSN2 2020-08-02 14:42:46 4,832 4.4 0.99 I TANK
Summary for MATERIALIZE
6 volumes
9,936 MB of transferred data
```

Report elements:

> **Volume label:** Label of the tape volume.
> **Start date:** Starting date of the operation.
> **Start time:** Starting time of the operation.
> **Data size:** Data size written or read by the NSK tape application.
> **Rate:** Transfer rate computed from the time the 1st data block is written/read, up to the unload time.
> **Compr. Ratio:** Compression ratio = user data size / storage size in the BackBox Data Store.
> **En-cryp:** Encryption indication = space, "Decr" or "Encr".

Severity:

> **I** - information, regular emulation
> **W** – warning, error occurred in the emulation, or the volume was manually unloaded
> **E** – severe error
> **VTC:** VT Controller identification

Extracting Statistics for Workstation Reporting Tools

The statistics files used to produce ENFORM reports OBB018, OBB019 and OBB025 are comma-delimited files that can be imported into MS-Excel, MS-Access or other similar database tools. These statistics files contain detailed information and a record per operation. MS-Access or other database tool must be used to produce summaries.

To get statistics in a workstation tool table to import comma-delimited files:

- A NonStop file is prepared by the macro BB030_EXTRACT_STATS.
- The prepared file is downloaded to the workstation.
- A PC tool is used to import the downloaded file as a comma-delimited file.

BB030_EXTRACT_STATS Usage

When extracting either from multiple statistics files or from a single file containing a chosen activity period, the same macro BB030_EXTRACT_STATS (used to prepare ENFORM reports) must be run.

In order to extract statistical data, the user must ensure that Backpak macros are loaded during the TACL session. Macros are located in the domain sub-volume.

Below is a sample of TACL commands that are subsequently devided in three line groups:

```
VOLUME domain-subvol
LOAD /KEEP 1/ BBSETUP MACROS
```

The period to extract must be set by TACL PARAMs:
```
PARAM CUTOFF-TIME hh:mn:ss
PARAM FROM-DATE yyyy-mm-dd
PARAM TO-DATE yyyy-mm-dd
```
This will select activity from FROM-DATE & CUTOFF-TIME (included) to TO-DATE & CUTOFF-TIME (excluded).
A shortcut to set these three PARAMs to the latest 24h period is to run the macro:
```
BB018_DEFAULTS
```

The extraction is triggered by a macro whose parameters set name and format of the extracted file:

```
BB030_ EXTRACT_ STATS  EXTRACT_ FILE  file- name  [,FIELD_ NAMES
YES|NO]
```

EXTRACT_FILE specifies the name of the NonStop file that will be re-created.
FIELD_NAMES YES will generate an extra first line with the name of the record fields (as the workstation import tools can use them).
A control report is generated by the macro sampled in the [BB030_EXTRACT_STATS Usage](#) in the Appendix.

The name of all statistics files matching the file name pattern configured in the domain is printed, with the total number of reads and writes executed.

The written NonStop file is an Enscribe Entry Sequenced file that must be downloaded as a text file.

```
ftp nonstop1
quote site nocrlf on
get $data21.temp.mystat stats.csv
bye
```

Usage in the Workstation Tool

Specify the file as comma-delimited, declared containing field names in 1st line (if extracted with the FIELD_NAMES YES parameter).

In MICROSOFT Access, in addition to checking **First Row Contains Field Names**, change two values in the default Import specifications window, by clicking the **Advanced** button:

Date order must be set to YMD

Date Delimiter must be set to "-"

There is a statistics line per volume of operation; this detail depends on the *Operation_cat* and *Operation* fields.

- A regular tape usage (for example a BACKUP process writing a volume) is reported by a line with *Operation_cat* = EMUL and *Operation* = LOAD. Distinction between backup and restore is given by *Read/Write* field.

EXPORT and IMPORT Operations are related to the VTC attached physical tape drives.

- A line with *Operation_cat* SCRIPT reports the execution of a Windows script. The *Operation* field ports the type of script BACKUP, RESTORE, DELETE.

If the Script Controller is enabled in scripts, there will be additional SCRIPT records: one record with *Operation* = BACK-BATCH or REST BATCH per execution of a sub-script.

Notes applicable in case of Script Controller:

The operation described by a BACKUP operation has no duration, as this execution is only a request for batch processing.
The operation described by a RESTORE operation contains the waiting of an available batch queue and the execution of the whole restore batch sub-script.
The throughput of actual backup or restore of the Windows files can be computed from records with *Operation* = BACK-BATCH or REST BATCH.
These records are not associated with a specific tape volume, as sub-scripts are submitted for a set of volumes. Several columns remain blank.

• Operation_cat LIBR is for tape library specific Operations:

MOVE-IN/-OUT is media moved from/to the I/O slots.
INVENTORY-IN/-OUT are changes detected in the inventory regular BackLib operations.
LABEL is for labelling new media.

All elapsed times are specified in seconds.

Fields with (note 1) have value only for labeled tape volumes used through a TACL TAPE DEFINE.

Report Fields

Field Name	Description	Sample Value for EMUL LOAD	Sample Value for SCRIPT BACKUP
Load_time	Load time	10-Jul-22 17:36:22	2022-07-09 14:33:06
Start_time	Operation starting time	10-Jul-22 17:36:22	2022-07-09 14:35:18
End_time	Operation ending time	10-Jul-22 17:36:37	2022-07-09 14:35:18
Operation_cat	EMUL or SCRIPT	EMUL	SCRIPT
Operation	**EMUL**: LOAD, EXPORT, IMPORT **SCRIPT**: BACKUP, RESTORE, DELETE **STORAGE ADMIN**: MOVE SCRIPT (Script Controller): BACK-BATCH, REST-BATCH LIBR (libraries): LABEL, LOAD, MOVE-IN, MOVE-OUT, INVENTORY-IN, INVENTORY-OUT, EXPORT, IMPORT.	LOAD	DELETE
Severity	**I** when there is no error. **W**, **E** and **F** are possible.	I	I
Domain	Domain name	BPAK	BPAK
Label_prefix	LB (labeled volume), or NL (unlabeled)	LB	LB
Label	Volume label	000264	000321
Label_type	BACKUP,TMF,ANSI,IBM or NL	BACKUP	BACKUP
Exec_time	Total elapsed time	0000015	000000132
Pre-load_time	Unused	0000000	000000000
Loading_time	Elapsed time in VTC to	0000001	000000000

Field Name	Description	Sample Value for EMUL LOAD	Sample Value for SCRIPT BACKUP
	load the volume		
Init_time	Elapsed time - from the time VTC is ready to report the tape drive ONLINE, - to the time VTC detects the 1st data block (i.e. after the processing of tape labels).	0000013	000000000
Data_time	Elapsed time of data blocks transferred. This is the base of throughput computation in OBB018.	0000001	000000132
Post_unload_time	Elapsed time in VTC after the unload	0000000	000000000
Read_byte_count	Number of bytes read by the NonStop host (including tape headers)	320	
Write_byte_count	Number of bytes written by the NonStop host (including tape headers)	52052	00000000000000150
Read_write	READ or WRITE on the virtual volume	WRITE	WRITE
Pre_load	**Y** if the volume was pre-loaded in the restore of a multi-volume backup		
Sequence	Sequence number of a multi-volume backup	1	000
Store	Data Store ID in the Domain Configuration	WIN3	WIN2

Field Name	Description	Sample Value for EMUL LOAD	Sample Value for SCRIPT BACKUP
Store_type	Data Store type (WINDISK or IBM Spectrum Protect™ TSM)	WINDISK	WINDISK
Volume class	Volume class as defined in the Volume Group		BACKUPS
VTC	VTC ID in the Domain Configuration	VTC85	VTC31
NSK_node	NonStop node where the tape device is attached	\MONT	
NSK_device	NonStop tape device	$VT8501	
NSK_access_node	NonStop node running the tape application	\MONT	
NSK_dui	NonStop User ID running the tape application	255.100	
Appl_process	NonStop CPU, pin and creation time of the tape application process	\ETINIUM.1.168 2022-07-15 17:29:43	
Volume_group	Volume Group ID in the Domain Configuration	ARCHIVES	MONT_BACKUPS
Data_size	NonStop data in bytes	52052	52052
Storage_size	Size of Windows file / or total size of IBM Spectrum Protect™ TSM objects	25124	25124
Compr_algo	Compression algorithm: 0 – none 1 – ZLIB 21 – IBM Spectrum Protect™ TSM API	3	

Field Name	Description	Sample Value for EMUL LOAD	Sample Value for SCRIPT BACKUP
Encrypt_algo	Encryption method: 0 – none 1 – NSK CLIM VLE	0	
Media_type	DSM/TC media type: CART3480, LTO3, LTO4 etc..	LTO3	
Compr_algo	Compression algorithm: NONE ZLIB IBM Spectrum Protect™ TSM	NONE	

OBB055 – Low Level Tape to Tape Copy

TACL OBEY command creates a clone copy of a physical tape or of any non-BackBox virtual tape to a BackBox virtual tape. After completion, a clone of the physical tape is created in BackBox with the same label in such a way that no catalog update is needed.
This OBEY file runs the program BB055 that copies any data block and any file-mark from the input tape to the output tape, without any interpretation or validation.
Set the tape drives used in input and output to BLPCHECK OFF.

MEDIACOM ALTER TAPEDRIVE $tape, BLPCHECK OFF

If the previous technology, be it a physical drive or otherwise, has the capacity to automatically process a mount request, once a tape has been processed by BackBox, a mount request may load the same label twice in two drives. It is possible to disable the automatic load in the specific BackBox Volume group that will receive migrated volumes by setting Migration to BackBox to Being prepared in the Volume group configuration.
Create a volume group for each DSM/TC pool from which volumes will be migrated.
Update the OBEY file before submitting.
Syntax:
```
TEDIT OBB055
OBEY OBB055
```

 For a content sample of OBB055 see OBB055 – Low Level Tape to Tape Copy in the Appendix.

Parameters:

BO55TRIGGER When the value is VOLUMELIST, an exhaustive list of volumes to clone needs to be provided in a file. The PARAM VOLUMELIST becomes mandatory and contains the file name where that list is. BB055 will sequentially generate mount requests for each tape on that list. When the value is OPERATORLOAD, the Operator needs to load each tape to clone, manually.

VOLUMELIST Filename. The file "filename" contains a list of volume labels (one per line) to be copied. The format is: *label, type.* Where valid types are BACKUP,AINSI,IBM,OMITTED or NL.

GROUPID name The name of the Volume Group where virtualized copies should be added.

If the string *search* is used as groupid, for each tape loaded, BB055 will look in the DSM/TC catalog to find its tape pools and then it will find the BackBox Volume Group associated with that pool.

For non-cataloged volumes, a valid Volume Group name is mandatory.

INDEVICE Device name for reading.

OUTDEVICE Device name for writing.

IDLEWAIT n In minutes value. Time waiting for volume mounts. Default is 15. Valid values are between 0 and 86400.

TIMEOUT n In seconds value. Time waiting for I/O including rewind. Default is 60. Valid values are between 30 to 600.

MAXNOWAIT n Number of blocks in memory. Default is 5. Valid values are between 5 and 30.

For an execution Sample, TACL Output see BB055 – Execution Sample in the Appendix.

For an execution Sample, EMS Log see OBB055 – Execution Sample, EMS Log in the Appendix.

⚠	• The errors Sense Key Blank check and DSM/TC REPLY ERROR: 100 have no impact on the processing. • With operational errors, the target tape is deleted if already created, and the next tape is loaded. With severe errors, the process stops immediately.

OEMS2 - EMS Messages Display

TACL OBEY file displays BackBox and tape related EMS events. It is recommended when the number of EMS events is very high, especially during BackBox installation.

Syntax:

```
RUN OEMS2
```

For a content sample of OEMS2 see OEMS2 – EMS Message Display in the Appendix.

OEMS - EMS Message Extraction

TACL OBEY file extracts EMS events related to tapes and BackBox.
Update this OBEY file before submitting.

Syntax:

```
        TEDIT OEMS
        OBEY OEMS
```

For a content sample of OEMS see [OEMS – EMS Message Extraction](#) in the Appendix.

TAPEWR – Performance Test

TAPEWR generates and writes blocks of data to the specified TAPE DEFINE with FORMAT U and LABEL ANSI.

TAPEWR does not support multi-volumes output. The data size to write must be 1 MB less than the configured maximum volume size.

For meaningful results, the amount of data to write should be at least a few gigabytes.

Syntax:

```
[PARAM UNLOAD ON | OFF]
[PARAM MAXNOWAIT 5 | number]
[PARAM BUFFERMODE ON | OFF]
[PARAM BACKBOXVOL ON | OFF]
RUN   TAPEWR  =tapeDef  blocksize   SizeToWriteInMB   &   minRe-
cordLenInBytes maxRecordLenInBytes
```

Where

`=tapedef` Specifies the TAPE DEFINE to write to

`Blocklen` Specifies the length of data blocks to write. Same value as the BLOCKLEN parameter in the tape DEFINE.

`SizeToWriteInMB` Number of MB to write.

`minRecordLenInBytes` Minimum record length.

`maxRecordLenInBytes` Maximum record length.

Optional PARAMs below should not be used without consulting ETI-NET support.

> **PARAM UNLOAD ON|OFF** OFF: avoid the volume unload at the end
> **PARAM MAXNOWAIT number** Maximum number of pending IO's
> **PARAM BUFFERMODE ON|OFF** OFF: avoid the execution of SETMODE 99
> **PARAM BACKBOXVOL ON|OFF** ON: verify 'SizeToWriteInMB' against the BackPak configuration and possibly reduce it to limit the size to a single volume. OFF: skip 'SizeToWriteInMB< verification.

For a sample of the TAPEWR - Performance Test see [TAPEWR – Performance Test](#) in the Appendix.

TAPERD – Performance Test

TAPERD reads a tape volume created by TAPEWR.

Syntax:

`RUN TAPERD =tapedef blocklen`

=tapedef Specifies the TAPE DEFINE to read from.

Blocklen Specifies the length of data blocks to read.

For a sample of TAPERD - Performance Test see TAPERD - Performance Test in the Appendix.

Trace Macros

The domain traces can be enabled or disabled. The location of the trace files is specified by modifying the **Domain Configuration** page of the UI. Various files are created at each operation when the trace is on. It is important, therefore, to turn the option off when not needed.

Syntax:

```
LOAD BBSETUP MACROS
LISTT file-name-pattern (list the trace files)
VIEWT file-name (visualize a trace file)
```

For a trace macro sample see Trace Macro in the Appendix.

Microsoft Windows Tools

Specific VTC tools can be accessed from the **Start/Apps Menu** screen or from the Windows **Start** button. Other Windows tools are provided for Windows scripts and documented in *BackBox VTC Scripting Option*.

Accessing Windows VTC Tools

In remote sessions, access VTC Tools via the Windows Search bar, click on **Start** and type "BackPak". All software elements are prefixed by BackPak. The Search dialog window will appear and allow you to choose BackPak version you want to use.
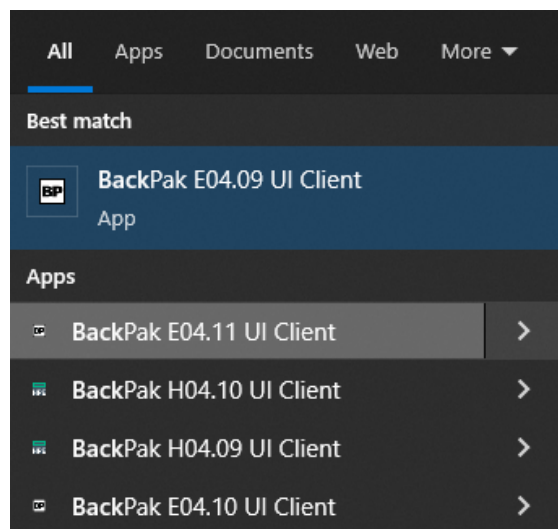
BackPak Collecting ticket information gathers the current VTC logs and configuration information in a zip file. See more in *BackPak Messages Manual and Troubleshooting*.

BackPak Default Folder(Local Disk(C:)\ProgramData\ETINET) points to the root of the VTC specific data folders, including the VTC internal configuration files that are set by the HPE field service engineer.

During a support call, a customer might be asked to browse some of these files.
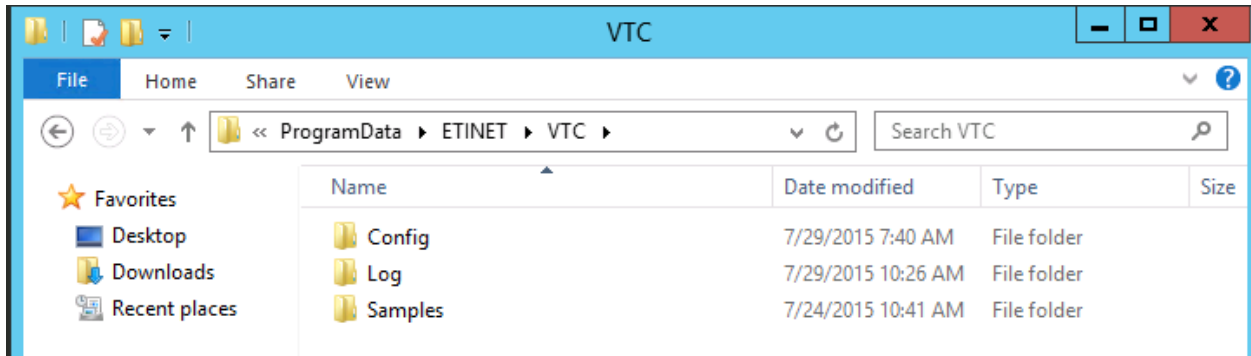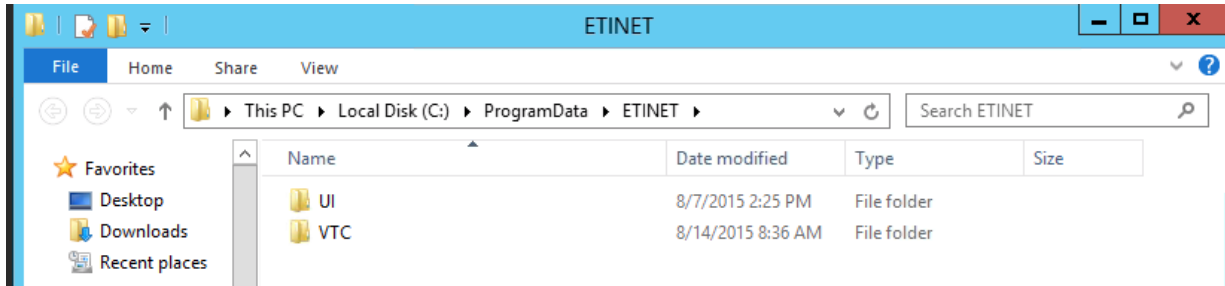
BackPak UI Client is a sub-menu containing the user interface shortcut (UI).

BackPak VTC Management Console starts the console that manages and configures the VTC. See VTC Management Console section.

VTC SOFTWARE COMPONENTS

VTC Server Services

On the VTC server, the following services are installed to provide BackBox functionalities:

VTC Admin

VTC Admin is a service that performs administrative tasks that don't require the FC/SCSI tape emulation connectivity:
- Creates/Deletes Virtual Media.
- Virtualizes/Materializes Physical Media.
- Performs Data Store query status.
- Performs Data Store access for maintenance (Cleanup, Move from Spare Pool to Storage Pool, backup script re-submit).

VTC Emulator (FC)

VTC Emulator (FC) is a service that emulates virtual tape devices over a Fiber Channel connection:
- Emulates Manage tape connectivity.
- Emulates Response device status.
- Handles tape session with the NonStop.
- Handles tape migration with VTS.

VTC Emulator (ISCSI)

VTC Emulator (ISCSI) is a service that emulates virtual tape devices over an iSCSI connection:
- Works only with virtual NonStop with Clim L19-03 or later (which supports iSCSI).
- Emulates Manage tape connectivity.
- Emulates Response device status.
- Handles tape session with the NonStop.

VTC Asynclog

VTC Asynclog provides asynchronous communication services with the BackPak Domain Server located on the HPE NonStop Server:
- Provides EMS message notification.
- Provides end operation on Virtual Media notification (load, virtualization, materialization, move).

VTC Script Controller

VTC Script Controller provides Windows scripts batching packages for the Enterprise Software Backup.

VTC Management Service

VTC Management Service provides management services to VTC Management Console UI.

VTC Configuration

This folder contains internal VTC configuration files. Other than the port emulation configuration file (**BBFcEmulPortCfg.xml**), these files should not be changed before communicating with ETI-NET support.

QoreStoreCfg.XML is a QoreStor-specific file that contains basic QoreStor configuration for VTC MC. If there is no QoreStor system set up for the domain, the file will not be part of the VTC configuration file.

The security configuration folder allows file reading by any user, but restricts changes to Local Administrator group users.

The following file descriptions are given for documentation purposes only and it does not need to be changed. The list of Edit tools are:

- **VTCMC** - the user interface VTC Management Console.
- **BPUI** - the user interface BackPak UI.

File	Description	Edit Tool
CommonServicesCfg.xml	Parameters common for VTC Admin and VTC Emulator (FC) services. Changes are used only when the service is restarted.	**VTCMC**
BBAdminAppCfg.xml	Parameters for the service VTC Admin. Changes are used only when the service is restarted.	**VTCMC**
BBFcEmulAppCfg.xml	Application parameters for the service VTC Emulator (FC). Changes are used only when the service is restarted. The service must be restarted only when the NonStop tape devices are stopped.	**VTCMC**
BBFcEmulPortCfg.xml	Emulation parameters for the service VTC Emulator (FC), such as changing the emulated device type LTO3 to LTO. Changes are used only when the service is restarted. The service must be restarted only when the NonStop tape devices are stopped.	**VTCMC**
BBIscsiEmulAppCfg.xml	Application parameters for the service VTC Emulator (ISCSI). Changes are used only when the service is restarted. The service must be restarted only when the virtual NonStop tape devices are	

	stopped.	
BBIscsiEmulPortCfg.xml	Emulation parameters for the service VTC Emulator (ISCSI), such as changing the emulated device type. Changes are used only when the service is restarted. The service must be restarted only when the virtual NonStop tape devices are stopped. Supported tape format LTO6.	
BBSL.opt	Data Store parameters for the service VTC Virtual Tape Devices. Changes are used for the next tape load. Supported tape format LTO6 or V505 (emulation used by vNonstop)	
Profile2.xml	Domain Address list and TLS/SSL parameters.	**VTCMC** or **BPUI**

BBSL.OPT File Content

Keyword	Description	Default
COMPRESSION_LEVEL	0 to 9 Parameter for STRONG compression 0 = disable compression 1 = best speed 9 = best compression	**6**
CONSOLE	0 or 1 Redirect trace files on the console.	**1**
MAX_OBJECT_COUNT	Number of IBM Spectrum Protect™ (TSM) objects. Used only for IBM Spectrum Protect™ (TSM) API Data Stores Maximum number of IBM Spectrum Protect™ (TSM) objects for a virtual volume.	**10 000**
MAX_KEEP_ALIVE_WAIT_ SEC	Number of seconds. Used only for IBM Spectrum Protect™ (TSM) API Data Stores. Time between two keep-alive procedures.	**45**

PARTIAL_OBJECT_RETRIEVE	1 – enabled; 0 – disabled. Used only for IBM Spectrum Protect™ (TSM) API Data Stores Must be disabled to enable the IBM Spectrum Protect™ (TSM) compression or IBM Spectrum Protect™ TSM Encryption by the IBM Spectrum Protect™ (TSM) API library.	**Disabled**
SYNC_DEPTH	Number of buffers for asynchronous processing of input SCSI commands.	**50 (if SCSI)** **100 (if FC)**
TRACING	Value 0, 1, 4, 8, 12 or 16. When active, it will create a file for each Virtual Volume loaded. The volume name will be used as a file name. No trace will be activated in the FcLog.log file. All trace Levels are cumulative and are similar to verbose functionality.<table><tr><td>Level</td><td>Description</td></tr><tr><td>1</td><td>Trace management activity does not produce any trace at each block of data</td></tr><tr><td>4</td><td>Level 1 + minimal data per data block</td></tr><tr><td>8</td><td>Level 4 + data block description</td></tr><tr><td>12</td><td>Level 8 + function call and call context description</td></tr><tr><td>16</td><td>All of the above + debugging values</td></tr></table>	**0**
WARNONLY_TRUNCATE_DATAFILE	Processing when a data file is detected truncated: 0 = the load request is rejected 1 = the load request is accepted and data file reading is attempted	**1**

VTC Performance Monitor

The VTC Server software integrates the standard Windows Performance Monitor.
Counters can be measured per Virtual Tape device, per Port, or per VTC.

VTC Performance Counters

Counter Name	Description
Host Bytes Read/sec	Number of data bytes read per second by a host.
Host Bytes Write/sec	Number of data bytes written per second by a host.
Host Read/sec	Number of reads per second by a host.
Host Write/sec	Number of writes per second by a host.
Host Avg. Bytes/Read	The average number of data bytes per read by a host.
Host Avg. Bytes/Write	The average number of data bytes per write by a host.
Host WriteMark/sec	Number of file marks written per second by a host.
Host Other CMD/sec	Number of SCSI commands per second that are not Read, Written or WriteMarked by a host.
Host Sync CMD/sec	Number of synchronization orders received to flush buffered data into the virtual media.
Device Buffered Queue Length	Number of Writes and WriteMarks currently in process.
Device Ready	Indicates if the device is ready (a virtual media is loaded).
Host Avg. Time I/O/sec	The average time passed to answer host I/O per second.
Device Avg. Time I/O/sec	The average time processing host I/O to be ready to perform Storage I/O.
Storage Avg. Time I/O/sec	Percentage of time waiting for a Storage I/O to be completed.
Storage Bytes Transfer/sec	Number of data bytes transferred per second.
Storage I/O/sec	Number of storage I/O per second.
Storage Avg. Bytes Transfer/I/O	The average number of data bytes transferred per I/O.
Storage Queue Length	Number of I/O pending to storage.
Device Avg. Bytes Compression	The average bytes compression ratio.

USER INTERFACE

Each page of the user interface contains the following elements:

Windows Title: contains the BackPak Domain ID.
Windows Menu: provides access to the main menu items.
Window Button Bar: provides access to a subset of the main menu items.
Tabs: provide access to sub-functions of the selected menu item.
Current Tab: the current page has a standard banner in the upper left corner and provides access to the current functionalities.
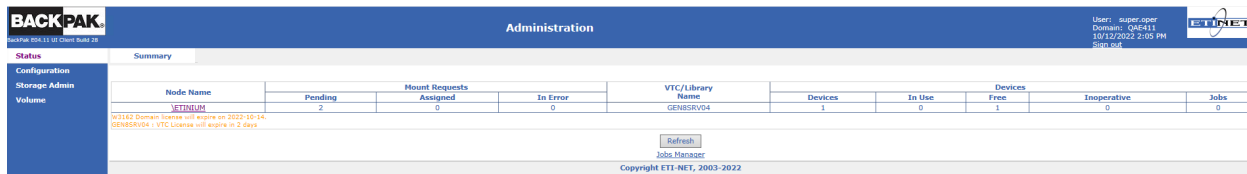
Windows title

An instance of the BackPak interface can connect to a single Domain at any time.
The domain ID (NGH410, in the screenshot above), user ID, and the connecting time are displayed in the page title.

Windows Menus
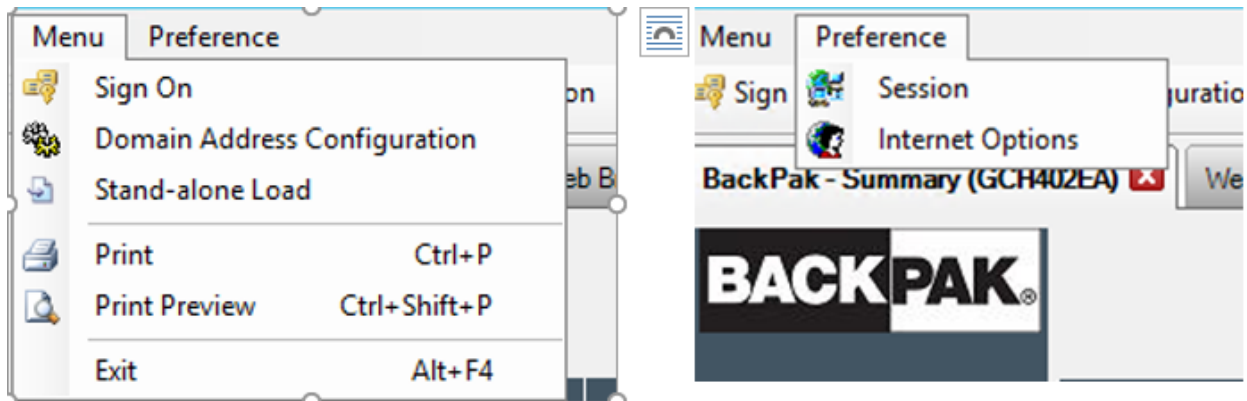
The menus above are used during the BackPak UI installation, but they can be accessed anytime to modify session preferences, Internet options, to sign on as another user, to modify the **Domain Address Configuration**, or to set up a **Stand Alone Load**.

Buttons Row

The three first buttons are BackPak specific; the remaining buttons are standard Windows buttons (**Back**, **Forward**, **Stop**, **Home**, **Print**, **Print Preview**).

The **Sign On**, **Domain Address Configuration** and **Stand-alone Load** pages are documented below.

Banner

The Banner is located at the top of each page and displays the BackPak logo and information about the current session.
Below the BackPak Logo: the UI release and build number.
On the right-hand side: user ID, Domain name, computer time, and Sign Out link for exiting the session.

Navigation Bar

The navigation bar is located on the left-hand side of the page. It allows access to the main functions of the user interface. The selected tab is highlighted.
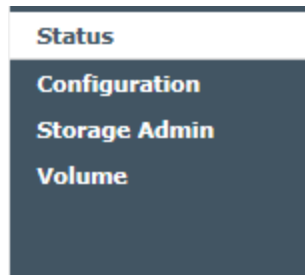
Tabbed Pages

When a page has more than one section, tabs across the top of the main page provide easy navigation between subsections. Each tab is highlighted when selected.

Domain	NSK Nodes	VT Controller	Key Manager	Data Store	Volume Group

Data Grids

In configuration mode, information is displayed in data grids (except the Domain page).
The grids allow the user to view, edit, delete any row of data, or to access additional information pages (such as **Volume Group Information** or **Advanced information**).

VT Controller ID	Status	Physical Location	TCP/IP Address	Comment		
TOUTATIS	Disabled ⌄		192.168.20.210		Advanced	Delete
ASTERIX	Enabled ⌄		192.168.20.88		Advanced	Delete

To edit a value:

1. Click **Switch to Edit Mode** button.
2. Click on the node, controller, library, data store or volume group to open the values menu, type the new value or choose an option from the drop-down list.

NSK Node Name	Profile	
\ETINIUM	DEFAULT	Delete

NSK Node Name*: \ETINIUM ▾

Profile*: DEFAULT ▾ [New Profile] [Delete Profile]

Profile Name*: DEFAULT

Tape IOP CPU Affinity: Preferred ▾

BBEXT Configuration

IO Timeout: 600 seconds

EMS Filter: EMSFILT1

Trace: ☐

Retry Control for Volume Load Failures

Error category	Maximum number of retries (-1 = infinite retries)	Delay between retries (seconds)
No available tape device (busy condition)	-1	120
Other failures or Busy condition retries exhausted	-1	900

[Update]

3. Click **Save** to accept the changes or **Cancel** if you wish to cancel.

> ⚠ The **Update** button does NOT save the change(s); it only updates locally and validates the inputs. **Save** will store the changes on the Nonstop configuration.
> Changes are not saved if you click **Cancel**.

Sign In/Out

Sign In

A successful sign in to the Domain Manager is required before accessing the BackPak functionalities. To sign in, the user must identify the BackPak Domain and must enter the credentials (user ID and password) for NonStop Guardian.

1. For single sign-in, the user needs to authenticate with Guardian User ID and password to the selected domain.

2. For two-factor authentication, the user logs in with User ID, password AND a PIN number (that is provided by the third-party).

⚠	If you need to reset the PIN number send a query to the third-party provider. The provider will generate a new PIN number for you.

A successful log in will display the main Status page. The behavior and the layout of the UI are the same regardless of the user's permissions.

⚠	If the Extractor is restarted while a UI session is in progress, any operation performed through the UI will be prompted with the error message "Invalid Session Token" (*example: E3525 Invalid Session Token: 497cae41d0f16a1b25a0487d62006910b326821d received from WEBUI for user:*). The user should log back in.

Page Elements

Domain: The Domain Name selected for the session. Domain addresses are managed using the **Domain Address Configuration** page.

Guardian user ID: A Guardian user name (group.user) who is configured for the domain.

Guardian Password: The Guardian password associated with the user ID.

⚠	Password is limited to 80 characters. If longer than 80 characters, the application will prompt an error message.

PIN: PIN number is provided by third-party authentication server. It may be required for two-factor authentication when two-factor authentication method is chosen. If no PIN provided, the field should be left empty.

Sign Out

Click the **Sign Out** link located on the upper right-hand corner of the user interface page.

Session Timeout

UI sessions are, by default, timed out after 20 minutes of inactivity. Attempts to access the user interface after timeout require a new log-in session. To set a different timeout value (in minutes), use the **Menu Preferences** session.

Session SSL

SSL must be enabled/disabled through the UI (**Preference**>**Session**), along with the other BackPak components. For more info refer to the *BackPak SSL Setup* manual.

Domain Address Configuration

A domain address identifies a BackPak Domain Manager.
Several domains can be identified and their corresponding addresses stored in a local file.
On a workstation, these addresses are bookmarked to ease the access to the domains.

In the VTCMC, domain address configuration is not available for the BackBox UI on a VTC.
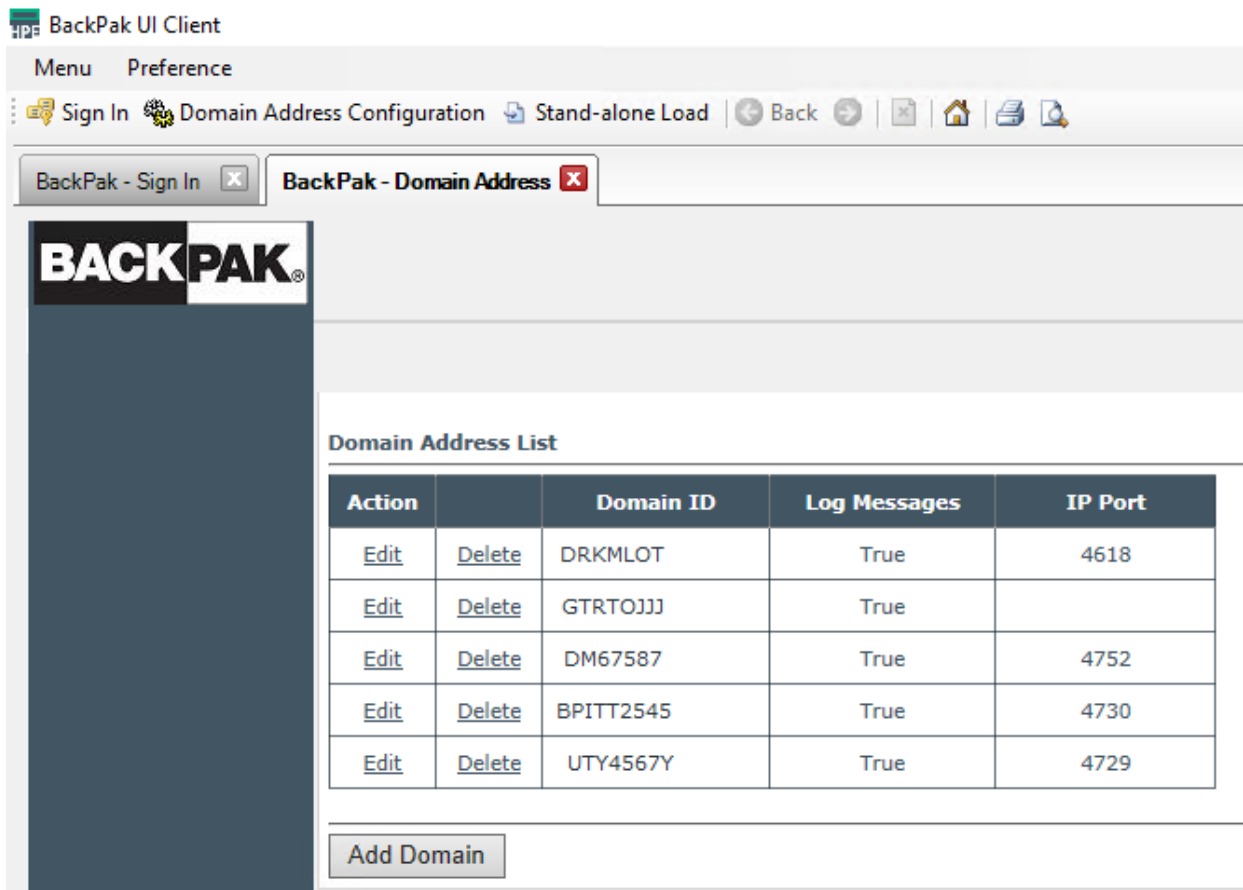
- When installed on a workstation, the **Domain Address Configuration** page allows the user to add, edit or delete a domain address. See *BackPak UI Installation* manual for further details.

- When installed directly on the VTC, the domain configuration is done through the VTC Management Console. See VTC Management Console section for details.

Stand Alone Load

The **Stand Alone Load** allows virtual tape mounting without the Domain Manager when:

- A NonStop is cold-loaded from a virtual SIT tape.
- The Domain Manager is not operational because the catalog (Guardian files VOLUME*) is not available. A tape with a backup of VOLUME* must first be restored.

The following restrictions apply:

- This is a low-level tool that requires the user to enter all configuration information.
- The UI must be running in a VTC directly attached to the NonStop and the tape drive used must be on that VTC.
- The volume is loaded in Read-Only mode.
- Encrypted volumes cannot be used.

The page layout varies depending on the selected Data Store Type.

Stand Alone Load – Common Elements

Port Type: FC or iSCSI
Port Number: Identifies the port number in the VTC internal configuration.
Target ID: The method by which individual devices are identified on the storage. The Target ID is the ID associated with each disk or chassis location. For the FC port type, the Target ID value is "0" by default and it's hard-coded (grayed out).
Lun: SCSI LUN ID assigned to the Guardian tape device by SCF (FC connections). Lun is a Logical Unit Number that can be used to refer to an entire physical disk, or a subset of a larger physical disk or disk volume.
Volume Label: Volume Label to load.
Label Type: Volume label type (value are ANSI, Backup, TMF, IBM or No-label).
Data Store Type: IBM Spectrum Protect™ TSM (TSM-API) or Windows data store (SMB/CIFS).
Volume Lock: Check box that locks the volume and prohibits the volume data to be updated by a tape application. It is equivalent to the lock found on physical media.
Unload Tape from Device Prior to Load Operation: This avoids inopportune unload commands that may abort a tape operation that is in progress.
The check box should be left unchecked, unless the user gets an "already in use" message and is able to confirm that no other user or application is using the device.

Stand Alone Load - Windows Data Store

⚠	For QoreStor Data Stores choose **Data Store Type**: Windows.

Port Type: For iSCSI port type, the available devices are listed under Target ID.

Target ID: Select the device (Target ID) from the drop-down list. These devices have to be previously added on the VTC MC to be listed under Target ID. For more details on adding devices see

User Account: User account to access the Windows disk pool.

Password: Account password.

Fully Qualified Path of the Index File: Name of the path containing the virtual media index file (*.IND file).

Stand Alone Load - IBM Spectrum Protect™ (TSM) Data Store

The page elements are similar to those for the Windows Data Store with a few specific features fields:

Client Option File*: Name of the path containing the client user option file (`dsm.opt` on Windows systems and `dsm.sys` on UNIX systems)

IBM Spectrum Protect™ (TSM) Filespace: Name of the group of files stored as a logical unit in a IBM Spectrum Protect™ (TSM) server.

Status Pages

Once logged into BackBox UI, the application opens with the **Status Summary** page.
This page displays the list of NonStop nodes and a summary of current operations.
This **Status Summary** is an overview of all operations in all nodes included in the domain.

- More detailed info for each device and mount can be queried for a specific node on the Status for NonStop node page.
- The detailed reports can be generated for both NonStop MEDIASRV process and VT Controller(s).

Home – Status Summary

This page displays:
- the list of NonStop nodes with their virtual tape devices
- information related to monitoring current operations

- warnings if the EMS Extractor is not running.
- link to the **Job Manager** page

⚠	The **Status Summary** gathers information from the OPER file that is updated at each load processing. This has very little impact on response time when a VTC is down. However, if the EMS Extractor is not running, MEDIASRV will still be accessed and all VTCs will be contacted with potentially long response time, if there is a TCP/IP timeout caused by a non-responsive VTC.

Job Manager link displays a list with all the job details currently available for each data store.

| ⚠ | If no job details are available, the job summary page will display the following message.

 |
|---|---|

You can use the **Job Manager** page to drill down specific info related to jobs, such as:

- **Data Store** name
- **Action** tha has been performed (type of job)
- **Start Time** (date and exact time)
- **Status** of the job
- **Total to Process** - number of files to be processed
- **Successful-** number of successully processed files
- **VTC Executor**- the name of the VTC Executor
- **% Progress**- job progress in percentage
- **Details** about the data store
- **Failure Reason**, if any job failure.

⚠️	Copy-Non-Copy file process cannot be started while other processes, such as Migration or Spare Move, are still running.

Use the **Search** feature to look for certain info based on search criteria. Type in the info you are looking for (partial or complete criteria); the returned results will be listed from the most recent.

Select the number of entries per page if you want to display 10/25/50/100 job entries.
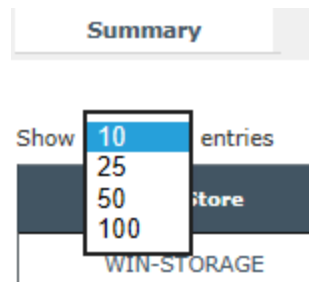
For job details and action status check the section [Jobs: Displays the status of jobs associated with the Data Store](#)

Status for NonStop Node

This page shows the detailed operational status for a NonStop node, both from the NonStop and the VT controller point-of-view. This page opens up in a separate dedicated window.

Page Elements

Mount Requests

Mount requests appear only if there are pending mounts in $ZSVR or if there are any BackBox generated pre-loads on pending.

All pending mount requests are displayed, including requests for tape volumes (such as physical tape media) that are unknown in BackPak.

NonStop View

The left part of a row shows the attributes of the mount request as seen by MEDIACOM.

> **Mount ID**: Tape mount ID as reported by MEDIACOM.
>
> **Device**: Guardian tape device specifically requested to load the volume.
>
> **Volume**: Volume label to be mounted or SCRATCH if the NonStop application requests a SCRATCH volume.
>
> **Label Type**: Requested volume label type. Values are ANSI, BACKUP, IBM, TMF and Unlabeled.
>
> **Tape Use**: Mount request tape use, IN or OUT.
>
> **Message**: Volume mount message.

BackPak View

The right part of the display shows the attributes of a mount request managed by the BackPak Domain Manager.

> **Volume in Domain**: Whether the volume is known by the domain or not.
>
> **Request Type**: $ZSVR for regular mount requests seen in MEDIACOM,
>
> PRELOAD for requests generated internally by BackBox.
>
> PRELOAD is a special BackBox feature for optimizing multi-volume restores. It is rarely used.
>
> For more info refer to Volume Group configuration
>
> **Load attempts**: Number of attempted loads.
>
> **Mount Status**: Request internal status:
>
> PENDING - Waiting for load completion

NO RESOURCE - a resource (drive, disk space) is not available

FAILED – last attempt failed for reason other than 'no resource'

LOADED – load internally completed

LOADING – load being processed, ex: a restore script is running

NO MORE RETRY – maximum number of retries set for the NSK Node in the Domain configuration.

Assigned device: Tape device assigned by BackPak for a loaded or loading request.

Details: Open a mount request detail window.

VTC Tape Devices

This list contains all devices that are configured on the current domain.

NonStop View

The left part of a row shows the attributes of the device as reported by MEDIACOM.

Device: NonStop device name.

Device type: Device type recognized by the NonStop tape system: CART3480, LTO2, LTO3, LTO4, and LTO6

Device status: Device status as reported by MEDIACOM, i.e. FREE, IN-USE, DOWN …

Volume: Volume label recognized by $ZSVR.

Label type: Label type processing.

VT Controller View

The right part of a row shows the attributes of the device as managed by the VTC.

VTC Name: Name of the Virtual Tape Controller

Port: Port type and port number (ex: SCSI-2, FC-0).

TID/Lun: For SCSI or BRIDGE port: Target ID Device. For iSCSI Target ID: iSCSI-1. For FC port: Lun.

Volume: Virtual volume ID, equal to the volume label for labeled volumes.

Device State: Internal device state set by the VTC.

NOT CONFIGURED – not configured on the VTC.

ACTIVATED – initial communication received from the NonStop, but SCF START TAPE not received.

INACTIVE – not polled by the host for three minutes

FREE – operational and free

LOADED – internal load completed, reply READY to host polling

LOADING – the load is being processed (a restore script is running)

UNLOADING – volume unload is being processed

LICENSE LIMIT – the port exceeds the license key limitations

NO REPLY – the VTC did not reply to the status request

DOWN – the physical port is down

Load time: Load request timestamp.

Init Time (sec): Initialization time up to the first data block transfer in seconds. This interval includes:

- the time spent internally to load the volume
- the time spent by the NonStop tape system to detect the READY state and recognize the label
- the delay between the completed tape OPEN and the first tape IO on a user data block.

Throughput (MB/s): Data throughput since the first user data block. Init time is excluded from computation.

Write Bytes: Quantity of data written since the volume was loaded. Includes tape labels.

Read Bytes: Quantity of data read since the volume was loaded. Includes tape labels.

Encryption / Decryption: When the Encryption is in effect. This is shown only when Encryption is licensed.

Action: Unload will immediately unload any virtual volume loaded on the device.

If a tape application is using the device, this action is equivalent to a cancel.

Mount Request Details

Click on the **Details** link in the **Mount Requests** table (last column in the table). The pop-up page shows mount request details from both the NonStop and BackBox point of view.

Buttons:

Reject – MEDIACOM REJECT command is issued. The tape application will fail.

Alter – MEDIACOM ALTER command is issued. DSM/TC or TMF will search for another SCRATCH volume.

Load – The load of the volume will be immediately attempted in BackBox.

Close – The window is closed without any action.
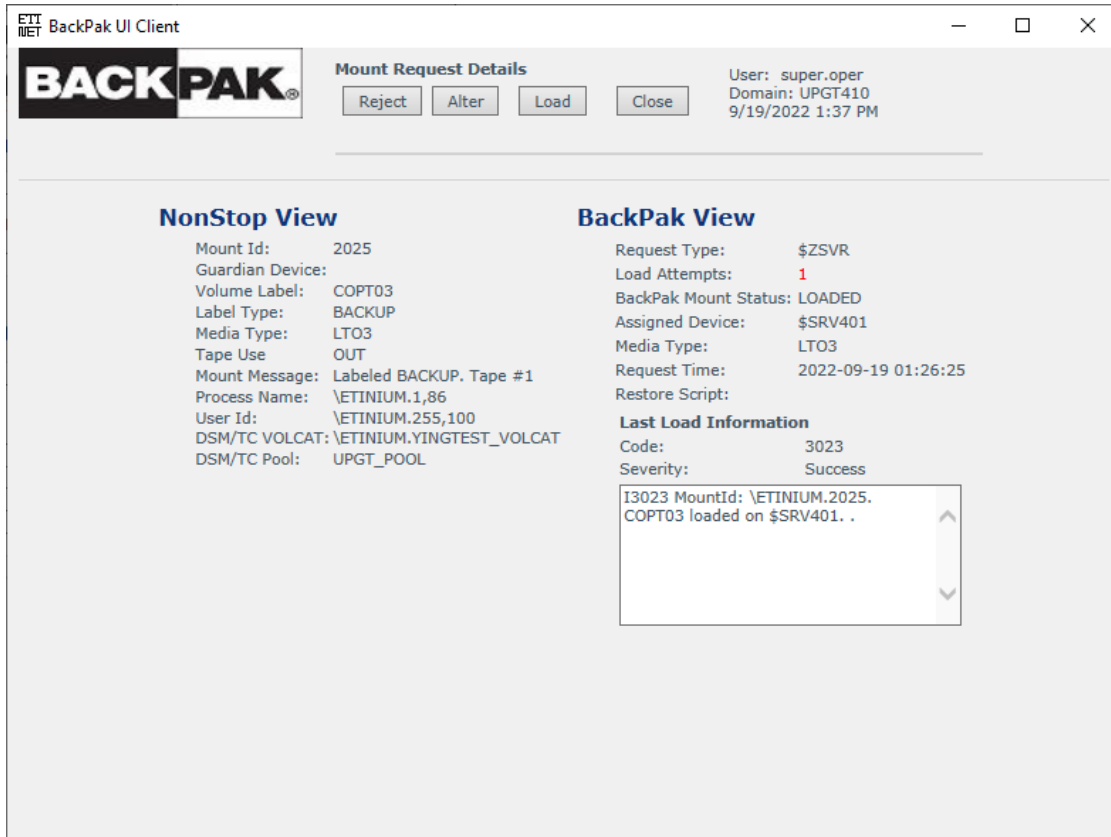
NonStop View

The left part of a row shows the attributes of the mount request seen by MEDIACOM.

> **Mount ID**: Tape mount ID as reported by MEDIACOM.
>
> **Device**: Guardian tape device specifically requested to load the volume.
>
> **Volume Label**: Volume label to be mounted or SCRATCH if the NonStop application requests a SCRATCH volume.
>
> **Label Type**: Requested volume label type. Values are ANSI, BACKUP, IBM, TMF and Unlabeled.
>
> **Tape Use**: Tape usage in the Mount request, IN or OUT.
>
> **Mount Message**: Volume mount message.
>
> **Process Name**: Name of the tape application process.
>
> **User ID**: User ID running the tape application process.
>
> **DSM/TC VOLCAT**: VOLCAT assigned by the TAPECATALOG DEFINE.
>
> **DSM/TC POOL**: POOL assigned by the TAPECATALOG DEFINE.

BackPak View

The right part of a displayed row shows the attributes of a mount request managed by the BackPak Domain Manager.

> **Request Type**: $ZSVR for regular mount requests seen in MEDIACOM,

PRELOAD for requests generated internally by BackBox (for multi-volumes restored with Pre-load option is enabled).

PRELOAD is a special BackBox feature for optimizing multi-volume restores. It is rarely used.

Load Attempts: Already executed load attempts.

BackPak Mount Status: Internal status of the request.

Assigned Device: Device assigned by load processing.

Request Time: Time when the request is known by BackPak.

In addition, the page displays the latest message issued by the latest load processing.

Configuration

The **Configuration** tabs allow navigation through the configuration pages. Any configuration change can be updated and then saved, if in edit mode.

Domain	NSK Nodes	VT Controller	Key Manager	Data Store	Volume Group

Once **Switch to Edit Mode** is activated, a message displays:**EDIT MODE ACTIVE**. You have to click the **Save** button to commit your changes to the Domain Manager.
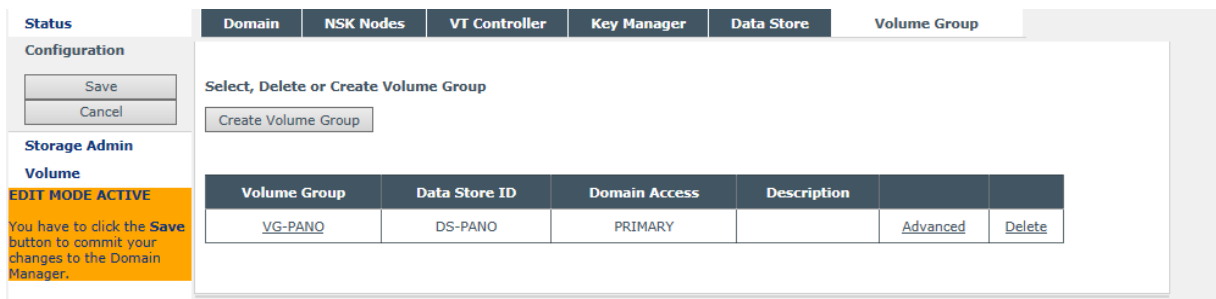
Domain: Configuration of the Domain entity (global parameters).

NSK Nodes: Use to add NSK Node and to assign a configuration profile.

VT Controller: Configuration of VTCs and virtual devices.

Data Store: Configuration of the storage of virtual volumes.

Volume Group: Configuration of how virtual volumes are created.

Domain

The **Domain** page allows making changes to the Domain Manager and tracing configuration.

Domain	NSK Nodes	VT Controller	Key Manager	Data Store	Volume Group

Domain ID*   NGH410E

Location   \ETINIUM.$DATA15.NGH410

Version: H04.AAQ

Release Date: 03DEC2021

EMS Collector* $0   Alerts Setup

EMS Verbose   ☑

Utilities Log $NULL

Trace Level   1

Trace Sub Volume   \ETINIUM.$DATA15.NGH41T

VT Controller Timeout*   300

Stats File Name   \ETINIUM.$DATA15.NGH409.STAT%YY%%MM%

Stats Retention   66   months

Mount Delay Threshold   60   minutes

☑ Run interactive processes under NonStop user ID

```
                    PRODUCTION  LICENSE KEY  number: 210026,  created 2021/05/18  for BackPak H04.09
License Key*        License To     : E5056900
License Details     Site name      : Montreal
                    Expiry Date    : 2022-05-14
                    Enabled products  : BACKBOX: Yes  BACKLIB: No
```

Domain ID*: Unique name of the domain. It must match the Domain name entered in the VT Controller Manager through the Domain Address tab.

Location: Read-only field showing the NonStop installation sub-volume.

Version: Read-only field showing the BackPak NonStop component version.

Release Date: Read-only field showing the release date of the BackPak NonStop component.

EMS Collector*: Guardian process name for the destination of the EMS log messages.

If the process name is not qualified by an NSK node name:

- The Collector process must run on all NSK nodes that have a virtual device configured.
- When an event is related to a specific NSK node, the Domain Manager will send EMS messages only to the NSK node involved.
- General messages are sent to the NSK node running the Domain Manager.
- If the EMS collector is qualified by an NSK node name (i.e. \NODE1.$0); all messages will be sent to this node.

EMS Verbose: When checked, more EMS messages are issued. This should be checked when virtual tape drives are installed or configured. If the EMS verbose check box is checked, the page displays additional information on the processing of pre-load.

Utilities Log: Destination by the Domain Manager (mainly CLIMCMD), for output to the NonStop utilities. The default value is $NULL; the $NULL process is assumed to be started on

each NonStop system. For troubleshooting, the output can be momentarily redirected to any valid collector. If not qualified, the process is used on the node where the query is performed.

Trace Level: The trace may be requested by ETI-NET support personnel to troubleshoot problems; to set the trace level, use "0" for no trace (off) or "1" to activate the trace on the Domain Manager.

> ⚠️ This is reserved for ETI-NET use. The trace creates a significant number of NSK files, which may cause system performance degradation.

Trace Sub Volume: Valid Guardian Disk and Sub Volume where the trace files and some temporary files are created. (Be sure to dedicate a sub volume for traces and temporary files, see Trace Level above).

VT Controller Timeout: Maximum waiting time (in seconds). The Domain Manager waits for a response from a VTC before a timeout.

Stats File Name: Guardian name of the BackBox statistics file. If required, the file will be created. The following wild-cards can be used to change the file name according to the start of the data collection.

%DD% will be replaced by the day number

%MM% will be replaced by the month number

%YY% will be replaced by the year (two digits)

%YYYY% will be replaced by the year (four digits)

The statistics file can be formatted by the OBB018 OBB021 OBEY files.

The default file name at installation is STAT%YY%%MM% in the installation sub-volume.

Stats Retention: Number of months the statistics are kept. The old statistics files are automatically deleted according to their name, if all included activity is older than the configured retention.

Mount Delay Threshold: Delay in minutes, after which the warning message #3373 "*Volume … still not loaded after … minutes …*" is issued to EMS. This warning is issued by the BBEXT program, whatever the cause of delay. This warning is a good candidate to be set as an Alert. See Alerts Setup section.

Run Interactive Processes Under NonStop User ID: Controls the user ID accessing the Guardian processes executing the UI commands.

If the setting is *Enabled* a full Guardian sign-on is executed with the credentials entered in the BackPak sign-on page.

The process owner of BBSV on NSK should be the same user as the logon user (owner of the PROGID program BBSV). When **Run Interactive Processes Under NonStop User ID** is enabled, MFA (Multi Factor Authentication users - requiring a PIN along with the regular log on credentials) signon is not supported.

> ⚠️ In order to enable the signon with MFA, the installer user (the owner of the domain) needs to log in and disable **Run Interactive Processes Under NonStop User ID**. Only when this feature is disabled, any MFA user can log in.

This default setting is *Disabled*: the NonStop user limitations are consistent with the UI user permissions. It doesn't allow the execution of UI commands under the user owning the BBSV program – which must be PROGID.

> ⚠️ All security features are available when upgrading to 4.09 or 4.10.

License Key*: License key number, along with creation date and the product name, as listed in the license file sent by ETI-NET.

License Options: Link to show available licensed options of the BackPak Domain.

Click on **License Details** to access the details page of your domain license.

```
ETI  BackPak-QAE411                                    —    □    ✕
NET

                                              User:  super.oper
BACKPAK.                                      Domain: QAE411
                                              10/12/2022 2:25 PM
BackPak E04.11 UI Client Build 28

                        Copyright ETI-NET, 2003-2022

PRODUCTION  LICENSE KEY  number: 220790,  created 2022/10/12   for BackPak E04.09
License To        : E5056900
Site name         : Montreal
Expiry Date       : 2022-10-14
Enabled products  : BACKBOX: Yes    BACKLIB: No

Data Store types, TSM API (Conduit mode): Yes
                  WINDISK (Disk files)  : Yes
                  Tape library (BackLib): No
WinDisk details
  Optimizations   : DataDomain NAS, VTC internal disk, StoreOnce NAS, FalconStor NAS, Quantum NAS, St
  Storage SNMP    : ignored
  Advanced disk pool is ENABLED
                  Copy Pool Sync: YES (Script controller allowed: Yes)
  Back-end scripts: Generic, TSM, Manual Restore
                  Script controller allowed: Yes
                  Advance Scripting option: Yes

Global options: TMF labels + other labels
                Catalog Sync is ENABLED
                Encryption is ENABLED for VLE and non-VLE (compatibility)
                ComForte SSL is  ENABLED
                Virtualize/materialize media through VTC
                    using standard physical tape drives.   YES
                    using legacy physical tape drives...   YES
                    using direct attached VTS...........   YES
                Virtualize/materialize media through NonStop is ENABLED

NonStop NODES
    Node      System    Run Domain  Virtual  Tape
    name      number    manager     tapes    libraries
    --------  --------  ----------  -------  ---------
    \ETINIUM  078275    Yes         Yes      No

VTC servers:  no limitation on VTCs and numbers of (FC,SCSI,iSCSI) ports,
              no limitation on the number of encryption drives
```
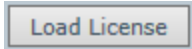
To load a license:

1. **Switch to edit mode** and click on **Load License** [Load License] button at the bottom of thec**Domain Configuration** page.

2. Load the file sent by your ETI-NET representative.
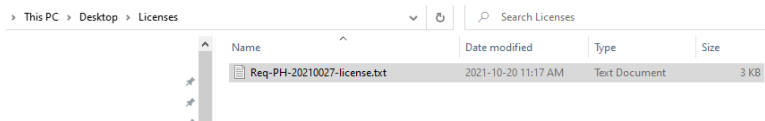
3. Click **Update** [Update] and then **Save** configuration.

License Loaded Successfully! Please update and save configuration.
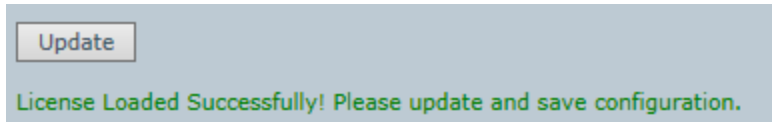
To modify the Domain:

1. Click the **Domain** tab.
2. **Switch to Edit Mode** to change data to specific fields.
3. In **Domain ID** and in other fields, type the changes.
4. Click **Update** to display the new data. In case of invalid data, red error messages are displayed next to the field.
5. Click **Save** to activate changes.

Alerts Setup

To make the monitoring of critical events easier, some EMS messages generated by BackPak can be highlighted and duplicated by an Alert message tagged with a unique event number.

Alerts can be enabled for some pre-defined events or event sets. They can also be enabled for users entering EMS event numbers. For example, if time waiting for a tape mount is critical, the message W3373 (which is just a warning) can be defined to appear highlighted and followed by a Special Alert message: W3373 Mount-id \MONT.2243. Volume VRT15 is still not loaded after 60 minutes. This message will be highlighted in the Viewpoint console. The message will be followed by this Additional message: W3171 Alert triggered by message 'W3373 Mount-id \MONT.2243. Volume VRT15 is still not loaded after 60 minutes.

If a monitoring tool is being used, it is necessary to configure the special EMS message 3171. This single generic message has to be forwarded to all messages in order to be specified by Alert Setup.

By default, all alerts are checked. If you uncheck some of them, click **Confirm** to save the changes. If you click **Close**, the Alerts Setup page will not save the changes.

> **Mount Delay Threshold**: Generates an Alert if a MEDIACOM mount request is not satisfied within the delay configured in the Domain page above (event 3373).
> **Windisk Space Threshold**: Generates an Alert during the production of a report on disk space for a Data Store, if the Data Store is having less free disk space than the configured threshold (event 3217).
> **DSM/TC Catalog Checks Required**: (event 3207).
> **Script Error**: Generates an Alert if error is reported for Windows script execution (events 5025, 5026, 5027, 5028, 5030, 5073, 5105, 5129, 11004, 11014).
> **License Expiration**: Generates an Alert if the BackPak license is going to expire in the next 7 days (event 3162).
> **Scratch Number Threshold**: Generates an Alert if, during the production of a Volume Group summary report, a Volume Group has less SCRATCH Volumes than the configured threshold (event 3313).
> **VTC Critical**: Critical messages from the VTC (events 116, 5104, 5106, 5114, 6008, 6009, 6015, 6016).
> **Message ID #1 to #4**: Generates an Alert if one of the above listed message event numbers is logged.

NSK Nodes

The NSK Nodes page contains a list of all known NSK Nodes and their assigned configuration profiles. By default, only the node where the domain is installed is automatically added. It is therefore important to (manually) add all the required peripheral nodes.

Domain	NSK Nodes	VT Controller	Tape Library	Key Manager	Data Store	Volume Group

NSK Node Name	Profile
\ETINIUM	DEFAULT

⚠	Since version 4.09 each peripheral node is controlled and managed by its own peripheral node license. Licenses are available upon request. Contact ETI-NET support for peripheral node license request.

1. Run the Obey file to start the extractor by specifying where the peripheral node license is located (see the sample below).
2. Modify the indicated line in the sample to point at the location of the peripheral node license.

If there is no peripheral node license, the specified line will be ignored by the extractor.

Sample:

```
$DATA15 BBE410 175> fup copy oext
COMMENT ********************************************************
COMMENT start manually the EMS extractor process
COMMENT ********************************************************
CLEAR ALL
RESET DEFINE *
DELETE DEFINE =BACKPAK_BBSETUP
ADD     DEFINE     =BACKPAK_  BBSETUP,     CLASS     MAP,     FILE
\ETINIUM.$DATA05.BPAK.BBSETUPDELETE DEFINE =TCPIP^PROCESS^NAME
ADD  DEFINE =TCPIP^PROCESS^NAME, CLASS MAP, FILE $ZTC0DELETE  DEFINE
=BBEXT_LICENSE
ADD      DEFINE     =BBEXT_   LICENSE,      CLASS      MAP,FILE
\ETINIUM.$DATA05.BPAK.BBEXTLIC
RUN $DATA05.BPAK.BBEXT /NOWAIT, TERM $ZHOME, name $BBEXT/
```

Node profiles can be viewed and modified (when in edit mode) by clicking on the NSK Node Name. If you want to use a Tape process (tape IOP) on the same CPU where the tape application program is running, select the type of CPU affinity desired in the profile of the NSK node. This option is by default set to active, but it can be disabled or set to mandatory (meaning that, if no tape IOPs are available in the same CPU, the mount request will not be answered).
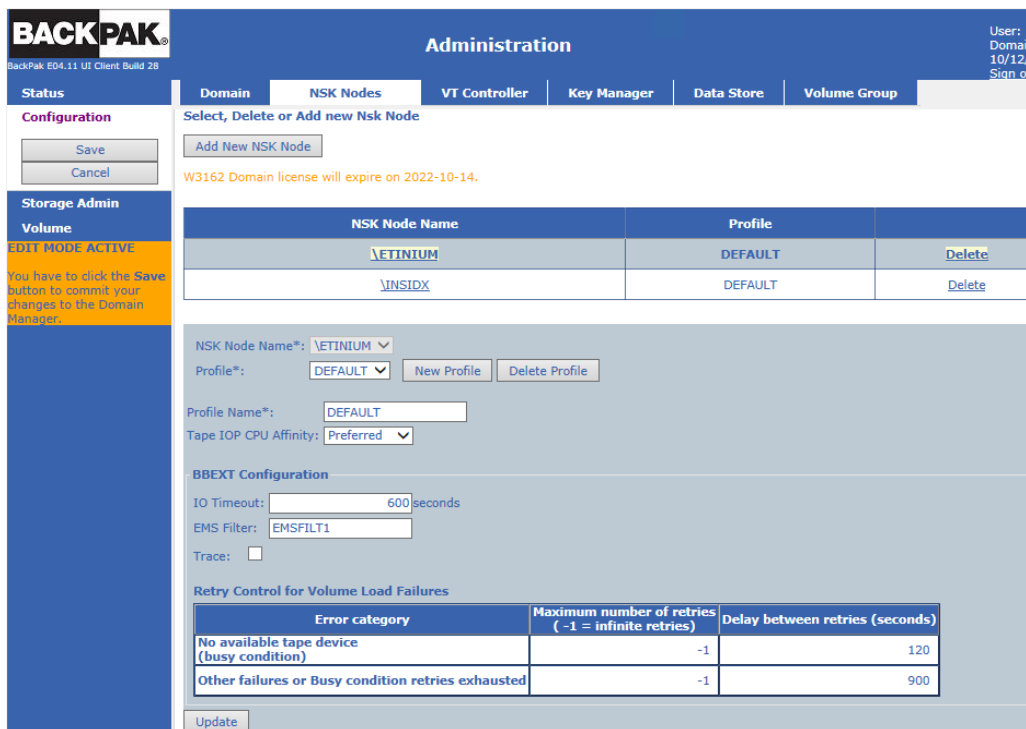
The profile screen now replaces the BBEXT file previously used to configure the values needed by the extractor.

> ⚠️ If the Tape IOP (Input/Output Processor) CPU affinity is set on **preferred** or **mandatory**, a different profile can be specified. This is a new criteria added in the selection of a tape drive for replying to a mount request. BackPak prefers tape IOPs that run on the same CPU as the tape application (BACKUP, TMFDR). This option is by default set to **active**, but it can be disabled or set to mandatory. In this case, if no tape IOP is available on the same CPU, the mount request will not be answered.

NSK Node Name*: Name given by default. It cannot be changed.
BBEXT Configurations that can be changed for a profile are:
I/O Timeout: Maximum wait time in seconds for response from the Domain Manager.
EMS Filter: Filter associated with the node profile. Use the default value.
Trace: Check the box to trigger the saving of trace files and temporary files associated with the process running on BBEXT.
Retry Control for Volume Load Failures: This section shows the error types and the retry time and number of retries for the specified failures.
Maximum number of retries (-1 = infinite retries)

- Value "**0**" is entered to suppress any retry.
- Value "**-1**" is entered to allow an infinite number of retries.

Delay Between Retries (Seconds): Delay in seconds between two retries, to load a volume on a busy virtual device.
No Available Tape Device (Busy Condition): When there is no tape device configured or the configured one is busy.
Other Failures or Busy Condition Retries Exhausted: Maximum number of times a volume load is retried for any other failure or when the busy condition retries are exhausted.

- Value "**0**" is entered to suppress any retry.
- Value "**-1**" is entered to allow an infinite number of retries.

The default profile is created during the installation and it usually fits most configurations.
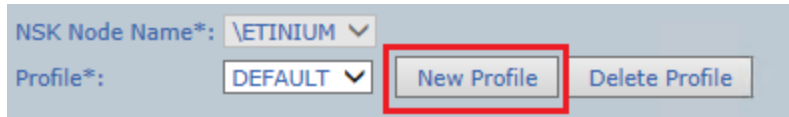
> ⚠️ NSK node deletion is a particular procedure and it should be performed with caution. Refer to Appendix G - Removing NonStop Nodes for details on how to delete an NSK node and data related to the specific node.

Profiles for a multi-node environment

For environments with peripheral nodes (multi-node environment), you can create, delete and assign profiles to nodes.

To add new profile:

1. Go to **Configuration** page.

2. **Switch to Edit Mode** and select the node you want to add new profile to.

3. Click **New Profile**.

NSK Node Name*:	\ETINIUM ∨		
Profile*:	DEFAULT ∨	New Profile	Delete Profile

4. Give a name to the new profile and set up Tape IOP CPU Affinity (**Preferred**, **None** or **Mandatory**).

5. Click **Update and Add Profile**.

To delete profile:

1. Go to **Configuration** page.

2. **Switch to Edit Mode** and select the node you want to delete the profile of.

3. Click **Delete Profile** and **Update** the change.

4. **Save** the configuration to exit edit mode.

VT Controller

The **VT Controller** page allows to configure the VTC. The configuration of a VTC consists of setting up:

- Its TCP/IP address.
- The definition of operational tape drives. BackBox matches the VTC tape configuration with the one obtained from the CLIM and SCF. The VTC and the host definitions are prerequisites. The VTC must be functional and its virtual tapes must be connected in order to allow the configuration in the domain.

The **VT Controller** page shows the list of existing VTCs (if any). If in **Switch to Edit mode**, the button **Create VT Controller** becomes active and a new VT controller can be added.

For the existing VT Controllers, the **Status** (enabled/disabled) can be changed or the controller can be deleted.

To see the VTC properties of a specific VT Controller, click on the VTC listed under **VT Controller ID**.

Top Section: List of all VTCs configured on the current Domain.

Virtual Tape Controller Information: Displays the selected VTC attributes.

Click **Update** to display the change(s) made to this section.

VTC Ports: List all physical ports prepared for BackPak operations inside the VTC. This section is read-only.

Virtual Devices: List the virtual drives already configured in the domain, including their internal status. To add these devices by groups of devices simply select the physical connection of the devices (the VTC port and the NonStop host).

Devices can also be removed from the Domain Configuration individually (individually "deleted").

All devices currently configured in the VTC can be updated globally.

The update is not required after a change to this section.

> ⚠️ Certain data is retrieved from queries to the VTC:
> **General information** such as Host name, OS and Version, and version of BackBox software.
> **VTC Ports**: Lists all physical ports prepared for BackPak operations inside the VTC, as well as their internal status.
> **Virtual Devices**: Lists the virtual drives already configured in the domain, as well as their internal status.

If there is no VTC connected (disabled VTC or the port associated with the configured devices has been removed from the internal VTC configuration), the information listed will be blank.
The **Refresh** button allows VTC query retries.
Some other information that comes from the NonStop host is kept in the BackPak configuration. The host is queried only when tape drives are added or updated through this page.

Host information:
- The host location, SAC name, or CLIM ID.
- The tape device name associated with the port and LUN/Target IDs, presented by the VTC.

Virtual Tape Controller Information

VT Controller ID	Status	Physical Location	TCP/IP Address	Comment	
FALBALIA	Enabled ∨		192.168.20.94		**Advanced**
GEN8SRV04	Enabled ∨		192.168.21.42		Advanced

Virtual Tape Controller Information

VT Controller ID* `FALBALIA`
Physical Location ` `
TCP/IP Address* `192.168.20.94`
Comments ` `

VTC Serial Number: 2M41411CVM
License To: E5056900
Expiration Date: 10/18/2022
Licensed Concurrent Operations:
FC Ports: 2
Encryption Devices: 2
ISCSI Devices: 2

Host Name: FALBALA
Server Model: HP ProLiant DL380p Gen8
System: Microsoft Windows Server 2022 Standard
Service Pack:
Architecture: 64
VTC Version: E04.11.24

VT Controller ID: Identifies the VTC. It must be unique and cannot be changed once added.
Physical Location: Optional information field that describes where the BackBox unit is physically installed.
TCP/IP Address: TCP/IP address or TCP/IP host name used by the Domain Manager to communicate with the VT Controller.
If the license key has restrictions on the allowed VTCs, this field must match one of the VTC entries in the license key.
Comments: Optional information field.

⚠	Click on either the **Update** button to display the changes or the **Exit Update Mode** button to keep the previous configuration. If you make changes and exit the page without updating them, they will not be saved.

VTC Details retrieved from the license key and from the VTC

For versions prior to 4.09, VTC license information for VTC was displayed as a section of the NonStop domain license. VTC didn't have its own license. With 4.09 version the VTC section from the NonStop Domain license has been removed and replaced with the **VTC license**. This more atomic license view simplifies license installation and gives flexibility to setting up license-related parameters.

⚠	If you are using a license acquiared prior to 4.09 release, you can keep using the site license with 4.09 version. **Exception**: QoreStor Data Store or Windows 2019 server OS. For QoreStor Data Store or Windows 2019 server OS a new NonStop license and a new VTC license need to be installed.

VTC Serial Number: 2M41411CVM   Host Name: FALBALA
License To: E5056900   Server Model: HP ProLiant DL380p Gen8
Expiration Date: 10/18/2022   System: Microsoft Windows Server 2022 Standard
Licensed Concurrent Operations: Service Pack:
FC Ports: 2   Architecture: 64
Encryption Devices: 2   VTC Version: E04.11.24
ISCSI Devices: 2

⚠	If **License To:** does not match the name of the Domain License (see License Details) an error message will state that there is a conflict between the License Customer Name and the Domain License Name). In such a case, you can request a change of the license name to match with the domain license name. Request the change by contacting Support.

This sub-section lists the settings allowed by the license key.

> **SCSI Ports**: Maximum number of SCSI ports that can be active at the same time. More ports can be configured and the associated tape devices started for failover purposes.

FC Ports: Maximum number of FC ports that can be active at the same time. More ports can be configured and associated tape devices started for failover purposes.

Encryption Devices: Maximum number of tape devices licensed to be concurrently in use for Encrypted volumes (VLE CLIM or VTC client to Key Manager).

ISCSI Devices: Maximum number of iSCSI connections on the network adapter.

This sub-section lists the settings allowed by the VTC.

Host Name: This is the BackBox server name.

Server Model: Model type server

System: Windows operating system release.

Service Pack: Microsoft Service Pack level.

Architecture: 64 bits.

VTC Version: VTC build level.

VTC Ports

VTC Ports   [Refresh]

Port	Port WWN/Serial #	Status	Speed	Card Module	Card Slot Id/Target IP	Card Channel Id	Host WWN
FC-11	2100001086023B7C	UP	8-Gb	FC-84EN	1	1	50014380331312E8
FC-12	2100001086023B7D	UP	8-Gb	FC-84EN	1	2	51402EC012415CA4
FC-13	2100001086023B7E	DOWN		FC-84EN	1	3	
FC-14	2100001086023B7F	DOWN		FC-84EN	1	4	
ISCSI-1	BBTIS000	UP		V0505 ETINET ISCSI V-Tape	192.168.5.1		
ISCSI-2	BBTIS002	UP		V0505 ETINET ISCSI V-Tape	192.168.5.1		
ISCSI-3	BBTIS005	UP		V0505 ETINET ISCSI V-Tape	192.168.5.1		
ISCSI-4	BBTIS006	UP		V0505 ETINET ISCSI V-Tape	192.168.5.1		

This table shows all target-mode ports installed and configured. Virtual devices can be added in the Domain configuration on these ports only.

When the VTC cannot be reached, only the ports with tape devices already configured are displayed, but the VTC configuration cannot be updated.

Port: VTC internal port identification. Type (SCSI, FC, BRIDGE, RELAY, EXTERN, or iSCSI) and port number.

> ⚠️ iSCSI provides block-level access to storage devices by carrying SCSI commands over a TCP/IP network. This type of protocol allows sending SCSI commands to storage devices (targets) on remote servers.
>
> ISCSI does not require dedicated cabling, switches or cards; therefore, it can be run over an existing IP infrastructure.

Port WWN: FC port WWN or iSCSI Target ID

Status: Port status.

Speed: Nominal port speed.

Card Module: HBA model.

Card Slot Id: Server slot number.

Card Channel Id: Port number in multi-ports HBA.

Host WWN: Host HBA WWN.

Refresh button: Refresh the VTC status.

Virtual Devices

This table shows the virtual tape devices configured for the domain. To add devices, the VTC must be reachable and there must be a link between the VTC and the host HBAs.

The **Add Devices Automatically** tab allows adding devices by automatically mapping Guardian and VTC devices sharing the same physical connection (same host port and VTC port). For FC connection, the user will select a Guardian node name and a VTC port. The UI will identify the host port by the host WWN detected by the VTC.

For a SCSI or BRIDGE connection, the user will also have to select the Guardian Port to fully identify the host port.

The Node will be queried and all tape drives defined in SCF can be added, providing the Guardian Device is set to **All Available Devices**; otherwise, they can be added individually. The UI will automatically match the SCF and VTC definitions by the LUN and Target ID.

The **Add Devices Automatically** tab is used to re-add all tape devices previously configured in the host for this connection. They can also be individually updated.

⚠️	SCSI and BRIDGE automatic connection updates are not supported and will be ignored by this process. To update such connections, all connected tape devices (same VTC port ID) must be deleted individually.

VTC Ports Refresh

Port	Port WWN/Target ID	Status	Speed	Card Module	Card Slot Id/Target IP	Card Channel Id	Host WWN
ISCSI-1	X22C100	UP	-	V0505 ETINET ISCSI V-Tape	172.17.233.36		-
ISCSI-2	X22C101	UP	-	V0505 ETINET ISCSI V-Tape	172.17.233.36		-
ISCSI-3	X22C102	UP	-	V0505 ETINET ISCSI V-Tape	172.17.233.36		-

Virtual Devices

Add Devices Automatically	Add Devices Manually

Guardian Node*   \VNSK6 ⌄
VTC Port*   ISCSI-1   X22C100 ⌄
VTC Device*   All Used ⌄
Guardian Device*   [   ]
Explicit Only   ☐

[Add Virtual Devices]

		Node	Guardian Device	Device Type	Serial Number	Port	Target	Lun	Explicit Only	Reserved For	Host WWN	Status	Guardian Port
Edit	Delete	\VNSK6	$B2C100	LTO6	BB22C100	ISCSI-1	0	0	False	...		FREE	
Edit	Delete	\VNSK6	$B2C101	LTO6	BB22C101	ISCSI-2	0	0	False	...		FREE	
Edit	Delete	\VNSK6	$B2C102	LTO6	BB22C102	ISCSI-3	0	0	False	...		FREE	

Choose the Guardian Node you want to automatically add devices to.

Open the drop-down list for the VTC Port* and choose the appropriate port name. The list contains all Fiber Chanel (FC) and iSCSI devices mapped for the selected Guardian Node.

The **Add Devices Manually** tab allows adding devices by manually mapping Guardian and VTC devices that share the same physical connection (same host port and VTC port).

⚠	Use this technique carefully. Invalid device mapping can result if the wrong information is entered. Adding devices manually should be used only if the host does not respond to queries.

Open the drop-down list for the VTC Port* and choose the appropriate port name. The list contains all Fiber Chanel (FC) and iSCSI devices mapped for the selected Guardian Node.

For FC, SCSI or BRIDGE connection, the user will select a Guardian node name, the VTC port and VTC Device Target, and also LUN. The user has to provide the Guardian device name to complete devices mapping.

		Node	Guardian Device	Device Type	Serial Number	Port	Target	Lun	VLE	Explicit Only	Reserved For	Host WWN	Status	Guardian Port
Edit	Delete	\ETINIUM	$ASTERI0	LTO3	BB02FAE600	FC-23	0	0		False	...	50014380331312E8	INACTIVE	$ZZSTO.#S100231
Edit	Delete	\ETINIUM	$ASTERI1	LTO3	BB02FAE601	FC-23	0	1		False	...		INACTIVE	$ZZSTO.#S100231

Virtual tapes can be updated or deleted individually in the list of Virtual Drives.

Updatable Attributes:

Node
Guardian Device
Port
Target or LUN
VLE
Explicit Only
Reserved For

⚠️ | iSCSI does not support automatic adding of a device. Use **Add Devices Manually** to add iSCSI devices.

Virtual Device Information

Node: Guardian system name.
Guardian Device: Guardian tape device name defined in SCF.
Device Type: Emulation provided by the VTC for this device, CART3480, LTO3, LTO4 or LTO6.
Serial Number: Tape device serial number.
Port: Port type (SCSI, FC, BRIDGE) and number.

BRIDGE corresponds to a SCSI physical port of the NonStop; in this case the port number is the FC port number shown in the Ports table, suffixed by CH1 or CH2 to distinguish the two corresponding SCSI Channels of the Bridge, ex: "BRIDGE-3-CH1"

Target: SCSI Target ID assigned to the Guardian tape device by SCF.

LUN: SCSI LUN ID assigned to the Guardian tape device by SCF.

VLE: VLE is displayed if this device was enabled for VLE Encryption by the SCF ALTER TAPE, KEYGENPOLICY command.

Explicit Only: Select "Yes" to exclude this device from the automatic device assignment provided. This device will be used only when specified explicitly in the command.

Reserved For: Link to the reservations list for this drive.

Host WWN: Host HBA WWN.

Status: Tape drive status in the VTC.

Guardian Port: Display the SAC name or CLIM ID

VT Controller Device Reservations

The **Volume Class List** page is opened when the **Reserved For** link of the VT Controller page is clicked. It lists the volume classes configured in Volume Groups and permits device reservation for one or several volume classes.
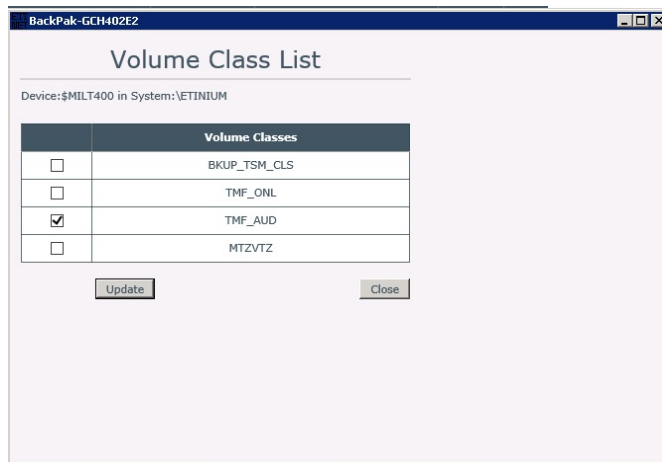
Device: Identifies the device.

Volume Class: Shows the volume class list. Check the classes for which the device must be reserved.

If no class is checked, the device is available to volumes belonging to any volume class.

VT Controller Advanced Properties

Top Section: Lists all VTCs configured in the current Domain, even when no VT Controller is selected.

Advanced Properties: Click **Update** to the display the changes made to the **Advanced** properties section.

Advanced Properties

SSL Proxy Ports

If the SSL Proxy Ports are not modified, the default values will be used.

SSL Proxy Ports: Check if the HP SSL Proxy is used to connect to the VTC.
The TCP/IP Ports for VTC services might have to be modified if the VTC is reached through the HP SSL Proxy. This is the case when several VTCs are in the domain: all VTCs are configured with

the same address of local proxy (127.0.0.1). To reach different VTCs, all port numbers configured in the local proxy clients must be different.

Admin TCP Port: Port for the Admin service.

8766 is required if the VTC is not reached through the HP SSL Proxy.

VTC Emulator (SCSI) TCP Port: Port for the VTC SCSI Emulator service.

8765 is required if the VTC is not reached through the HP SSL Proxy.

VTC Emulator (FC) TCP Port: Port for the VTC FC Emulator service.
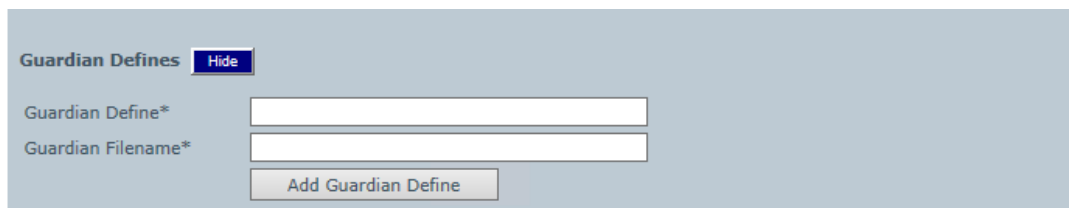
8764 is required if VTC is not reached through the HP SSL proxy.

VTC Emulator (ISCSI) TCP Port: Port for the VTC iSCSI Emulator service.

8767 Port for VTC Emulator (ISCSI).

Guardian Defines

This section allows redefining the TCP/IP Guardian environment provided by the TCP/IP LISTENER to the BackPak Domain Manager.

DEFINE is used when the Domain Manager communicates with the VTC. If a DEFINE is specified in this section, all TCP/IP Defines passed by the LISTNER are deleted in the process context, then the TCP/IP Defines configured here are created before accessing the NonStop socket interface.

For more information, please consult the Guardian TCP/IP Configuration Manual.

> **Guardian Define**: Valid Guardian environment variable name (define) supported by the TCP/IP stack, such as =TCPIP^PROCESS^NAME and =TCPIP^HOST^FILE.
> **File Name**: Value associated with the Guardian Defines.

Physical Tape Device Attached

This section allows declaration of physical tape devices attached to the VT Controller to use for virtualization/materialization operations.

The user chooses the devices that will be used for Virtualize/Materialize operations from the list supplied by Windows.

> **Alias**: Symbolic name to identify the tape drive. The name must be unique.
> **Vendor, Product, Version and Serial number**: Attributes returned by the device.
> **Bus, Target ID, Lun**: SCSI or FC address of the device reported by Windows.
> **Status**: Current status of the device.

Device Protocol: Reports if the tape drive is a Standard device handled through a Windows driver or if it is a *Legacy* drive handled in raw mode. Operation of legacy drives requires a license option.

Data Store

The Data Store page contains information about the storage configuration for the virtual tape volumes. The initial view shows the list of existing Data Stores. If in edit mode, **Create Data Store** button and **Delete** are available.

Click on the **Data Store ID** link to see additional information about that store.

Data Store Information: Data store properties.
Windows Details, Windows Pool: Windows disk data store properties
Storage Route: For the selected Data Store, list of the VTCs that can access the storage.

⚠	To delete a BackBox VTC from the storage route list is not supported.

QoreStor Storage Route   Add   Verify Configuration

	VT Controller ID*
Delete	BBPROD

Could not delete this route, it's a QoreStor route.
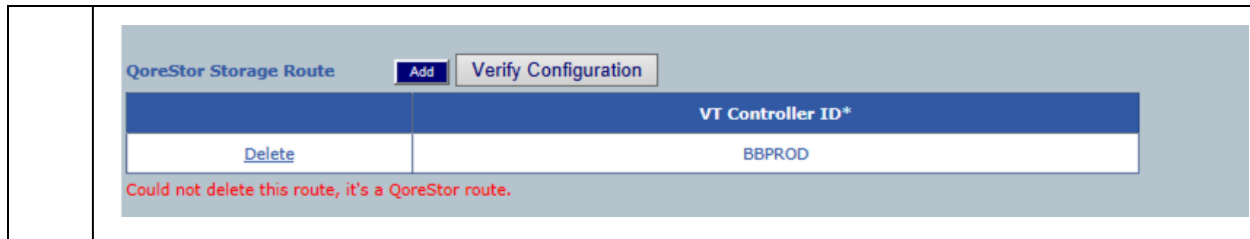
Data Store Information

Store ID: Identifies the Data Store. Must be unique and cannot be modified after it is added.

Data Store Type: Cannot be modified after it is added. Refer to the related section in the Configuration chapter for details.

WINDOWS FILE: To store virtual volumes in the Windows file system or in a compatible remote file server.

QORESTOR: To store virtual volume in embedded CIFS NAS. For the domain QoreStor data store is very similar of a Windows data store.

TIVOLI STORAGE MANAGER: To store virtual volumes on a IBM Spectrum Protect™ (TSM) server.

Status: Indicates whether the Data Store volumes can be used.

ACTIVE: Default, no restriction to volume operations.

INACTIVE: Tape volumes cannot be loaded to be read or written. Automatic operations such as the free-up of expired storage are disabled.

As an exception, catalog Export/Import functions (Catalog Sync) are still active.

Domain Access to Data Store: Qualifies the ownership of the Data Store virtual volumes.

PRIMARY: This is the usual value. The current domain owns and manages the Data Store, writes and reads virtual tapes.

> ⚠️ This value is equivalent to "OWNER" in previous BackBox versions.

SECONDARY: The Data Store is being prepared for Disaster/Recovery, receiving updates to the BackPak, and DSM/TC tape catalogs. The domain has a read-only view of the Data Store and cannot execute backups.

RESTRICTED: The Data Store is an alternate view of a Data Store owned by another domain.

The Data Store is read-only and the DSM/TC and TMF tape catalogs will not be modified; they should remain as configured. The user must manually register the volumes in the BackPak catalog.

Primary Data Store ID: Identifies the source PRIMARY Data Store ID.
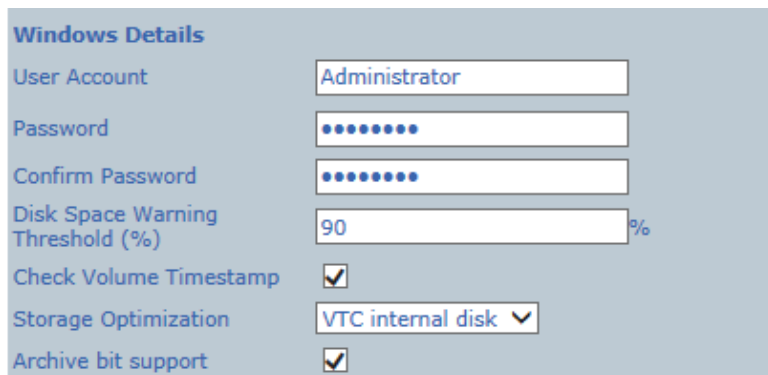
Available only for a SECONDARY or RESTRICTED Data Store, pointing to virtual volumes copied from or shared with an original PRIMARY Data Store in another domain.

When configuring Data Stores pointing to the same data or to copies of the same data, it is convenient to give them the same ID. The Primary Data Store ID allows linking the two Data Stores, even if they don't have the same ID.

Description: Optional user description.

Administrative Link: Optional URL of an administrative client for the Data Store (available only for IBM Spectrum Protect™ - TSM Data Store Type).

Data Store – Windows/ QoreStor Data Store type-Access Protection

Password: Data Store is password protected to ensure secure access to data. The password gives the user log-in access to the server.

For a given user, there are two ways of updating the password:

1. Use the UI password field to update the password.

2. Go to the NonStop and update the password through BB004_PASSWORD_UPDATE macro function.

The user Account can be either a **domain user** or a **work group user**. All I/O performed by the VTC for this data store will be done under that user security.

For **Active Directory** user- the VTCs , NAS (including QoreStor embedded NAS) need to join the domain. The user password is managed by the Domain.

To verify the path access to data stores, use the **Storage Administration** page.

⚠	In the example below, for two different Storage Routes (ETI4DISK and OBELIX) the access to the data stores (paths) have been verified and the Path Status has been tagged as Good. The paths with errors are tagged in red with the error code description.

DS_1COPY_DD Administration

Data Store DS_1COPY_DD

Storage Route   First Available VTC ▾   Reply from: BBOX2019-1   [Refresh]

Pool	Free Space(MB)	Number Of Files	User Data Size(MB)	Non-Backed-Up Files	Last Update
Storage - Spare		0		0	
Copy	700,412.52	2	104.04		10/4/2021 5:35:58 PM

Detail Report By: ⦿ Path   ○ Volume Group   ○ Jobs

Pool	Volume SerialNumber	Disk Space	Disk Free Space	Path	Rank	Number of Files	User Data Size (MB)	Number of Non-Backed-Up Files	Size of Non-Backed-Up Files(MB)	Last Update	Path Status
Storage				\\192.168.20.22\QA\	1						Error code: 20061. Folder access test as failed: (53) The network path was not found.
Copy	1621582091	698.38 GB	434.61 GB 62.23%	\\BBOX2019-1 \DS_DD_COPY\		2	104.04			10/4/2021 5:35:58 PM	Good
Copy	0	353.02 GB	249.39 GB 70.65%	\\192.168.20.22 \DDOS_7305\		0	0.00				Good

Data Stores - QoreStor

To add a data store type QoreStor go to **Configuration** > **Data Store**, **Switch to Edit Mode** and **Create Data Store**. On the bottom panel, select for the field **Data Store Type** from the drop-down list: QoreStor.

Data Store Information

Data Store ID*   QS_DataStore

Data Store Type   QoreStor ▾

Status   Active ▾

Domain Access to Data Store   Primary ▾

Description

User Account   Admin

Password   ••••••••••••

Confirm Password   ••••••••••••

Disk Space Warning Threshold (%)   90 %

Check Volume Timestamp   ☑

Storage Optimization   RapidCIFS ▾

Archive bit support   ☑

[Add]   [Exit Add Mode]

User Account: The User Account is used to access the paths of the Windows disk pool. The account can be unqualified or qualified by a Windows domain name, and must allow for a non-interactive login in the VTCs named as routes to this Data Store.

When qualified by a domain, the syntax can be **<domain>\<account>** or **user-@domain.mycorporation.com**.

> ⚠️ The maximum number of characters allowed for the user account name is 64.

If the account is unqualified (e.g. USER1), the VTC will execute a local Windows login. The account must exist in each VTC with the same name and password.

Password: The password for the account above.

Disk Space Warning Threshold (%): This parameter is used by the NonStop TACL macro BB022_ CHECK_SPACE to check the total free space available in all Windows Data Stores. When the space occupied on disk is higher than this threshold, the EMS message 3217 is issued by the daily job OBB017.

Check Volume Timestamp: When enabled, the VTC checks that the Windows index and data files match the timestamp of the last load for output registered in the domain catalog.

These checks are normally enabled, increasing the control of restore operations.

Storage Optimization: For Data Store type QoreStor, the storage optimization field is set to **Rapid CIFS** and it cannot be modified. Value in the field is grayed out.

Archive bit support: The file system optimization supports Archive Bit. This value is grayed out and cannot be modified, .

For QoreStor Polices and QoreStor Pool should be set through **QoreStor Data Store Configuration Wizard** by clicking on **Add**.

> For Data Store type QoreStor, the storage optimization field is set to RapidCIFS and it cannot be modified. Value in the field is grayed out.

QoreStor DataStore Configuration Wizard

The QoreStor Data Store Configuration Wizard allows you to set up policies for encryption, QoreStor replication and Copy Pool Sync replication.

QoreStor Data Store
Configuration

Step 1

QoreStor Encryption

Encryption at rest ☐

Step 2 >>   Cancel

If you want to use encryption at rest, check the box and click **Step 2** button to go to the next step.

QoreStor Data Store
Configuration

Step 2

QoreStor Replication

QoreStor Replication ☐

Step 3 >>   Cancel
<< Step 1

Check the box if you plan on using inter-VTC replication or don't check anything and click **Step 3** button to go to the next wizard option.

⚠	Tape volumes associated to that specific data store will be written into a replicated container if the QoreStor has a target peer configured.

All along the QoreStor Data Store configuration process you can go back step by step using the **Step** button, if you want to change the data store policies.

QoreStor Data Store Configuration

Step 3

QoreStor Cloud Tiering WORM Media

Cloud Tier ☐
Note: The appendable tape volumes are not supported with the Cloud Tier option.

[<< Step 2] [Step 4 >>] [Cancel]

Check the box if you want to enable Cloud Tiering option.

QoreStor Data Store Configuration

Step 4

QoreStor Copy Pool Sync

Copy Pool Sync ☐

[Step 5 >>] [Cancel]
[<< Step 3]

Check the box if you plan on using inter-VTC replication or don't check anything and go to the next wizard option.

If you enabled copy pool sync feature, the usage of local storage is forced, so all VTC should have their own embedded QoreStor. Copy pool sync will work if you have at least 2 VTCs . For 2 VTCs (A and B), data written on one VTC (A) will be copied on the other VTC (B) after the unload and the other way around.

At thist step, select the route from the drop-down list and click **Add Route** button. Once the route is added, you will see it listed as *Selected Route:* in your wizard.

Click on the **Summary** to view the Configuration summary. Summary gives you the option to review the configuration before saving it. If necessary, you can go back and modify the configuration.

QoreStor Data Store Configuration

Step 6

QoreStor Summary

Note: Storage paths automatically created, if needed, when you save the configuration.

QoreStor Encryption is : Enabled
QoreStor Replication is : Enabled
Copy Pool Sync is : Enabled
Cloud Tier is : Enabled
The Following VTC will be added as route : BBOX2019-1

| << Step 5 | Save | Cancel |

Once you click **Save**, the entire configuration of the data store will be displayed, including the default created paths for the selected polices (replication, copy pool sync and encryption, if the case).

QoreStor Data Store Configuration

Step 7

QoreStor Configuration Overview

Creating Route BBOX2019-1
Adding Path \\qs34
\cryp2replicateCT\QCH409
\DIANAQS success
Adding copy sync Path \\qs34
\cryplocalCT\QCH409
\DIANAQS\copypool success
Adding replication Path
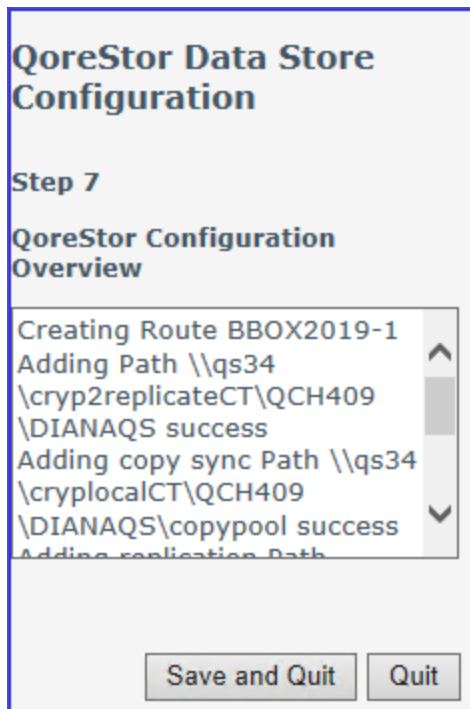
| Save and Quit | Quit |

Click **Save and Quit** to save your configuration or **Quit** to quit the wizard.

Click on **Verify Configuration** to run a verification process on the QoreStor Storage route(s).

In the newly opened window start the verification process by clicking on **Start Verification** .

BACKPAK **Verification For QS_DATASTORE** User: SUPER.ETINET
Domain: PLANBAAQ
1/4/2022 8:48 AM

Verification might take some time, press Start to execute.
Start Verification
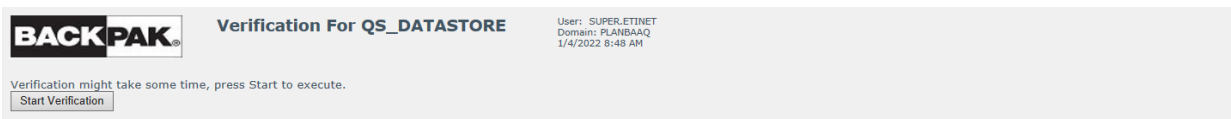
The results of the configuration verification process will be displayed on the same page as a **Verification Report**, listing the details for each path created during the wizard configuration. If there are more than one storage route, the **Summary** will show all the verified paths for all the storage routes.

BACKPAK **Verification For QS_DATASTORE** User: SUPER.ETINET
Domain: PLANBAAQ
1/4/2022 8:52 AM

Press Next Route button to proceed with the next Route verification
Next Route

Verification Report for Route - GEN8SRV04

Account Access Verification
User : etinet.local\ywu
Result : OK
Path Verification
Path : \\BBQS236.ETINET.LOCAL\CRYPLOCAL\PLANBAAQ\QS_DATASTORE\
Result : OK

Path : \\GEN8SRV04QS\CRYPLOCAL\PLANBAAQ\QS_DATASTORE\
Result : OK

End of Verification for Route GEN8SRV04

BACKPAK **Verification For QS_DATASTORE** User: SUPER.ETINET
Domain: PLANBAAQ
1/4/2022 8:55 AM

Press View Summary button to a view summary of the Route verification
View Summary

Verification Report for Route - TOUTATIS
Account Access Verification

User : etinet.local\ywu
Result : OK

Path Verification

Path : \\BBQS236.ETINET.LOCAL\CRYPLOCAL\PLANBAAQ\QS_DATASTORE\
Result : OK

Path : \\GEN8SRV04QS\CRYPLOCAL\PLANBAAQ\QS_DATASTORE\
Result : OK

End of Verification for Route TOUTATIS

*** End of Verification, No More Route to Check ***

Click on **View Summary** to display all the paths verified by the process. See below an example of the **Verification Summary**.

Once the data store QoreStor type saved, the data store will be listed on the Data Store page with the given ID.

Data Store ID	Store Type	Status	Domain Access	Description		
DS_QORESTOR	QORESTOR	Active	PRIMARY		Catalog Sync Export	Advanced
DS_QS1	QORESTOR	Active	PRIMARY		Catalog Sync Export	Advanced
DS_SHE409	QORESTOR	Active	PRIMARY		Catalog Sync Export	Advanced
QS_ADBT	QORESTOR	Active	PRIMARY		Catalog Sync Export	Advanced
QS_DI	QORESTOR	Active	PRIMARY		Catalog Sync Export	Advanced
ZXTEST	QORESTOR	Active	PRIMARY		Catalog Sync Export	Advanced

If you click on the data store ID in the table, the bottom panel will display all the info related to that specific data store. In the example above, because the store type is QoreStor, the bottom panel will display info on QoreStor Policies, details, QoreStor Storage Route and QoreStor pool.

The bottom of the Data Store Information panel will display all QoreStor related data store details:

QoreStor Storage Route	Verify Configuration	
VT Controller ID*		
GEN8SRV04		
TOUTATIS		

QoreStor Pool

Storage Pool	**Spare Pool**	**Copy Pool**

Path	Rank	Reserved For
\\BBQS236.ETINET.LOCAL\CRYP2REPLICATECT\PLANBAAQ\QS_DATASTOREI\	1	ANY
\\GEN8SRV04QS\CRYP2REPLICATECT\PLANBAAQ\QS_DATASTOREI\	1	ANY

The policies configured with the wizard are listed, check-marked if active, and grayed-out; they cannot be modified even if you switch to edit mode.

QoreStor Storage Route indicates the main storage route to the server.

QoreStor Pool indicates the paths for each Storage Pool, Spare Pool and Copy Pool.

Click on **Storage Pool** tab to see details on the automatically created storage pool paths.

The **Spare Pool** is not automatically created. If you plan on using spare pool(s), you have to manually input the path for spare pool(s).

If you click on the **Copy Pool** tab, the panel will list all the default paths for the copy pool.

Path: The path name where virtual volumes will be stored. Each path must be a fully qualified Network Share entered as a UNC path (e.g. \\SVR1\BBOX\STORE1). In exceptional cases, the path name can be also defined as a local directory (e.g. C:\BBOX\STORE1)

Rank: The preference rank of the path in the pool. Path(s) with Rank 1 will be chosen first and filled before writing on other paths. Paths of the same Rank will be distributed according the workload and to the available free space.

⚠️	When migrating from old to new storage, it's possible to define a spare path to run the backup in case of new storage unavailabilty. To force-use that spacific path, choose a rank value from 1 to 9 (rank 1 corresponds to the highest priority).

			Path	Rank	Reserved For
Update Cancel	Delete		\\BBOX2019-1\DS_2COPY_SPARE\	2 ×	ANY ▾
Edit	Delete		\\BBOX2019-2\DS_1ST_2COPY_SHARE\	1	ANY

Reserved For: Allows entering a Volume class for which the path will be dedicated.

The copy pool sync paths are as well automatically created, based on the two routes (added with the Wizard) for each embedded QoreStor appliance.

> ⚠️ The Copy Pool Sync functionality is not available if there are less than 2 routes set up for the VT Controllers.

Data Store – IBM Spectrum Protect™ (Tivoli Storage Manager – TSM)

Node: IBM Spectrum Protect™ (TSM) node name used by the VT Controller to log in to the IBM Spectrum Protect™ (TSM) Server. This node must be created by a IBM Spectrum Protect™ (TSM) administrator.
If omitted, the IBM Spectrum Protect™ (TSM) client configuration file (dsm.opt) must contain the node name and password.
Password: Password associated with the IBM Spectrum Protect™ (TSM) node. This password is used by the VT Controller to log in to the IBM Spectrum Protect™ (TSM) server.
File Space: Optional specification of a IBM Spectrum Protect™ (TSM) File Space that will contain all virtual volumes of this group. If left blank, a File Space name will be created for each virtual volume and named according to its volume label. When a File Space is created for each volume label, it is possible to delete or export/import the data of a single virtual volume.

A typical IBM Spectrum Protect™ (TSM) client creates a limited number of File Spaces. The IBM Spectrum Protect™ (TSM) administrator should be contacted before creating hundreds of File Spaces.

Storage Routes

This section defines the routes to data; it lists the VTCs that are connected to the storage.

Rank: Indicates the route priority. The highest priority is 1.

VT Controller ID: Identifies the VTC connected to the selected Data Store.

IBM Spectrum Protect™ (TSM) Client Option File: Name of the DSM.OPT file the VTC will use as local IBM Spectrum Protect™ (TSM) configuration for accessing a IBM Spectrum Protect™ (TSM) Data Store. Must be a local file (C:\...) to allow a VTC operations when another VTC is down. This local file must be in the same location in all VTCs, for a given Data Store.

Data Store Advanced Properties – IBM Spectrum Protect™ (Tivoli Storage Manager – TSM)

Restore on Same VTC: When checked, and when the TAPE DEFINE set for restore (USE IN) does not specify a tape device, the volume will be read from a device on the same VTC on which this volume has been initially written.

Data Store – Windows Files

User Account: The User Account is used to access the paths of the Windows disk pool. The account can be unqualified or qualified by a Windows domain name, and must allow for a non-interactive login in the VTCs named as routes to this Data Store.

When qualified by a domain, the syntax can be **<domain>\<account>** or **user-@domain.mycorporation.com**.

⚠️	The maximum number of characters allowed for the user account name is 64.

If the account is unqualified (e.g. USER1), the VTC will execute a local Windows login. The account must exist in each VTC with the same name and password.

Password: Data Store is password protected to ensure secure access to data. The password gives the user log in access to the server.

⚠️	Make sure the user account matches the account for the storage (BackBox, QoreStor, StorageOne, etc).

⚠️	BB004 macro can be used to periodically update the account password that protects the DataStore. In case the user needs to change the password periodically, he/she can implement it by scripting with BB004 on Tandem side.

Disk Space Warning Threshold (%): This parameter is used by the NonStop TACL macro BB022_CHECK_SPACE to check the total free space available in all Windows Data Stores. When the space occupied on disk is higher than this threshold, the EMS message 3217 is issued by the daily job OBB017.

⚠️	If value is set to **0%**, the autoscratch cannot be triggered.

Check Volume Timestamp: When enabled, the VTC checks that the Windows index and data files match the timestamp of the last load for output registered in the domain catalog. These checks are normally enabled, increasing the control of restore operations.

> ⚠️ If a volume must be loaded despite a timestamp discrepancy, it is recommended to disable the timestamp check for that specific volume rather than for the Data Store. If the Data Store check is enabled, the volume timestamp check will be automatically set again when the volume is re-written by a new backup.

Storage Optimization: This selects a de-duplication engine. Depending on the client storage, data store could be optimized with BoostFS, RapidCIFS, DataDomain NAS, StoreOnce NAS, VTC internal disk, etc.

```
---- Select ----
Other storage
DataDomain NAS
BoostFS
StoreOnce NAS
VTC internal disk
RapidCIFS
```

> ⚠️ When running a backup with RapidCIFS optimization, the volume groups (NOC, CAT, TMF, etc.) sub-folders are automatically created within the data store folder. Ex:
> \\192.168.20.153\QA_Container\VG_NOCAT , \\192.168.20.153\QA_Container\VG_CAT

Archive Bit Support: This is a flag that indicates if the WINDISK file system (optimization) supports the Archive Bit. The default value is active (Archive Bit Supported), even for customers migrating from a version previous to H4.02.

> ⚠️ If there was a Delete Archive File for StoreOnce, it will be ineffective until StoreOnce has a fixed version or until the user updates the configuration.

Windows Pool

This section permits adding or modifying a path for storing Windows files in three different pools:

Storage pool is the normal pool.
Spare pool is an emergency pool for writing new backups when the Storage pool is not available.
Copy pool is assumed to contain a copy of the files in the Storage pool and it's used only for a restore when the volume is not found in the Storage pool. Files are either copied via the Copy Sync Pool option (provided with the customer installation) or copied independently of the Back-Box.

⚠	The Spare and Copy pool tabs can be accessed only if the licensed option **Windows advanced pool management** is enabled.

In a pool, the VTC will choose a path when a tape is created and may move it to a better location when re-writing the volume for a new backup.

Path: The path name where virtual volumes will be stored. Each path must be a fully qualified Network Share entered as a UNC path (e.g. \\SVR1\BBOX\STORE1). In exceptional cases, the path name can be also defined as a local directory (e.g. C:\BBOX\STORE1) For more information, refer to the Windows Files Data Store section.

Rank: The preference rank of the path in the pool. Path(s) with Rank 1 will be chosen first and filled before writing on other paths. Paths of the same Rank will be distributed according the workload and to the available free space.

Reserved For: Allows entering a Volume class for which the path will be dedicated.

Storage Routes

Storage Route	Hide		
Rank*	1 ▾		
VT Controller ID*	ASTERIX ▾		
	Add Storage Route		

		Rank*	**VT Controller ID***
Edit	Delete	1	TOUTATIS

This section lists all VTCs with access to the storage.

Rank: Indicates the route priority. The highest priority is 1.

VT Controller ID: Identifies the VTC connected to the selected Data Store.

Data Store Advanced Properties - Windows Files

Data Store ID	Store Type	Status	Domain Access
QC-DATASTORE	TSM	Active	PRIMARY
WIN403-LOCALDISK	**WINDISK**	**Active**	**PRIMARY**

Advanced

Restore On Same VTC ☐

Disk Block Size (KBytes) [128 ▾]
Copy Pool Sync [No ▾]
Force Local Path ☐

[Update]

Enterprise Backup Software Scripting
Script Type [No scripts ▾]

[Update Script Information]

Script Parameters [Add]

Restore on Same VTC: When checked, and when the TAPE DEFINE set for restore (USE IN) does not specify a tape device, the volume will be read from a device on the same VTC on which this volume has been initially written. When VTC local storage is used for a Data store (DAS or SAN), it is generally better, for performance reasons, to mount the tape on a drive from the same VTC (more chance the data still on that VTC local storage).

For example, in a Windows file Data Store where each VTC provides local disks for storage, checking the **Force Local Path** means that, at restore time, the VTC that has written the file on a local disk will be preferred to the one that has to access the Data Store through a shared drive.

Disk Block Size (KBytes): This parameter defines how large the Disk IO should be. When writing a Windows disk file, the VTC prepares large buffers to minimize the number of IOs sent to the file system. Increasing the default value might improve the throughput, especially when there are several tape volumes being written concurrently on the same disk.

Copy Pool Sync: Activates the synchronization between the Storage Pool and the Copy pool via the CopySync program. This program will be submitted via the regular backup script after a backup or on demand via the UI. It can be used with or without the Script Controller. Enabling this option will automatically disable the implicit backup script in the scripting section.

If any script type is chosen, a backup script running the CopySync program will replace it.

Copy Pool Sync Bandwidth utilization can be controlled via the parameter BBOX_COPY_ IOPACING (default value "0"). The value assigned to the parameter is in milliseconds and indic-

ates to the Copy Pool Sync program the amount of time to wait between two IO data blocks written to the copied files.

Force Local Path: Checking this box changes the regular algorithm used to choose a path when a virtual volume file is re-created for a volume mount request. Only local disks will be considered as candidate for destination path. A load request is rejected if there is not enough space on the local path – even if there is enough space on a remote path. **Force Local Path** is always on when the copy pool sync option is selected.

Enterprise Backup Software Scripting: Optionally specify Windows command files to be executed following specific tape events. For more info refer to Scripting/Background Migration on Tape.

- For Manual Restore, the backup method is hardcoded and it is triggered by the Enterprise Backup Software.
- For Generic script type, the following fields are available:

Backup Method: available options are BackPak Backup Script (the script provided by BackPak) or Other methods (Triggered by Enterprise Backup Software).

Backup Script: command file to be executed after a volume unload. Not available when Copy Pool Sync is active.

Restore Script: command file to be executed at volume load, when a virtual media cannot be found on the Data Store.

Delete Script: command file to be executed after a volume has been deleted.

Post Restore Script: command file to be executed after a volume requiring the RESTORE script and mounted for input (USE IN) has been unloaded.

Script Parameters: They are optional and user-defined. Named parameters that will be passed on to the scripts. Up to ten parameters can be entered in the Domain configuration. These parameters will be passed as Windows environment variables to the shell executing the script, in addition to the parameters generated by the VTC to identify the files to be processed in the script.

> **Name**: The name of the parameter. Do not specify the % sign after or before the name.
> **Value**: The value of the parameter.

Refer to section Scripting/Background Migration on Tapes for more information.

Volume Group

The **Volume Group** page is used to define attributes common to a group of volumes.

These attributes are used and applied at volume creation and each time a volume is re-written with a new backup.

The **Volume Group** main page shows the list of existing Volume Groups. If in **Edit mode**, the following options are available: **Create Volume Group** and **Delete**.

Click on the name of the Volume Group to display additional parameters. The default values can be modified if in Edit Mode.

The page layout and the page elements vary according to the Data Store. The example above is for a group associated to a DSM/TC pool and a Primary Data Store.

The Advanced properties are common to all Volume Groups and documented at the end of this section.

For Windows files data stores, the page layout varies depending on the catalog type.

> Windows files – no tape catalog (or CA catalogs)
> Windows files – DSM/TC catalog
> Windows files – QTOS catalog
> Windows files – TMF catalog

For IBM Spectrum Protect™ (TSM) data stores, the same catalogs are possible – although only the DSM/TC layout is presented below.

Volume Group Windows Files – No Tape Catalog (or CA Catalogs)

Volume Group Windows Files – DSM/TC Catalog

Volume Group Windows Files – QTOS Catalog

Volume Group Information

Volume Group ID*	H403-CAT-WINDISK
Description	
Data Store ID	WIN403-LOCALDISK
Tape Catalog	QTOS
Auto Scratch at Load Time	YES - data discarded only for expired volumes
Delete Expired Volumes	Yes
Media Type	LTO3
Warning Threshold (Min % Of Scratch Volumes)	0 %
Migration to BackBox	None — Switch to the BackBox storage is completed. Virtualization is still available, but Auto-import is disabled.

Delete Backedup Files ? ☑

Days Past Last Update	0
Days Past Last Access	0
Min File Size For Deletion(MBytes)	0

Catalog Information - QTOS

Catalog File	
Vault	

Class Information

Compression Algorithm	None
Volume Class	CLASS25
Max Volume Size(MB)*	25000
Encryption Algorithm	None
Key Manager ID	

[Update Volume Group] [Exit Update Mode]

Volume Group Windows Files – TMF Catalog

Volume Group Information

Volume Group ID*	H403-CAT-WINDISK
Description	
Data Store ID	WIN403-LOCALDISK
Tape Catalog	TMF
Auto Scratch at Load Time	YES - data discarded only for expired volumes
Delete Expired Volumes	Yes
Media Type	LTO3
Warning Threshold (Min % Of Scratch Volumes)	0 %
Migration to BackBox	None — Switch to the BackBox storage is completed. Virtualization is still available, but Auto-import is disabled.

Delete Backedup Files ? ☑

Days Past Last Update	0
Days Past Last Access	0
Min File Size For Deletion(MBytes)	0

Catalog Information – TMF

Guardian Node*	

Audit Dump Class Information

Compression Algorithm	None
TMF Audit Dump Class	
Max Volume Size(MB)*:	25000
Encryption Algorithm	None
Key Manager ID	

Online Dump Class Information

Compression Algorithm	None
TMF Online Dump Class	
Max Volume Size(MB)*:	25000
Encryption Algorithm	None
Key Manager ID	

[Update Volume Group] [Exit Update Mode]

Volume Group IBM Spectrum Protect™ (TSM) – DSM/TC Catalog

Volume Group Information

Volume Group ID: Identifies a Volume Group. It must be unique and cannot be modified after it is added. If the Data Store type is RESTRICTED or SECONDARY, this Volume Group ID is usually identical to the corresponding Volume Group ID in the primary domain.

Description: Optional user description.

Data Store ID: Specifies in which Data Store the virtual volumes will be created. This value applies to new virtual volumes created in this group. It cannot be modified to change the location of volumes previously created.

Primary Volume Group ID: Specifies the corresponding Volume Group ID in the primary site, when it is different. This parameter is presented only when SECONDARY or RESTRICTED Data Store are selected.

Tape Catalog: Specifies the catalog type (None, DSM/TC, TMF, QTOS or CA).

Auto Scratch at Load Time: Indicates if the content of an expired virtual volume can be deleted at load time. The expiry test depends on the tape catalog type and its integration in BackPak.

> ⚠️ For QTOS and CA catalogs, there is no expiry test when auto-scratch is enable. Any tape volume requested for output is assumed to be expired. Refer to the Auto-Scratch Mechanism section.

Delete Expired Volumes: Indicates if a volume that has become SCRATCH in DSM/TC, TMF or QTOS must be deleted in storage. This controls the functionality of the macro BB017_FREE_ EXPIRED (in OBEY OBB017).

Media Type: Specifies the media type that will be registered in the TAPEVOLUME entry of the DSM/TC when the volumes are created. This must match the device type returned by the command MEDIACOM INFO TAPEDRIVE $virtual-tape-drive. To solve a mount request, BackPak will search for a media compatible tape device. The default media type provided by the VTC tape emulation is LTO3.

For old Guardian tape systems not supporting LTO3, it is possible to change this default for 3480 in the internal VTC configuration; the Volume Groups must then be configured with CART3480 media type.

LTO4 media type is available to support the VLE tape Encryption. Non-Encrypted LTO4 media types can be mounted on LTO6 tape drive emulation.

LTO2 media type is also available to support old tape catalog versions (CA tape catalog). LTO2 media must be operated on LTO3 tape drives.

Warning Threshold (Min % of SCRATCH Volumes): Specifies a threshold that is tested in the daily OBB017 job. When the number of SCRATCH Volumes is less than the specified percentage, the message #3313 is issued to the EMS. For example, the message "Only nn% of SCRATCH Volumes are available in Volume Group <name>" would be issued when the number of SCRATCH tapes fall below the configured percentage. This setting applies only when the Tape Catalog is set to DSM/TC or TMF.

⚠	If value is set to **0%**, the autoscratch cannot be triggered.

Migration to BackBox: Indicates the migration status from a legacy virtual tape solution. This parameter is available to Volume Groups attached to a PRIMARY Data store only.

Possible values:

- **None**: Migration is completed. Volume virtualization is still available, but without the migration specific Auto-import automation.
- **In Progress**: Migration of historical backups from a legacy storage system to BackBox has started, but is not completed. Tape applications may access some media not yet migrated using the legacy system.
- **Being Prepared**: Migration is in progress but all NonStop backups and restores are still executed using the legacy storage system.

Migration to BackBox enables or disables migration features for the following functionalities: **Volume Virtualization**, **Import of Volumes from Tape Catalog**, and **Auto-import of SCRATCH Volumes**.

For further information see [Concurrent Operation of Legacy System and BackBox](#).

Catalog Information (DSM/TC Version)

The following fields are available when Tape Catalog is set to DSM/TC.

This information is not used when the Data Store is RESTRICTED.

> **Volcat**: Indicates the DSM/TC volume catalog where the tape volumes are cataloged. This must be prefixed with the Guardian Node Name (ex: \NODE.TAPECAT).
>
> **Pool**: Indicates the DSM/TC pool where the tape volumes are cataloged. This pool must be defined in DSM/TC using MEDIACOM before creating new virtual volumes. Pools should be created by the MEDIACOM command ADD POOL with all default values. There must be a distinct pool per BackPak Volume Group and vice-versa.
>
> **Filecat**: Indicates the DSM/TC file catalog where the tape files and disk files are written by the BackPak catalog replication (Catalog Sync option). This parameter is applicable only for SECONDARY Data Stores. The filecat must be prefixed with the Guardian Node Name (ex: \NODE.TAPECAT).

For more information see the related manual *Catalog Sync Option*.

Catalog Information (QTOS Version)

The following fields are available when Tape Catalog is set to QTOS.

This information is not used when the Data Store is RESTRICTED.

> **Catalog File**: Fully qualified Name of the NonStop file where QTOS registers the volumes that it manages. The QTOS unqualified file name is TAPES.
>
> **Vault**: Indicates the QTOS vault where the tape volumes are cataloged. There must be a distinct vault per BackPak Volume Group and vice-versa.

Catalog Information (TMF version)

The following fields are available when Tape Catalog is set to TMF.

This information is not used when the Data Store is RESTRICTED.

Guardian Node: Indicates the Guardian Node where TMF is running. (ex: \NODE1).

Delete Backed Up Files

Delete Backed Up Files must be used with caution, especially when set on IBM Spectrum Protect™ (TSM) with backup objects. For more information, see *BackBox VTC Scripting Option Manual*.

- Enables and controls the deletion of virtual volume Windows files that have been backed up by an Enterprise Backup software.

A file is recognized as backed up if its archive bit is reset.

The following criteria control the deletion of virtual media files. All conditions must be true in the same time for the deletion to occur:

Delete Backed Up Files: Enables the deletion of backed up files.
Days Past Last Update: Number of 24 hour periods the files are kept after the last file write.
Days Past Last Access: Number of 24 hour periods the files are kept after the last file access.
Min File Size For Deletion (MB): Files under 1MB will not be deleted, even if other criteria may apply.

Volume Class Information (non TMF)

This information is available when Tape Catalog is not set to TMF and the Data Store type is Windows file.

Compression Algorithm: For Windows files Data Stores only, enables the software compression. Values:
None – No compression.
Light - Low compression, less CPU usage.
Strong – High compression, high CPU usage.
Volume Class: Class to associate with all volumes of this Volume Group.
Max Volume Size (MB): Indicates the maximum capacity (compressed data in megabytes) of the virtual volumes.

Audit Dump Class Information (TMF Audit Dumps)

These characteristics are applied when Tape Catalog is set to TMF, the Data Store type is Windows file, and the volume is loaded to write an AUDIT dump, according to the EMS mount message.

Compression Algorithm: Enables the software compression. For Windows files Data Stores only. Possible values:
None – No compression.
Light - Low compression, less CPU usage.
Strong –High compression, high CPU usage.

When the file server is a Data Domain appliance, refer to the Data Domain section.

TMF Audit Dump Class: This class will be assigned to volumes of this group.
Max Volume Size (MB): Indicates the maximum capacity (compressed data in megabytes) of the virtual volumes.

Online Dump Class Information (TMF Online Dumps)

These characteristics are applied when Tape Catalog is set to TMF, the Data Store type is Windows file, and the volume is loaded to write an ONLINE dump, according to the EMS mount message.

Compression Algorithm: Enables the software compression. For Windows files Data Stores only. Possible values:
None – No compression.
Light - Low compression, less CPU usage.
Strong – High compression, high CPU usage.

When the file server is a Data Domain appliance, refer to the Data Domain considerations in the Configuration section.

> **TMF Online Dump Class**: This class will be assigned to all volumes in this group.
>
> **Max Volume Size (MB)**: Indicates the maximum capacity (compressed data in megabytes) of the virtual volumes.

Volume Class Information for IBM Spectrum Protect™ TSM (non TMF)

The following fields available when Tape Catalog is not set to TMF and the Data Store type is IBM Spectrum Protect™ (TSM).

> **Volume Class**: BackPak class to associate to all volumes of this Volume Group.
>
> **Max Volume Size (MB)**: Indicates the maximum capacity (compressed data in megabytes) of the virtual volumes.
>
> **IBM Spectrum Protect™ TSM Max Object Size (MB)**: BackBox creates multiple IBM Spectrum Protect™ (TSM) objects per tape. This parameter controls the size of these objects.
>
> **IBM Spectrum Protect™ (TSM) Management Class**: Name of the IBM Spectrum Protect™ (TSM) Management Class to assign to the objects. This is the way to assign different storage services to different Volume Groups. Default assigns the default management class in IBM Spectrum Protect™ (TSM) for the IBM Spectrum Protect™ (TSM) node specified in the data store configuration.

Volume Group Advanced Properties

> **PreLoad**: Enabling PreLoad can be useful for the NonStop restore/recover of multi-volume tape files, when a restore script must be executed before the volume can be read by the NonStop. When PreLoad is enabled, the load of the next volume is anticipated (and the restore script initiated) while the previous volume is being read by the NonStop tape application. For more info refer to the PreLoad section. The PreLoad processing requires two virtual tape drives per NonStop restore process.

Auto Unload Timeout: Minimum time (in seconds) that a volume will be kept loaded but unused. A tape loaded by a process that is no longer running should be unloaded when resources are required for a new mount request.

Automatic Scratch Options: Click **Edit** to automatically scratch volumes, based on set up parameters.

In the pop-up window check the box **Allow volume to be automatically created**, specify the Volume Label*, Quantity* (mandatory fields) and Increment Base. **Update** the settings.
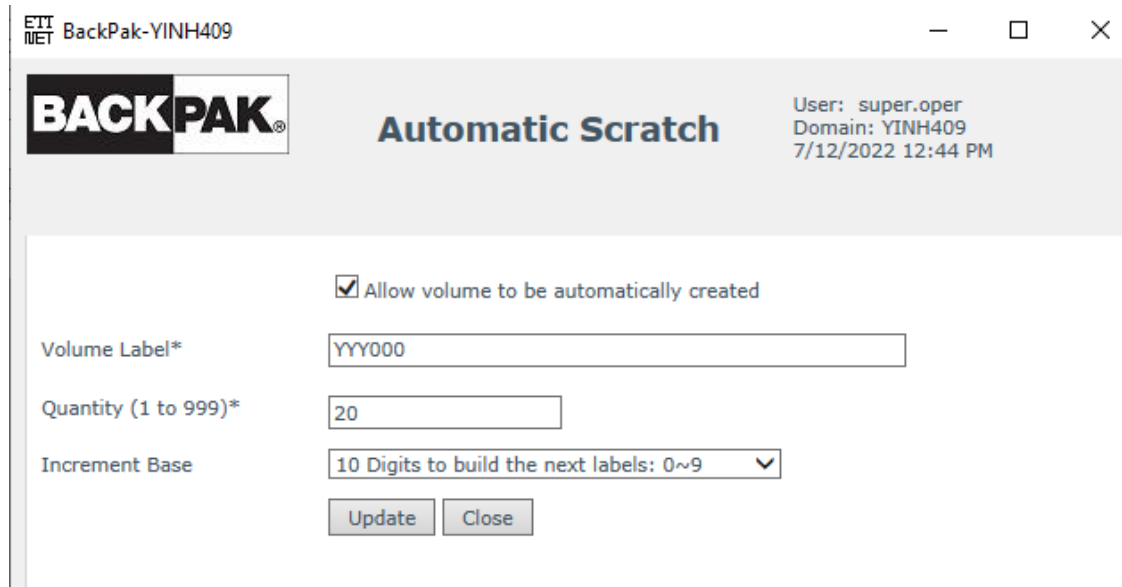
Once updated, the information displayed under **Automatic Scratch Options** will reflect the changes that have been updated.
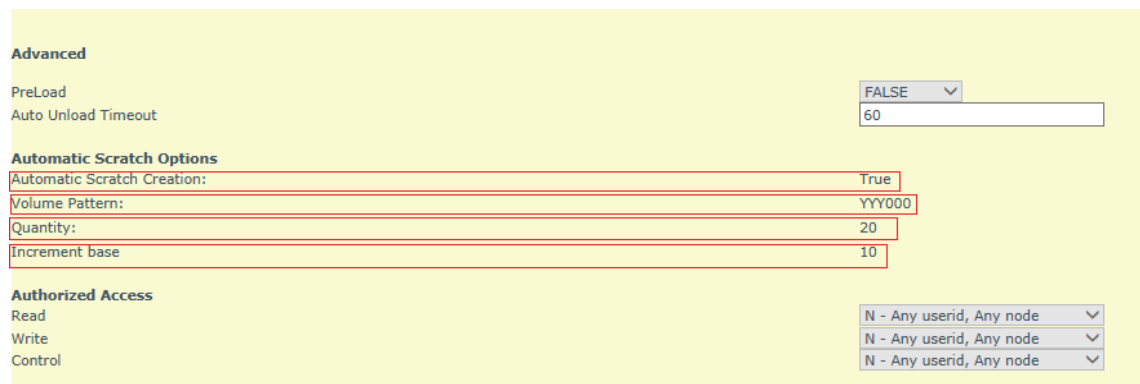
Authorized Access : This section defines the default authorizations that are assigned to the volumes each time they are loaded for output. Each element of the section defines a group of user IDs, relative to the owner of the volume:

    N Any node, any user ID

    C Any node, same group number

    U Any node, same user ID

    A Same node, any user ID

G Same node, same group number

O Same node, same user ID

? Use authorizations that were set at backup time

. Disabled access

? is a special value that cannot be entered, but is displayed by the BackPak UI for volumes that were created in a RESTRICTED Data Store.

For such volumes, the domain does not hold the RW authorizations; the access control is done by the VTC against the authorization specifications that were set at backup time and copied as metadata in the Data Store.

. is another special value that cannot be entered or removed. This is the value displayed for WRITE access when a volume is in a RESTRICTED or SECONDARY Data Store. Such volumes can never be written for a new backup.

Read: User ID allowed read access.

Write: User ID allowed to read/write/delete data.

Control: User ID allowed to change the owner or the authorization of the BackPak catalog.

Volumes Collocation

When the Storage Optimization of the Data Store is set as Rapid CIFS, sub-folders are automatically created by Tape Catalog (DSM/TC, TMF, CA, QTOS).

Ex: \\192.168.20.153\QA_Container\VG_NOCAT , \\192.168.20.153\QA_Container\VG_CAT .

1. Go to **Configuration** > **Data Store** > **Switch to Edit Mode** and click **Create Data Store**.

2. Fill out the Data Store Information fields. Select **Windows File** as Data Store Type and **RapidCIFS** for Storage Optimization.

3. Click **Add** to save the created Data Store.

4. **Add Path to the Primary Storage Pool** and **Add Storage Route** for the BackBox server. Update the Data Store Information and **Save** the configuration.

5. Go to **Volume Group** page, **Switch to Edit Mode** and create a volume group. Fill out the Volume Group Information fields and select the Data Store ID you have created before.

6. Click **Add Volume Group** and **Save** the configuration.

7. Go to **Administration** > **Create Volume**. Specify a label for volumes and choose the Volume Group you just created. Click **Add**.

When running a backup, the sub-folder of the volume group (VCOLL in the example above) is automatically created on the server.
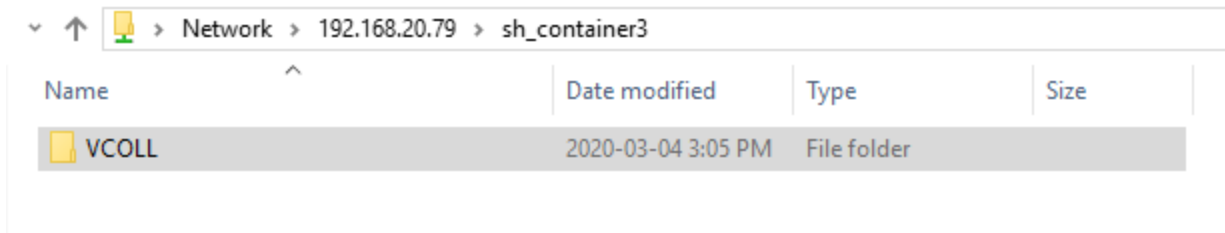
User Management

User Management page allows you to set/reset permissions to different profiles and assign profiles to users. All authorized users are listed on the **User Management** page.

After the initial installation, there are two (2) user profiles automatically predefined: *Super.Super* and *Super.x*, where "x" stands for the domain installation owner. Ex: *Super.Oper* or *Super.QC*

> ⚠️ *Super.Super* user type is not displayed on the UI, as it's a user with full access permissions and it cannot be managed through the interface.

After a fresh install, the default users (*Super.Super* and *Super.X*) have the following User Management capabilities:

- *Super.Super*: administrator permissions with user management capabilities
- *Super.X*: administrator permissions without user management capabilities

The available default profiles to assign users to are: **Administrator**, **Super Operator**, **Operator** and **Security**.

> ⚠️ The default profiles are not editable; the permissions cannot be customized.
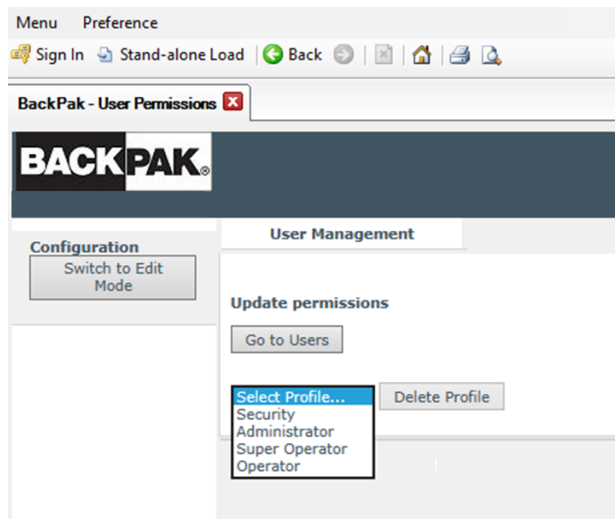
Administrator permissions: full access to all options, except user management
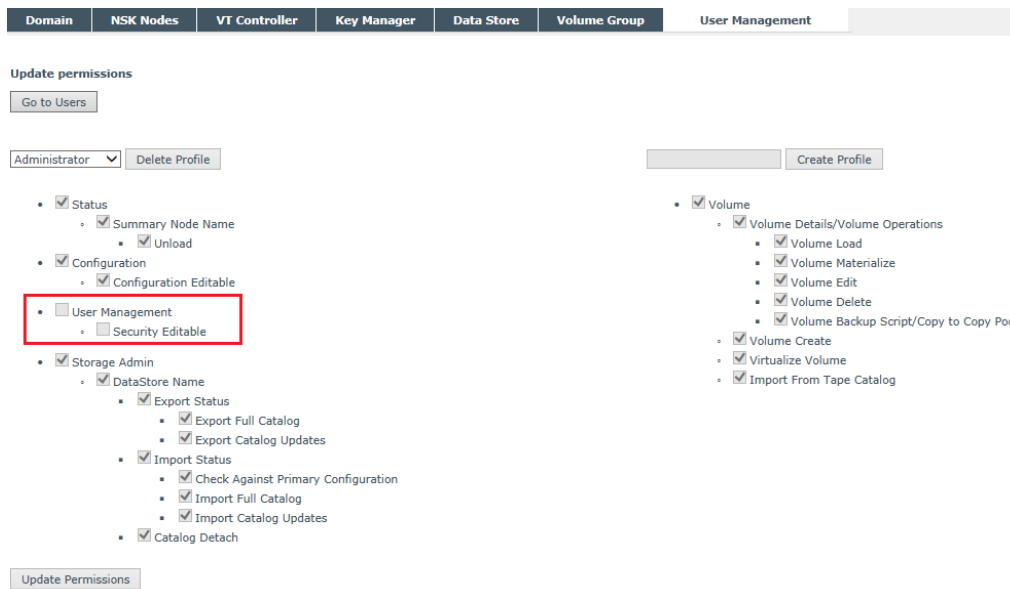
Super Operator permissions: Does not have access to **Configuration Editable** and **User Management – Security Editable** options.
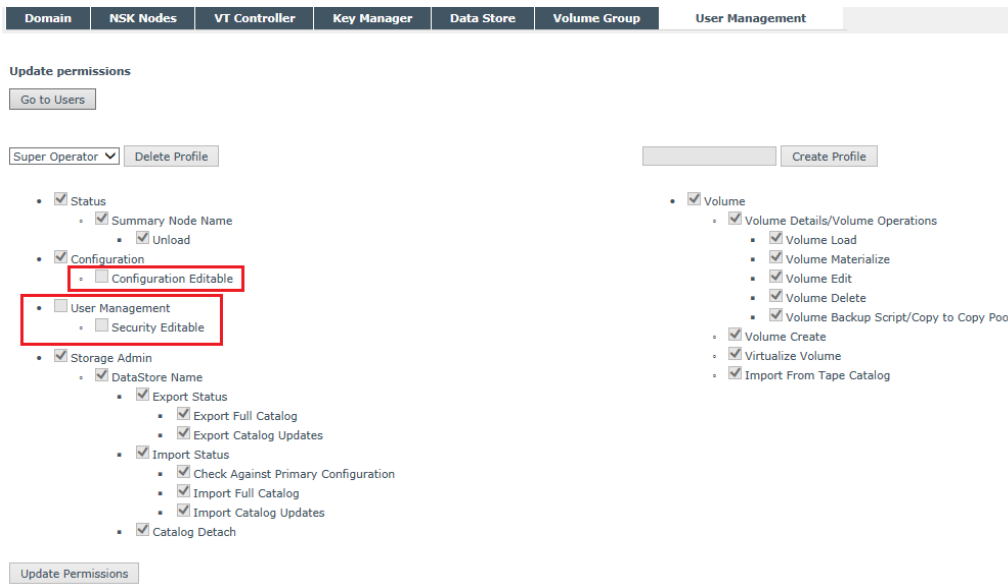
Operator permissions: Does not have access to **Configuration Editable**, **User Management - Security Editable**, **Unload** Device and **Volume Delete** optiuons.
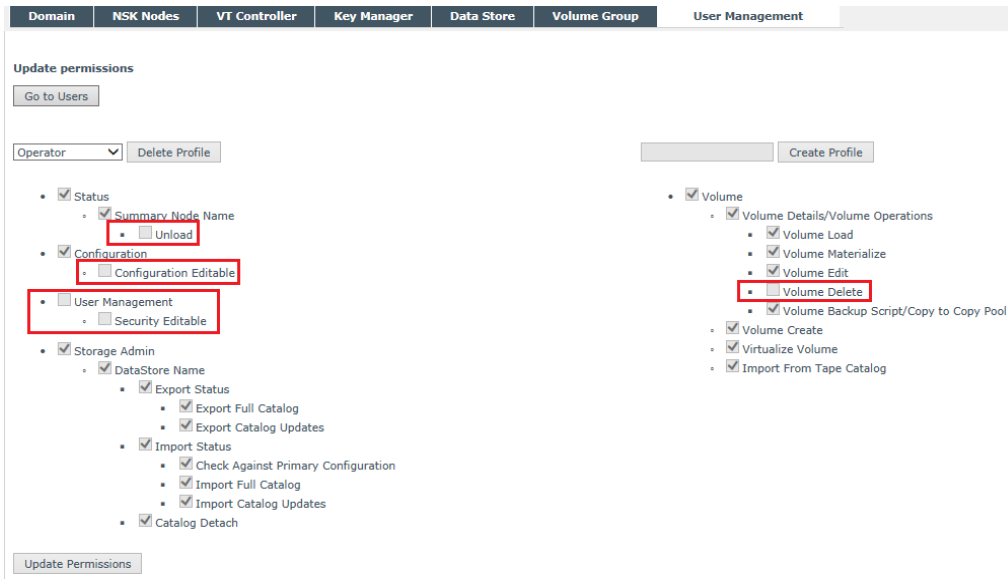
Security permissions: access to **User Management-Editable Security** page ONLY; can create, delete and edit any customized-profile user.

To edit users, profiles and/or permissions, click **Switch to Edit Mode**.

To add a user:

1. Specify the name. Make sure the username matches the existing username set up on the NonStop system.

2. Assign a profile to this user. The default options are **Administrator**, **Super Operator**, **Operator** and **Security**.

3. Click **Add User**.

⚠	The default profiles are not editable; the permissions cannot be customized.

To create a new profile:

1. On the **User Management** main page click on **Go to Profiles**.

2. Give a name to the profile you are about to create and click **Create Profile**.

3. Once the profile is created, you can assign different permissions to this profile. Check the appropriate permissions from the list.

4. Click **Update Permissions** and save the changes.

5. Once the profile has been created, you can assign users to it. Go to **User Management** page and add new user. Give the user a name and select the user to be assigned to the profile you just created. Click **Add User** to add it to the list.

6. The new user is listed under the user name.

		User Name	Profile
Edit	Delete	SUPER.OPER	Administrator
		SUPER.ETINET	Administrator
Edit	Delete	etinet.*	ProfileA
Edit	Delete	130,100	Operator
Edit	Delete	Test_Alias	Super Operator
Edit	Delete	Fernand	ProfileA
Edit	Delete	*.*	Administrator
Edit	Delete	Diana	New Operator

7. You can edit the user name and the profile the user is assigned to by clicking on the **Edit** button.

Update Cancel | Delete | Diana | Super Operator ∨

Click **Update** to save the changes you made to that specific user.

8. To delete user click **Delete**.

To delete a profile:

1. Go to **User Management** page and switch to edit mode.
2. **Go to Permissions** page and select the profile.
3. **Delete** the selected profile.

⚠	Profiles with users assigned to them cannot be deleted. An error message will state to delete the users before deleting the profile. Delete all user settings with this profile before you delete.
⚠	Default profile permissions cannot be modified.
⚠	No more than 3 custom profiles can be created. You cannot add more than 3 custom profiles.

If you are signed in with a security profile, you can assign a profile to any user.

⚠️	If the Guardian user is not defined and listed on the **User Management** page, the user cannot log into the UI.
⚠️	Any user/alias defined in the NonStop are not displayed by default on the UI.

⚠️	Different aliases (log-in names) can be added in the NonStop to the same user parent group*. If aliases (ex: Mike, Sophie, Greta) belonging to the same user parent group* are not found when trying to log into UI, the displayed log in info is gonna be the info of the user parent group* the respective alias belongs to.

Volume

The virtual tape volumes are accessed through the **Volume** tab.

Volume List: Displays a virtual volumes list. May be used to delete several volumes in a single operation and can also be used to display the detail of a particular volume.

Volume Operations: Displays the Volume Detail page and the operations available to be performed on the specified volume. The available operations are: Load/Materialize/Edit/Delete.

Create Volume: Creates and labels new virtual volumes and adds them to the domain catalog.

Virtualize Volume: Copies the image of an external tape to a BackBox virtual volume, and adds it to the domain catalog.

Import From Tape Catalog: Registers in the domain catalog volumes that are already known in a NonStop tape catalog, such as DSM/TC. This function does not move any volume data.

⚠️	To register the volumes in the domain catalog and to migrate the volume data to BackBox storage, use the Virtualize Volume link described above.

Summary : Displays summarized information for all volume groups.

Volume List

Use the **Volume List** page to list the domain virtual volumes.

Output is limited to a "page size", defined as a maximum number of returned volumes. **Next** and **Previous** buttons allow scrolling the complete list of volumes. The list can be filtered according to selection criteria.
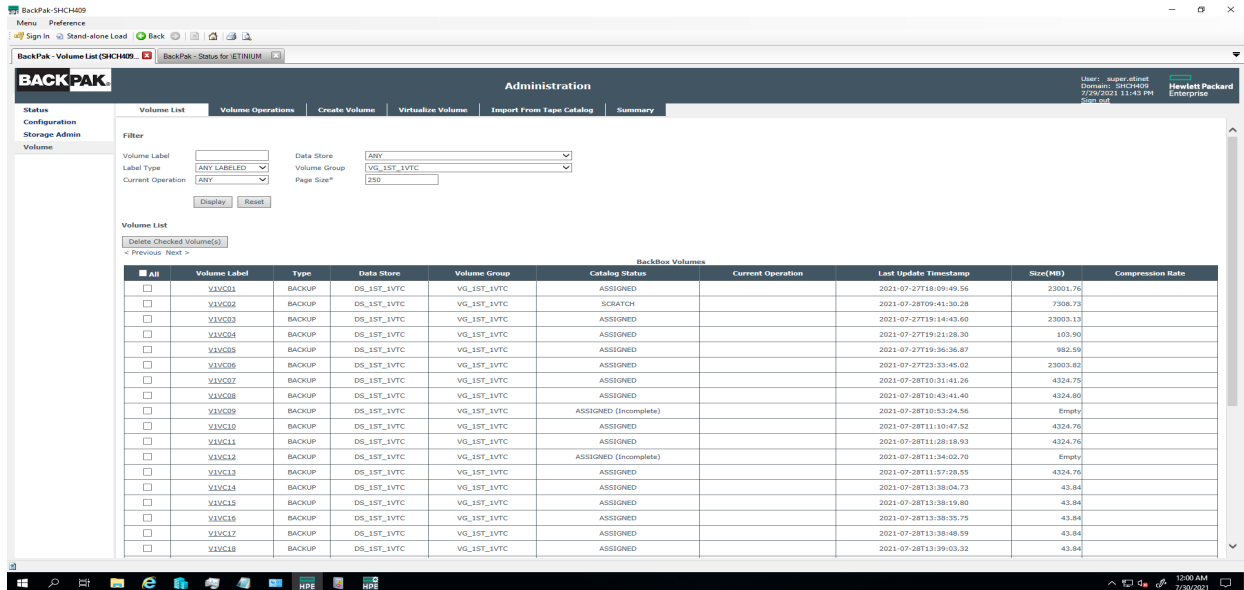
Filters applied to select specific volumes. To activate the filters and to display the Volume List click Display. The volume list filter section is used to specify the volume selection criteria.

Volume List: The volume list with returned results after applied filters to volumes.

Clicking on the **Display** button without changing any criteria will display all volumes.

> **Volume Label**: Specify the volume label. Blank indicates that no filtering is applied to the volume name. To get more than one result use wildcard characters (accepted characters "*" and "?"). For example, JN* will list all the volumes whose labels start with "JN".
> **Label Type:** Filters volumes based on the label type.
> **Current Operation**: Current operation on the volume.
> **Data Store**: Filters volumes based on the data store they belong to.
> **Volume Group**: Filters volumes based on the volume group.
> **Page Size**: Maximum number of results to be displayed on the page. To browse through pages use **Previous** and **Next** buttons.
> The Volume List section displays the virtual volumes that match the specified filter(s). Under the **Volume List** section:
> **Delete Checked Volume(s)**: Button that deletes all the checked volumes.
> **All Checkboxes**: Check or uncheck all volumes displayed.
> **Volume Checkbox**: Check or uncheck the volume.
> **Volume Label**: Volume label or BackBox internal volume ID for NL volumes. The volume labels are linked to the volume detail page.
> **Type**: Volume label type.
> **Data Store**: Data Store to which the volume belongs.

Volume Group: Volume Group to which the volume belongs.

Catalog Status: If the volume group is associated with a catalog, shows the catalog status known from the last operation or the last execution of the daily batch OBB017.

To check the status of a specific volume, open the volume detail page.

To refresh the status of all volumes, the TACL job OBB017 must be re-executed.

Catalog Statuses (depending on the backup progress and performance) can be the following:

- ASSIGNED
- ASSIGNED (Incomplete)
- SCRATCH
- IN USE

☐	V1VC02	BACKUP	DS_1ST_1VTC	VG_1ST_1VTC	SCRATCH		2021-07-28T09:41:30.28	7308.73
☐	V1VC03	BACKUP	DS_1ST_1VTC	VG_1ST_1VTC	ASSIGNED		2021-07-27T19:14:43.60	23003.13
☐	V1VC04	BACKUP	DS_1ST_1VTC	VG_1ST_1VTC	ASSIGNED		2021-07-27T19:21:28.30	103.90
☐	V1VC05	BACKUP	DS_1ST_1VTC	VG_1ST_1VTC	ASSIGNED		2021-07-27T19:36:36.87	982.59
☐	V1VC06	BACKUP	DS_1ST_1VTC	VG_1ST_1VTC	ASSIGNED		2021-07-27T23:33:45.02	23003.82
☐	V1VC07	BACKUP	DS_1ST_1VTC	VG_1ST_1VTC	ASSIGNED		2021-07-28T10:31:41.26	4324.75
☐	V1VC08	BACKUP	DS_1ST_1VTC	VG_1ST_1VTC	ASSIGNED		2021-07-28T10:43:41.40	4324.80
☐	V1VC09	BACKUP	DS_1ST_1VTC	VG_1ST_1VTC	ASSIGNED (Incomplete)		2021-07-28T10:53:24.56	Empty
☐	V1VC10	BACKUP	DS_1ST_1VTC	VG_1ST_1VTC	ASSIGNED		2021-07-28T11:10:47.52	4324.76
☐	V1VC11	BACKUP	DS_1ST_1VTC	VG_1ST_1VTC	ASSIGNED		2021-07-28T11:28:18.93	4324.76
☐	V1VC12	BACKUP	DS_1ST_1VTC	VG_1ST_1VTC	ASSIGNED (Incomplete)		2021-07-28T11:34:02.70	Empty

Current Operation: Indicates the current operation (load, export).

Last Update Timestamp: Date and precise time of the latest modification made to the volume.

Size: Number of megabytes exchanged over the SCSI or fiber link. Empty is displayed when the volume contains only the tape headers and trailers.

Compression Rate: If compression was enabled, Compression Rate displays the ratio (uncompressed data size) divided by the compressed data size.

Use **Previous** (<)**Next** (>) links at the bottom of the data grid to navigate through the list.

Volume Operations

The **Volume Operations** tabbed page allows the user to identify a virtual volume and directly access the volume detail page.

Status	Volume List	Volume Operations	Create Volume	Virtualize Volume	Import From Tape Catalog	Summary
Configuration	**Volume Detail**					
Storage Admin						
Volume	Label Prefix	● Labeled Volumes ○ Unlabeled Volumes				
	Volume Label	[ ]				
		Get Details				

Label Prefix: Indicates whether the volume is labeled or not.

Volume Label: The label of the volume.

Get Details: Link to the **Volume Detail** page.

Volume Details

The **Volume Details** page displays the info available in the BackPak catalog for a specific virtual volume. The operations available for any volume are **Load**, **Materialize**, **Edit**, **Delete**, **Run Backup Script**.

Status	Volume List	Volume Operations	Create Volume	Virtualize Volume	Import From Tape Catalog	Summary
Configuration						
Storage Admin						
Volume						

Load	Materialize	Edit	Delete

Volume Details Refresh

Volume Label	HARRY
Label Type	BACKUP
Data Store	WIN403-LOCALDISK (WINDISK)
Domain Access to Volume	Primary
Volume Group	H403-CAT-WINDISK
Volume Lock	False
Automatic Mount	True
Current Operation	
Last Update	by SUPER.QC on 1/13/2017 1:05:34 PM
Comment	
VTC Host Name	
Status of Catalog Export	Done
Creation Time	1/13/2017 1:05:34 PM
Last Load for Output	
Last NonStop Operation	
	Preload: False
	Last Loaded Device:
	Effective Load Time:
Last Operation	
	Operation Type:
	Last Unload Time:
	Severity:
	Read Bytes Count: 0 bytes
	Write Bytes Count: 0 bytes
Data Size	0 Bytes
Storage Size	0 Bytes (No compression)
Encryption Algorithm	
Key Manager ID	
Encryption Key ID	
Volume Class	CLASS25
Guardian Owner	\ETINIUM 255,50
Authorized Access	NNN
Maximum Volume Size	25,000 MB
Guardian Catalog	Volcat: \ETINIUM.VOLCAT, Pool: H403_POOL_WINDISK
Volume Status In Catalog	SCRATCH
DSM/TC TAPEFILE	
Last Update Index Path	
Check Volume Timestamp	True
Last Storage Unit	
Number Objects	
Check Volume Timestamp	

> **Load**: Links to the **Load** page.
> **Materialize**: Links to the **Volume Materialization** page.

Edit: Links to the **Edit Volume** page.

Delete: Deletes the virtual volume.

Run Backup Script: Not shown if the script option is not licensed, the script is not configured or if you have the Windows Advance Pool Management licensed. Click to run the backup script to backup this volume.

If you have the Windows Advance Pool Management licensed and if the Copy Pool Sync option is activated, it will be replaced by the Copy to Copy pool button. If the volume needs to be sync, the button will be activated and will force the copy of the selected volume. Otherwise, it will be deactivated. If the Copy Pool Sync option is not activated, the button will not be shown.

Refresh: Refreshes the data displayed.

Volume Label: Identifies the virtual volume.

Label Type: Label type, NL, ANSI, IBM, BACKUP or TMF.

Data Store: Identifies the Data Store and its type. (WINDISK or IBM Spectrum Protect™ TSM).

Domain Access to Volume:

PRIMARY: This is the usual value. The current domain owns and manages the Data Store.

SECONDARY: The volume belongs to a Data Store using the CatSync option.

RESTRICTED: The domain has a read-only view of the Data Store. It will miss several metadata associated with the volumes in the domain containing the PRIMARY Data Store.

Volume Group: Identifies the virtual volumes group.

Volume Lock: Manual lock; it prohibits the update of the volume data by a tape application. Equivalent to the read-only lock found on physical media.

Automatic Mount: Manual setting to enable automatic mount when a request is issued by a tape application.

Current Operation: *ANY*, *Free*, *In Use*, *LOAD* (volume loaded and in use), *VIRTUALIZE* (virtual volume being written from external media), *MATERIALIZE* (volume being cloned to physical media), *LABEL* (labeled volume), *TRF_IN* (transfer in), *TRF_OUT* (transfer out), *POST_TRF* (post-transfer).

Last Update: User name and timestamp of the last update of the volume entry in the BackPak catalog. The user name may be an interactive user. The name is "AUTOMATE" for an update executed by the EMS Extractor when loading the volume on a drive.

Comment: User information.

VTC Host Name: Is a VTC that executed the last volume emulation for write or the last backup script.

Status of Catalog Export: *Pending*, *Done*, or *None*. *Pending* if the catalog information has been changed and must be exported, *Done* if the catalog has been exported, *None* if the Catalog Sync Option has not been configured.

Creation Time: This is the time when the virtual volume was created and initially registered in the catalog.

Last Load for Output section:

    Timestamp of the last load for output.

    Tape application process that requested the volume.

Last Operation section:

    Timestamp of the last load.

    Tape Application Process that requested the volume.

    Operation Type: LOAD, VIRTUALIZE, MOVE.

    PreLoad: Indicates if the volume was pre-loaded.

    Effective Load Time: This is different from the last load time, when the VTC replied to the load request with a LOADING, rather than LOADED status, because a long internal operation has prevented a quick reply.

A typical long operation is the execution of a restore script.

Last Unload Time section:

Severity: Severity (success, error, information) of the last operation.

Success indicates that the virtual tape operations were successful. *Error* indicates that a load failed. *Warning* indicates that a volume was loaded, but some event occurred after the tape was loaded. Such events are Data Store I/O errors or manual unloads.

Last Loaded Device: Last device where the volume was loaded.

Volume Sequence Number: Rank in a multi-volume backup set.

Read Byte Count: Bytes read by the NonStop host (last load).

Write Byte Count: Bytes written by the NonStop host (last load).

Data Size: Number of bytes written by the NonStop and stored in the virtual volume.

Storage Size: Number of bytes kept for storing the virtual volume and if compression was used.

Encryption Algorithm: When volume is Encrypted, specify the type of Encryption used (VLE or Non-VLE)

Key Manager ID: Identifies which key manager has been used to generate and store the Encryption key.

Encryption Key ID: Identifies the Encryption key ID.

Volume Class: BackPak current volume class. This volume was assigned to the class specified in the Volume Group when it was loaded for output.

Guardian Owner: Node and user ID running the last tape application that requested the volume for output. This user ID can be identified only if the mount was executed in the context of a load request, i.e. automatically or manually requested from a pending mount. For other

manual loads, the owner will be the BackBox interface user. Before the first load, the owner is the user who created the volume in the domain catalog.

When the Data Store is RESTRICTED, the owner kept in the domain is used only for authorizing Control Access. The access to data is controlled by the ownership copied along with the volume data in the Data Store at backup time.

Authorized Access: Authorizations set when the volume was created or the last time the volume was loaded for output.

When the Data Store is RESTRICTED, the authorization kept in the domain is used only for authorizing Control Access. The access to the data is controlled by the Authorizations copied along with the volume data in the Data Store at backup time.

Maximum Volume Size: Maximum volume size, effective last time the volume was loaded for output.

Guardian Catalog: It is for a DSM/TC catalog, VOLCAT, for POOL names, and for a TMF, and Guardian node name.

Volume Status in Catalog: Status of the volume in the Guardian tape catalog (DSM/TC, TMF, QTOS, none).

DSM/TC TAPEFILE: The first non-expired TAPEFILE in DSM/TC, associated with this volume.

1st TAPEFILE HEADER: Information extracted from the first HDR1 tape header of the volume. It is displayed only if the catalog type is not DSM/TC or TMF. Displayed items: the file ID, the generation, and the expiration date.

> ⚠️ The expiration is to be interpreted carefully as there may be an override by a third party catalog on the NonStop system ID.

Last Update Index Path: Windows disk path containing the index file of the volume the last time the volume was written by the NonStop host. In the restore script, this path is used to qualify and identify the backup software for the Windows files to restore.

Last Update Data Path: Windows disk path containing the data file of the volume and the last time the volume was written by the NonStop host. In the restore script, this path is used to fully qualify and identify the backup software for the Windows files to restore.

The data path is almost always equal to the index path, and therefore not displayed when equal to the index path.

Check Volume Timestamp: When the Timestamp checking is enabled in the Data Store configuration, the VTC checks if the volume timestamp given by the Domain Manager (Last Load for Output) matches the time stamp stored in the Windows files.

Volume Load

The **Volume Load** page allows manually loading a media file on a NonStop tape drive, even if the mount hasn't been required by the system.

> ⚠️ The manual load could be initiated through the Status page for the NonStop Node where the pending mounts are listed. The load will then execute the mount, even if the mount hasn't been required by the system.

When a volume is loaded using this page, the load is executed without the context of a mount request. Therefore, it might fail because of the configured automation. If the volume was created in an "Auto-scratch" Volume group associated to DSM/TC, an error - such as "file not found" - can occur; the volume will be created only by running a BACKUP with a TAPECATALOG DEFINE.

| Status | Volume List | Volume Operations | Create Volume | Virtualize Volume | Import From Tape Catalog | Summary |

Load Volume into Tape Device

Volume	HARRY BACKUP
Node*	\ETINIUM
Device*	** AUTO-ASSIGN **
Comment	
Volume Lock	☐
Tape Use	IN – Read only mode

[Load]

Volume: The volume label and label type to load.
Node: Guardian node of the tape device where to load the volume.
Device: Guardian tape device to load the volume on. If left to AUTO-ASSIGN, the Domain Manager will choose a device.
Comment: Free text kept in the BackPak catalog for the volume.
Volume Lock: Check to prohibit updates of the volume by a tape application.
Tape Use: IN or OUT, tape use of the mount request.
Load: Submits the load request to the Domain Manager.

Volume Materialization

The **Volume Materialization** page is used to clone a single virtual volume to a physical media loaded on a VT Controller attached drive.
This operation was named "Volume Export" in older BackBox versions.
The physical media capacity must be able to contain the whole virtual volume. Check Data Size on the volume detail page.

Status		Volume List	Volume Operations	Create Volume	Virtualize Volume	Import From Tape Catalog	Summary
Configuration							
Storage Admin		**Volume Materialization** Status					
Volume							

Volume Materialization Status

Volume Label   HARRY

Windows Tape Device

VT Controller ID*   * Select VT Controller * ▾

Tape Device*   ▾

Compression   ☑

Idle Time out   10   min

[Materialize] [Cancel]

Status: Links to a Status page that will show all virtualizations and materializations on all VTCs that have configured physical/external tape drives.

Volume Label: Volume label to export.

The **Windows Tape Device** section describes the target device for this operation.

VT Controller ID: Identifies the VT Controller that is equipped with a tape device to write on and that is a route for the Data Store attached to the Volume Group.

Tape Device: Allows to select physical tape device that is attached to the specified VT Controller. The physical tape device needs to be declared in the VT Controller Advanced configuration page prior to being used in materialization.

Compression: If applicable, the **Compression** checkbox can be checked on to enable the compression feature of the device.

Idle Time Out: Maximum time the VTC will wait for the media to be loaded before ending the Materialization session.

On materialization the UI will issue the following message: *I3386 Materialization initiated in VTC xxxx on device device.*

The EMS will report the starting, the ending of the Materialization session, and the status of the volume process (e.g. "ended successfully").

```
15:55 \ETINIUM BPAK-TINTIN-I5110 Starting MATERIALIZE session
on tape device SDLT
15:56 \ETINIUM BPAK- TINTIN -I5050 Materializing virtual volume
BBC001 started successfully
15:57 \ETINIUM BPAK- TINTIN -I5046 Materializing virtual volume
BBC001 ended successfully
15:57 \ETINIUM BPAK-TINTIN-I5111 Ending MATERIALIZE session on
tape device SDLT
```

Volume Details Edit

Volume Label: Volume label to update.

Last Update: Date and time of the last update.

Domain Access to Volume: Domain access to this specific volume.

PRIMARY: Volume owned and regularly operated by the domain.

SECONDARY: Volume replicated from a PRIMARY site.

RESTRICTED: Volume owned by another domain.

This attribute can be updated only when the Data Store has been promoted from RESTRICTED to PRIMARY, as the volumes are progressively migrated to the PRIMARY state as they are rewritten.

Volume Lock: Prohibits the update of the volume data by a NonStop tape application. It is the equivalent of the lock found on some physical media.

Check Volume Timestamp: When the Timestamp checking is enabled in the Data Store configuration, the VTC compares the volume timestamp stored in the BackPak catalog to the timestamp stored either in the Windows files (WINDISK) or the IBM Spectrum Protect™ (TSM) objects (TSM API).

Automatic Mount: Enables the automatic mount.

Current Operation: Applicable if the volume is currently known as "in use". Reset the current operation of the volume to none. This is an option to be used when the end of an operation was not registered by the BackPak domain.

The current operation status (such as LOAD or MATERIALIZE) is set when an operation starts and is reset when the VT Controller returns results and statistics to the Domain Manager. If the end

of an operation is not received by the Domain Manager, the VT Controller will retry for up to seven days, then it stops.

The operation status is used as a lock to avoid concurrent operations on a volume. Check the Reset box, to allow a new operation.

Guardian Node Owner, Guardian User ID Owner: Owner of the volume used for access control. Updatable only if the user, logged to the UI, has Control Access to the volume or is SUPER.SUPER.

Comment: The comment box allows the user to add a comment.

Authorized Access: Updatable only if the user logged to the UI has control access to the volume or is SUPER.SUPER.

> **Read Access**: User category authorized to read access.
>
> **Write Access**: User category authorized to read/write/delete access.
>
> **Control Access**: User category authorized to change security settings.

Last Update Index Path (WINDISK only): Gives the last known location of the .IND file. This is a Windows disk path, used as the original path name for a restore operation in the restore script. This field should be modified only if a restore script fails and if the user knows the correct original path name for the restore command.

Last Update DAT File Path (WINDISK only): Gives the last known location of the .DAT file. This is a Windows disk path, used as the original path name for a restore operation in the restore script. This field should be modified only if a restore script fails and the user knows the original path name for the restore command.

The 'Last Update DAT File Path' is almost always equal to the 'Last Update Index Path'. These two values are changed only when the NonStop writes a new backup on the virtual volume, and when the Admin service moves volumes from the Spare Pool to the regular Storage Pool.

Volume Deletion

Volume Deletion feature can be accessed through the **Volume List** page or the **Volume Detail** page.
- Once deleted, the selected volumes will be:
- Deleted in storage
- Deleted in its associated catalog (DSM/TC or TMF)
- Removed from the BackPak domain catalogue of virtual volumes.

Validations:

- A volume of a Volume group associated with an integrated catalog (DSM/TC, TMF) cannot be deleted in storage if it is not marked as SCRATCH or BAD in the catalog. This validation cannot be overridden unless the action is only to remove the volume from the BackPak domain catalog of the virtual volume.

- As an additional safety measure, volumes cannot be deleted when not expired in accordance with their original retention specification, as stored in the HDR1 tape header. This safety validation can be overridden on the **Volume Deletion** confirmation page.
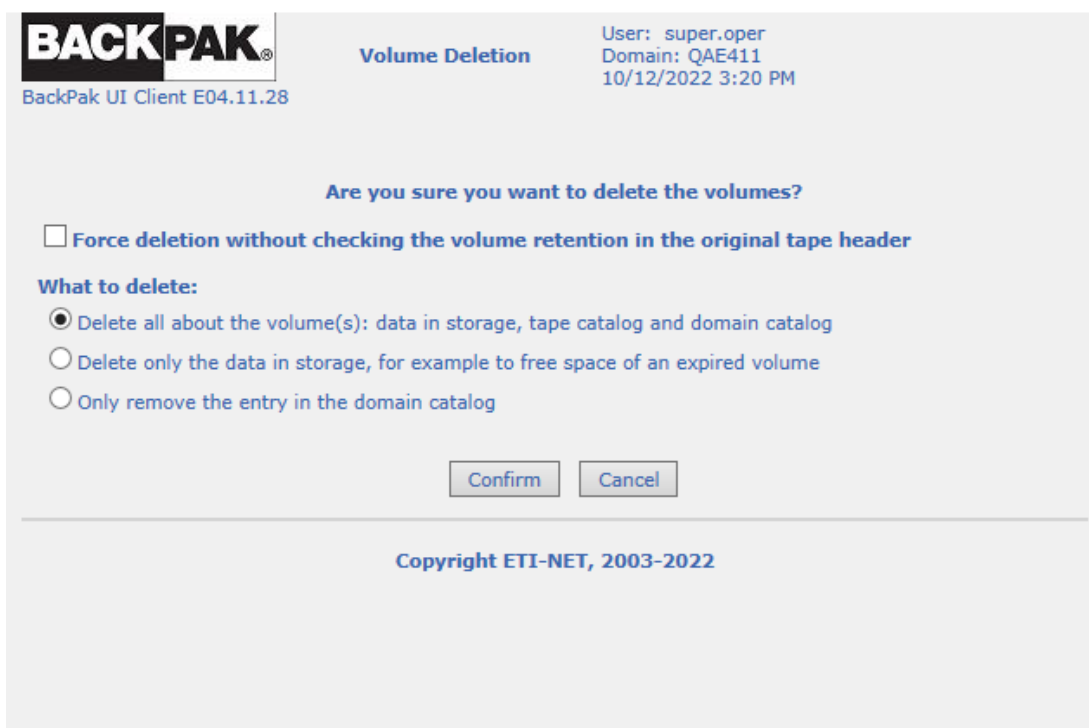
Force deletion without checking the volume retention in the original tape header

This is a safety feature to protect against unexpected manual handling and against wrong / in-progress configuration.
BackPak deletes expired volumes and validates the manual volume deletion after verifying the status of either SCRATCH (in DSM/TC) or TMF.
During migrations or setup modifications, it might happen that the link of a BackPak volume group to the DSM/TC is invalidated, or that the DSM/TC which must be migrated from another system is not yet populated.

⚠️	To prevent data deletion, BackPak verifies the expiry date written in the first HDR1 tape header at backup time. For the online storage, this data is verified in the tape image itself, and for the offline storage, the data is verified in the HDR1 image saved in the BackPak domain at backup time.

There are legitimate deletion cases prevented by this. If an aborted backup is usually made "SCRATCH" by the DSM/TC the day after rather than exactly on the expiry date, the delete action takes place. Another case is if a user wants to delete an useless backup through "MEDIACOM DELETE TAPEFILE".
The free-up of storage for SCRATCH Volumes will be rejected in BB017_FREE_EXPIRED with an error message such as:

> E2617 Deletion of Volume xxx rejected. Volume is not expired according to the original expiry date 2017-07-22. To delete anyway, specify **force** in the UI Volume Delete confirmation window. To keep the volume in catalogs, choose **Delete only data** in UI.

As indicated in the message, the storage free-up must be forced manually by the BackPak UI Delete volume page with the Force and Delete only data options.

The scope of the deletion can be adjusted while confirming the deletion.

What to delete:

- Delete all about the volume(s), data in storage, tape catalogue and domain catalogue. This is the default option, where the data, the volume entry in the DSM/TC and in the BackPak domain will be deleted.

- Delete only the data in storage, for example, to free space of an expired volume. The volume will still be available for the next backup and the volume entry in the DSM/TC and BackPak domain are retained.

> ⚠️ This is the option recommended to avoid the repetition of messages E2617 issued by BB017_FREE_EXPIRED for volumes that have been prematurely scratched.

- Remove only the entry in the domain catalog. The volume which can still be available in another tape system may be a physical tape. There is no check mark against the DSM/TC or TMF volume status; the status can be ASSIGNED. This is an option to use after a virtualization executed with wrong parameters, and it must be re-executed.

Create Volume

The **Create Volume** page is used to create new volumes, label them, add them to the library, and catalog them in an external catalog (i.e. DSM/TC or TMF), if needed.

| Volume List | Volume Operations | Create Volume | Virtualize Volume |

Volume Description

Volume Label*

Label Type* `BACKUP ▼`

Comment

Volume Group* `* Select Volume Group * ▼`

Quantity (1 to 999)*

Increment Base `10 Digits to build the next labels: 0~9 ▼`

☑ Allow volume to be automatically mounted

`Add`

Volume Label: Specifies the label of the first volume to be created. To create more than a single volume, the end of the label must be consistent with the "Quantity" and "Increment Base" below.
E.g.: 3 digits are required to create 100 volumes in base 10.
Label Type: Indicates the volume label type. Values are: Unlabeled, ANSI, Backup, IBM and TMF.
Comment: User comments describing the purpose or the content of the volume. This comment is preserved with the volume in the catalog.
Volume Group: Selects the Volume Group in which to add the volume. The Volume Group determines in which Data Store the volume will be created, as well as which other attributes, such as the associated DSM/TC pool, are to be considered.
Quantity: Indicates the number of volumes to be created. You can create 999 volumes at a time.
Increment Base: Select the base used to compute the next label to create more than a single volume. By default, only 1 digit will be used (base 10). To create more volumes in a range of labels, use hexadecimal (base 16) or base 36 (0 to Z) digits.

Increment Base

```
10 Digits to build the next labels: 0~9
16 Digits to build the next labels: 0~9A~F
36 Digits to build the next labels: 0~9A~Z
```

Allow Volume to be Automatically Mounted: Check the box to have the created volume(s) automatically loaded when a mount request is issued in EMS.

The Tape Creation - Progress page appears when the volume creation is in progress.

Tape Creation – Progress
Please Wait - Tape creation still in progress
Currently creating tape 1 of 20

Cancel
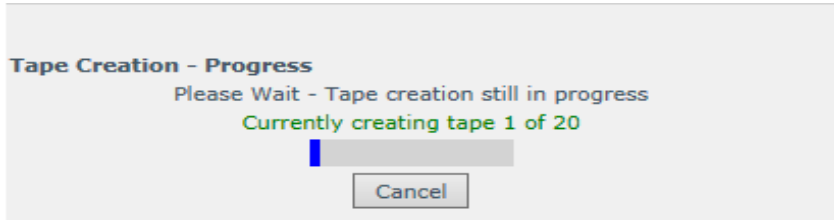
A message is displayed when the process is complete.

Tape Creation – Progress
Tape Creation is now completed
20 volume(s) created from label BBOB00 to BBOB19

Back to Volume Creation
Back to Volume List
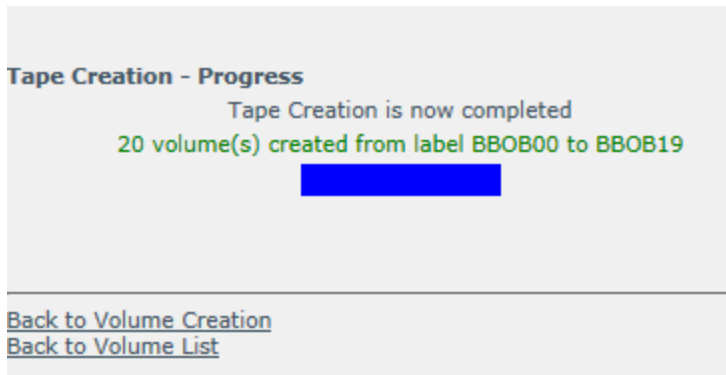
Virtualize Volume

The **Virtualize Volume** page is used to clone physical or other legacy media to a BackBox virtual volume. Before or after initiating the operation, a physical media must be loaded on a VT Controller attached tape drive or a volume materialization must be initiated in a third party VTS connected to a VTC. At the end of the virtualization, the media is unloaded and any subsequent media presented by an auto-loader or an operator will be virtualized without manual intervention in BackBox.
The virtualization task stops if no media has been loaded during the entered Idle time out time.
Physical drives and drives used to directly connect another Virtual Tape System are presented and managed in the same way.

- For a Non-Labeled volume, the BackPak name for this volume must be entered to allow the virtualization to be submitted for a single volume.

- For Labeled volumes, the label will be read from the physical media and cannot be changed.

The maximum volume size configured in Volume Groups must be able to contain the entire physical media.
The NonStop tape catalogs associated with the Volume Groups (TMF, DSM/TC or QTOS) are not updated. The media that has to be virtualized must be already cataloged if the Volume Group is associated with a NonStop tape catalog.
A Status page shows the running virtualization-materialization tasks and allows task cancellation at any time.

| Volume List | Volume Operations | Create Volume | Virtualize Volume | Import From Tape Catalog | Summary |

Volume Virtualization Status

☐ Searching in DSM/TC, TMF and QTOS catalogs

○ Labeled Volume   ◉ Non-Labeled Volume
Windows Tape Device
VT Controller ID*   [KRAKEN ▼]
Tape Device*   [DIANATAPE (IBM-ULT3580-TD4) ▼]
Idle Time out   [10] min
New Virtual Volume Label*   [ECIY07]
Volume Group*   [BACKUP_ETI_NOCAT ▼]
     Description:
     Volume Capacity: 25000 MB
     Data Store: KRAKEN_STORE01(WINDISK)
     Catalog Type: No Catalog

Comment   [   ]

☐ Allow virtual volume to be automatically mounted.
☐ Volume lock

[Virtualize]

Status: Link to a Status page that will show all virtualizations and materializations on all VTCs that have physical/external tape drives configured.

Searching in DSM/TC, TMF and QTOS Catalogs: Check when the volumes are already known in one of these NonStop tape catalogs: TMF, DSM/TC and QTOS.

When the volume is found in one of the catalogs associated with BackPak Volume Groups, the volume to virtualize is automatically associated with the corresponding Volume Group.

This allows submitting batch virtualization for any volume.

Only catalogs associated with Volume Groups belonging to PRIMARY Data Stores are considered.

The volumes that are not found in any catalog will be rejected, unless a Volume Group for Non-Cataloged Volumes is specified.

VT Controller ID: VTC where physical tape devices are attached for reading the tape volumes.

Tape Device: Select a device among physical tape devices configured in the VT Controller Advanced properties or select "All tape devices".

Idle time Out: Maximum time the VTC will wait for the first media and for a new media to be loaded (by manual load or by the auto-loader) before ending the Virtualization session.

Catalog Search in Node: Select one of the nodes that contains tape catalog(s) named in Volume Groups or select "ALL NODES" to search in all catalogs.

Send volumes of a single node in a virtualization batch and specify the node name in this field to avoid inter-node mix-ups.

Volume Group for Non-Cataloged Volumes: Selects the Volume Group where the volume is created. The Volume Group determines in which Data Store the volume is created, as well as other characteristics of the virtual volume (e.g. capacity, external catalog, etc.)

TMF DUMP Type: This element is required, if the chosen Volume Group catalog type is TMF. The possible values are AUDIT DUMP and ONLINE DUMP.

Comment: User comment. This comment is stored in each created volume entry in the BackPak catalog.

Allow Virtual Volume to be Automatically Mounted: Check to have the created volumes automatically loaded when a mount request is issued in EMS.

Volume Lock: This prohibits any update of the volume content by the NonStop tape applications. This is similar to an infinite retention. This attribute is also stored in the volume entries created in the BackPak catalog.

Volume List	Volume Operations	Create Volume	Virtualize Volume	Import From Tape Catalog	Summary

Volume Virtualization Status

☐ Searching in DSM/TC, TMF and QTOS catalogs

◉ Labeled Volume   ○ Non-Labeled Volume
Windows Tape Device
VT Controller ID*   [* Select VT Controller * ▼]
Tape Device*   [▼]
Idle Time out   [10] min
Volume Group*   [* Select Volume Group *   ▼]

Comment   [   ]

☑ Allow virtual volume to be automatically mounted.
☐ Volume lock

[Virtualize]

       Labeled/Non-Labeled Volume: Type of media to virtualize. If Non-Labeled, the BackPak name for this volume will be requested.

The UI will show the following messages: `I3385 Virtualization initiated on 1 devices in VTC VTC85.`

EMS will report the virtualization starting and ending session and each volume processing status.

```
15:03 \ETINIUM.BPAK-MTLBBLAB1-I5108 Starting VIRTUALIZE session on
tape device OVERLAND
15:03 \ETINIUM BPAK-MTLBBLAB1-I5051 Virtualizing physical volume
OBCD53 started successfully
15:04 \ETINIUM BPAK-MTLBBLAB1-I5053 Virtualizing physical volume
OBCD53 ended successfully
15:05 \ETINIUM BPAK-MTLBBLAB1-I5051 Virtualizing physical volume
OBCD51 started successfully
15:06 \ETINIUM BPAK-MTLBBLAB1-I5053 Virtualizing physical volume
OBCD51 ended successfully
15:12 \ETINIUM BPAK-MTLBBLAB1-I5044 Cannot open tape device OVERLAND
: No media in drive.
15:12 \ETINIUM BPAK-MTLBBLAB1-I5109 Ending VIRTUALIZE session on tape
device OVERLAND
```

Virtualization / Materialization Status

This page can be accessed by a link in the **Materialization / Virtualization** page.
It shows all VTCs that have physical tape drives configured (or drives directly connected to a Virtual Tape System). For each listed VTC, the materialization/virtualization running tasks are listed.

VTC name (Show/Hide Details…)

The external devices are listed by VTC names. Click **Show Details** to see the tasks related to the attached physical devices.

> **Check Box**: Select the tasks to be cancelled.
> **Alias Name**: Name given to the device in the VT Controller Advanced Properties.
> **Serial Number**: Device serial number.
> **Domain**: The Domain that has initiated the task.
> **Operation**: VIRTUALIZE or MATERIALIZE.
> **Task State**:
>> IDLE (waiting for a media be loaded)
>> PROCESSING (media loaded being processed)
>> CANCELLING (a cancel task has been initiated).
> **Encrypted**: Encrypted volume
> **Volume Label**: Volume label being materialized/virtualized.
> **Load Time**: Time when the volume was loaded.
> **Elapsed Time**: Time since the volume was loaded.
> **Unit Ready Time**: Elapsed time after the volume is loaded, waiting for the 1st data block.
> **First Data Time**: Elapsed time until 1st data block is written.
> **Write Byte Count**: Size of data written to the BackBox virtual volume.
> **Read Byte Count**: Size of data read from the BackBox virtual volume.

Import From Tape Catalog

This page is used to register certain volumes (those already known in a tape catalog on the NonStop DSM/TC, TMF or QTOS) in the BackPak catalog.
This procedure is normally used at the beginning of a migration from a legacy storage system to Back-Box; in this case only SCRATCH Volumes will be registered.
For a migration, the registration of ASSIGN media must be done by the function Virtualize Volume that transfers data and registers the volume.

Experienced users can use this function to re-register all tape volumes of a Volume Group.

Import from Tape Catalog updates only three items:

- Create volume entries in the BackPak Domain.
- Create empty volumes in the storage for SCRATCH and RELEASE volumes associated with a Volume Group that is not set for Auto-scratch.
- If needed, update the media type in DSM/TC to match the media type configured in the BackPak Volume Group.

Volumes that already exist in the domain are skipped if they belong to the same Volume Group. If they belong to another Volume Group, they will migrate to this new group.

> **Volume Group**: Selects the Volume Group for which virtual volumes will be registered. BackPak will get the volume entries in the tape catalog associated with this Volume Group (for example, a DSM/TC pool in a given DSM/TC VOLCAT).
> All SCRATCH Volumes (or all volumes) of a DSM/TC pool, a QTOS vault, or a TMF node catalog in a node, will be registered in the domain.
> **Import only the SCRATCH Volumes for a migration to BackBox**: Check to select only the SCRATCH and RELEASED Volumes.

Feedback

The UI replies with the message below and processes the media in the background.
I3447 Process $Z50C initiated to import scratch & released volumes from the catalog DSM/TC volcat: \ETINIUM.TAPECAT, pool: BBOX_WIN1 (Volume group BBOX_WIN1).
EMS messages are issued to report the process start and process completion.

```
11:23 29AUG13 222,01,207 BPAK-I3447 Process $Z50C initiated to
import  scratch  &  released  volumes  from  the  catalog  DSM/TC
volcat: \ETINIUM.TAPECAT, pool: BBOX_WIN1 (Volume group BBOX_
WIN1).
11:23 29AUG13 222,01,207 BPAK-I3448 Process $Z50C import from
the catalog DSM/TC volcat: \ETINIUM.TAPECAT, pool: BBOX_WIN1 to
Volume group BBOX_WIN1ended. 11 volumes were created in Back-
Pak, 0 volumes were migrated from other Volume groups.
```

Summary

The summary displays the overall statistics information of virtual volumes per Volume Group. The information is based on data from the VOLUME file only.

					Administration			

Volume List	Volume Operations	Create Volume	Virtualize Volume	Import From Tape Catalog	Summary

Data Store ID	Store Type	Volume Group	Number of Volumes	User Data Size (MB)	Storage Size (MB)	Average Compression Ratio	Number of Scratch Volumes	Potential Size of Scratch Volumes (MB)
WIN1	WINDISK	NOCAT1	5	105	105	1.00	n/a	n/a

To display this page, the volume status in DSM/TC, TMF or QTOS is assumed to be the same as it was the last time the media was loaded.
To refresh the status of all volumes, re-execute OBB017.
The Summary section displays the following information:

Data Store ID: The Data Store name.
Store Type: The Data Store type (IBM Spectrum Protect™ TSM or WINDISK).
Volume Group: Volume Group name.
Number of Volumes: Number of volumes in this Volume Group.
User Data Size: The total size of all volumes data in this Volume Group. The computed size is based on the length of data buffers received from the NonStop host last time each volume has been written. This is the uncompressed size.
Storage Size: The total size of storage allocated to the volumes of the current Volume Group. This is the compressed size for both WINDISK and IBM Spectrum Protect™ (TSM) Data Stores.
Average Compression Ratio: [User Data Size] divided by [Storage Size].
Number of SCRATCH or Scratch Volumes: Applies only to Volume Groups associated with DSM/TC or TMF catalog. This is the number of SCRATCH Volumes in this group. Volumes are considered SCRATCH if they had the SCRATCH status in DSM/TC or TMF last time BB017_FREE_ EXPIRED was executed or last time the volume detail was displayed.
Potential Size of SCRATCH or Scratch Volumes: Maximum space available for new backups, based on the number of Scratch Volumes. This number is computed by multiplying the number of Scratch Volumes by the maximum volume size set in the Volume Group. The Potential Size info does not give any indication on the actual storage available to the Data Stores in Windows disks or IBM Spectrum Protect™ (TSM) storage pools.

DataStore Administration

The **Storage Admin** page displays a list of the configured Data Stores.

Data Store	Type	Status	Domain Access	Catalog Sync Import/Export		Running Jobs
DS-GUARDIAN	WINDISK	Active	Primary	Export Status	Catalog Detach	
DS-OSS	WINDISK	Active	Primary	Export Status	Catalog Detach	
DS_DATADOMAIN	WINDISK	Active	Primary	Export Status	Catalog Detach	SpareMove(1)
DS_DATADOMAIN_DD_BOOST	WINDISK	Active	Primary	Export Status	Catalog Detach	
DS_QURESTORE	WINDISK	Active	Primary	Export Status	Catalog Detach	
DS_STOREONECE	WINDISK	Active	Primary	Export Status	Catalog Detach	SpareMove(1)
DS_WIN_REMOTE	WINDISK	Active	Primary	Export Status	Catalog Detach	
OLDVTCQS_DS-GUARDIAN	QORESTOR	Active	Primary	Export Status	Catalog Detach	
OLDVTCQS_DS-OSS	QORESTOR	Active	Primary	Export Status	Catalog Detach	
QS_DATASTORE	QORESTOR	Active	Primary	Export Status	Catalog Detach	SpareMove(1)
QS_DATASTORETEST	QORESTOR	Active	Primary	Export Status	Catalog Detach	
TEST-PATH1	WINDISK	Active	Primary	Export Status	Catalog Detach	SpareMove(1)

Page elements

Data Store: Data Store name. This is a link to the actual management of WINDISK Data Stores. TSM is managed through a IBM TSM administrative client.

Type: Data Store type: WINDISK, TSM or QORESTOR

Status: Activation status configured for the Data Store.

Domain access: Domain access configured for the Data Store.

Catalog Import/Export: Link to the status page of catalog Export or Catalog Import. Refer to the Back-Pak Catalog Sync Option manual. This link is present only if the BackPak Catalog Sync Option is enabled by the license key.

Catalog Detach: Link to a window that will detach the Data Store and its tape volumes from the current BackPak Domain.

Running Jobs: Displays the jobs currently running on the Data Store. If the job(s) has been completed, there will be no value showing in the column. To see all the jobs completed on the Data Store, see Data Store details page and select **Jobs** in the Detail Report panel.

Catalog Detach

This function is a tool to help a reorganization of BackPak domains, to help changing the distribution of virtual volumes in different domains. It is most often used to complete the move of a Data Store from a domain to another, by removing the source.

> ⚠️ The 'Catalog Detach' will just remove the virtual volumes of a specified Data Store from the catalog of the current BackPak Domain.

The images of virtual volumes in the storage and the possible corresponding entries in DSM/TC & TMF catalogs are not deleted or altered in any way.

Considering only the BackPak catalog (not considering the volumes in storage and DSM/TC), the complete scenario of moving a Data Store from a BackPak Domain to another domain consists in:

1. The volumes entries are first replicated into a SECONDARY Data Store of the new domain by the Catalog Sync Option. Or, they are registered in the new domain manually by creating series of consecutive labels into a RESTRICTED Data Store.

2. The volumes entries are then "de-registered" from the original domain by a Catalog Detach.

3. The domain access of the Data Store in the new domain is promoted from SECONDARY (or from RESTRICTESD) to PRIMARY to allow regular operations including backups.
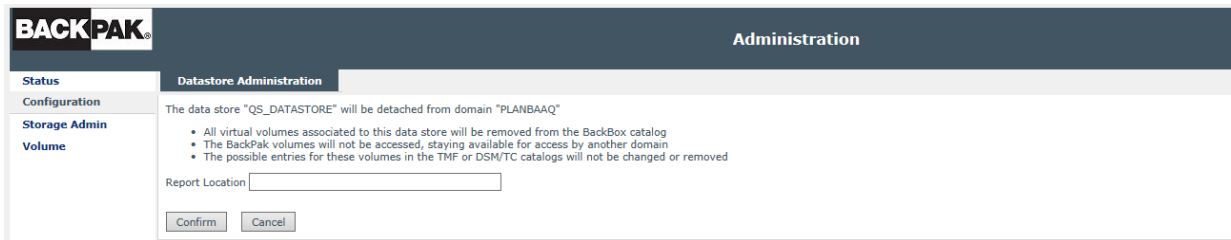
Page sections

Report Location: Destination of the control report that will list the detached volumes. It can be a disk file name or a spooler specification such as $S.#BPAK.DETACH.

Windows Files Administration

Several management tasks for Windows files Data Stores, such as creating directories or shared drives, setting security are accomplished by using Windows tools on the VTC.

BackBox specific Data Store tasks are accessed from the Data Store Admin page by clicking on the name of the Data Store.

This page shows information about the virtual media files present on the disks configured in a Data Store. The file numbers and sizes are computed as reported by the Windows file system. Note that both the index and data files are counted and summarized in the size.

> ⚠️ Files deleted containing empty volumes or archived by Enterprise backup software are not included.

Data Store DS_1COPY_DD

Storage Route [First Available VTC ⌄]   Reply from: BBOX2019-1   [Refresh]

Pool	Free Space(MB)	Number Of Files	User Data Size(MB)	Non-Backed-Up Files	Last Update
Storage - Spare		0		0	
Copy	700,412.52	2	104.04		10/4/2021 5:35:58 PM

Detail Report By: ● Path   ○ Volume Group   ○ Jobs

Pool	Volume SerialNumber	Disk Space	Disk Free Space	Path	Rank	Number of Files	User Data Size (MB)	Number of Non-Backed-Up Files	Size of Non-Backed-Up Files(MB)	Last Update	Path Status
Storage				\\192.168.20.22\QA\	1						Error code: 20061. Folder access test as failed: (53) The network path was not found.
Copy	1621582091	698.38 GB	434.61 GB 62.23%	\\BBOX2019-1 \DS_DD_COPY\		2	104.04			10/4/2021 5:35:58 PM	Good
Copy	0	353.02 GB	249.39 GB 70.65%	\\192.168.20.22 \DDOS_7305\		0	0.00				Good

Page sections

Storage route: choice of the VTC that will gather the information. The "1st available VTC" or a specific VTC can be chosen in the selection list

Reply from: actual VTC that provided the data

Detail Report: The sum of files distributed by:

Path: List of paths configured in the Data Store (initial view).

Volume Group: List of Volume Groups configured in the Data Store

Jobs: Displays the status of jobs associated with the Data Store

Page elements for Summary

Pool: the Summary in two sub-totals by pool:

- "Storage and Spare": all volumes of the Data Store, excluding the duplicates from the "Copy": pool
- "Copy": only the replicated volumes

Free Space (MB): Total of free disk space.

Number of Files: Number of files in all paths and their subdirectories.

User Data Size(MB): Total size of all files.

Non-backed-up Files: Number of files that have the Archive bit set. This is not shown for StoreOnce NAS.

Last Update: Most recent updated files

Backup all non-backed-up files: This link is shown if the Data Store is not configured for "StoreOnce NAS" optimization and is configured with a backup script.

This function submits a backup script for each file that has the Archive bit still set.

The backup script is normally automated after each backup and if enabled, the script controller will automatically retry failed backups. Files marked as not backed up are usually either still being backed up or in the script controller input queue.

This button is for re-submitting manually the backup scripts that have failed for reason unrelated to the software like communication or power failures. Notice that the Script controller (the script contains the BBBACKUP command) contains its own retry mechanism; in this case the manual retry is required only after the controller stops retrying, such as after a VTC reboot.

When the "Storage Route" is set for a specific VTC, the scripts will be submitted only to this VTC.

When the "Storage Route" is set for "1st available VTC" the scripts will be distributed depending on preferences according the volume information available in the domain:

- The VTC which contains the Windows files of the volume will be preferred. The VTC is supposed to contain the volume if the last known file location has an UNC syntax, such as \\svr1\share1, and the server name part is equal to the VTC IP address or to the last known VTC hostname.
- The VTC who has written the Windows files is preferred.
- If the preferred VTC is not reachable by TCP/IP, does not contain the backup script, or is not able to submit the script, another route will be tried.

Move Files from Spare pool: This link is shown there are some files in the Spare pool.

Clicking this button asks for confirmation, then it submits to the VTC specified in "Storage Route" a task for moving all files corresponding to virtual volumes of the Data Store from the Spare pool to the regular Storage pool.

The moving task in the VTC reports its startup and end in EMS, and potential errors.

```
2013-09-19 17:35:44 \ETINIUM.$X1FA ETINET.100.100 5120 BPAK-DUPONDT-
I5120 Start moving data store WIN1 files from Spare pool to Storage
pool Event time:2013-09-19 17:22:04
```

```
2013-09-19 17:35:44 \ETINIUM.$X1FA ETINET.100.100 5124 BPAK-DUPONDT-
I5124 Moving data store WIN1 files from Spare pool to Storage pool
completed Event time:2013-09-19 17:22:05
```

> ⚠️ In case of spare pool capacity limitations (less than 10% of total space available), space error messages will be shown in the **Path Status** column. Nonetheless, both **Backup all non-backed-up files** and **Move Files from Spare pool** functions are available.

Note if a restore script is configured: it is assumed the files will be backed up again by the Enterprise Backup when the files are discovered in the new disk location. The current BackBox version does not submit backup script after a **Move from Spare**; if the Data Store is configured for backups by script, the user has to manually initiate the backup of the moved file.

Because of this assumption, the last known location of the Index and data files is updated in the Back-Pak catalog for the moved volumes. If there is no new backup, any future restore script will fail simply because the Enterprise Backup does not know the file, even if a copy produced from the Spare pool by the backup script is present in the Enterprise Backup.

Page elements for Detail Report by Path

Pool: "Storage", "Spare", "Copy" or "Migration"

Volume Serial Number: Corresponds to each storage path. If different storage paths point at the same storage volume, the volume serial number appears the same for the respective paths. In the table on the **Storage Admin** page, **Disk Space** column and **Disk Free Space** column will display the same value, as the volumes pointed at are the same.

> ⚠️ In some cases, such as StoreOnce, the same volume serial number can be shared among different volumes across different servers. For QoreStor servers, even though the containers are defined based on the same storage volume, they'll have different volume serial numbers listed on the **Storage Admin** page.

Disk Space: Total disk capacity

Disk Free Space %: Percentage of free space in the Disk Space.

Path: Path name, as configured in the Data Store pool.

Rank #: Configured rank of the path in the pool.

Number of Files: Number of Windows files in the path.

User Data Size(MB): Used space with value given in MB (megabytes)

Number of Non-Backed-Up Files: Total number of files that haven't been backed-up.

Size of Non-backed-up Files (MB): Total size of non-backed-up files with value given in MB (megabytes).

Last Update: Time stamp of the latest update

Path Status: Path Status verified by the system. If validated, the status will be shown Good. In case of a path error the column will display the error code and message.

DS_1COPY_DD Administration

Data Store DS_1COPY_DD

Storage Route — First Available VTC — Reply from: BBOX2019-1 — Refresh

Pool	Free Space(MB)	Number Of Files	User Data Size(MB)	Non-Backed-Up Files	Last Update
Storage - Spare		0		0	
Copy	700,412.52	2	104.04		10/4/2021 5:35:58 PM

Detail Report By: ● Path ○ Volume Group ○ Jobs

Pool	Volume SerialNumber	Disk Space	Disk Free Space	Path	Rank	Number of Files	User Data Size (MB)	Number of Non-Backed-Up Files	Size of Non-Backed-Up Files(MB)	Last Update	Path Status
Storage				\\192.168.20.22\QA\	1						Error code: 20061. Folder access test as failed: (53) The network path was not found.
Copy	1621582091	698.38 GB	434.61 GB 62.23%	\\BBOX2019-1 \DS_DD_COPY\		2	104.04			10/4/2021 5:35:58 PM	Good
Copy	0	353.02 GB	249.39 GB 70.65%	\\192.168.20.22 \DDOS_7305\		0	0.00				Good

Page elements for Detail Report by Volume Group

BACKPAK

Administration

User: super.oper
Domain: SHCH409
10/19/2021 1:32 PM
Sign out

Hewlett Packard Enterprise

Status
Configuration
Storage Admin
Volume

DS_1COPY_DD Administration

Data Store DS_1COPY_DD

Storage Route — First Available VTC — Reply from: BBOX2019-1 — Refresh

Pool	Free Space(MB)	Number Of Files	User Data Size(MB)	Non-Backed-Up Files	Last Update
Storage - Spare		0		0	

Detail Report By: ○ Path ● Volume Group ○ Jobs

Volume Group	Number of Files	User Data Size(MB)	Number of Non-Backed-Up Files	Size of Non-Backed-Up Files(MB)
VG_1COPY_DD	0	0.00	0	0.00

Volume Group: Volume Group name of the volume stored on disks.

Number of Files: Number of Windows files in all paths of the Data Store.

Space used (MB): Total size of Windows files.

Number of Files: Number of Windows files in the path.

User Data Size (MB): Used space with value given in MB (megabytes)

Number of Non-Backed-Up Files: Total number of files that haven't been backed-up. Number of files that have the archive bit set. This is not shown for StoreOnce NAS.

Size of Non-backed-up Files (MB): Total size of non-backed-up files with value given in MB (megabytes).

Page elements for Detail Report by Job

Data Store WINDOW-STORAGE

Data Store	Action	Start Time	Total to Process	Successful	VTC Executor	Status	% Progress	Details	Failure Reason
WINDOW-STORAGE	COPYSYNC	2022-08-25 14:29:46	2	2	GEN8SRV04	Ended	100%	Details	
WINDOW-STORAGE	COPYSYNC	2022-08-25 14:19:37	2	0	GEN8SRV04	Ended	100%	Details	
WINDOW-STORAGE	COPYSYNC	2022-08-25 13:59:02	10	0	GEN8SRV04	Ended	100%	Details	
WINDOW-STORAGE	COPYSYNC	2022-08-25 13:54:26	10	0	GEN8SRV04	Ended	100%	Details	
WINDOW-STORAGE	COPYSYNC	2022-08-25 13:52:58	10	0	GEN8SRV04	Ended	100%	Details	

Showing 1 to 5 of 5 entries

The **Jobs** page will display various details on the jobs executed for the specific Data Store, such as:

Details: Click on the link provided in this column to open a new page with information on the job performed or running.

The **Job Details** page displays information about the job, such as action, domain name, DataStore ID, start and end time, number of objects processed, successfully moved , etc.

☐ Failures Only

```
Action: SpareMove
Domain: SHCH409
BackboxId:
DataStore: DS_2COPY_GENX_NEW
Start Time: 2021-09-02 04:36:27
End Time:
Nb Objects To Process: 16414
Nb Objects Done: 1
Nb Objects Success: 1
Last Progress Update: 2021-09-02 04:48:40
Failure Reason: No activity for at least 30 minutes.
Failure Time: 2021-09-02 05:24:15
****************
Name: LBG10001
Start Time: 2021-09-02 04:36:27
Done: NO
Failed: NO
Message:
Elapsed Time: 0
Progress Done: 0%
****************
Name: LBG10002
Start Time: 2021-09-02 04:36:27
Done: NO
Failed: NO
Message:
Elapsed Time: 0
Progress Done: 0%
****************
Name: LBG10003
Start Time: 2021-09-02 04:36:27
Done: NO
Failed: NO
Message:
Elapsed Time: 0
Progress Done: 0%
****************
```

To display the failed operations only check the radio button on the top of the **Job Details** page.

☑ Failures Only

Use the *Copy* or *Save To File* buttons at the buttom of the page to save the job details information for future use.

Action: Type of job that is being executed on the Data Store

⚠️	Copy-Non-Copy file process cannot be started while other processes, such as Migration or Spare Move, are still running.

VTC Executor: Name of the VTC the job is running on

Status: Job status (Failed/ Ended/Running/Suspended)

The job status is action-flagged in the table as follows: Failed/Ended/Suspended/Running.

⚠️	If no job details are available, the job summary page will display the following message.

Start Time: Time stamp (in the format: yyyy-mm-dd hh:mm:ss) of the job started. The jobs are displayed starting with the most recent ones.

Total to Process: Number of files to be processed

Successful: Number of successully processed files

 VTC Executor: Name of the VTC

% Progress: Percentage of the completed job

Details : Link to the data store

Failure Reason: In case of a job failure, error message and/or details on the failure reason.

Use the **Search** feature to look for certain info based on search criteria. Type in the info you are looking for (partial or complete criteria); the returned results will be listed from the most recent.

Select the number of entries per page if you want to display 10/25/50/100 job entries.

Control the job status by clicking on the respective status. Follow the instructions in the pop-up.

Details	Data Store	Action	VTC Executor	Status	Start Time	Number of processed objects of Total	Number of moved objects of Processed	Failure Reason
Details	QSTORE	SpareMove	PANORAMIX	Suspended	2022-04-12 16:41:02	0 of 12	0 of 0	
Details	QSTORE	SpareMove	PANORAMIX	Failed	2022-04-08 14:20:14	1 of 2	1 of 1	Job is aborted

A suspended job can be resumed or aborted.

If you choose to change the job status, another pop-up window will prompt you with a message on the change that you just performed.

If the job is aborted, the summary table will list the job status as Failed.

Details	Data Store	Action	VTC Executor	Status	Start Time	Number of processed objects of Total	Number of moved objects of Processed	Failure Reason
Details	QSTORE	SpareMove	PANORAMIX	Failed	2022-04-12 16:41:02	2 of 12	2 of 2	Job is aborted

> ⚠️ Jobs details are kept in the log for no longer than 365 days. The older job logs are auto-matically deleted from the list.

VTC MANAGEMENT CONSOLE
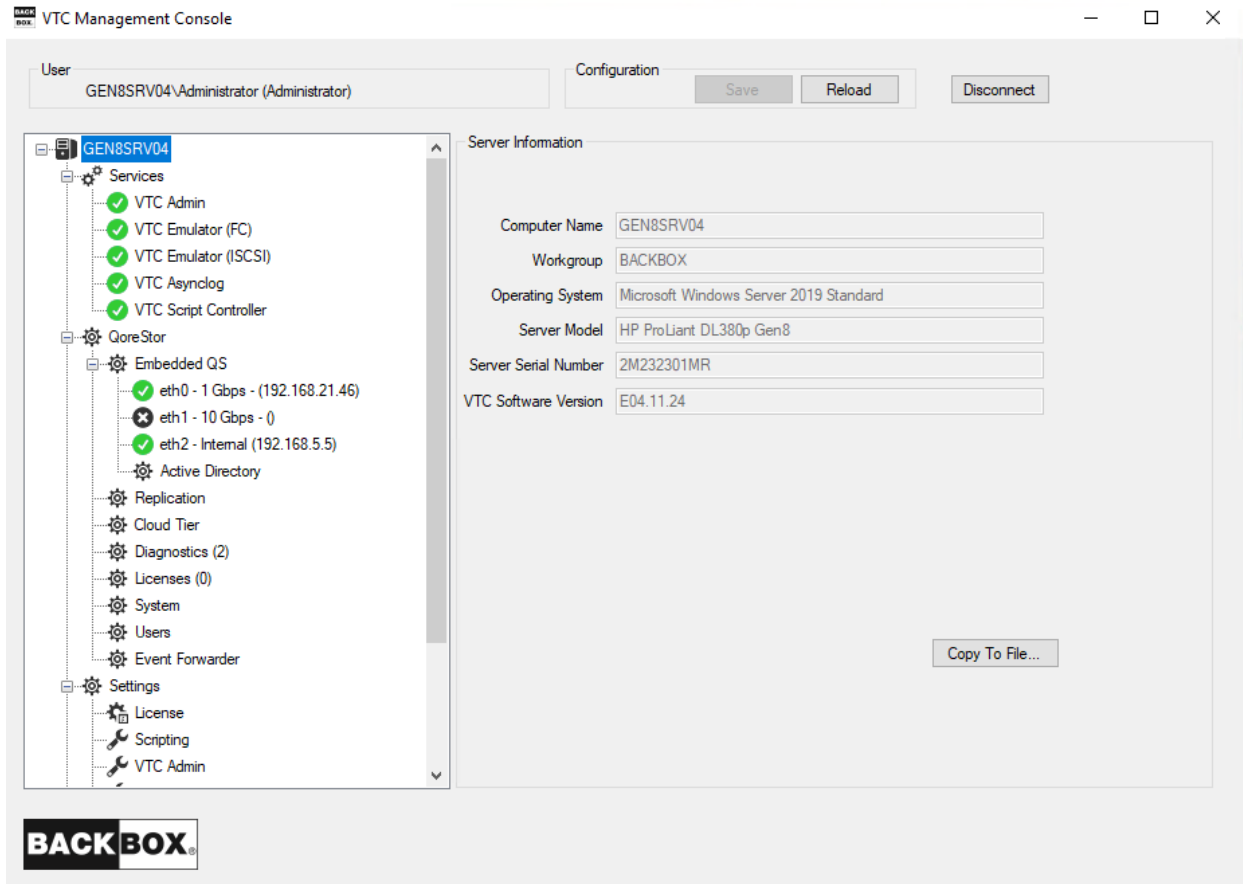
Security and Access Rules

To configure the security and access rules on the VTC server, the **VTC Management Console** has to be started using an interactive user with permissions to log on to the VTC Server.
The VTC Management Console attempts to connect to the local VTC Management Service.
The default connected user and their profile are displayed in the user identification box.
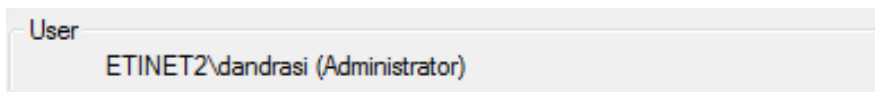
Console Access Restrictions

Some restrictions apply when accessing the VTC Management Console.
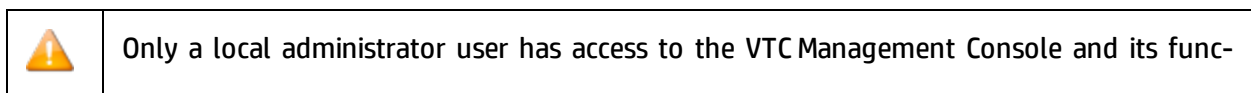
> ⚠️ Only a local administrator user has access to the VTC Management Console and its func-

tionalities. A non-admin user, when attempting to access the VTC MC, will be prompted with an error message stating that the account must have the right privileges in order to connect to the console.
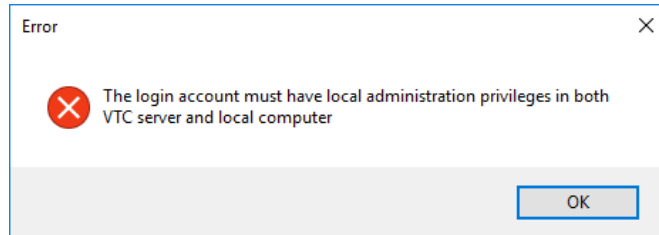
Administrating Remote VTC Server

To connect to a VTC Server through a local VTC Management Console of another VTC Server, all VTC Servers must be reachable on the Network. Both Workgroup and Active Directory deployment can be used to get them connected.

To connect to a remote VTC Server right-click on the server node and select the **Connect** action. If different credentials need to be provided, "uncheck" the **Current User** box and enter the new credentials. To complete, click on the **Connect** button.
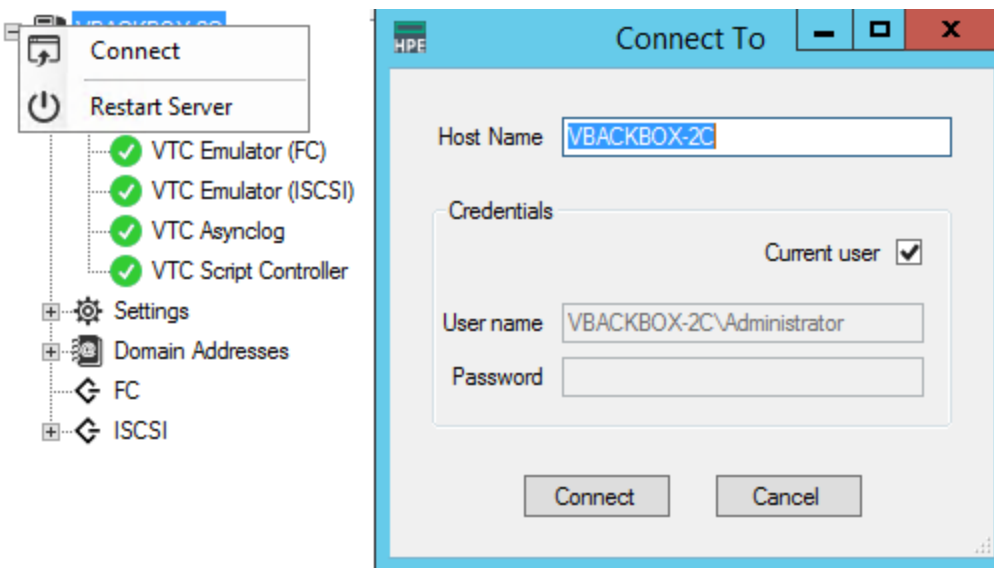
To connect from a workstation/laptop the VTC-Software has to be installed on Windows 7, Windows 8.1, Windows 10, Windows 2016 or Windows 2019. Only the VTC Management Console will be installed with this specific setup; the other BackBox components will not be affected.

⚠	The workstation needs to reach the VTC through the network.

For WORKGROUP deployment, all users accounts for remote administration must be created on each server and must have the same user name and password. To avoid workgroup requirements, it is recommended to use only the domain user to create a local user on the workstation.

> ⚠️ When started from a workstation, the VTC Management Console opens with a connect dialog. Provide the remote name of the VTC server to which you want to connect.

User Interface

The user interface has four sections:

1. User
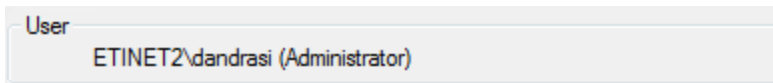
2. Configuration

    When connected, the configuration section shows an active **Reload** button. If the configuration has been modified outside of the management console or by another user through another log-in session, the **Reload** button refreshes the configuration.
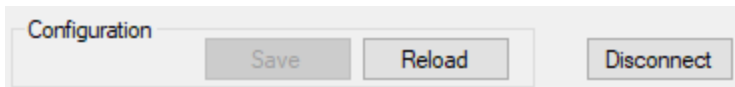
    Following a configuration or a settings change, **Save** & **Cancel** buttons become available.

3. Server Tree Nodes Panel (left-side panel)

    This panel lists the server elements. Nodes can be expanded; they are grouped into different management categories. Right-click on the nodes or elements to see the available actions. If an action is not possible, it appears grayed out.
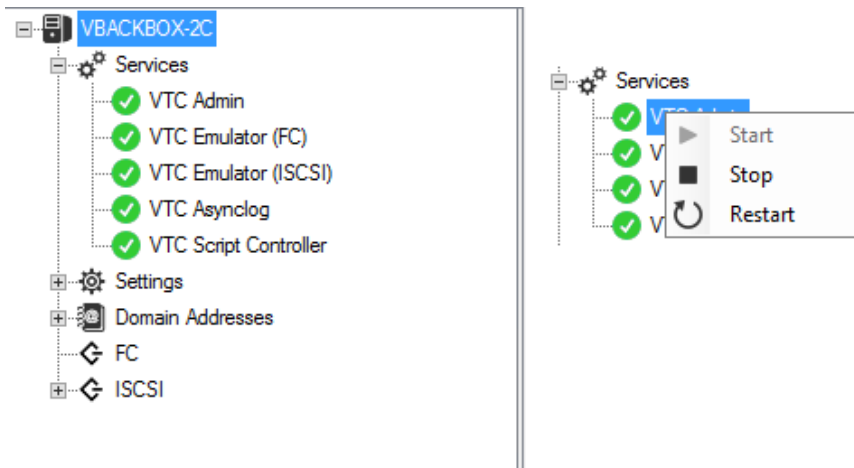
4. Server Information Panel

    When a server is selected, the information displayed on the right side is related to that specific server. Not all server nodes have information to display when selected (e.g. Service nodes); in this case, the last accessed information is displayed in the panel.
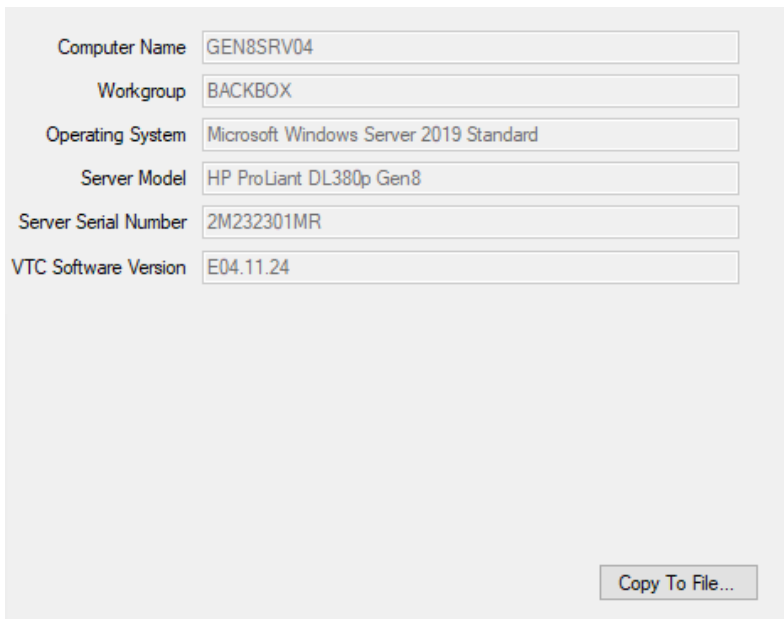
Use **Copy to File ...** button to save the server information in a **.txt** file. The file will be saved with the default name **Server Information** and default location **Desktop**. For support and reference purposes, location and name of the file can be changed at any time.

```
ETIDEV02.txt - Notepad

File  Edit  Format  View  Help
Computer Name: ETIDEV02
Domain: etinet.local
Operating System: Microsoft Windows 10 Enterprise
Server Model: Microsoft Corporation Virtual Machine
Server Serial Number: 3307-7822-6025-2460-6863-0520-15
VTC Software Version: H04.11.16
UUID: 4C21A2DD-D49A-483A-90E9-1F6C9FF5FFD5


License Number: xxxx0017
License Expiration : 2022-08-25T18:08:15.8508719Z
License Creation : 2022-08-11T18:50:43.9568756Z
License To: ETINET
Serial Number: 3307-7822-6025-2460-6863-0520-15
Hpe Number: 111
License Type: Emergency
Host Name: ETIDEV02
Release Version: H
Software Version: 4.09
Product: Unknown
Os Version: Windows Server 2019
Number Of FC Ports : 6
Number Of Encryption Devices: 0
Number Of Iscsi Devices: 0
Number Of Devices Per Port : 64
QoreStor Enable: True
QoreStor ID: 16C04481AB444E42AC43C41C636B11FA
```

Real-time process tracking

On VTC MC, any background process is real-time tracked. Activate the real-time tracking by clicking on any process button, such as **Start**, **Stop**, **Restart**.
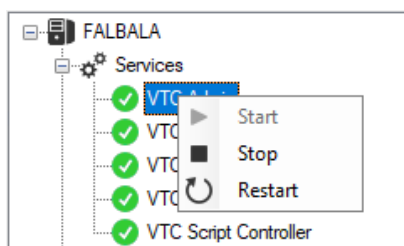
Server Nodes

When connected, the **Server Node** is always initialized with the server computer name. Under the **Server Node** there are the four main categories handled by the VTC Management Console: **Services**, **QoreStor**, **Settings**, **Domain Addresses**, and **FC/ISCSI** nodes.

When the server node is selected, basic information related to the Server is shown in the right-hand side panel.

Right-click on the node to see the actions that can be performed at the Server Node level.
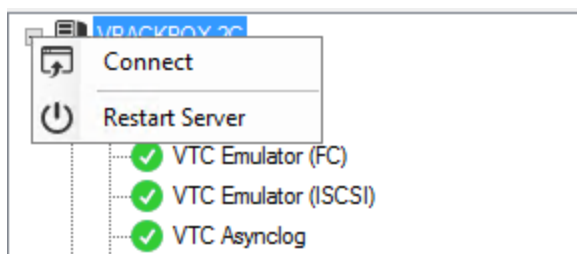
Lists all VTC services available on the server. Each service is represented by a service name: **VTC Admin**, **VTC Emulator (FC)**, **VTC Emulator (ISCSI)**, **VTC Asynclog**, **VTC Script Controller**.

When selecting any of the Service categories, there is no related information to be displayed in the right-hand side panel.
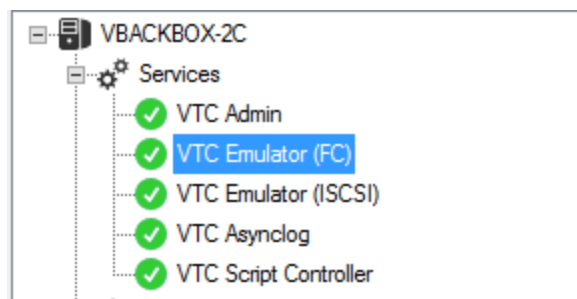
Service states	Description
✅	Started
❌	Stopped
⚡	Stopping / Starting

The available actions are activated when right-click on the service: **Start**, **Stop**, **Restart**.

If one service is selected, the available actions will be performed at service level, not at server level. The grayed-out actions are not available.
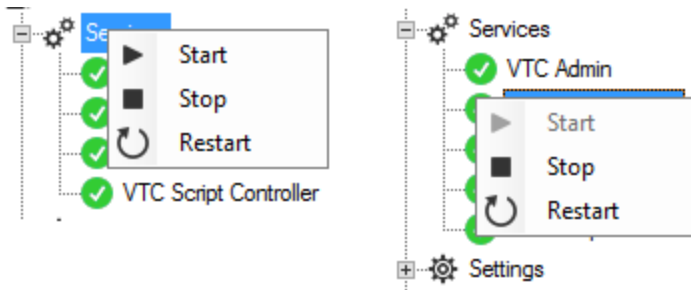
QoreStor

If you purchased a VTC MC license with embedded QoreStor, you have to set up the QoreStor.

When opened up, the QoreStor node displays **Embedded QS**, **Replication**, **Cloud Tier**, **Diagnostics**, **Licenses**, **System** and **Users**. See below the available settings for each of them.

Embedded QS

If you are on Workgroup, you will need to update your HOST file to have the QoreStor name displayed by VTC MC.

Otherwise, make sure the QoreStor hostname is set up in Active Directory.

If you want to change the hostname:

1. Enter Hostname IP address/name and click **Verify** to check if the entered hostname points at the right IP address.

2. Click **Save** or **Cancel** to undo the change(s).

The embedded QoreStor has 3 virtual NICs:

- **eth0** is used to connect to corporate Network
- **eth1** is for dedicated network (if available as Datapath)
- **eth2** is for private network (used only by the VTC to communicate with its embedded QoreStor VM by control path)

eth0 and **eth1** NIC can be configured as Automatic (DHCP)/Manual or simply be disabled

For embedded QoreStor there are some connection settings that need to be configured:

- To configure **ethx** Automatic

a. Change IPv4 setting.

b. If Automatic, nothing else to change and click on **Save** to save.

c. If Diabled, nothing else to change and click on **Save** to save.

d. Or click on **Cancel** to undo changes.

- Configure **ethx** Manual

eth0/eth1 – Automatic or Disabled

a. Change IPv4 setting.

b. If Automatic, nothing else to change and click on **Save** to save.

c. If Disabled, nothing else to change and click on **Save** to save.

d. Or click on **Cancel** to undo changes.
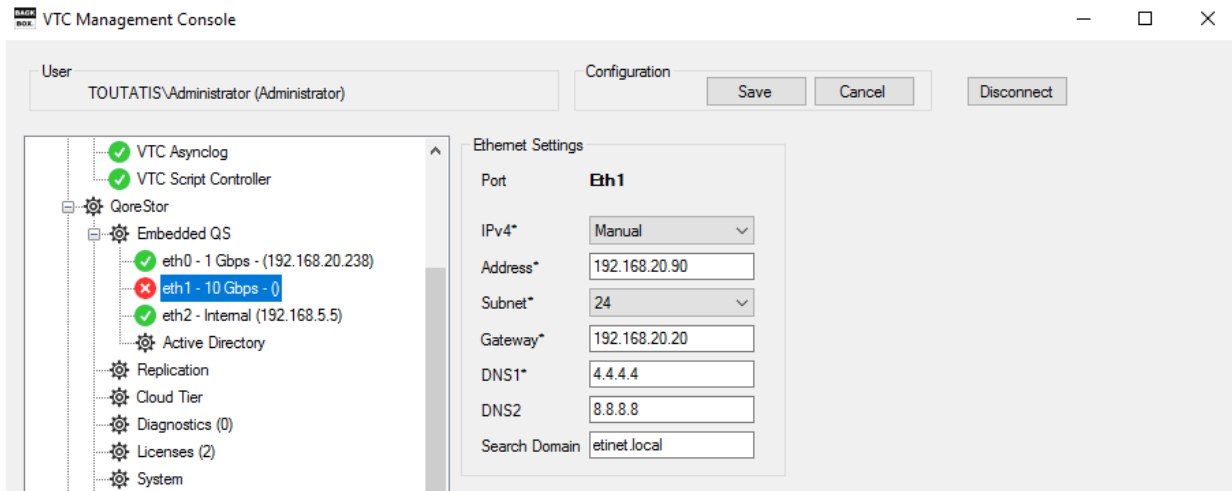
eth0/eth1 – Manual

a. Change IPv4 setting to manual.

b. Enter the address.

c. Select Subnet (ex: Subnet=24). For **eth0** make sure to use Subnet value in Windows format, otherwise an *Invalid subnet mask* message is generated and the value is not accepted. For more details on the valid subnet values see Microsoft Network Classes.

d. Enter the Gateway.

e. Enter DNS 1.

f. Enter DNS 2.

g. Enter Search Domain.

h. Click on **Save** to save.

i. Or click on **Cancel** to undo changes.

Active Directory Domain (access permissions)

Use Active Directory Domain to manage and centralize users' permissions.

QoreStor can use **local user** or **Active Directory user**.

For local user, the same user (with the same password) needs to be created on VTC to match the user at QoreStor level.

> ⚠️ Default user for CIFS access is **BackBox**, with default password **St0r@ge!**

For **Active Directory user** the QoreStor needs to join the domain via VTCMC. The Active Directory user can access data on the Embedded QoreStor.

Assign users' permissions through Active Directory Domain to allow access to QoreStor and Data Store.
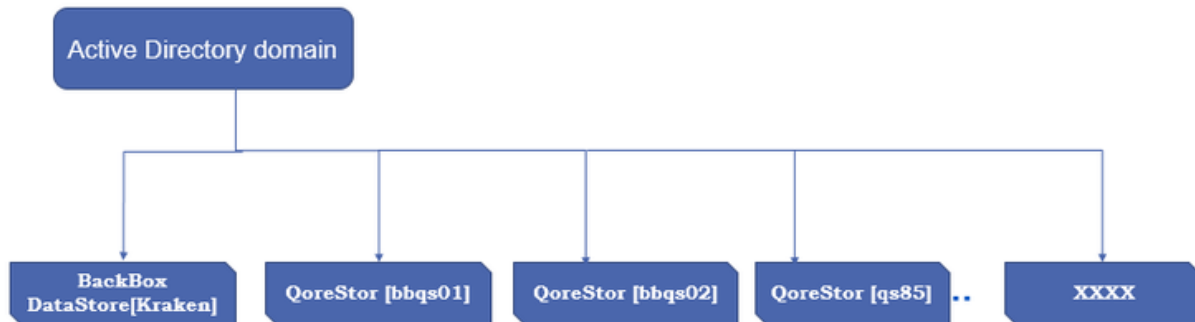
To join Active Directory Domain by VTC MC:

1. Open the VTC MC

2. Click on the node Embedded QS. Open the node and select **Active Directory**.
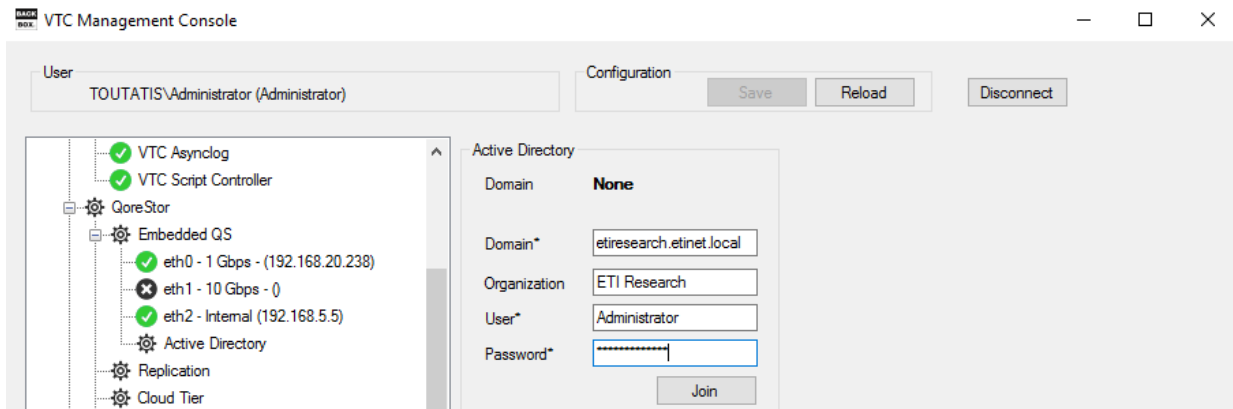
3. Set up the domain*, user* and password* (mandatory).

4. Click the **Join** button.

⚠️	To join or leave the domain, the user needs to be an Active Directory administrator.

To leave Active Directory domain:

1. Select the Active Directory node.

2. Input User/Password information.

3. Click the **Leave** button.
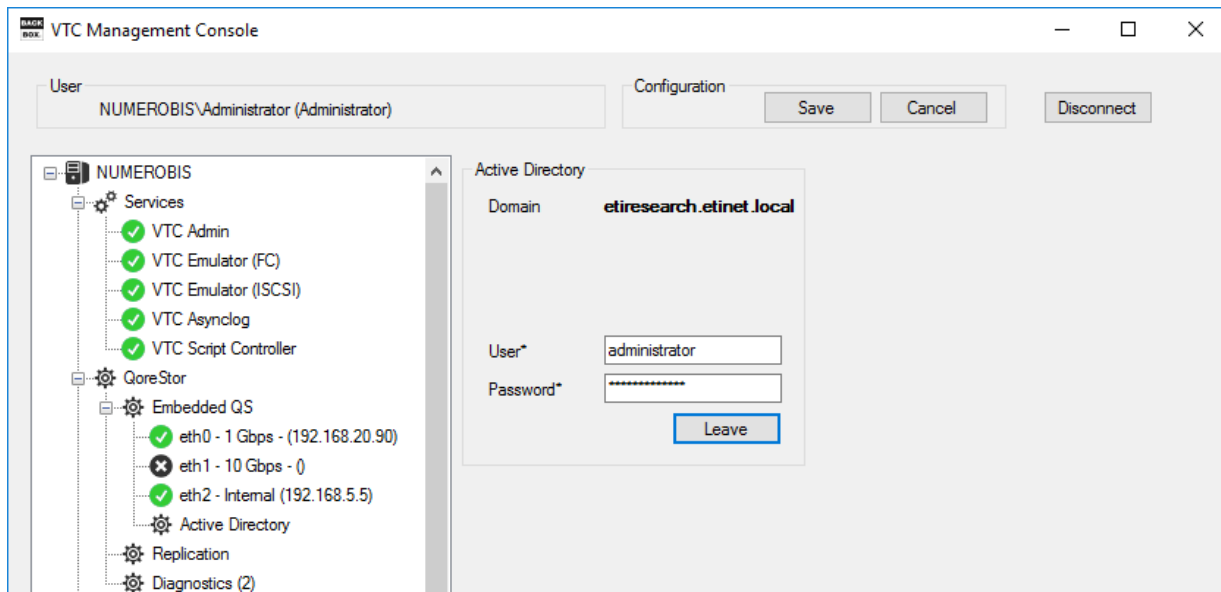
> ⚠️ If any account seems to have lost ownership of the files and folders generated after joining the Windows Domain, log into VTC server with Domain Administration account and change the ownership. Follow the procedure described in Appendix F – Procedure for files/folders ownership recovery .

Replication

To set up replication, either add to the HOST file the replication points (source and target) with their IP addresses and hostname or modify your network's DNS entries.

Click **Setup** to view if the target hostname points to the right IP address (the status of the target and source containers for the replication process).
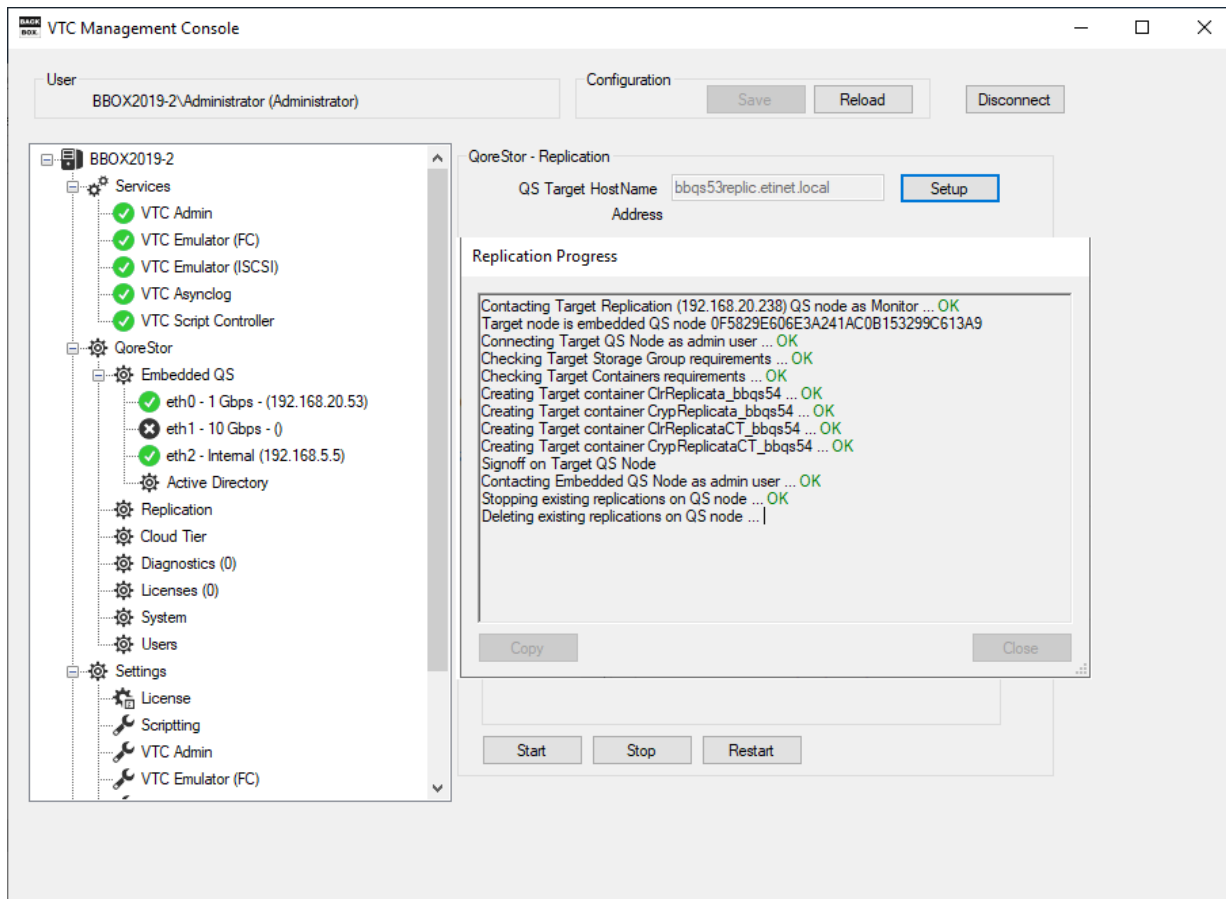
Once the replication setup progress has been finished and the state is marked **INSYNC**, the initial replication setup is complete.
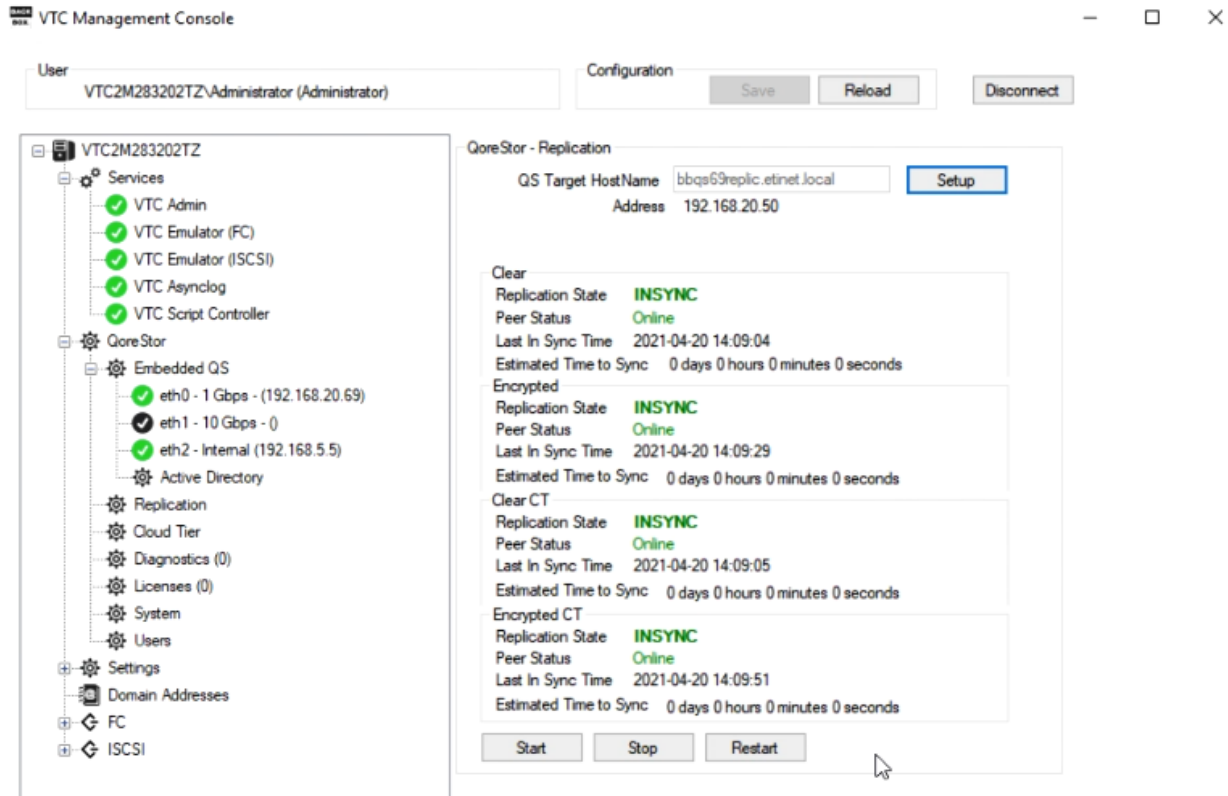
To view replication status:

- Click **Start** to start replication.
- Click **Stop** to stop replication.
- Click **Restart** to restart replication.

As some of these processes might take some time to run, the pop-up stays on the screen as long as the process is running, to let the user know about the running process in the background.
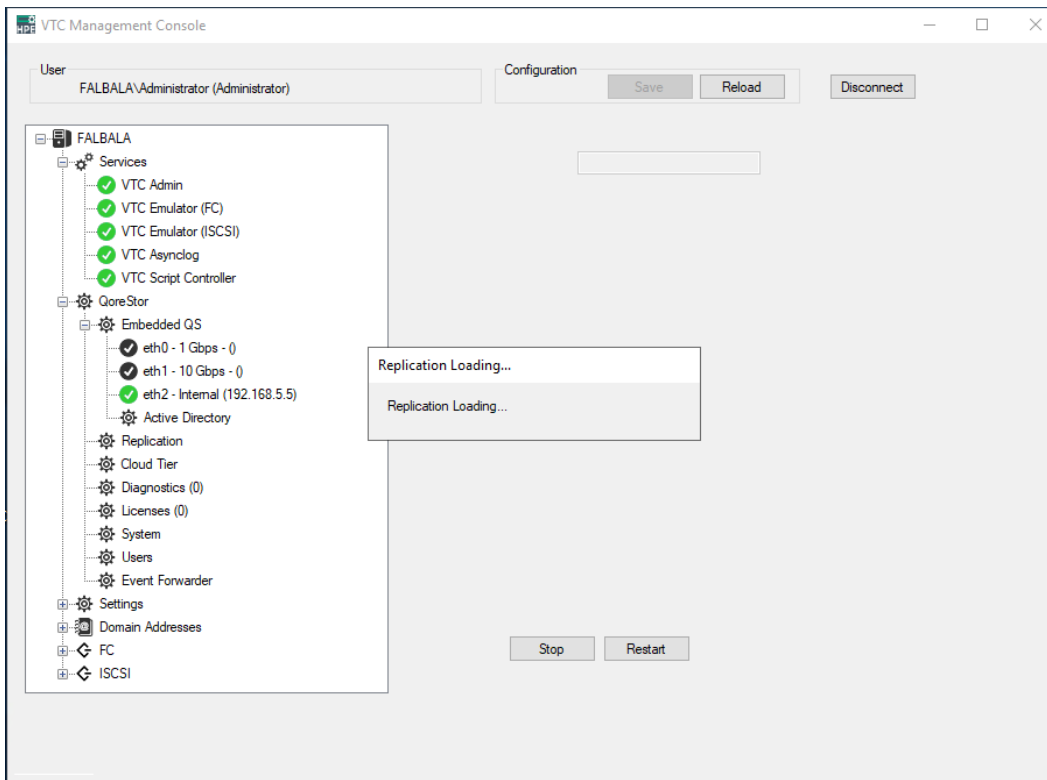
In the example above, the process running in the background and real-time tracked is the Replication. The pop-up displays info on the ongoing **Replication Loading...** process.

Diagnostics

Remotely generate, delete and/or download diagnostics log(s) using the diagnostics feature .
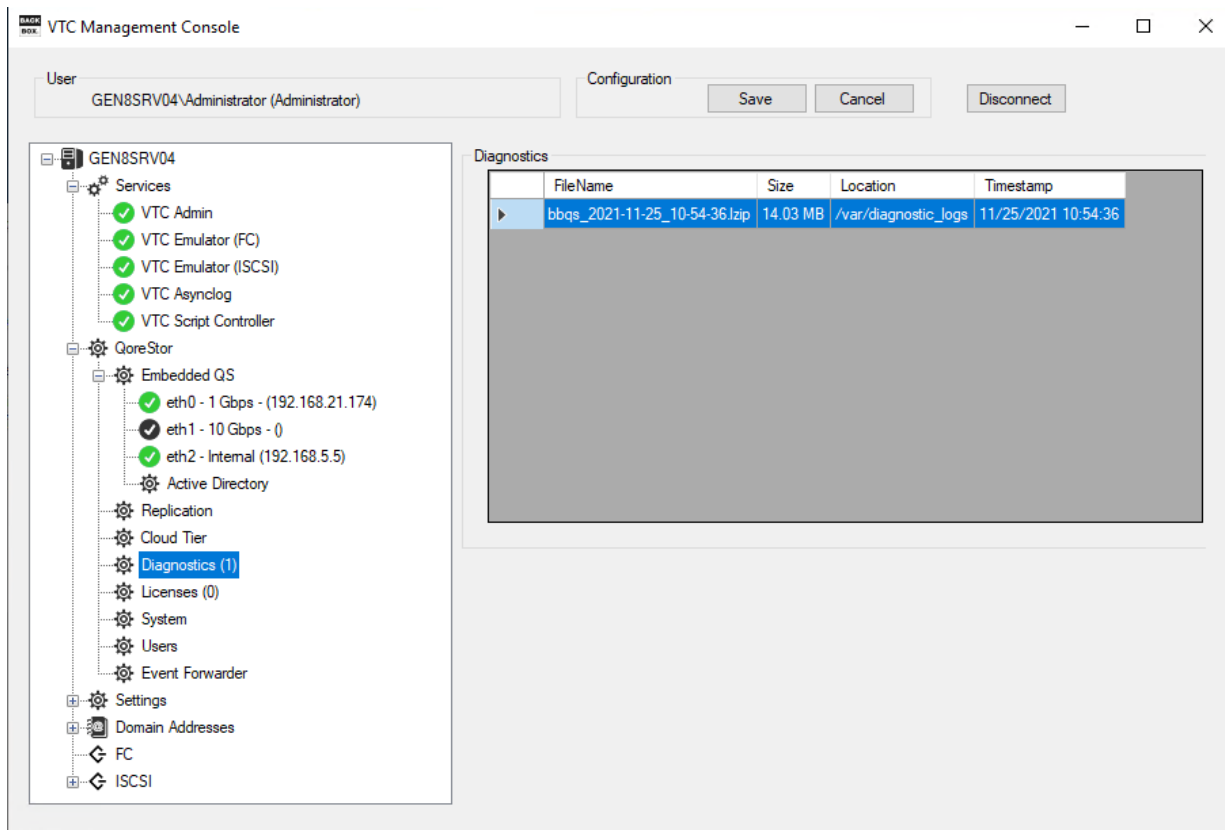
Click on the **Diagnostics** node under QoreStor and the right-hand panel will display all the generated diagnostics log files.

To generate a new diagnostics file right-click on the **Diagnostics** node and **Generate Diagnostics**. The generated file has a default name and location. You will be prompted with the message that the diagnostic request has been sent.
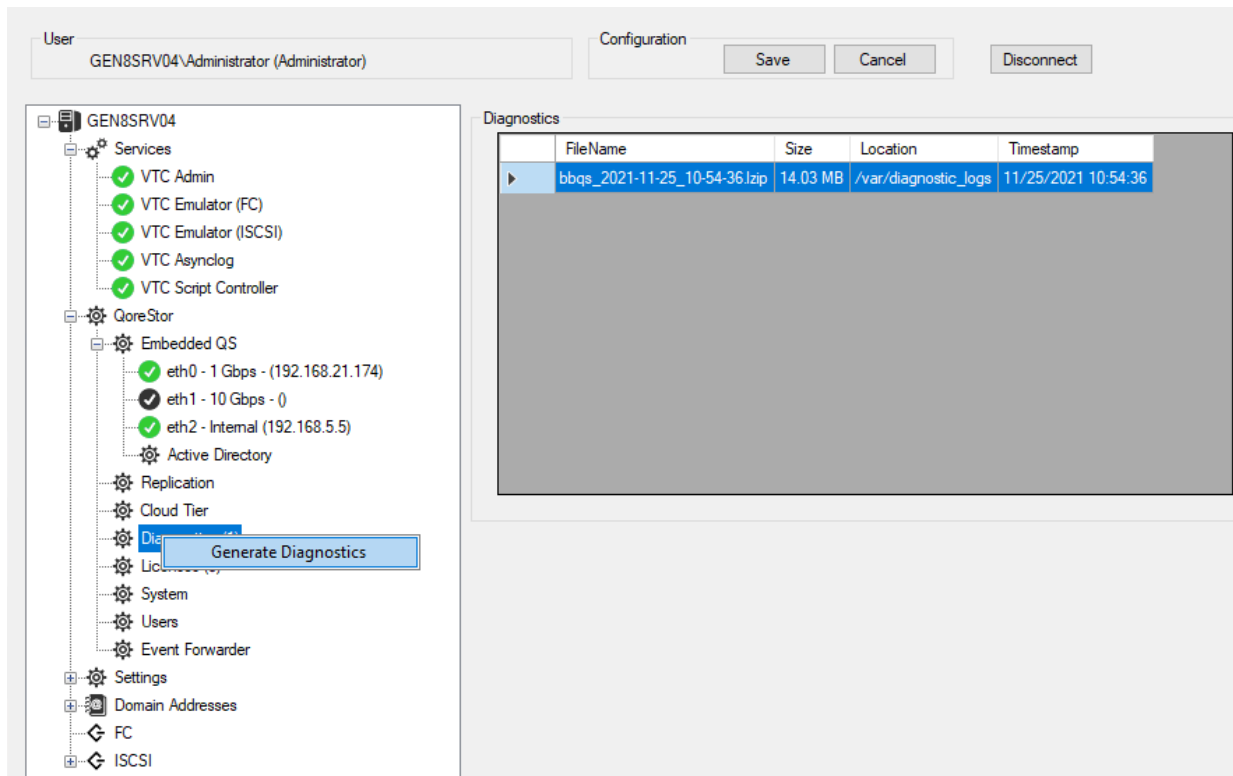
The files are in sync with the QoreStor log files and they contain the name of the embedded QoreStor and the timestamp of the log file.

Once the file is generated it can be either downloaded or deleted. Select the file and right-click on it to choose **Download Diagnostic** or **Delete Diagnostic**.
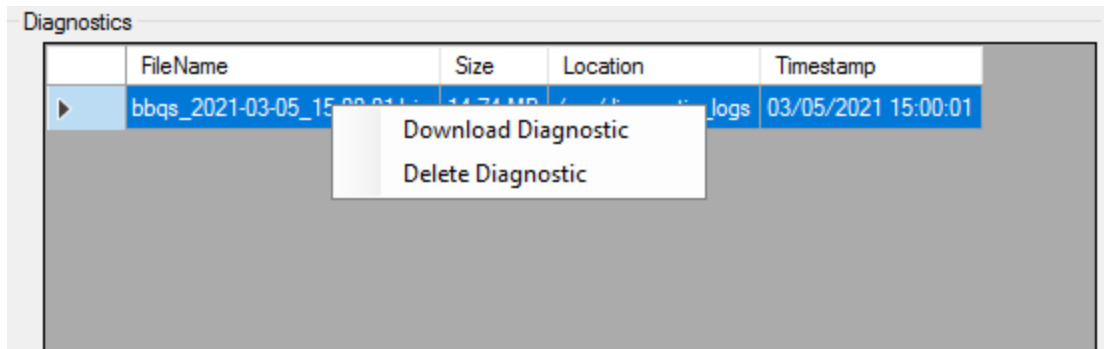
The diagnostic log file is by default saved in an automatically created folder on the local machine with the path name: `C:\ProgramData\ETINET\VTC\Diagnostics`.

You can change the location of the diagnostic file after it has been generated, but any deleted or newly generated diagnostic files will not be automatically updated in this folder `C:\ProgramData\ETINET\VTC\Diagnostics`.

Licenses

The node lists all active QoreStor licenses.
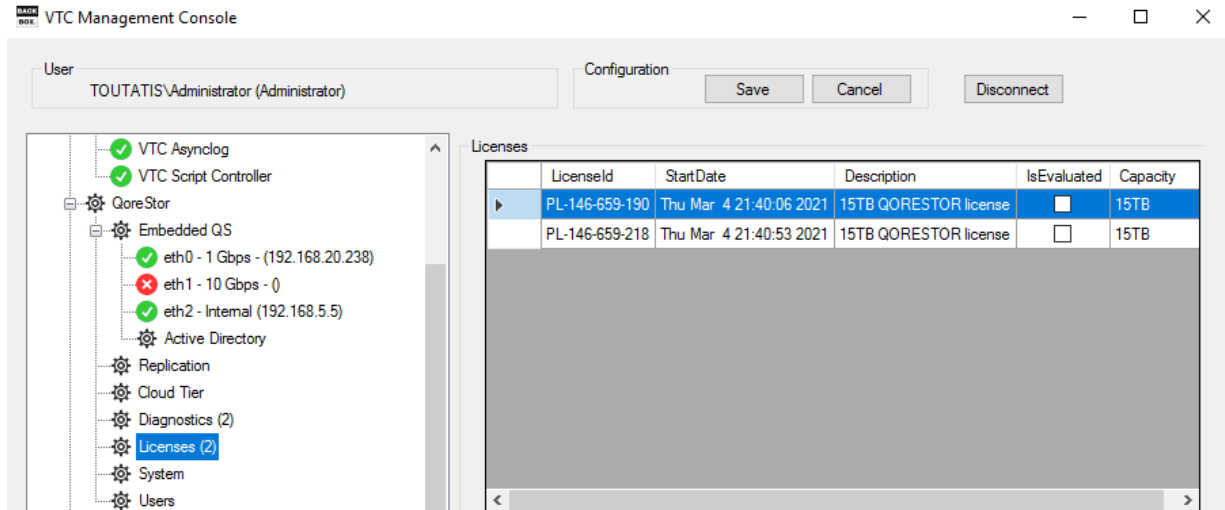
To upload a new license right-click on the license node.
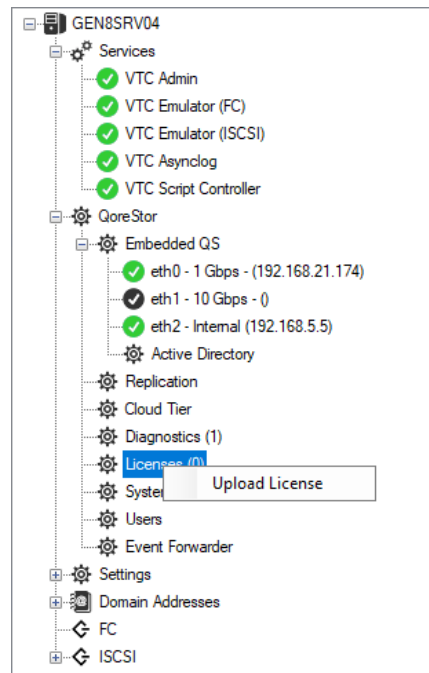
In the Windows Explorer select the license file provided by the ETI-NET representative. The license is provided in a **.dlv** format (DLV File).

The right-hand panel displays the license ID, licensing starting date, description and the storage capacity associated with the license.

To delete a license right-click on the respective license and delete it.

Confirm the deletion in the pop-up window by clicking **YES**. Click **NO**, if you don't want to delete the license.
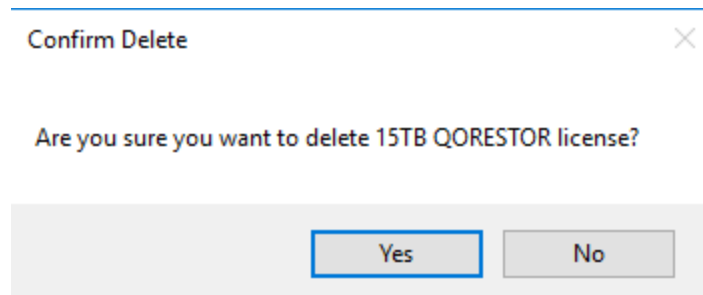
Cloud Tier

Cloud Tier will appear has a new node under the QoreStor section. Once selected, a call to the REST API will notify if QoreStor Cloud Tier is defined or not.

To configure Cloud Tier:

1. Select **Cloud Tier** node under QoreStor.
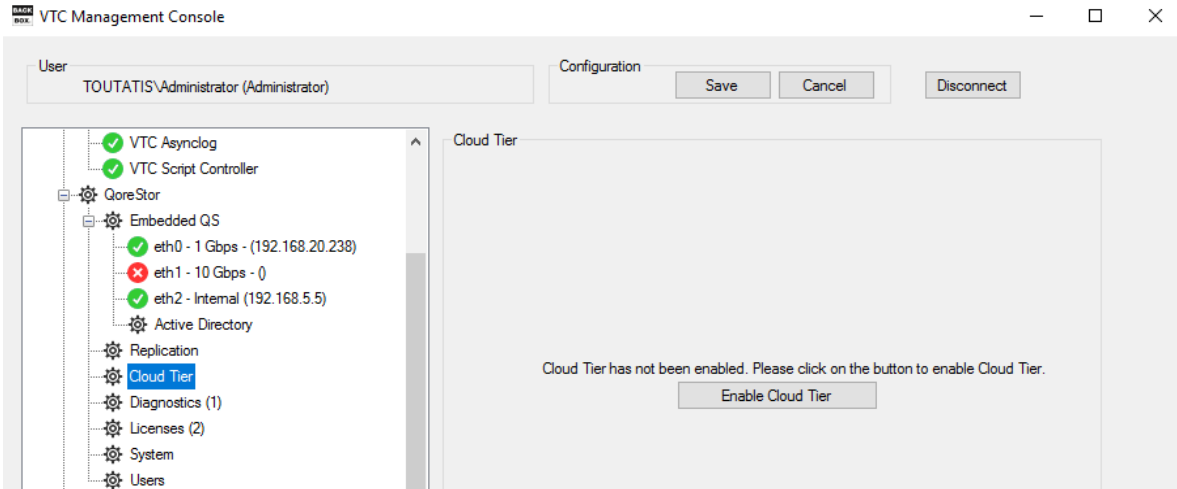
2. When pressing the button **Enable Cloud Tier**, a warning will pop up to inform the user that the enabling option is not reversible.

⚠	Once the cloud tiering is enabled and set up, it can no longer be disabled.

The pop-up will offer the choice to continue with the current operation or to keep the cloud tier disabled.
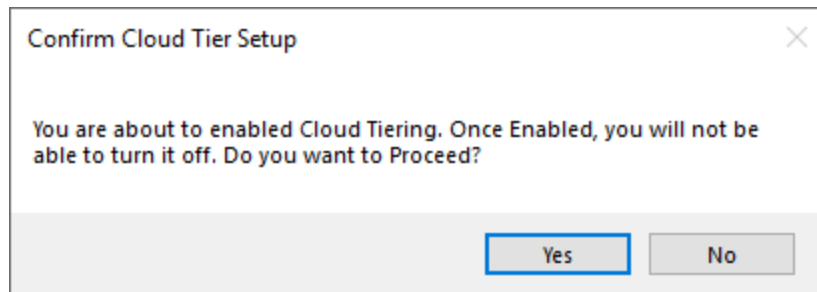
3. Click **Yes** if you want to configure Cloud Tiering.

4. The Cloud Tier pop-up allows you to set up parameters for cloud tiering, such as connection string, cloud container and associated password, cloud service, cloud migration and retention age.
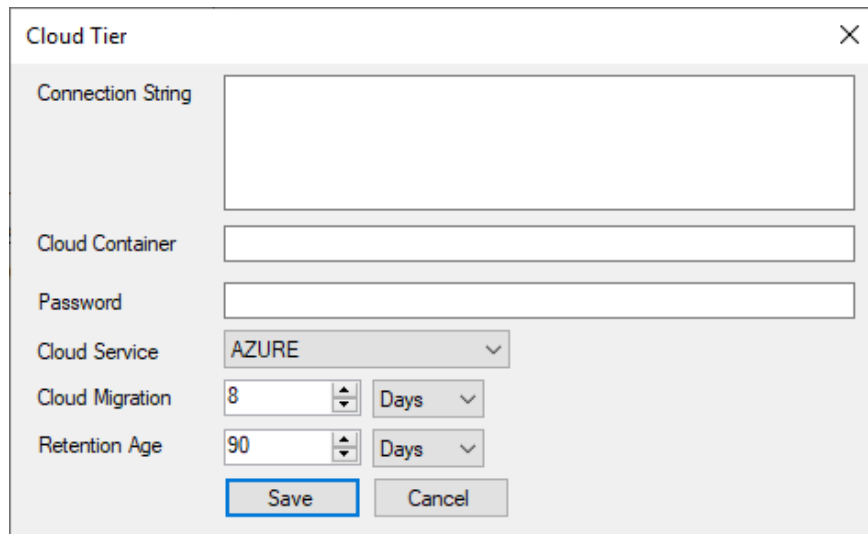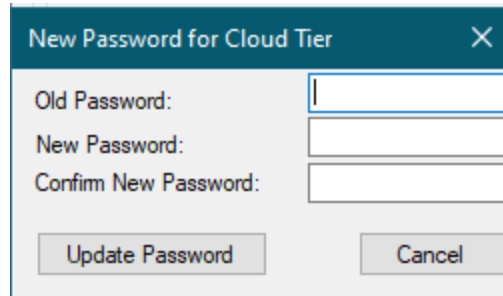
Once the Cloud Tier configuration is set up, details and editing options are displayed in the right-hand panel.
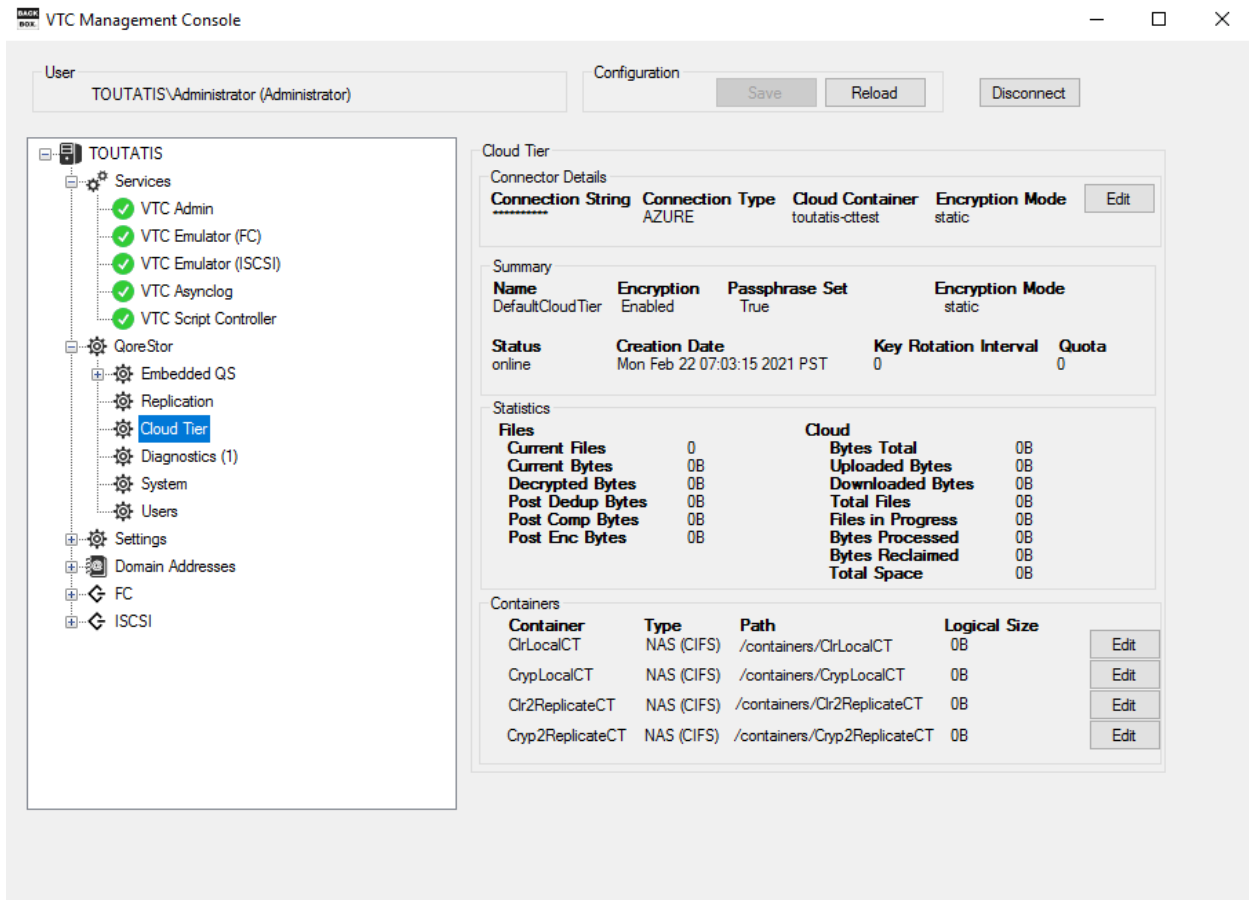
The Cloud Tier panel has four sections with details on **Cloud Tier** connection (String, Type, Container and Encryption Mode), **Summary** (Name of the cloud tier, encryption status and mode, passphrase setting, creation date, etc.), various **Statistics** and the cloud tier **Containers**.
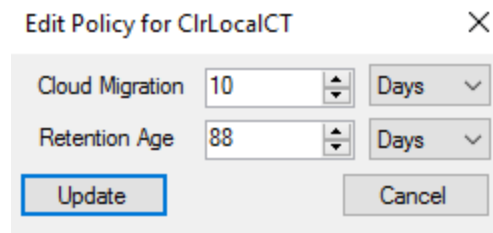
To change the password for Cloud Tier, click **Edit** in the **Connector Details** panel section.

In the pop-up window enter the old password, then the new passowrd and confirm it. Click **Update Password** to have the new password updated.

To modify containers' policies, click **Edit** for the specific container you want to change the policy to.

Edit the policies according to your specific requirements: cloud migration (in days and hours) and retention age (in days).

Click **Update** to save the new policies or **Cancel**.
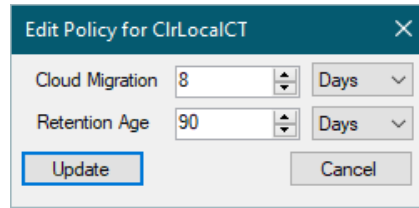
Container Errors

⚠️ If Cloud Tier is not enabled for a specific container, the respective container is red-flagged in the **Containers** panel.

Use the **Fix** button right next to the container error to edit the policy.

In the dialog pop-up edit the policy for the container or simply click [Update] button to reset the container and have the error fixed.

System

The **System** tab displays both QoreStor and OS current versions. The tab allows automatic updates of the embedded QoreStor and/or OS for Oracle Linux Server.

The update is gonna be done sequentially, by running the QoreStor update first and then the OS (in this order).
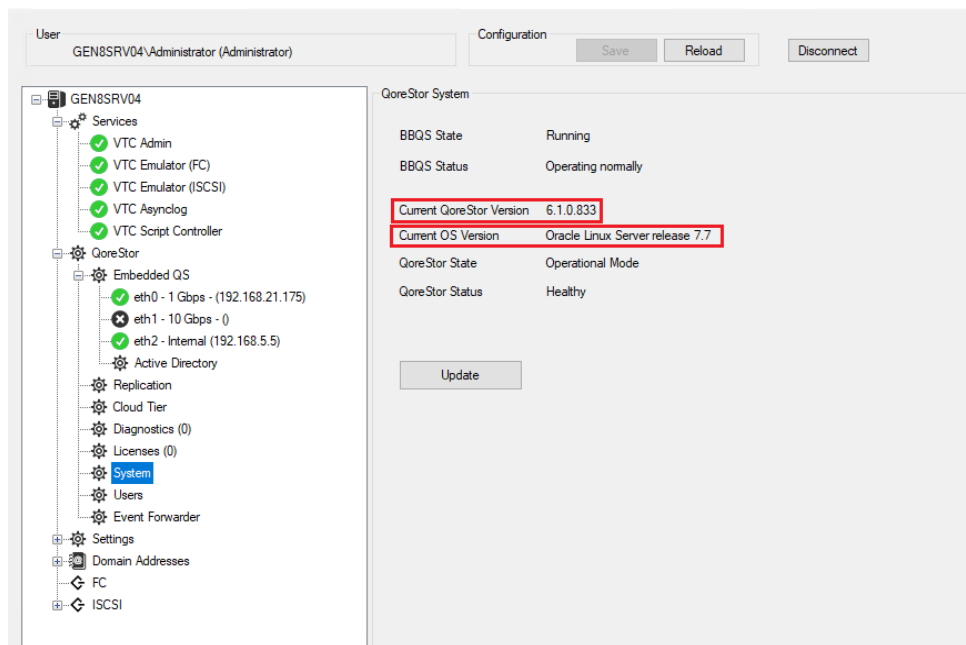
Before proceeding with the automated update, locate both ISO files necessary for the procedure:

ISO File	Location
QoreStor Update ISO	
OS Update ISO	

- Copy to the server the provided QoreStor ISO file.

- Mount the ISO file in Windows.
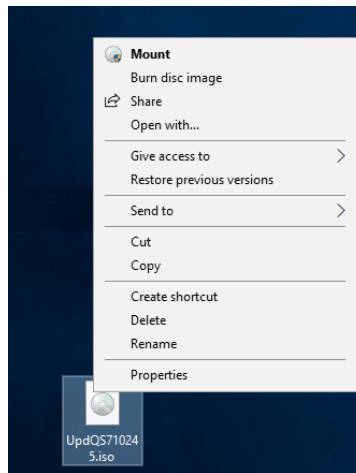
- Start PowerShell Windows and go to the mounted ISO file.
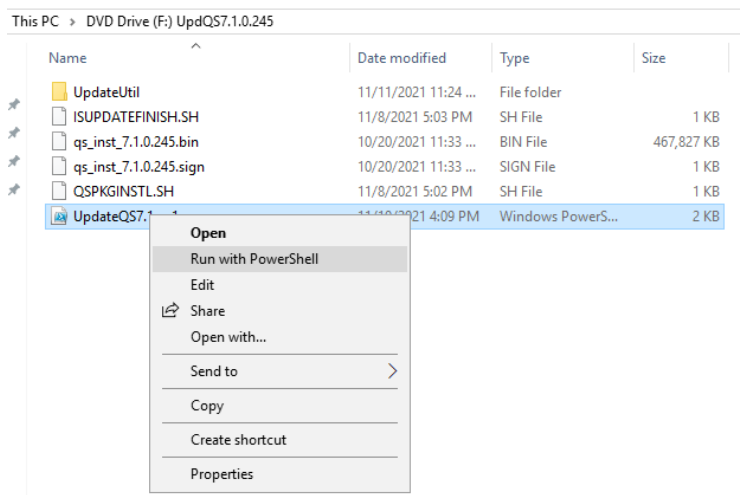
- Run **UpdQS7.1.ps1** script under PowerShell
- Eject the ISO file
- Proceed with the system upgrade following the steps in VTC MC:

1. Click on the **System** node under QoreStor. If there are any updates available, you can update the QoreStor by clicking on **Update** button.
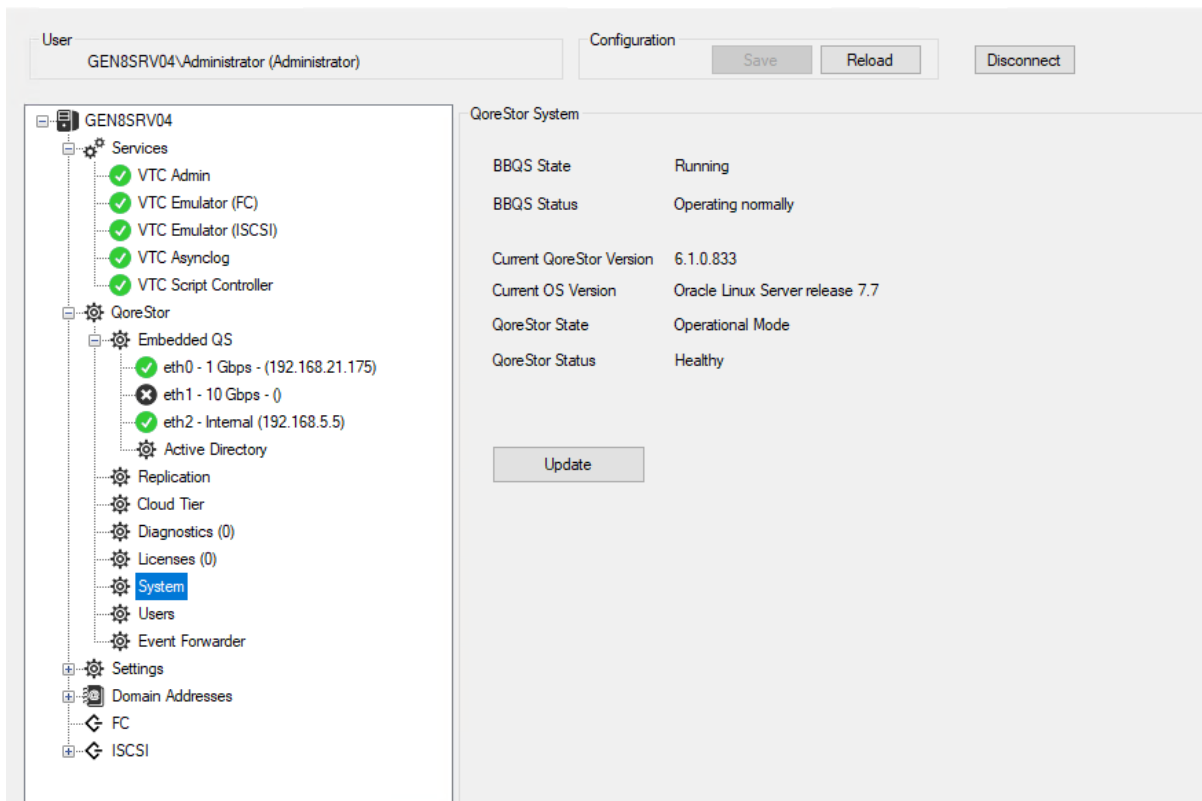
2. Mount the QoreStor ISO file received from ETI-NET support to update the embedded QoreStor VM. Copy and paste the location of the ISO file and click **Mount**.
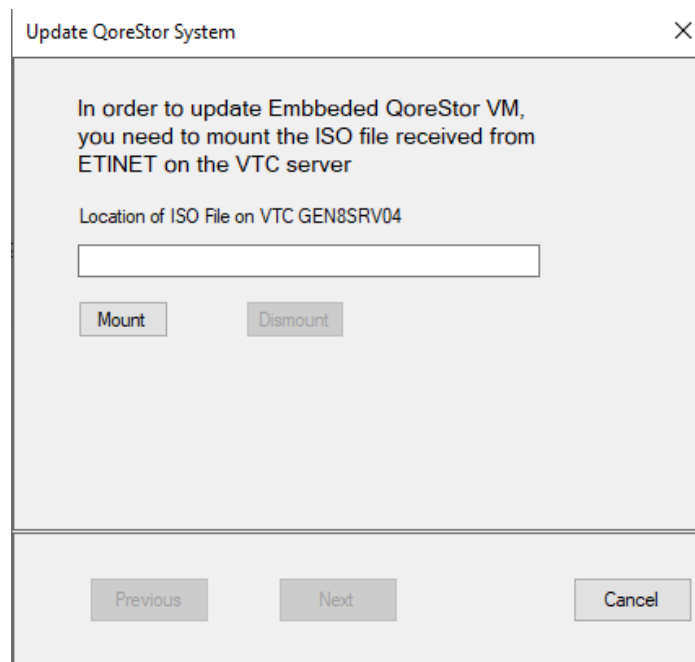
3. Once the ISO file is successfully mounted, click **Next**.
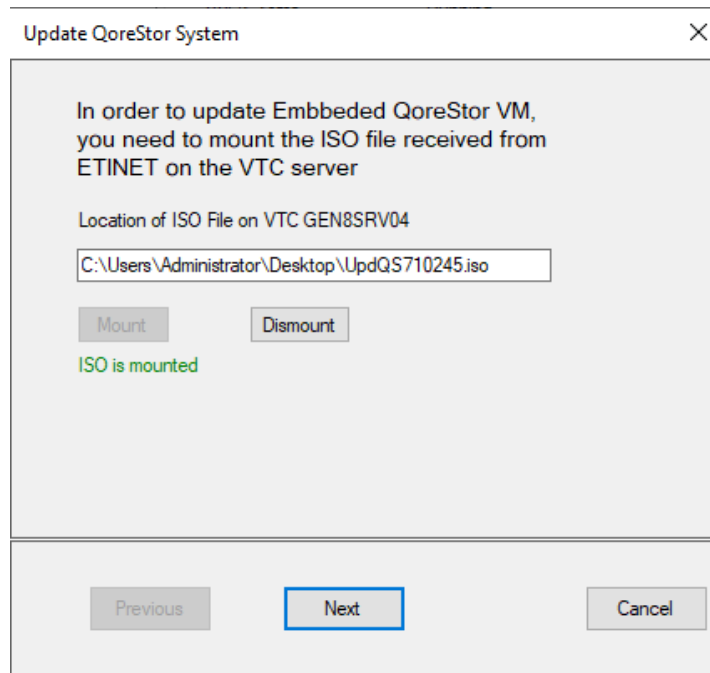
A warning message will inform you that the update process will start after you click **Complete**. Once the updating process is started, it cannot be interrupted.
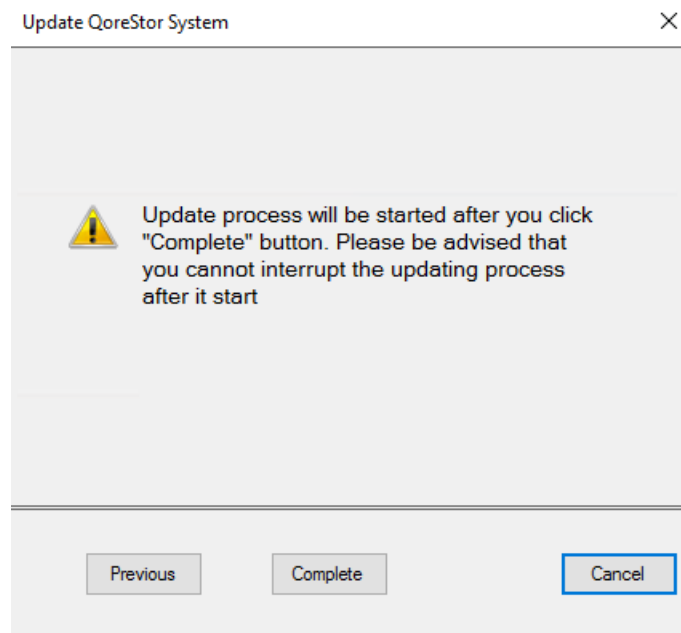
A progress bar will show the status of the update during the process. Once the update is completed the system panel will display all the info related to the QoreStor system.
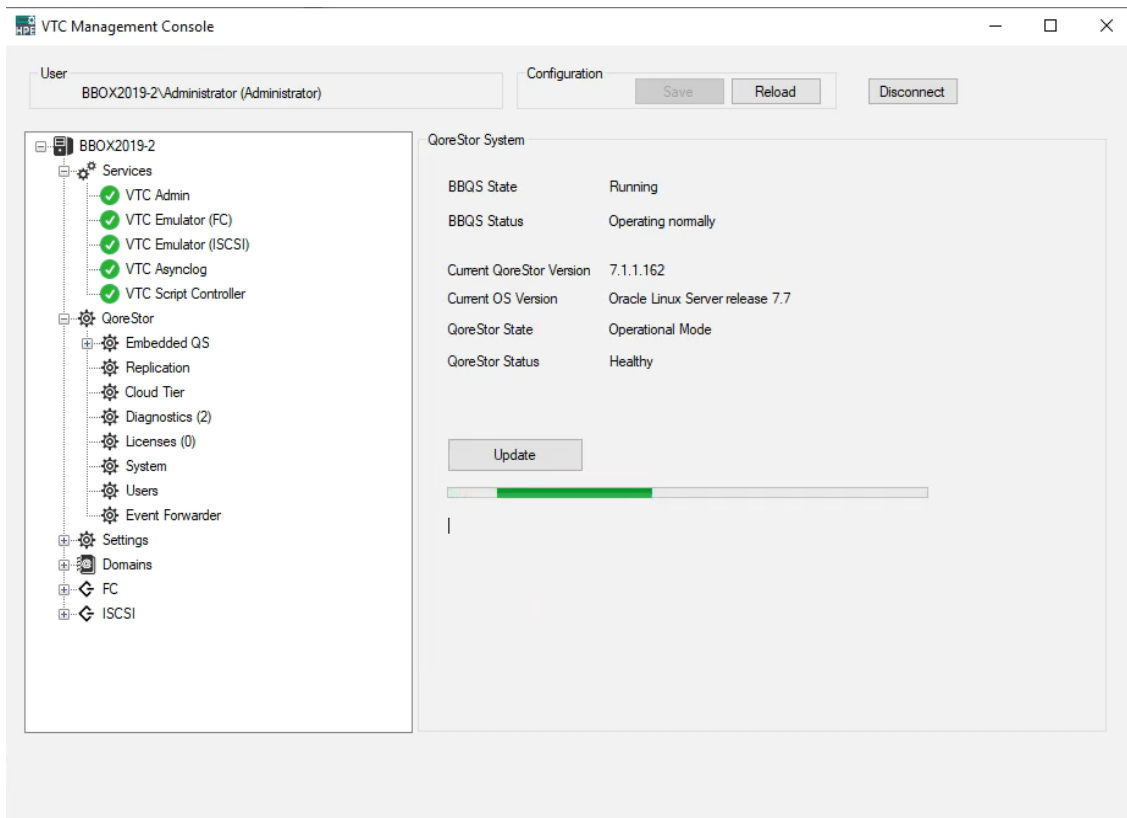
The updating process might take several minutes. Don't interrupt the process while updating, even if warning messages are issued by the system.
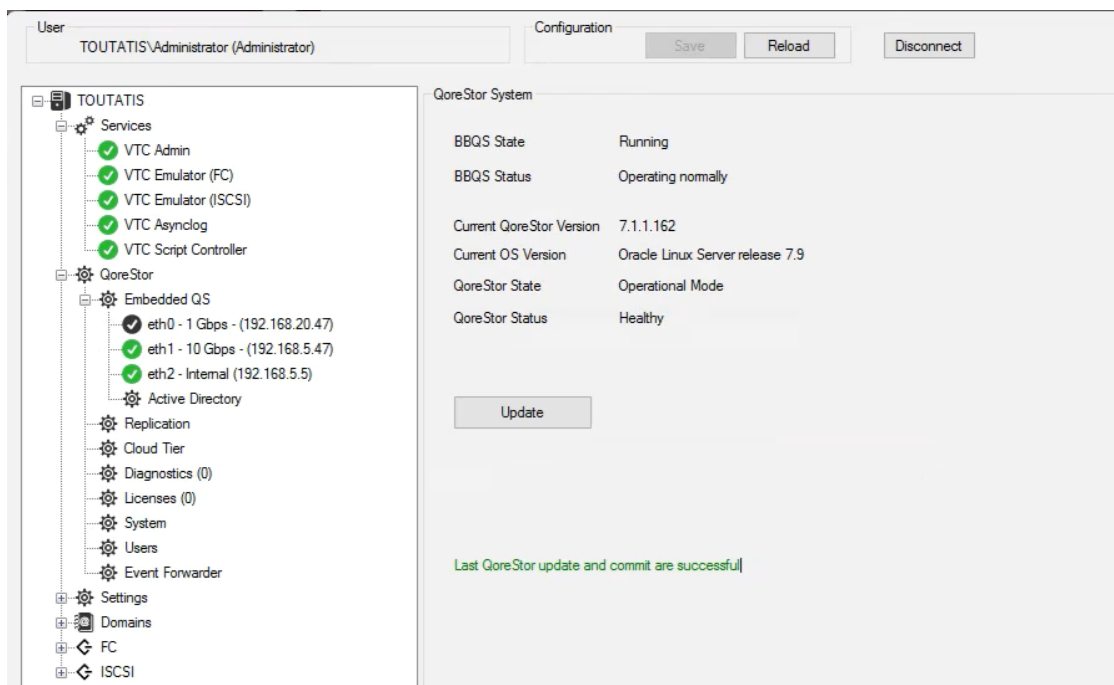
> ⚠️ If the update fails, an error message will be displayed and the version will be rolled back.
>
> For for details on update error(s), verify the QSUpdate Log.

Once the QoreStor update is successfully completed (see the green message at the bottom on the updating window), click **Update** again to start the OS update process.

Mount the OS ISO file received from ETI-NET support to update the OS. Copy and paste the location of the ISO file and click **Mount**.

Follow the same process as for the QoreStor update and click **Complete**.

The updating process might take several minutes. Don't interrupt the process while updating.
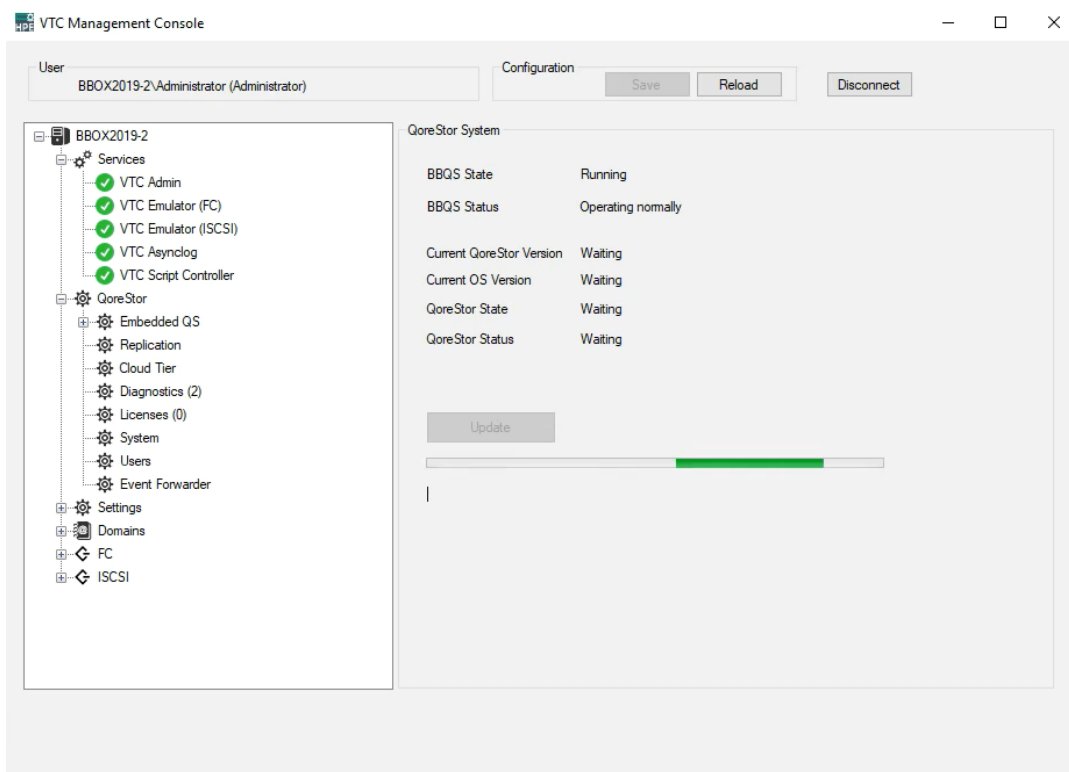
At the end of the updating process, the **System** tab will display both QoreStor and OS versions updated to.

Verify the update log, located in the VTC Log folder, for more details.
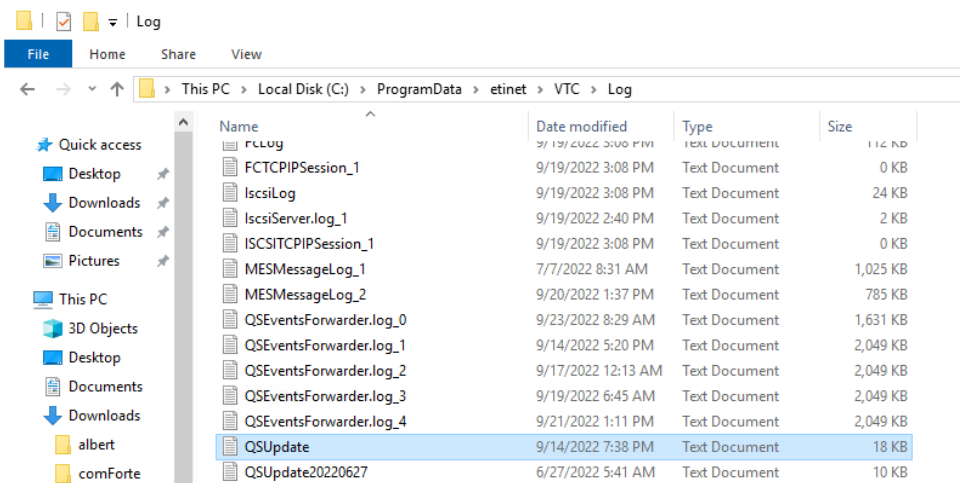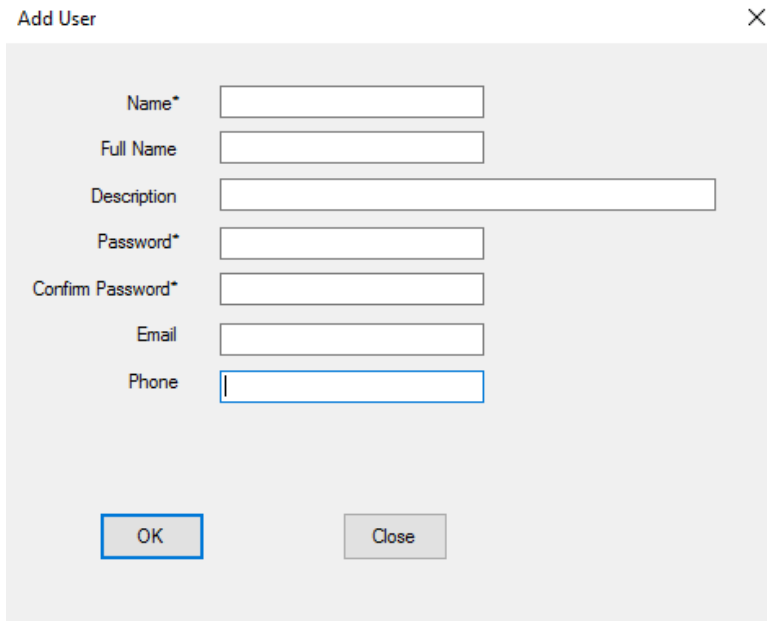
Users

QoreStor users are listed on the right-hand panel when the **Users** node is selected.
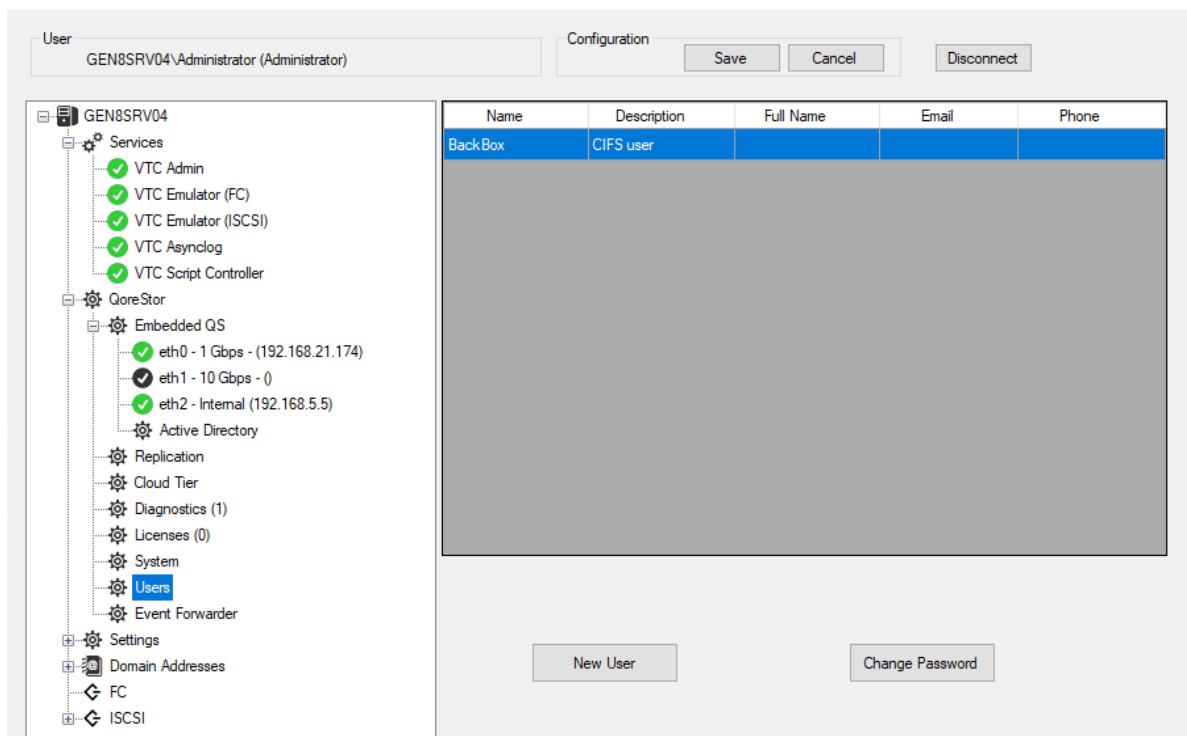
To add a new user, click **New User**.
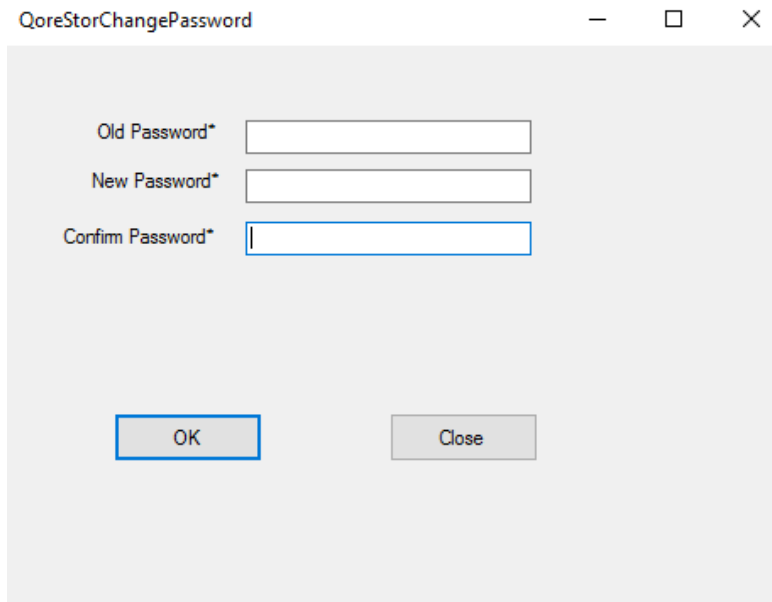
Specify the values for the mandatory fields* (Name, Password, Confirm Password) and click OK to save the entry.

To change the password for an existing user, select the user from the users list and click **Change Password**.

The pop-up window allows changing the password for the selected user. All fields are mandatory.

Click **OK** to save the password change.

Event Forwarder

Use the Event Forwarder node to enable/disable forwarding QoreStor events to the NonStop.

The default setting of the Event Forwarder is **disabled**.
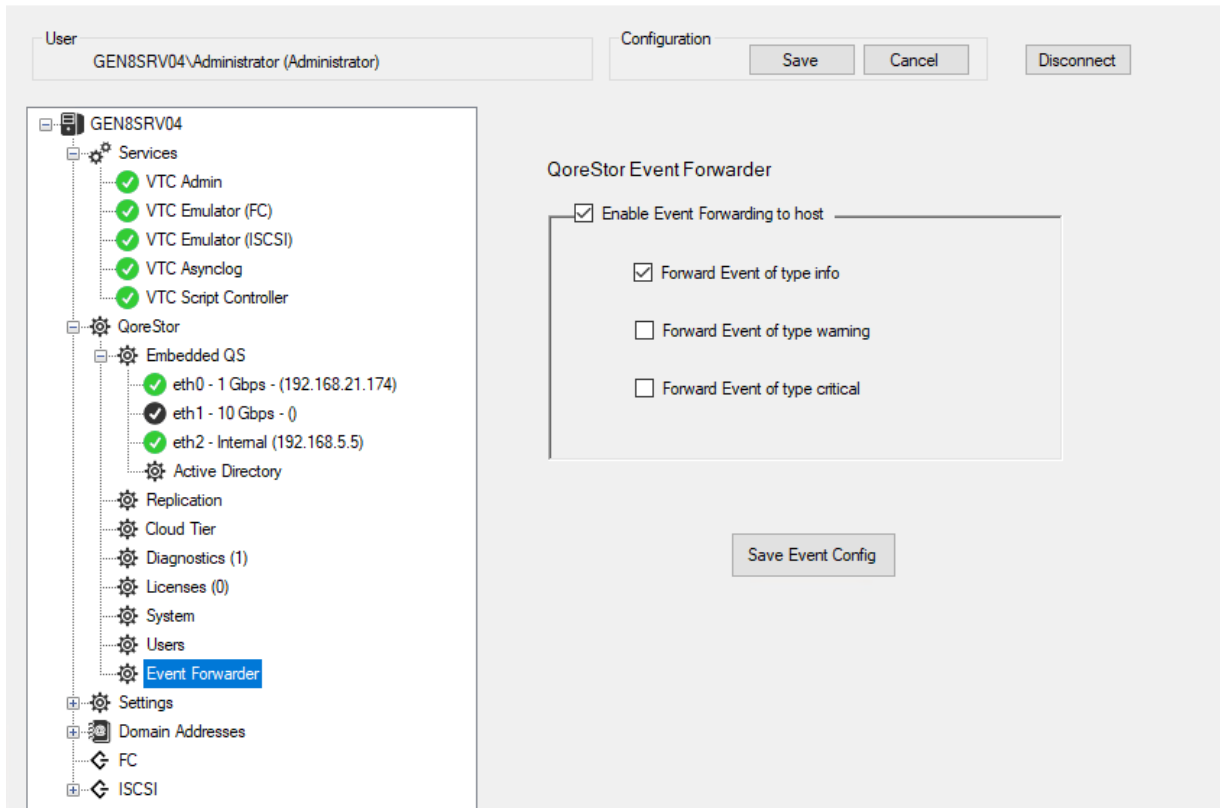
You can forward the events by severity: info, warning or critical. Choose any of the applicable or all of the event types to be forwarded to the NonStop.

Save the event configuration by clicking [Save Event Config] button. A pop-up window will confirm that the event configuration setting has been automatically saved.
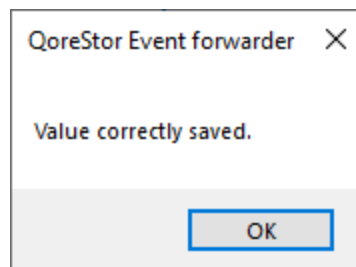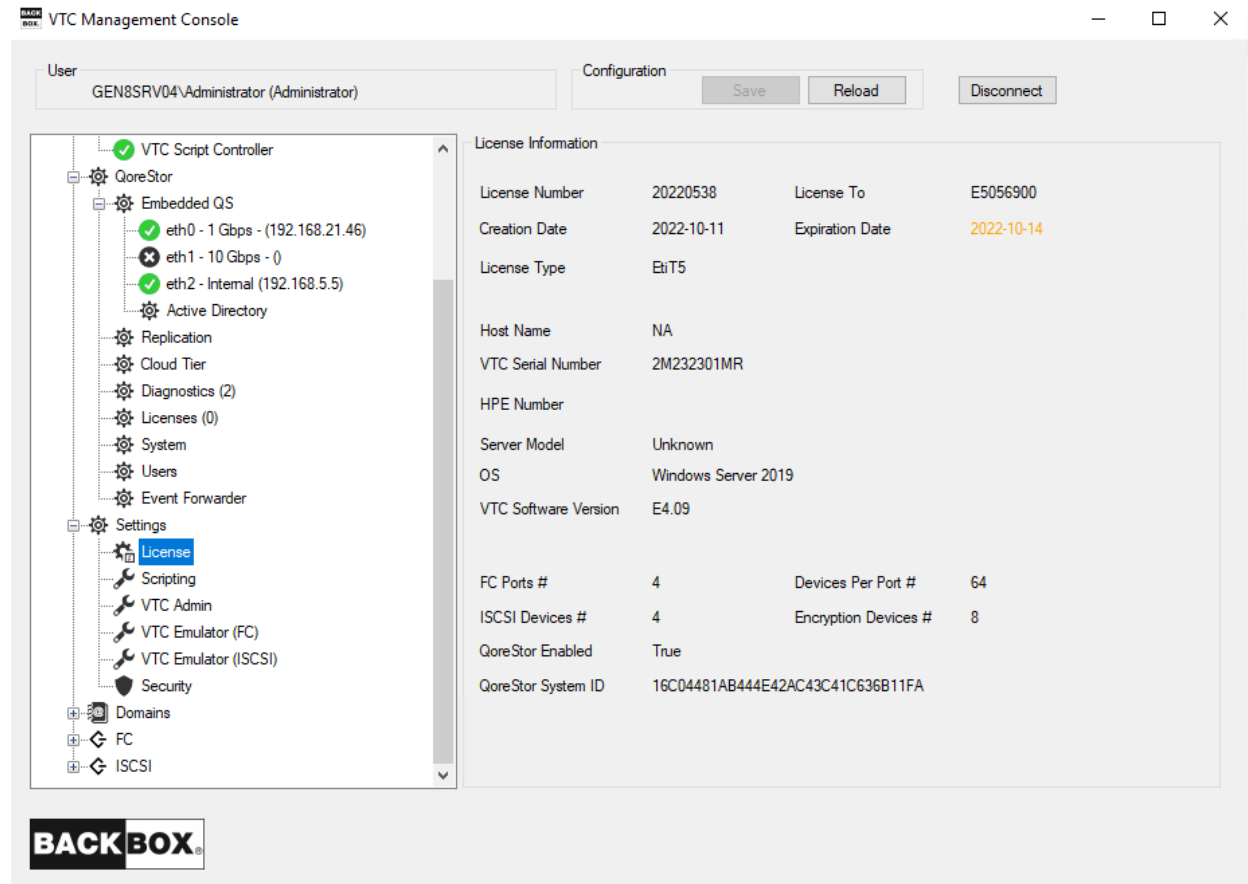
Settings

The following settings are available:

License

All details (including, expiration date, license number and type, host name details, FC ports, iSCSI devices connected and system ID) related to the active license are listed under the **License** node.

Right-click on the license node to import (as an .xml file) a new license file.
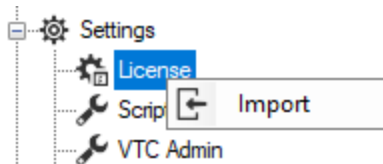
Once you click on the **Import** button, a folder browsing pop-up will open to let you select the location of the license you want to import.
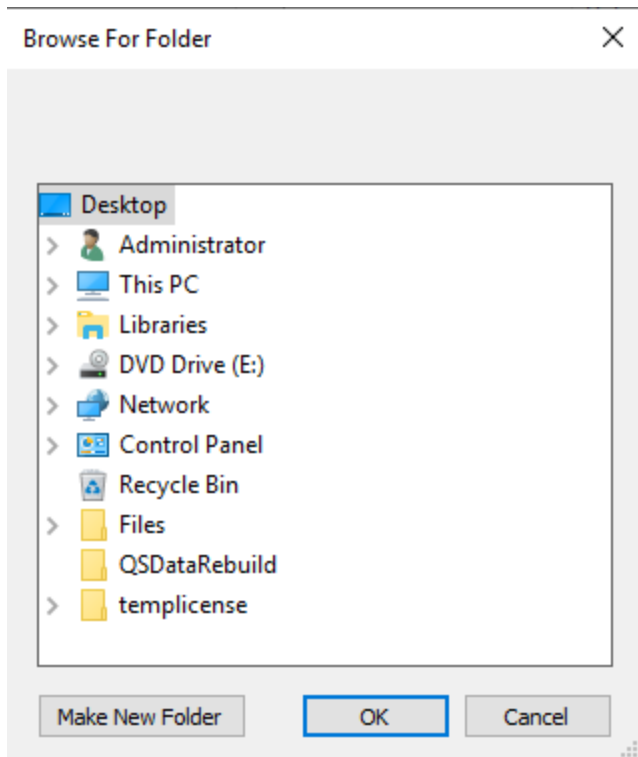
Browse for the license folder and select it to install it.

To install a new license:

Import the license .xml file provided (via email along with the report .txt file) by your ETI-NET representative.

The License is sent via email containing two files: license & license report.

License	file ready for download
License Report	file with relevant license details

1. Download the license and save it locally on the folder of your choice.

2. Import the license using **VTC MC**>**Settings**>**License**>**Import**

3. Click **Import** and select the license you saved at step 1.

4. Once the license is imported, all the license-related details will be available on BackBox UI under

Scripting

When selected, properties for script execution are displayed on the screen in the right-hand side panel. There are no actions when the mouse is right-clicked on the Scripting setting node. These properties

apply only when scripts are running without the Script Controller.
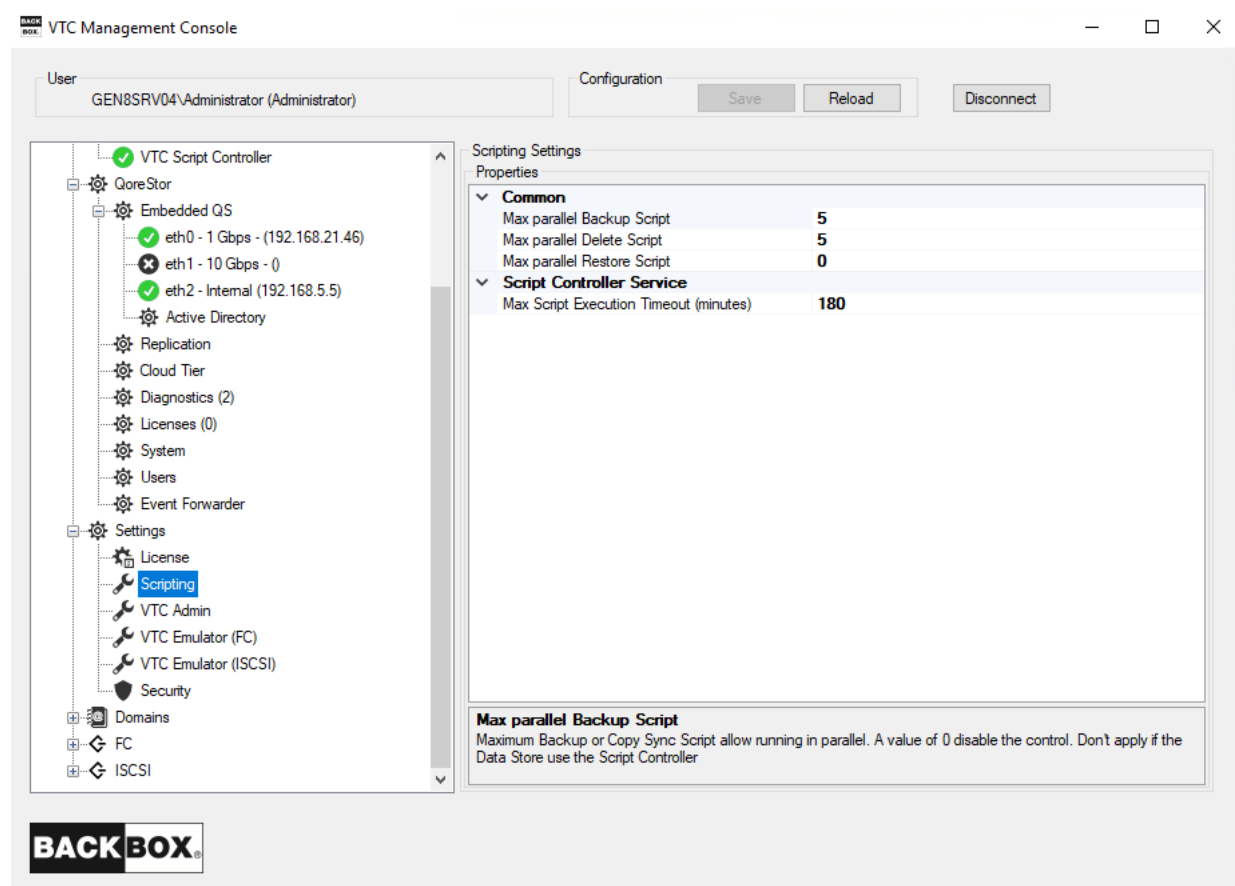
A grey-scaled panel indicates the read-only properties associated with the specified setting. When selected, any of the listed properties is shortly explained at the bottom of the window.

Any change made to this setting requires restarting all the services listed under **Services**: right-click **Services** > **Restart**.

VTC Admin

⚠️	These settings should not be changed before communicating with technical support.

When VTC Admin is selected, the available properties for the service are displayed on the screen in the right hand side panel. There are no actions available when right-clicking on the VTC Admin setting node.

A grey-scaled window indicates read-only properties associated with the specified setting. When selected, any of the listed properties is shortly explained at the bottom of the window.

Any change made to the setting requires restarting the server services.

VTC Emulator (FC)

⚠	These settings should not be changed before communicating with technical support.

When VTC Emulator (FC) is selected, the available properties for the service are displayed on the screen in the right-hand side panel. There are no actions available when right-clicking on the VTC Emulator (FC) setting node.
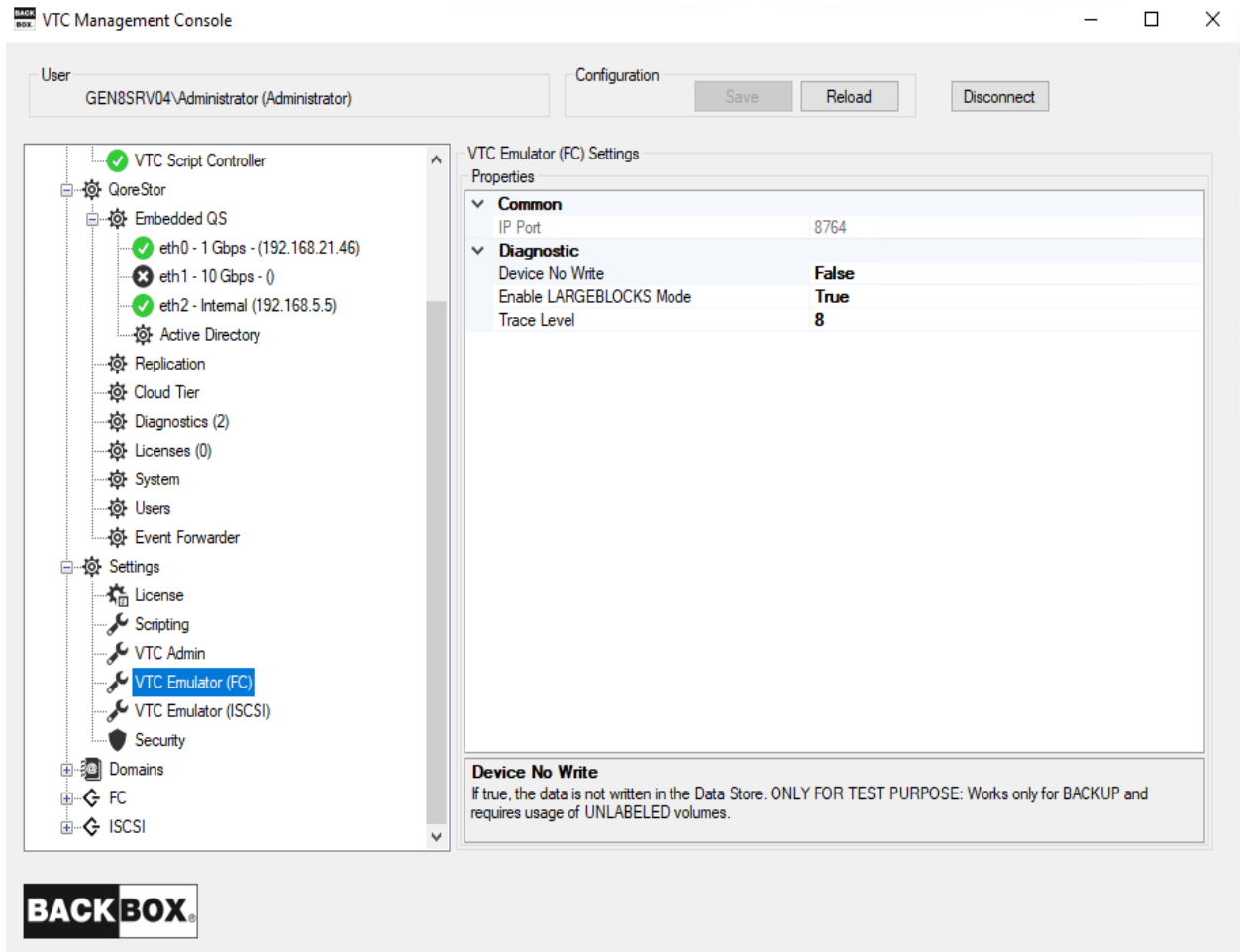
A grey-scaled window indicates read-only properties associated with the specified setting. When selected, any of the listed properties is shortly explained at the bottom of the window.

Any changes made to this page requires restarting **Services** for the change to take effect.

VTC Emulator (ISCSI)

⚠️	These settings should not be changed before communicating with technical support.

When VTC Emulator (ISCSI) is selected, the available properties for the service are displayed on the screen in the right-hand side panel. There are no actions available when right-clicking on the VTC Emulator (ISCSI) setting node.
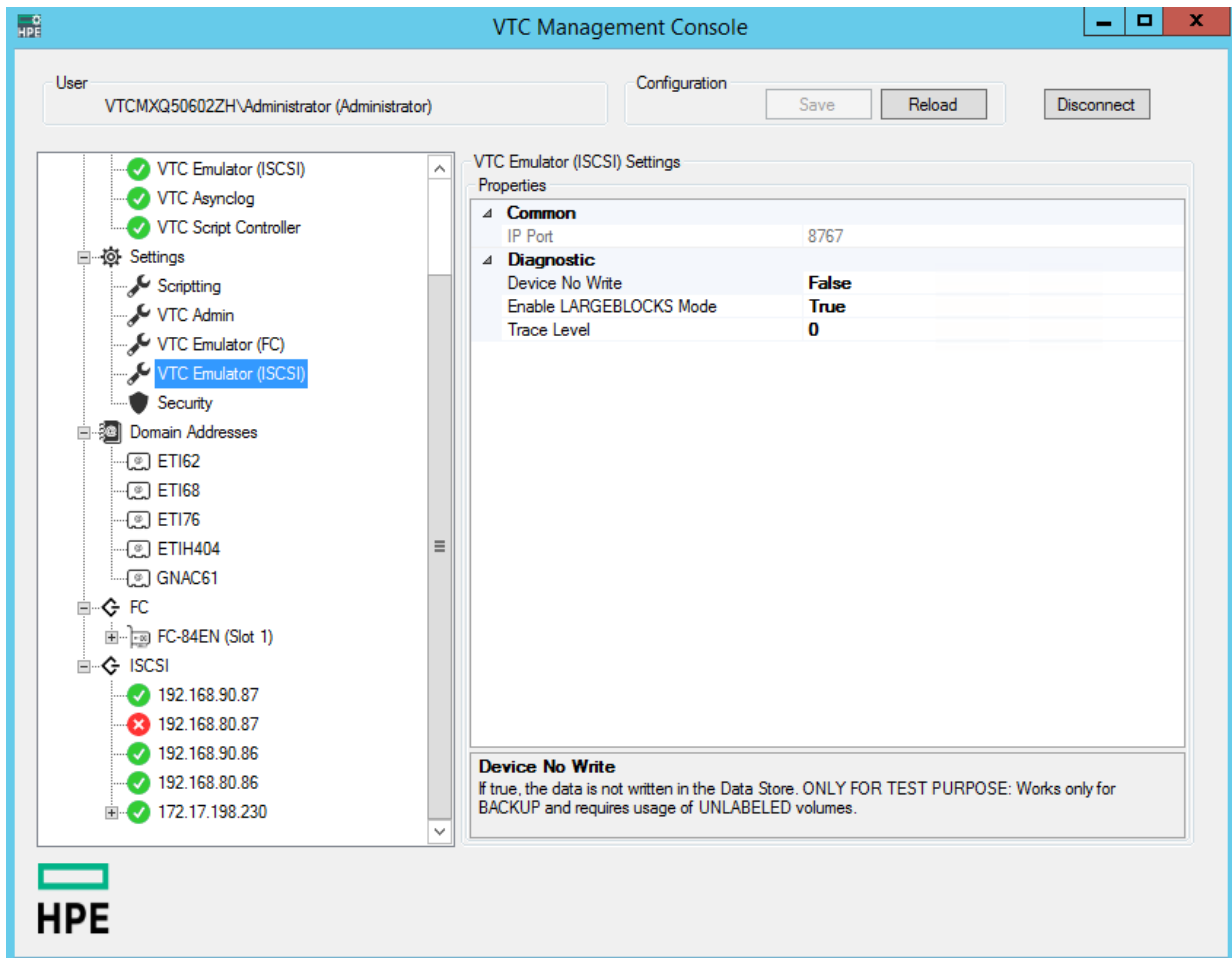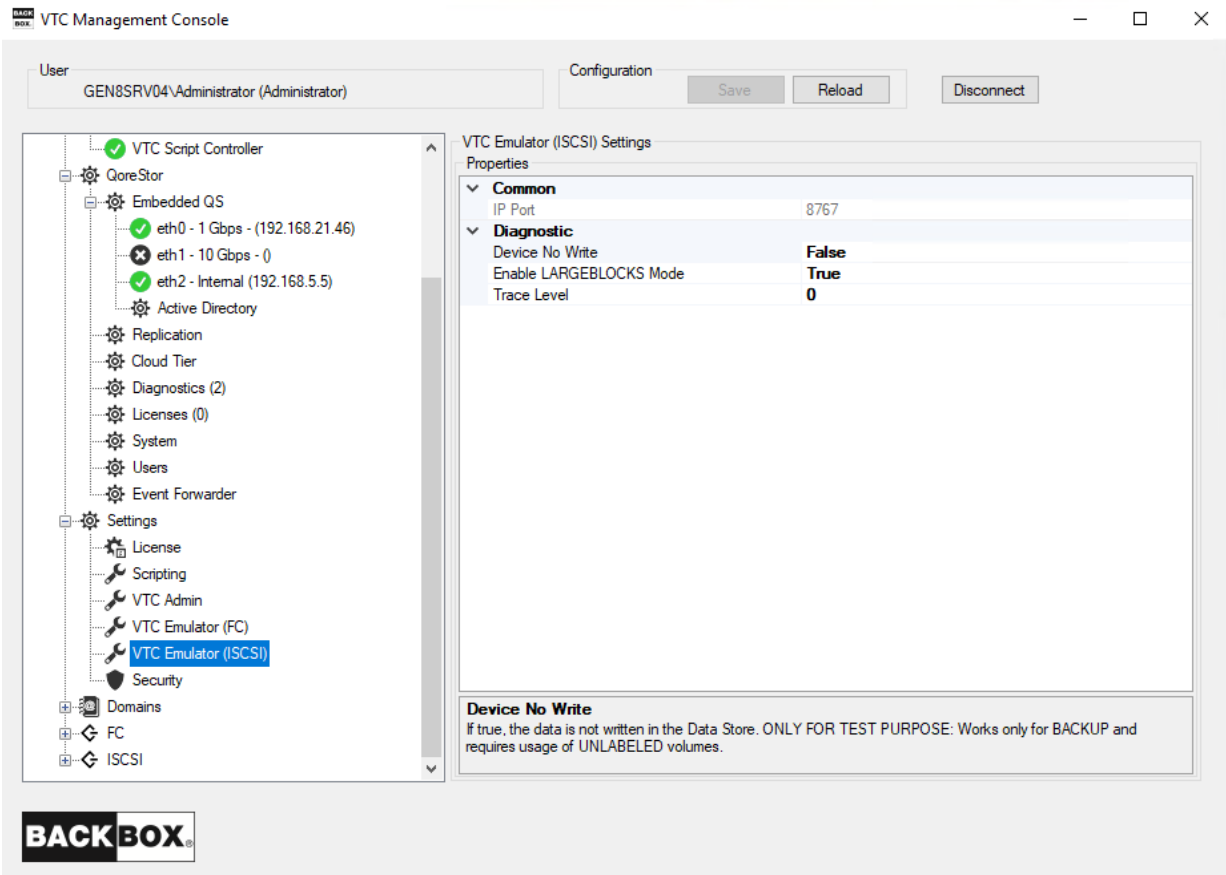
A grey-scaled window indicates read-only properties associated with the specified setting. When selected, any of the listed properties is shortly explained at the bottom of the window.

Any changes made to this page, requires restarting the **Services** for the change to take effect.

Security

When selected, information related to the support of TLS/SSL from the VTC server is displayed in the right-hand side panel.

LARGEBLOCK mode is set to ON at installation for both FC and iSCSI. It is recommended to leave it ON as it has no impact on the system when not using this option. On the contrary, turning it OFF on the VTC and having it ON on the NonStop will result in error when performing any backup operation.
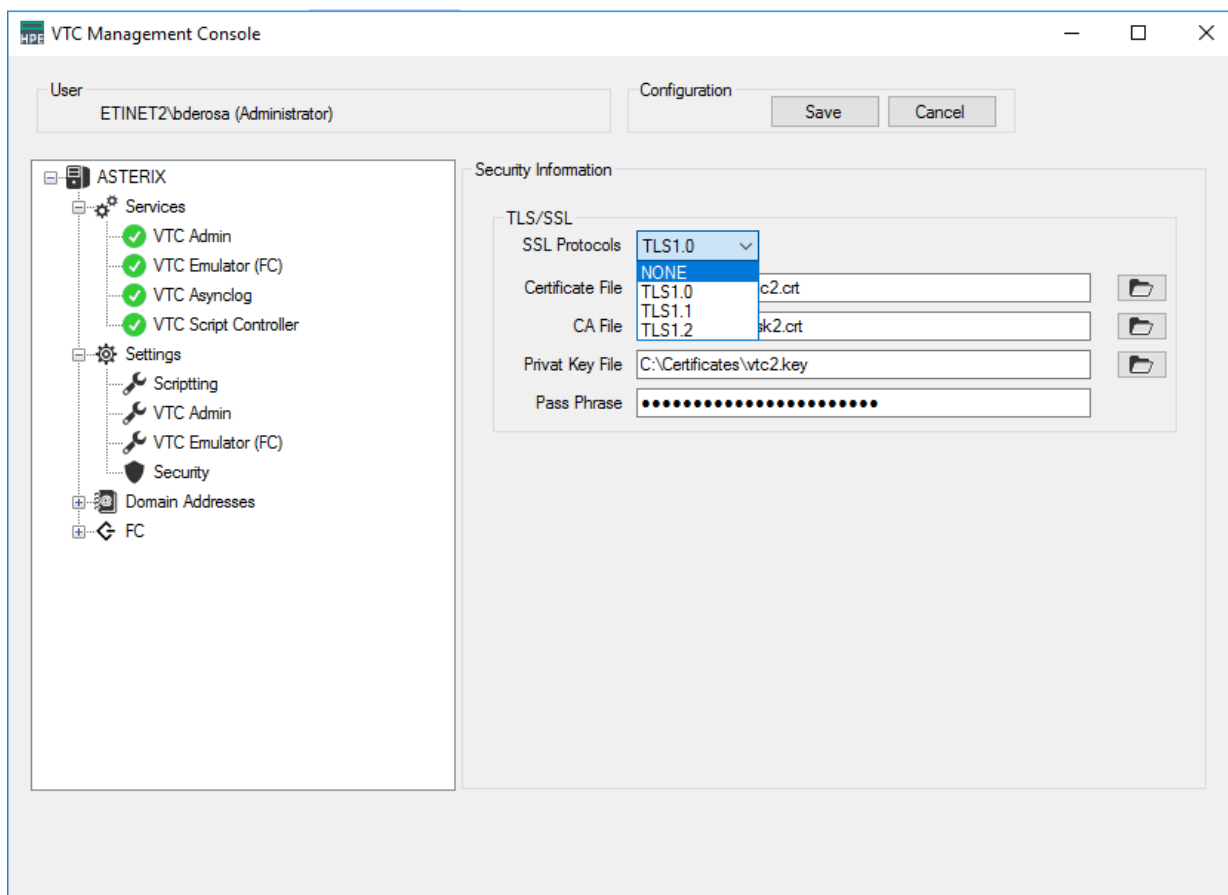
SSL Protocols: To indicate to VTC Server components what kind of TLS/SSL channel communication should be used The available protocols are shown in the drop-down list: NONE, TLS1.0, TLS1.1, TLS1.2.

Certificate File: Point to a mandatory PEM format certificate file used to identify the VTC Server in TLS/SSL channel communication. Only PEM format is supported. The certificate file provided by ETI NET is the file located in **C:\ProgramData\ETINET\VTC\Cert\vtc.crt**.

CA File: Point to an optionally PEM format certificate file that identify the Certificate Authority use in TLS/SSL channel communication. Only PEM format is support. CA certificate must also be added into the Trust Root Certification Authorities Store. The CA file provided by ETI NET is the file located in **C:\ProgramData\ETINET\VTC\Cert\nsk.crt**.

Private Key File: Point to a mandatory PEM format file that contain the private key use in TLS/SSL channel communication. Only PEM format is support. The private key file should be protected using a password. The private key file provided by ETI NET is the file located in **C:\ProgramData\ETINET\VTC\Cert\vtc.key**.

Pass Phrase: Password used to protect the private key. If you use ETI NET certificate, the pass phrase is: test

The Pass Phrase - if generated along with the certificate - will be validated by VTC MC.

Certificate, **CA** and **Private Key** files need to be granted for the SYSTEM local user with full access. See the screenshot below:
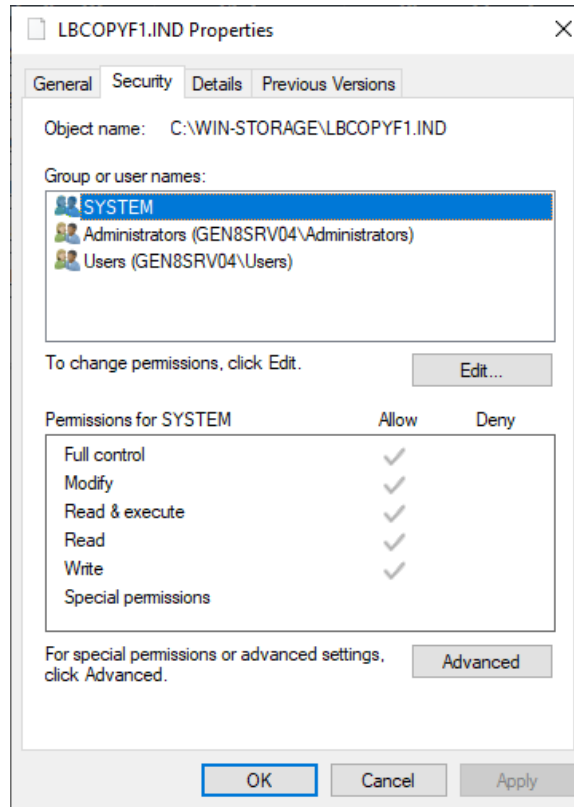
All VTC services need to be restarted for the changes to take effect. You can restart all services by right-clicking on the **Services** node and selecting the **Restart** action. The action will be applied to all services at once.

For additional information see the *BackBox SSL Setup* manual.

Domain Addresses

When expanded, the **Domain Addresses** node displays all domains currently configured on the VTC server.

⚠	Each VTC Server has its own Domain list. When the **Domain Addresses** category node is selected, there is no related information shown in the right hand side panel.
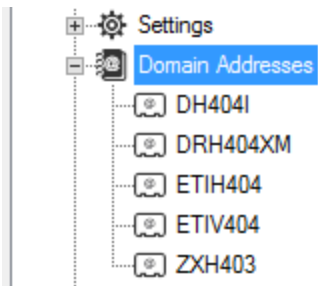
A new domain can be added to the list by right-clicking on the **Domain Addresses** category node and selecting **Add** or by pressing the Insert key while the Domain Addresses category node is selected. Type the name of the domain and press **Enter** to complete the node insertion.
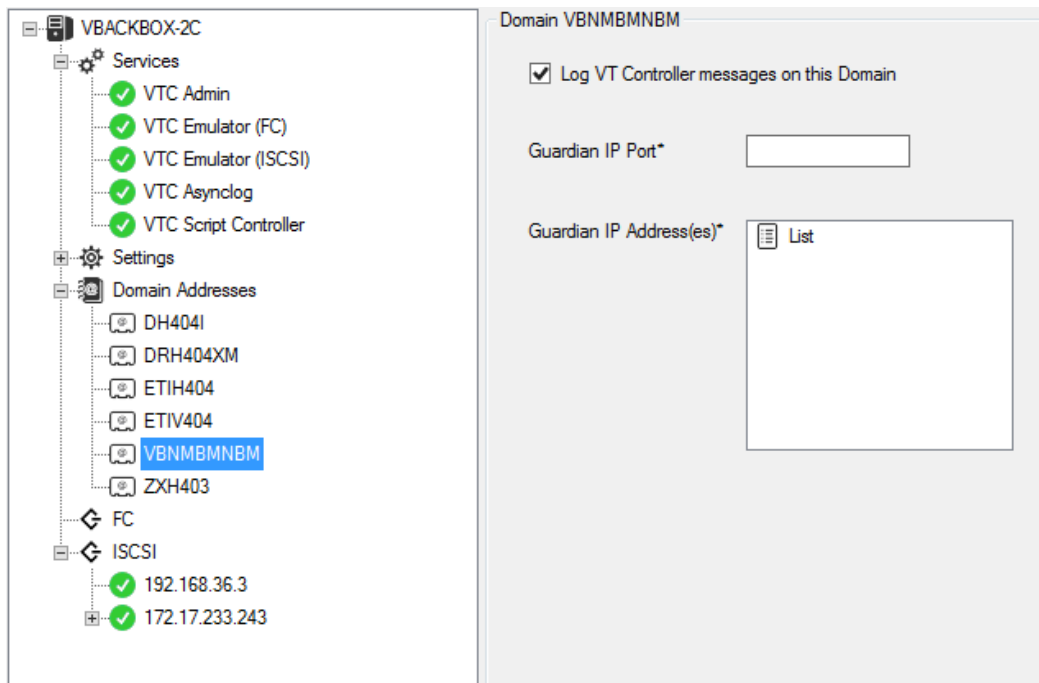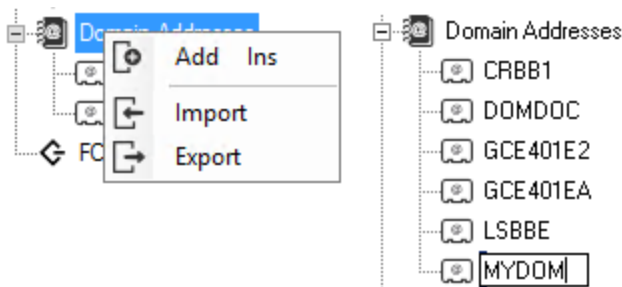
Complete the domain registration by entering the appropriate information in the fields on the right-hand side panel.

To add a Guardian IP Address, right-click on the **List** node and select **Add** or press the Insert key while the List node is selected. A new IP node will be added in the list. Enter the network address in either numeric or DNS form.
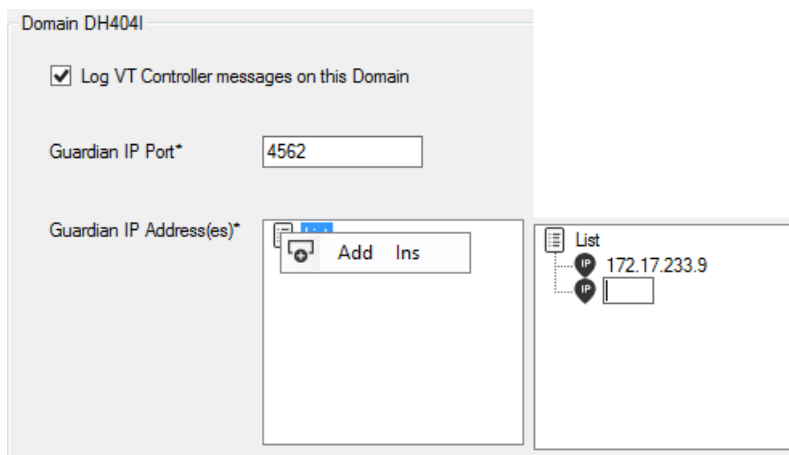
If missing or invalid information is entered, an error marker ⬤ will appear to the right side of the field.
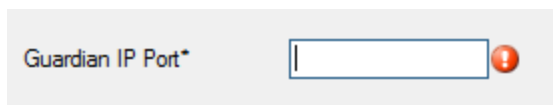
Hover the pointer on the error marker to get the error description.

When the registration process has been completed, **Add** a new domain name or **Save** the modification (s).

To browse or edit a domain in the List expand the Domain Addresses list and select the targeted domain. Domain related information will be shown in the right-hand panel.
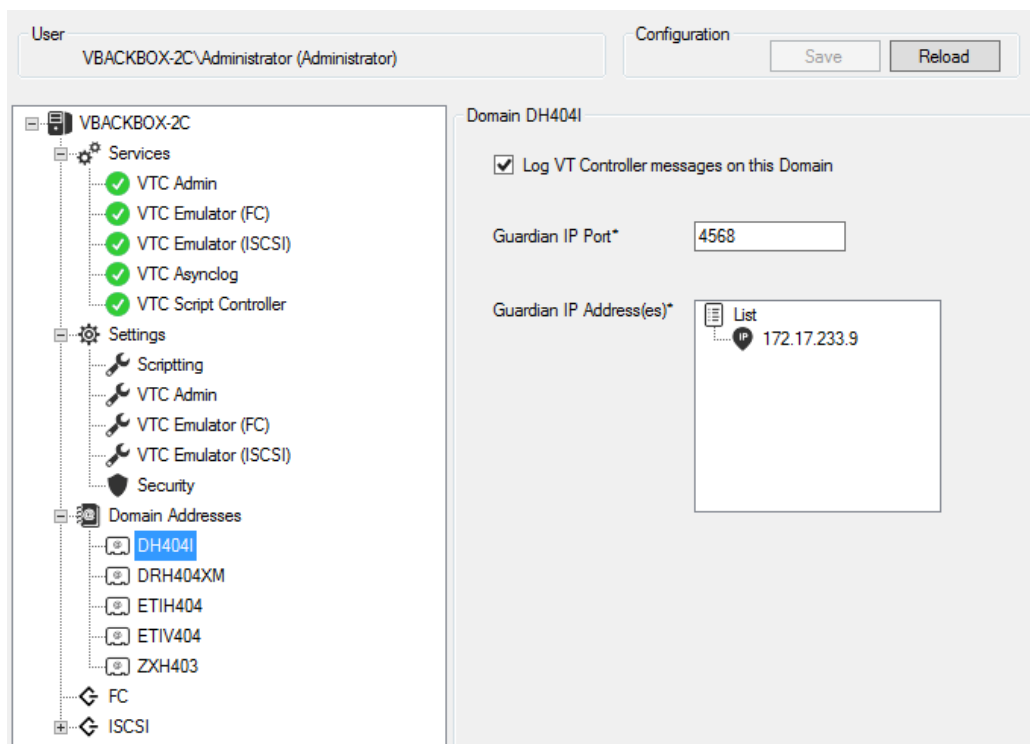
To **Delete** or **Rename** a domain, select it and right-click on it: **Delete** (or press the **Delete** key while the Domain is selected) or **Rename** (or press the F2 key while the Domain is selected).
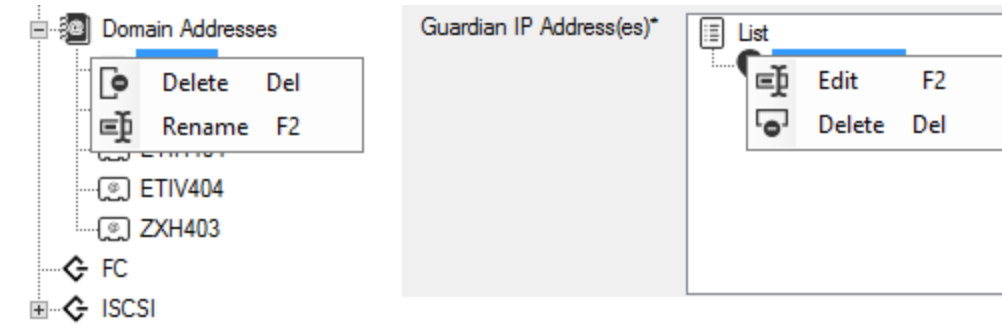
To **Export/Import** a Domain Addresses List right-click on the Domain Addresses node and select either Export or Import. The Export feature allows using the Domain Addresses list on another VTC server of the same domain by extracting the (Domain Addresses) list and placing it in a local file as backup.
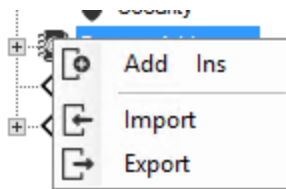
- **Export**: it opens a **Save** dialog box with the server name as a predefined filename. You can change both the name and the destination or keep the default values. Press **Save** to save your values.
- **Import**: to copy the list to another server, connect to the target VTC server, right-click on the Domain Addresses node, and select **Import**. A dialog window opens up. Navigate to the exported file, press the **Open** button, then **Save** the configuration changes.

FC Node

All VTC Fiber Channel configurations are grouped under the FC category node. Changing of any of the elements described below requires restarting **Services** for the change to take effect.
When expanded, the FC category node lists all target mode cards installed on the VTC Server. When the FC category node is selected, no information is shown in the right-hand panel.
Right-click on the FC node to configure ATTO registry entries, to enable/disable Initiator, and to enable/disable Target mode Celerity HBA features. These features are based on family models and they apply to all ATTO Celerity HBA files installed on the server. ATTO Celerity family models supported are FC-4, FC-8, and FC-16. Family models are shown only if one or more Celerity HBA files are installed on the server.
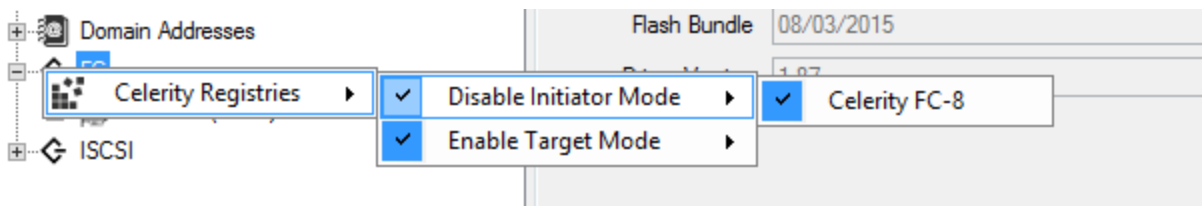
When enabled, the feature will be checked [✓] .

A diamond [◆] indicates that the feature is enabled only for part of the HBAs on the server.

To enable or disable a feature, simply check or uncheck the feature on the model and **Save** the modification.
All ATTO Celerity features require a server reboot to be enabled.

Target Mode Cards List

When the FC category node is expanded a list of all target mode cards available on the server is displayed. When a target mode card node is selected, basic card information is displayed on the right hand panel. No functions are available if right-clicking on a target mode card.
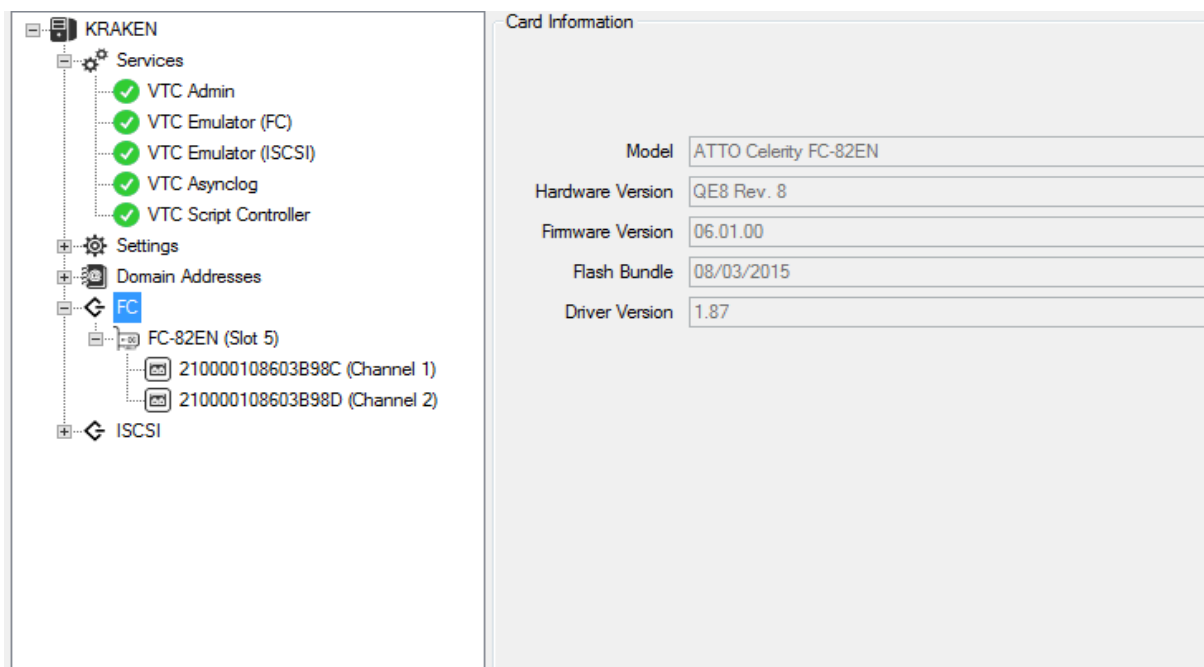
Card Ports List

When the target mode card node is expanded, a list of all the available ports on the card are shown. Each node represents a specific Fiber Channel port that can be identified by its port name (WWN) When the card port is selected, all port related configurations are displayed on the right hand side panel. There are no functions available when right-clicking on a card port.
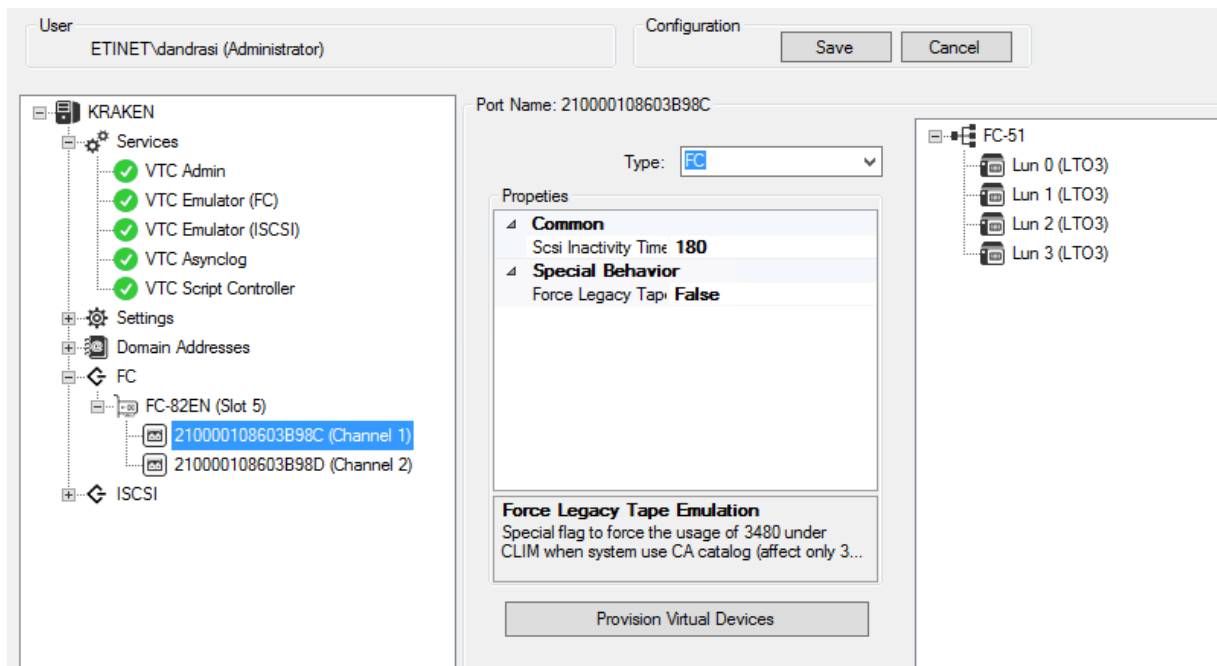
Port Configuration Elements

- Port Type

To change the port type, open the Type selection box and select one of the types.

⚠️	Changing a port type automatically resets the port configuration elements to the default values as per the newly selected type. (e.g. The number of the LUN is reset, as is the device emulation).
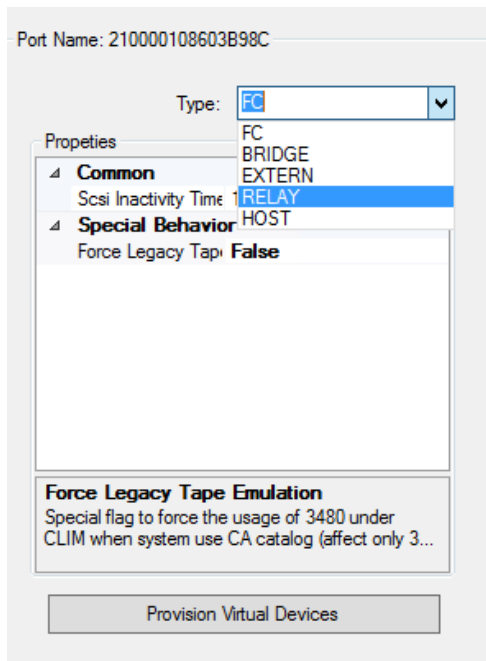
FC type is used when connected to a NonStop system.

BRIDGE type is used when connected to a NonStop S-Series system using SCSI via ETI-NET SCSI-to-FC bridge.

EXTERN type is used when connected to a Virtual Tape System for LTS media migration.

RELAY and **HOST** type are reserved for BackLib usage. See BackLib installation manual for more details.

Port Properties

Port properties are related to the port type. A "greyed-out" property indicates a read-only section. When a property is selected a message will be displayed at the bottom of the page.
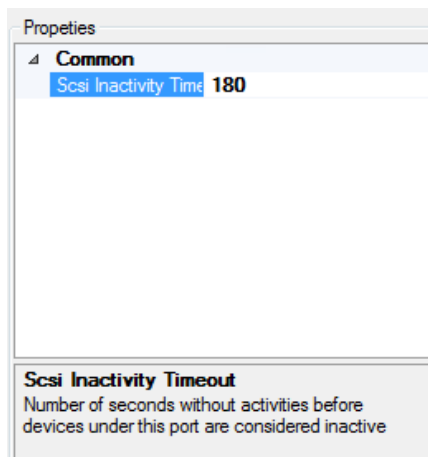
Provisioning Virtual Devices

To add or remove LUN in the port available device list use the **Provision Virtual Devices** button.

This button launches a dialog box that allows adding or removing LUN by checking or unchecking the LUN number.

⚠	Always keep **LUN 0** checked.
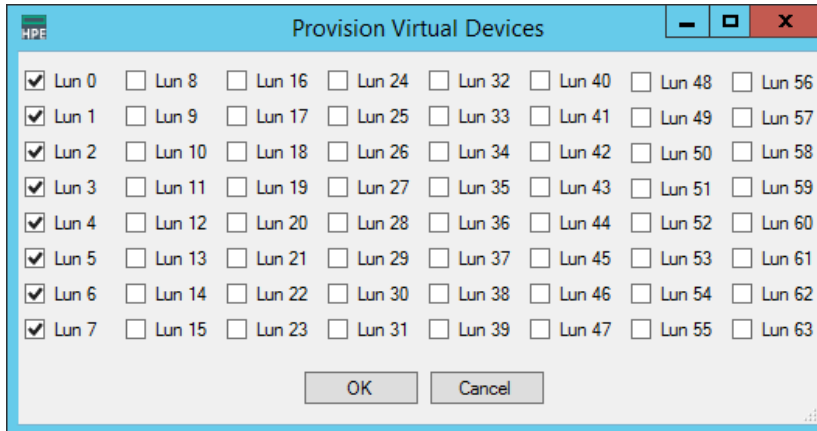
Port LUN List

The port Alias used in the BackPak Domain serves as a Root Element to regroup the configured LUN for a port. Each child node represents a specific Virtual tape device that will be presented to the NonStop host. Each LUN can have its own emulation type. To change the emulation type select the desired LUN by right-clicking on it. Select the new emulation type in the drop down box.

⚠	Available emulation can change according to the port type chosen.
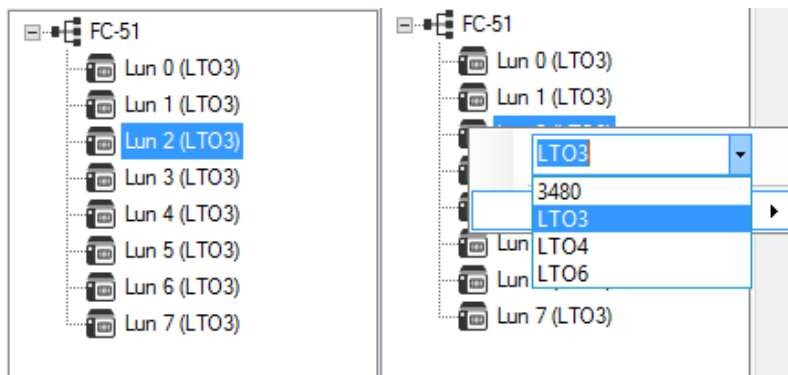
If an emulation type needs to be changed for a port, that can be done by right-clicking on the port node and selecting the new type in the emulation drop down box.

> ⚠️ The **Actions** buttons displayed underneath the list with the tape types (**Manual Load** and **Manual Unload**) are not available for this product version. Therefore, they appear greyed-out.

iSCSI Node

All VTC iSCSI configurations are grouped under the iSCSI category node. Changing of any of the elements described below requires restarting **Services** for the change to take effect.
When expanded, the iSCSI category node lists all target IP addresses installed on the VTC Server. When the iSCSI category node is selected, no information is shown in the right-hand panel.

Installing iSCSI

The iSCSI option is available with versions E4.11 and E4.11 VTC installation package.

> ⚠️ The iSCSI VTC only works with a vNSK platform. Both iSCSI and FC can be used on a physical BackBox when properly licensed.

Configuring iSCSI

Configuration of the iSCSI is done thru the VTC Management Console. The VTCMC displays the available NIC card as nodes (node name is IP address of the NIC). Under each node you can add up to 12 iSCSI devices. These devices must be added to the interface that reaches the virtual NonStop public LAN address. Limitation on the number of devices is done by the license in the Domain Manager.

Open the VTC Management Console and follow the procedure to add the iSCSI devices:

1. Click on the iSCSI node in the VTC Management Console to see the available NIC under which you can add iSCSI devices/targets.
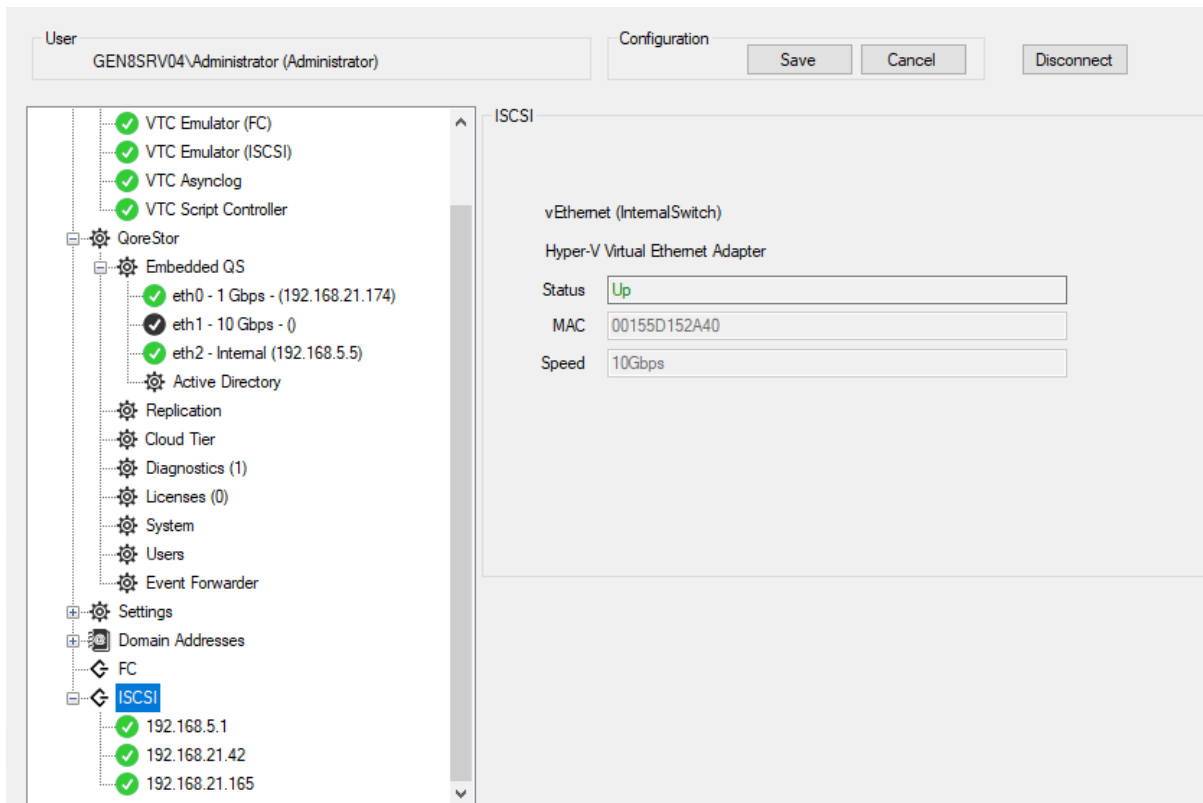
2. Right-click on the node (IP address) you want to provision. Click **Add**.
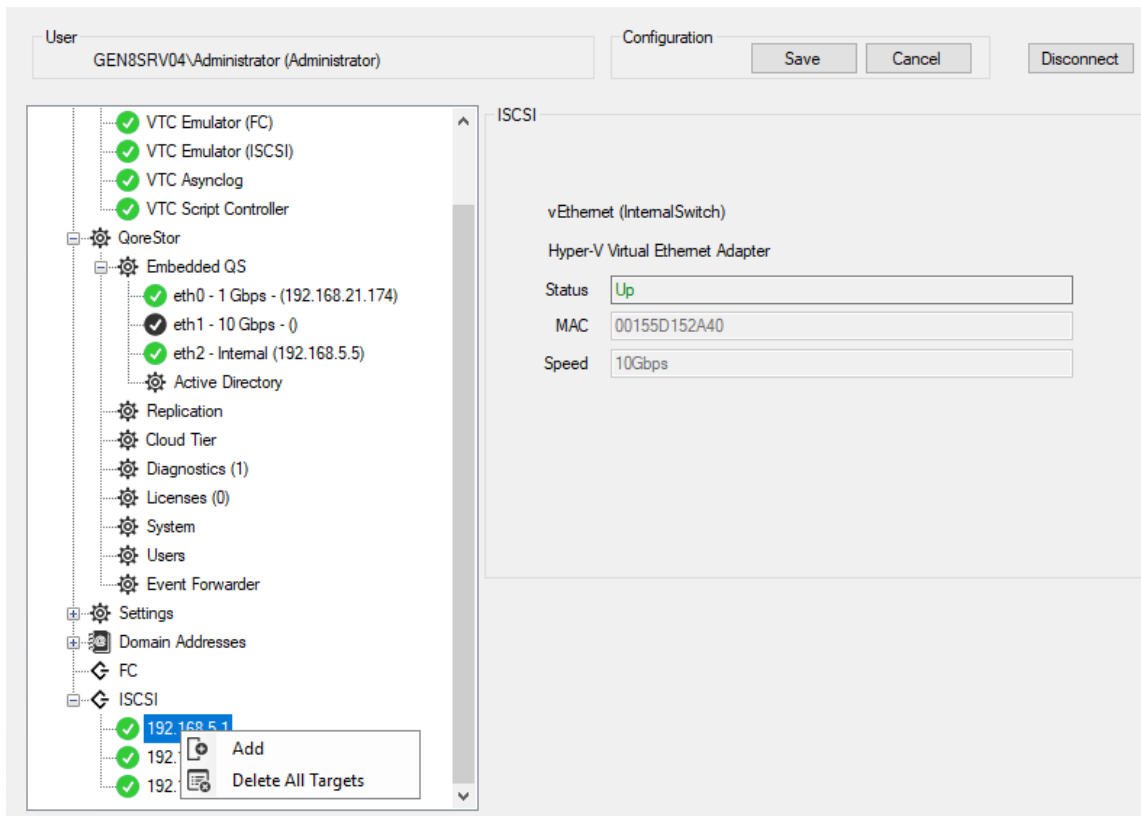
3. In the pop-up window choose the number of targets to be added. You can add up to twelve (12) devices per Network Address. The number of usable devices is determined by the Domain License.
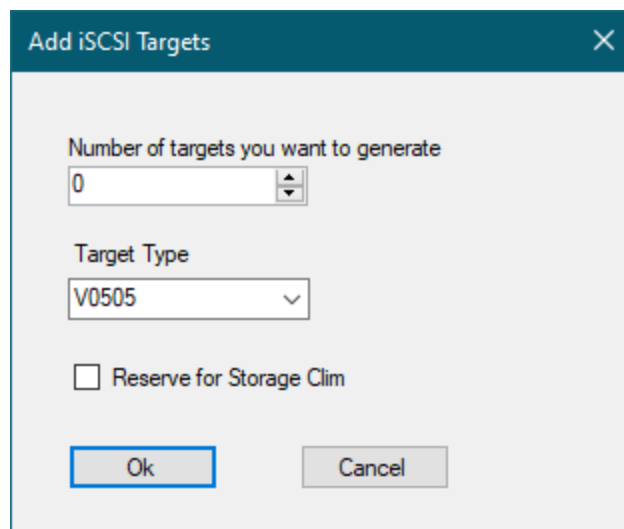
Select from the drop-down list the number of targets to add and the target type. Once the number of targets and the targets type is set up, click **ok** to add them.

Check the **Reserve for Storage Clim** box if you plan on running a Bare Metal Restore. With the Bare Metal Restore function voulmes can be directly loaded by **Stand Alone Load** on BackBox UI.

For more deatils, see [Stand Alone Load](#) section.

4. To delete an existing target, right-click on the selected target and **Detele**.
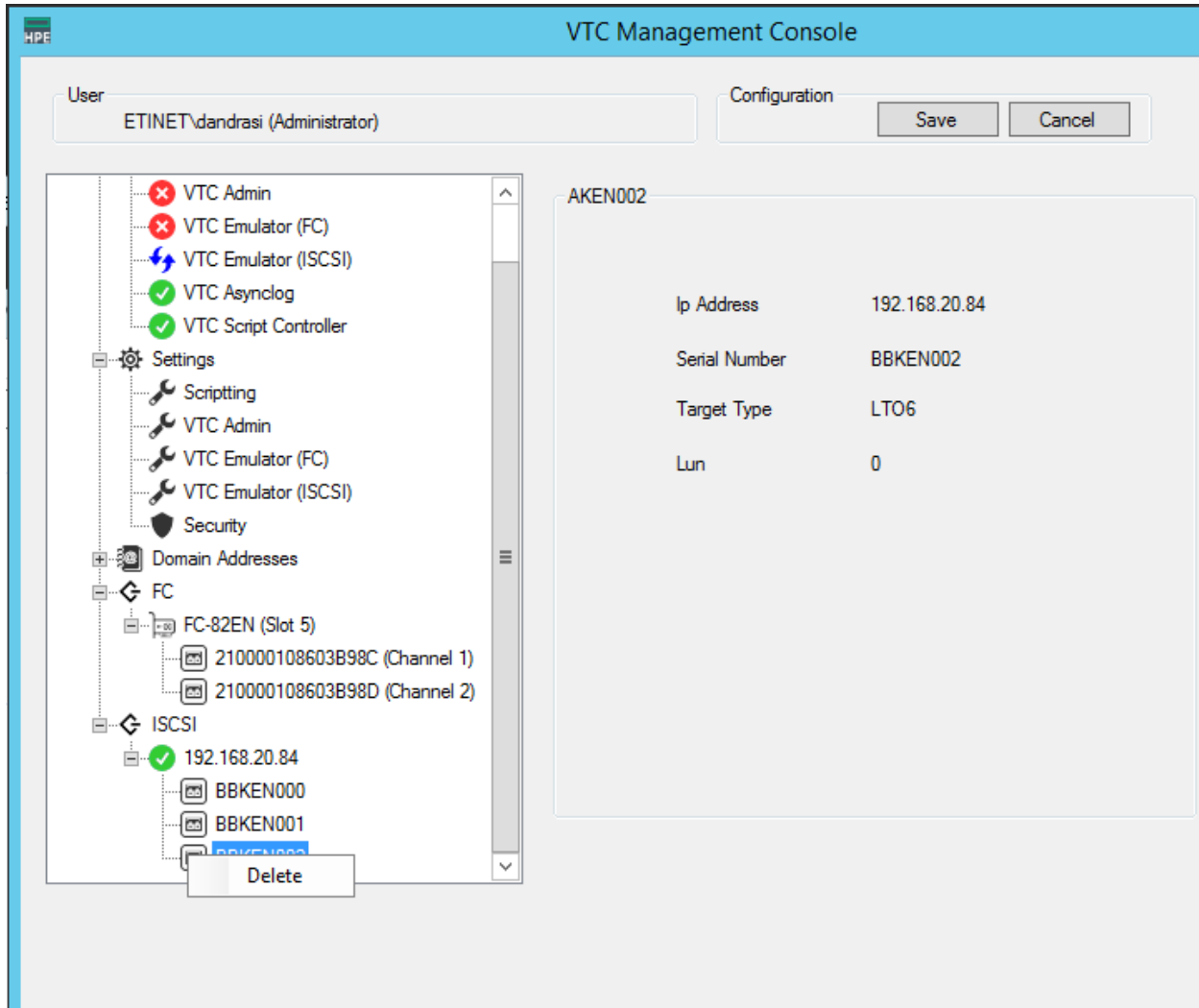
5. Once the targets are added, they will be shown under the IP address with their respective IDs/-names.

⚠	Devices that allow the Ring option - CLIM-reserved targets - are identified in the target list by the prefix identifier **XX** followed by the target specific ID.
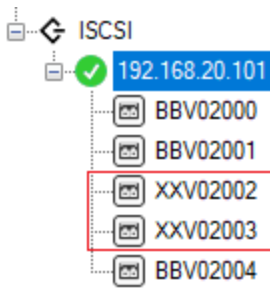
The other devices – that don't allow Ring option – are identified by **BB** followed by the device ID.
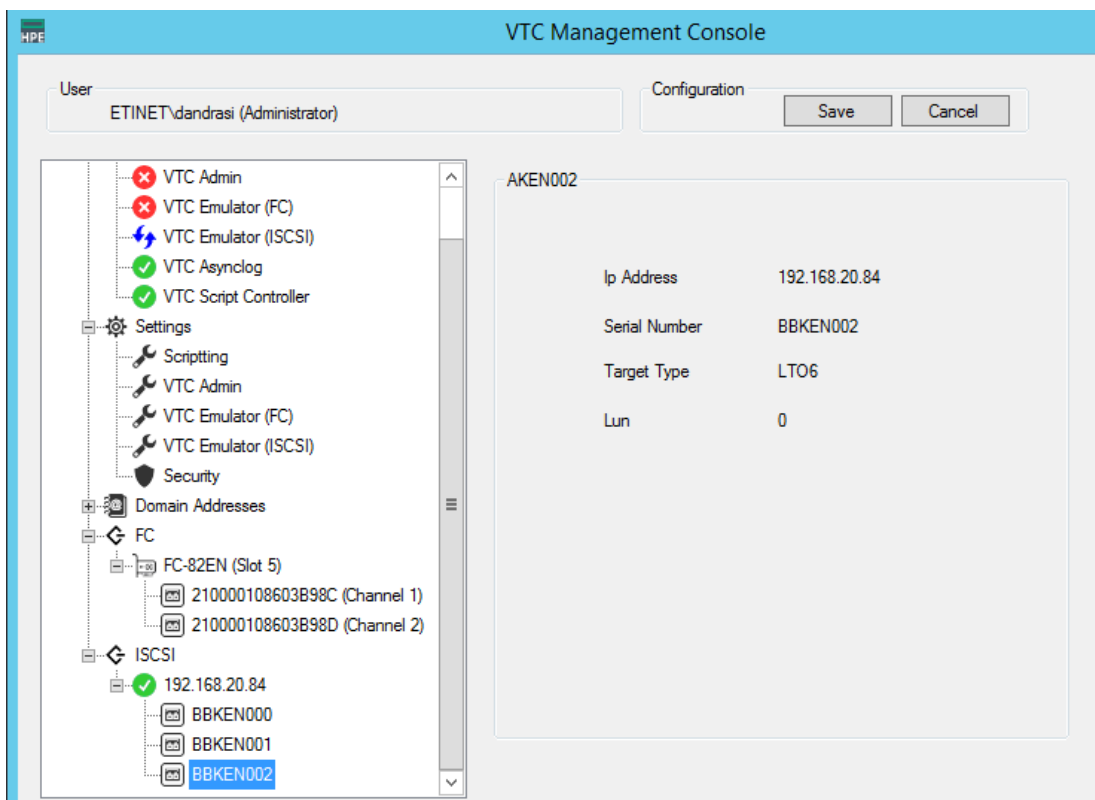
The NonStop will scan and display only the non-reserved devices, namley the ones with **BB** prefix.

```
$ETINET QCTEST 2> climcmd sclim000 lunmgr --addiscsitape 192.168.20.78
192.168.20.78:3260,-1 iqn.2000-01.com.etinet:bbtis100
192.168.20.78:3260,-1 iqn.2000-01.com.etinet:bbtis101
```

6. **Save** the configuration or **Cancel** it.
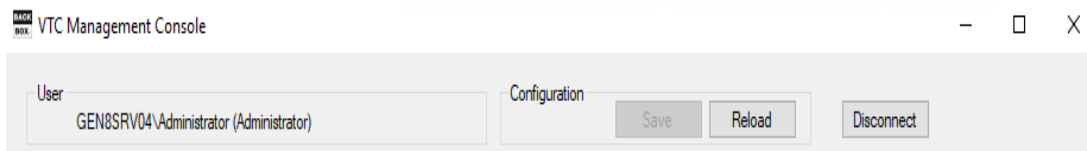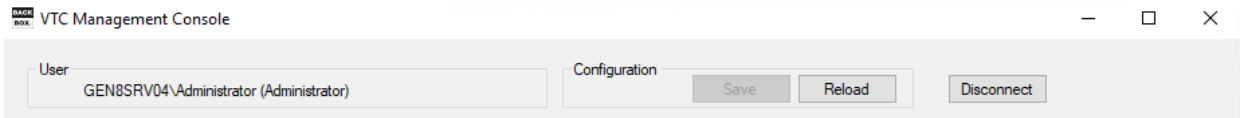
Once you have completed your change, you will have to restart VTC Services by right clicking on the **Services** node and selecting the restart option.
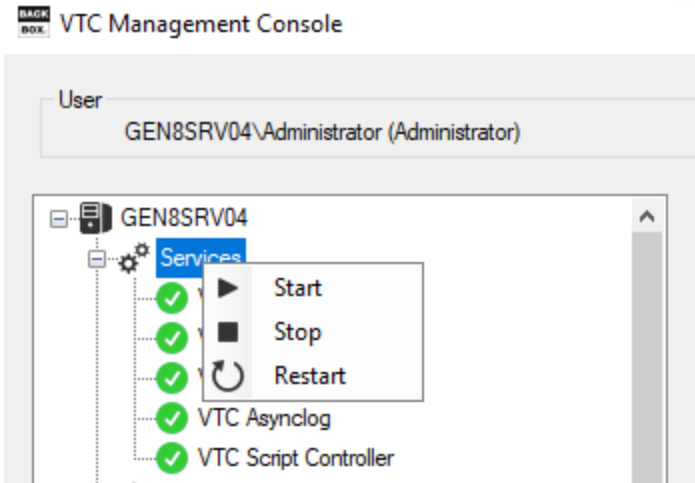
APPENDIX A - GUARDIAN TOOLS SAMPLES

BBREST – Restore Files Through MEDIACOM

Scenario Using the Detailed Report:
$DATA15 SHE409 4> run bbrest
Specify a single filename or filename template at the prompt.
Disk file(s) name / pattern: \ETINIUM.$DATA06.QCINPUT.E2KR05M
Optional tape file name / template :SHE409-OBK11DEF
Default tape file generation is the latest generation.
Optional tape file generation (ALL/nn) : all
Maximum backup time (2020-11-17 11:25):
**** executing MEDIACOM query
Disk file(s) name / pattern: \ETINIUM.$DATA06.QCINPUT.E2KR05M
Tape file name / pattern: SHE409-OBK11DEF
Tape file generation : all
Detail report, Summary, or Quit (D/S/Q): D
(1) File Catalog \ETINIUM.FILECAT
Tape File SHE409-OBK11DEF
Generation 4
Version 0
Time Archived 17Nov20 11:13
File Name Code EOF Last Modified Status
--------- ------- ----------------------- ------------- ------
\ETINIUM.$DATA06.QCINPUT
E2KR05M 0 5120000 30Apr03 16:04 VALID
(2) File Catalog \ETINIUM.FILECAT
Tape File SHE409-OBK11DEF
Generation 3
Version 0
Time Archived 17Nov20 11:12
File Name Code EOF Last Modified Status
Page pause: enter 'E' to end or any key to continue:
--------- ------- ----------------------- ------------- ------
\ETINIUM.$DATA06.QCINPUT
E2KR05M 0 5120000 30Apr03 16:04 VALID
(3) File Catalog \ETINIUM.FILECAT
Tape File SHE409-OBK11DEF
Generation 2
Version 0
Time Archived 17Nov20 10:48
File Name Code EOF Last Modified Status
--------- ------- ----------------------- ------------- ------
\ETINIUM.$DATA06.QCINPUT
E2KR05M 0 5120000 30Apr03 16:04 VALID
(4) File Catalog \ETINIUM.FILECAT

```
Page pause: enter 'E' to end or any key to continue:
Tape File SHE409-OBK11DEF
Generation 1
Version 0
Time Archived 15Nov20 21:06
File Name Code EOF Last Modified Status
--------- ------- ----------------------- ------------- ------
\ETINIUM.$DATA06.QCINPUT
E2KR05M 0 5120000 30Apr03 16:04 VALID
4 disk files returned.
Enter (#) of tape file to recover from (or Q for quit):1
Recover destination subvol : $DATA07.RESTORE
Recover report output ($S.#DSMTC.RESTORE):
... testing if LOCALTOREMOTE is required ...
About to execute:
RECOVER DISKFILE \ETINIUM.$DATA06.QCINPUT.E2KR05M, TAPEFILE SHE409-
OBK11DEF, GEN
4 ,
MAP NAMES (\ETINIUM.$DATA06.QCINPUT.E2KR05M TO $DATA07.RESTORE.*),
OUT $S.#DSM
TC.RESTORE,
LISTALL, OPEN, TAPEDATE, AUDITED
Confirm execution (Y/N): y
**** executing MEDIACOM recovery
MEDIACOM - T6028H01 (31JUL2014)
(C) Copyright 1993-2002, 2004 Hewlett-Packard Development Company,
L.P.
The tape file selected is shown as the following:
File Catalog \ETINIUM.FILECAT
Volume Catalog \ETINIUM.VOLCAT
Pool Name SHE409_POOL1
Tape File SHE409-OBK11DEF
Generation 4
Version 00
Physical Copy 01
Logical Copy 1
Time Archived 17 NOV 2020, 11:14:09
Tape File Mode FILEMODE BACKUP
Catalog Files YES
Tape Name RT304
Total count of valid matching disk files: 0000000001
Do you want to see the matching disk files ? (y/n) y
File Name Code Last Modified Status
----------------------------------- ------ ------------- -------
\ETINIUM.$DATA06.QCINPUT.E2KR05M 00000 30APR03 VALID
Do you want RESTORE to be started? (y/n) y
Starting RESTORE...
Tape volumes used: RT304
```

```
Summary Information
Files restored = 1 Files not restored = 0
1 recover diskfile completed.
```

Scenario Using the Summary Report:

```
$DATA15 SHE409 5> run bbrest
Specify a single filename or filename template at the prompt.
Disk file(s) name / pattern: \ETINIUM.$DATA06.QCINPUT.E2KR05M
Optional tape file name / template :SHE409-OBK11DEF
Default tape file generation is the latest generation.
Optional tape file generation (ALL/nn) : all
Maximum backup time (2020-11-17 11:30):
**** executing MEDIACOM query
Disk file(s) name / pattern: \ETINIUM.$DATA06.QCINPUT.E2KR05M
Tape file name / pattern: SHE409-OBK11DEF
Tape file generation : all
Detail report, Summary, or Quit (D/S/Q): S
ETI-NET: TapeFiles listed in backup time
=======================================================================
File Catalog
Tape File Gen Ver Time Archived
----------------------------------------- ------- ------ -------------
( 1) SHE409-OBK11DEF 4 0 17Nov20
( 2) SHE409-OBK11DEF 3 0 17Nov20
( 3) SHE409-OBK11DEF 2 0 17Nov20
( 4) SHE409-OBK11DEF 1 0 15Nov20
=======================================================================
Enter (#) of tape file to recover from (or Q for quit):2
Recover destination subvol : $DATA07.RESTORE
Recover report output ($S.#DSMTC.RESTORE):
... testing if LOCALTOREMOTE is required ...
About to execute:
RECOVER  DISKFILE  \ETINIUM.$DATA06.QCINPUT.E2KR05M,  TAPEFILE  SHE409-
OBK11DEF, GEN
3 ,
MAP  NAMES  (\ETINIUM.$DATA06.QCINPUT.E2KR05M  TO  $DATA07.RESTORE.*),
OUT $S.#DSM
TC.RESTORE,
LISTALL, OPEN, TAPEDATE, AUDITED
Confirm execution (Y/N): y
**** executing MEDIACOM recovery
MEDIACOM - T6028H01 (31JUL2014)
(C) Copyright 1993-2002, 2004 Hewlett-Packard Development Company,
L.P.
The tape file selected is shown as the following:
File Catalog \ETINIUM.FILECAT
Volume Catalog \ETINIUM.VOLCAT
```

```
Pool Name SHE409_POOL1
Tape File SHE409-OBK11DEF
Generation 3
Version 00
Physical Copy 01
Logical Copy 1
Time Archived 17 NOV 2020, 11:13:08
Tape File Mode FILEMODE BACKUP
Catalog Files YES
Tape Name RT303
Total count of valid matching disk files: 0000000001
Do you want to see the matching disk files ? (y/n) y
File Name Code Last Modified Status
------------------------------------ ------ ------------- -------
\ETINIUM.$DATA06.QCINPUT.E2KR05M 00000 30APR03 VALID
Do you want RESTORE to be started? (y/n) y
Starting RESTORE...
Tape volumes used: RT303
Summary Information
Files restored = 1 Files not restored = 0
1 recover diskfile completed.
```

TMFC2 – Extensions to TMFCOM Commands on Media

Sample 1

```
    $DATA15 RUE409 15> tmfc2 info media tmfb*
    TMFCOM - T8652J01 - (15AUG2014- TMF)
    (C)2005 Hewlett-Packard Development Company, L.P.
    TMF 1> INFO MEDIA TMFB00
    Media Name Media Type Media Status
    --------------------------------------
    TMFB00 tape assigned
    TMF 2> INFO MEDIA TMFB01
    Media Name Media Type Media Status
    --------------------------------------
    TMFB01 tape assigned
    TMF 3> INFO MEDIA TMFB02
    Media Name Media Type Media Status
    --------------------------------------
    TMFB02 tape assigned
    $DATA15 RUE409 16> tmfc2 info media tmfd*
    TMFCOM - T8652J01 - (15AUG2014- TMF)
    (C)2005 Hewlett-Packard Development Company, L.P.
    TMF 1> INFO MEDIA TMFD00
    Media Name Media Type Media Status
    --------------------------------------
```

```
TMFD00 tape assigned
TMF 2> INFO MEDIA TMFD01
Media Name Media Type Media Status
--------------------------------------
TMFD01 tape assigned
TMF 3> INFO MEDIA TMFD02
Media Name Media Type Media Status
--------------------------------------
TMFD02 tape assigned
TMF 4> INFO MEDIA TMFD03
Media Name Media Type Media Status
--------------------------------------
TMFD03 tape assigned
TMF 5> INFO MEDIA TMFD04
Media Name Media Type Media Status
--------------------------------------
TMFD04 tape assigned
TMF 6> INFO MEDIA TMFD05
Media Name Media Type Media Status
--------------------------------------
TMFD05 tape assigned
TMF 7> INFO MEDIA TMFD06
Media Name Media Type Media Status
--------------------------------------
TMFD06 tape assigned
TMF 8> INFO MEDIA TMFD07
Media Name Media Type Media Status
--------------------------------------
TMFD07 tape assigned
TMF 9> INFO MEDIA TMFD08
Media Name Media Type Media Status
--------------------------------------
TMFD08 tape assigned
```

Sample 2

```
$DATA15 RUE409 38> tmfc2 PEEK, file tmfin, alter media tmf*,
select status released, status scratch
ALTER MEDIA TMFD07 ,status SCRATCH
ALTER MEDIA TMFD08 ,status SCRATCH
2 RECORDS TRANSFERRED
$DATA15 RUE409 39> fup copy tmfin
ALTER MEDIA TMFD07 ,status SCRATCH
ALTER MEDIA TMFD08 ,status SCRATCH
2 RECORDS TRANSFERRED
```

Sample 3

```
$DATA15 RUE409 40> tmfc2 alter media tmf*, select status
released, status scratch
TMFCOM - T8652J01 - (15AUG2014- TMF)
(C)2005 Hewlett-Packard Development Company, L.P.
TMF 1> ALTER MEDIA TMFD07 ,status SCRATCH
TMF 2> ALTER MEDIA TMFD08 ,status SCRATCH
```

BB000_COLLECT – Gather Information for Support

Sample:

```
$DATA15 SHE409 23> BB000_COLLECT TARGET SHE409T
... creating \ETINIUM.$DATA15.SHE409T.COL222* files for node number
222
WARNING - $DATA15.SHE409T.COL222*: ERR 11
0 FILES PURGED
CREATED - $DATA15.SHE409T.ETINIUM
1 RECORDS TRANSFERRED
MEDIACOM - T6028H01 (31JUL2014)
(C) Copyright 1993-2002, 2004 Hewlett-Packard Development Company,
L.P.
MEDIACOM - T6028H01 (31JUL2014)
(C) Copyright 1993-2002, 2004 Hewlett-Packard Development Company,
L.P.
MEDIACOM - T6028H01 (31JUL2014)
(C) Copyright 1993-2002, 2004 Hewlett-Packard Development Company,
L.P.
2 RECORDS TRANSFERRED
$DATA15.SHE409T.COL222X PURGED.
1 FILE PURGED
SCF - T9082H01 - (23JUN11) (02MAY11) - 11/17/2020 18:36:36 System
\ETINIUM
(C) 1986 Tandem (C) 2006 Hewlett Packard Development Company, L.P.
SCF W20052 Creating file \ETINIUM.$DATA15.SHE409T.COL222J
SCF W20052 Creating file \ETINIUM.$DATA15.SHE409T.COL222G
SCF - T9082H01 - (23JUN11) (02MAY11) - 11/17/2020 18:36:37 System
\ETINIUM
(C) 1986 Tandem (C) 2006 Hewlett Packard Development Company, L.P.
default times
... extracting events from 2020-11-16 18:36:30 to EOF
CREATED - $DATA15.SHE409T.COL222E
... creating PAK file \ETINIUM.$DATA15.SHE409T.COL222P
PAK - File compression program - T1255H01 - (2014-04-29)
File Mode BACKUP Program - T9074H01 (10JUL2015) (AGP)
(C)2000 Compaq (C)2007 Hewlett-Packard Development Company, L.P.
Drives: (\ETINIUM.$Z40X)
System: \ETINIUM Operating System: J06 Tape Version: 3
```

```
Backup options: AUDITED, BLOCKSIZE 8, NO IGNORE, OPEN, PARTONLY OFF,
INDEXES IMPLICIT
*WARNING-7147* Files created and stored via OSS and SQL/MX objects
are not
supported.
*WARNING-7033* This tape can only be restored with TNS/II RESTORE
(B41, C00 or
later).
Summary Information
Files dumped = 57 Files not dumped = 0
Total bytes: 2871488
Compressed bytes: 745534
CREATED - $DATA15.SHE409T.COL222M
FILES DUPLICATED: 1
----> Two files to pick up:
----> binary file \ETINIUM.$DATA15.SHE409T.COL222P
----> text file \ETINIUM.$DATA15.SHE409T.COL222A
STOPPED: 0,190
CPU time: 0:00:00.027
1: Process terminated with warning diagnostics
Total Errors = 0 Total Warnings = 3
```

BB010 - Extraction of BackPak Catalog Record

```
$DATA15 SHE409 11> run bb010 RT3* report
BB010 - Extraction of the BackPak catalog to file VOLEXT
2020/11/17 11:50


Selection of volumes matching the label pattern: RT3*

Label : RT301 BACKUP
Max volume size: 25000 MB
Automatic mount: Y
Creation time : 2020/11/15 21:05
Last load time : 2020/11/16 19:36
Expiration date: 2020-11-17
fileId: SHE409-OBK11DEF , gen=0001, fileSeq=0001, fileSet-
t=RT301
Owner : \ETINIUM 255,50
Volume group : VG_CAT_WIN3
Store id : DS_WIN1
Store type : WINDISK
Index path : \\KRAKEN\DS_WIN1\

Label : RT302 BACKUP
Max volume size: 25000 MB
Automatic mount: Y
```

```
Creation time : 2020/11/15 21:05
Last load time : 2020/11/17 10:48
Expiration date: 2020-11-22
fileId: SHE409-OBK11DEF , gen=0002, fileSeq=0001, fileSet-
t=RT302
Owner : \ETINIUM 255,50
Volume group : VG_CAT_WIN3
Store id : DS_WIN1
Store type : WINDISK
Index path : \\KRAKEN\DS_WIN1\
```

Label : RT303 BACKUP
```
Max volume size: 25000 MB
Automatic mount: Y
Creation time : 2020/11/15 21:05
Last load time : 2020/11/17 11:31
Expiration date: 2020-11-22
fileId: SHE409-OBK11DEF , gen=0003, fileSeq=0001, fileSet-
t=RT303
Owner : \ETINIUM 255,50
Volume group : VG_CAT_WIN3
Store id : DS_WIN1
Store type : WINDISK
Index path : \\KRAKEN\DS_WIN1\
Label : RT304 BACKUP
Max volume size: 25000 MB
Automatic mount: Y
Creation time : 2020/11/15 21:05
Last load time : 2020/11/17 11:28
Expiration date: 2020-11-22
fileId: SHE409-OBK11DEF , gen=0004, fileSeq=0001, fileSet-
t=RT304
Owner : \ETINIUM 255,50
Volume group : VG_CAT_WIN3
Store id : DS_WIN1
Store type : WINDISK
Index path : \\KRAKEN\DS_WIN1\
Label : RT305 BACKUP
Max volume size: 25000 MB
Automatic mount: Y
Creation time : 2020/11/15 21:05
Last load time : 2020/11/17 10:37
Expiration date: SCRATCH
fileId: , gen=0001, fileSeq=0001, fileSet=
Owner : \ETINIUM 255,255
Volume group : VG_CAT_WIN3
Store id : DS_WIN1
```

```
        Store type : WINDISK
        Index path : K:\UNSPECIFIED_BBPATH\
        Number records read : 18
        Number records extracted : 5
```

BB044 –Series of Tape Label Reports

Sample:

```
$ETINET RTE409 11> run bb044 BPAK_REPORT y, CATALOG_REPORT y, MERGED_
REPORT y
RTE409-BB044 Series of tape labels 2020-11-18 20:58:55
Number of volumes in BackPak : 16
Number of volumes in DSM/TC of \INSIDX : 741
Number of volumes in TMF of \INSIDX : 10
BB044-1 Labels in BackPak domain RTE409
Labels Number of Label Media Catalogue
from to volumes type type type Volume Group
---- -- ------- ------- ----- ---- --------
VNCP01-VNCP08 8 BACKUP LTO3 BackPak VG_NC_SN
VWCP01-VWCP08 8 BACKUP LTO3 BackPak VG_WC_SN
*** end of report BB044-1 ***
BB044-2 Labels in catalogs seen from system \INSIDX and from domain
RTE409
Labels Number of Label Media Catalogue
from to volumes type type type pool, volcat
---- -- ------- ------- ----- ---- --------
BBA000-BBA739 740 BACKUP LTO3 DSMTC BBOXPOOL, INSIDCAT
DAVE -DAVE 1 BACKUP OPEN DSMTC DAVE, DAVETEST
INSID0-INSID9 10 TMF TMF TMF \INSIDX
*** end of report BB044-2 ***
BB044-3 Labels in BackPak domain RTE409 and in catalogs seen from
\INSIDX
Labels Number of Label BackPak TMF node, or
from to volumes type Volume group Catalog DSM/TC pool,volcat
---- -- ------- ------- -------------------- ---------------------
BBA000-BBA739 740 BACKUP (unknown in BackPak) BBOXPOOL, INSIDCAT
DAVE -DAVE 1 BACKUP (unknown in BackPak) DAVE, DAVETEST
INSID0-INSID9 10 TMF (unknown in BackPak) TMF \INSIDX
VNCP01-VNCP08 8 BACKUP VG_NC_SN (no catalogue)
VWCP01-VWCP08 8 BACKUP VG_WC_SN (no catalogue)
*** end of report BB044-3 ***
```

OBB011 – List of Volumes in Windows Files Data Stores

Sample:

```
$DATA15 SHE409 17> run obb011 RT3*
```

```
BB010 - Extraction of the BackPak catalog to file VOLEXT 2020/11/17
12:03
Selection of volumes matching the label pattern: RT3*
Number records read : 18
Number records extracted : 5
Enform^Plus - T0295H01^AAR - (18JAN12)DATE - TIME : 11/17/2020 -
12:03:08
(C)2005, 2008-2012 Hewlett-Packard Development Company, L.P.
BB011 Volumes RT3* sorted by index path 2020-11-17 12:03
Volume Label Last load last load Owner Owner DSMTC - TMF
label type date time node user status
------ ------ ---------- --------- -------- --------- -----------
Store id : DS_WIN1
Index path: K:\UNSPECIFIED_BBPATH\
RT305 BACKUP 2020/11/17 10:37:21 \ETINIUM 255,255 SCRATCH
1 volumes in path
Store id : DS_WIN1
Index path: \\KRAKEN\DS_WIN1\
RT301 BACKUP 2020/11/16 19:36:48 \ETINIUM 255,50 ASSIGNED
RT302 BACKUP 2020/11/17 10:48:27 \ETINIUM 255,50 ASSIGNED
RT303 BACKUP 2020/11/17 11:31:18 \ETINIUM 255,50 ASSIGNED
RT304 BACKUP 2020/11/17 11:28:27 \ETINIUM 255,50 ASSIGNED
4 volumes in path
5 volumes in the report
```

OBB012 - List of Virtual Volumes

Sample:

```
$DATA15 SHE409 10> run obb012 RT3*
BB010 - Extraction of the BackPak catalog to file VOLEXT 2020/11/17
14:47
Selection of volumes matching the label pattern: RT3*
Number records read : 18
Number records extracted : 5
Enform^Plus - T0295H01^AAR - (18JAN12)DATE - TIME : 11/17/2020 -
14:47:05
(C)2005, 2008-2012 Hewlett-Packard Development Company, L.P.
BB012 List of BackPak volumes RT3* 2020-11-17 14:47
Volume Label Last load last load Tapecat Tapecat VTC owner hostname
label type date time node status or Library slot
------ ------ ---------- --------- -------- ---------- --------------
Store id: DS_WIN1 Store type: WINDISK
RT301 BACKUP 2020/11/16 19:36:48 ASSIGNED OBELIX
RT302 BACKUP 2020/11/17 10:48:27 ASSIGNED OBELIX
RT303 BACKUP 2020/11/17 11:31:18 ASSIGNED OBELIX
RT304 BACKUP 2020/11/17 11:28:27 ASSIGNED OBELIX
RT305 BACKUP 2020/11/17 10:37:21 SCRATCH
```

5 volumes in the report

OBB018 - Statistics Report

Sample:

```
$DATA15 SHE409 27> obey obb018
COMMENT
*********************************************************************
COMMENT * *
COMMENT * BB018: List the BackBox activity from the statistic files *
COMMENT * *
COMMENT
*********************************************************************
LOAD /KEEP 1/ $DATA15.SHE409.BBSETUP $DATA15.SHE409.MACROS
Loaded from $DATA15.SHE409.BBSETUP:
BBSV_ADDR BBSV_PORT BBSV_TCPIP VTC_OBJECT EZX_MAXRETRY
EZX_RETRYDELAY EZX_TIMEOUT
Loaded from $DATA15.SHE409.MACROS:
BB_BPAK_PGM_VERSION BB_041_TIMEOUT
BB_041_DEVICE BB_041_LABELS
...
VIEWT TMFC2
BB054_SHUTDOWN
COMMENT
*********************************************************************
COMMENT * STEP 1: Sets the selection parameters *
COMMENT * for the two next steps, file extraction and report. *
COMMENT * *
COMMENT * By default, the last 24 hour period will be selected. *
COMMENT * *
COMMENT * Two parameters can be forced before calling BB018_DEFAULTS:
COMMENT * CUTOFF-TIME hh:mn:ss *
COMMENT * tells when the 24 hours periods end *
COMMENT * default value is the next round hour *
COMMENT * RELATIVE-START-DAY number *
COMMENT * choose the starting 24 hour period relatively to today*
COMMENT * default value is 0 (current period) *
COMMENT
*********************************************************************
CLEAR ALL
COMMENT PARAM CUTOFF-TIME 00:00:00
COMMENT PARAM RELATIVE-START-DAY -1
BB018_DEFAULTS
PARAM CUTOFF-TIME 14:00:00
PARAM RELATIVE-START-DAY 0
PARAM FROM-DATE 2020-11-16
PARAM TO-DATE 2020-11-17
```

```
ASSIGN STATS-FILE-REC, STAT2011
COMMENT
**********************************************************************
COMMENT * STEP 2: Extracts an extract file for the following step, *
COMMENT * from the statistic files matching the pattern *
COMMENT * configured in the BackPak domain configuration. *
COMMENT * Set an ASSIGN STATS-FILE-REC to the extract file. *
COMMENT * *
COMMENT * Input PARAM's: *
COMMENT * CUTOFF-TIME hh:mn:ss *
COMMENT * FROM-DATE yyyy-mm-dd *
COMMENT * TO-DATE yyyy-mm-dd *
COMMENT * *
COMMENT  *  Activity  is  selected  from  FROM- DATE  &  CUTOFF- TIME
(included)*
COMMENT * to TO-DATE & CUTOFF-TIME (excluded) *
COMMENT
**********************************************************************
BB030_EXTRACT_STATS EXTRACT_FILE STATEXT
SHE409-BB030 - Extraction of statistic files 2020-11-17 13:29
Stats file names : \ETINIUM.$DATA15.SHE409.STAT%YY%%MM%
Extract file : STATEXT
Selection from : 2020-11-16 14:00:00 to: 2020-11-17 14:00:00
Existing statistic files Records read Records extracted
----------------------- ------------ -----------------
\ETINIUM.$DATA15.SHE409.STAT2010 skipped 0
\ETINIUM.$DATA15.SHE409.STAT2011 16 10
Total records written: 10
COMMENT
**********************************************************************
COMMENT * STEP 3: Produce report *
COMMENT * from the file specified in ASSIGN STATS-FILE-REC *
COMMENT * *
COMMENT * Input PARAM's: *
COMMENT * CUTOFF-TIME hh:mn:ss *
COMMENT * FROM-DATE yyyy-mm-dd *
COMMENT * TO-DATE yyyy-mm-dd *
COMMENT * *
COMMENT  *  Activity  is  selected  from  FROM- DATE  &  CUTOFF- TIME
(included)*
COMMENT * to TO-DATE & CUTOFF-TIME (excluded) *
COMMENT
**********************************************************************
ENFORM /IN BB018 /
Enform^Plus - T0295H01^AAR - (18JAN12)DATE - TIME : 11/17/2020 -
13:29:51
(C)2005, 2008-2012 Hewlett-Packard Development Company, L.P.
SHE409 -BB018 BackBox activity by data store page 1
```

```
From: 2020-11-16 14:00:00 to: 2020-11-17 14:00:00
Data store: DS_WIN1
Start End R Volume Data size Rate Se
time time Oper. W label MB MB/s ve VTC
-------- -------- -------- - ------ ---------- ------ -- -----------
---------
Start date: 2020-11-16
14:15:25 15:50:25 LOAD W RT302 0 0.0 W ETI4KDISK
14:20:42 15:52:10 LOAD W RT303 0 0.0 W ETI4KDISK
14:42:13 16:20:23 LOAD W RT304 0 0.0 W ETI4KDISK
15:51:48 11:12:52 LOAD W RT303 0 0.0 W ETI4KDISK
16:20:01 11:14:02 LOAD W RT304 0 0.0 W ETI4KDISK
Start date: 2020-11-17
10:48:27 10:48:50 LOAD W RT302 50 4.2 I OBELIX
11:12:30 11:13:01 LOAD W RT303 50 3.6 I OBELIX
11:13:39 11:13:58 LOAD W RT304 50 4.5 I OBELIX
11:28:27 11:28:41 LOAD R RT304 4 0.0 I OBELIX
11:31:18 11:31:28 LOAD R RT303 4 4.0 I OBELIX
BackBox activity summary for DS_WIN1
10 volumes accessed
162 MB of transferred data
```

OBB019 - Statistics Report – Script Controller

Sample:

```
$DATA15 SHE409 10> obey obb019
COMMENT
********************************************************************
COMMENT * *
COMMENT * BB019: List the script controller activity *
COMMENT * from the statistic files *
COMMENT
********************************************************************
COMMENT
********************************************************************
COMMENT * STEP 1: Sets the selection parameters *
COMMENT * for the two next steps, file extraction and report. *
COMMENT * *
COMMENT * By default, the last 24 hour period will be selected. *
COMMENT * *
COMMENT * Two parameters can be forced before calling BB018_DEFAULTS:
*
COMMENT * CUTOFF-TIME hh:mn:ss *
COMMENT * tells when the 24 hours periods end *
COMMENT * default value is the next round hour *
```

```
COMMENT * RELATIVE-START-DAY number *
COMMENT * choose the starting 24 hour period relatively to today*
COMMENT * default value is 0 (current period) *
COMMENT
*******************************************************************
CLEAR ALL
COMMENT PARAM CUTOFF-TIME 00:00:00
COMMENT PARAM RELATIVE-START-DAY -1
BB018_DEFAULTS
PARAM CUTOFF-TIME 13:00:00
PARAM RELATIVE-START-DAY 0
PARAM FROM-DATE 2020-11-18
PARAM TO-DATE 2020-11-19
ASSIGN STATS-FILE-REC, STAT2011
COMMENT
*******************************************************************
COMMENT * STEP 2: Extracts an extract file for the following step, *
COMMENT * from the statistic files matching the pattern *
COMMENT * configured in the BackPak domain configuration. *
COMMENT * Set an ASSIGN STATS-FILE-REC to the extract file. *
COMMENT * *
COMMENT * Input PARAM's: *
COMMENT * CUTOFF-TIME hh:mn:ss *
COMMENT * FROM-DATE yyyy-mm-dd *
COMMENT * TO-DATE yyyy-mm-dd *
COMMENT * *
COMMENT  *  Activity  is  selected  from  FROM- DATE  &  CUTOFF- TIME
(included)*
COMMENT * to TO-DATE & CUTOFF-TIME (excluded) *
COMMENT
*******************************************************************
BB030_EXTRACT_STATS EXTRACT_FILE STATEXT
SHE409-BB030 - Extraction of statistic files 2020-11-19 12:35
Stats file names : \ETINIUM.$DATA15.SHE409.STAT%YY%%MM%
Extract file : STATEXT
Selection from : 2020-11-18 13:00:00 to: 2020-11-19 13:00:00
Existing statistic files Records read Records extracted
----------------------- ------------ -----------------
\ETINIUM.$DATA15.SHE409.STAT2010 skipped 0
\ETINIUM.$DATA15.SHE409.STAT2011 30 10
Total records written: 10
COMMENT
*******************************************************************
COMMENT * STEP 3: Produce report *
COMMENT * from the file specified in ASSIGN STATS-FILE-REC *
COMMENT * *
COMMENT * Input PARAM's: *
COMMENT * CUTOFF-TIME hh:mn:ss *
```

```
COMMENT * FROM-DATE yyyy-mm-dd *
COMMENT * TO-DATE yyyy-mm-dd *
COMMENT * *
COMMENT  *  Activity  is  selected  from  FROM- DATE  &  CUTOFF- TIME
(included)*
COMMENT * to TO-DATE & CUTOFF-TIME (excluded) *
COMMENT
********************************************************************
ENFORM /IN BB019 /
Enform^Plus - T0295H01^AAR - (18JAN12)DATE - TIME : 11/19/2020 -
12:35:09
(C)2005, 2008-2012 Hewlett-Packard Development Company, L.P.
SHE409 -BB019 Scripts submitted by Script controllers page 1
From: 2020-11-18 13:00:00 to: 2020-11-19 13:00:00
Start Start End Data size Rate Se
VTC date time time Oper. MB MB/s ve
-------------------- ---------- -------- -------- -------- ----------
- ------ --
OBELIX 2020-11-19 12:37:01 12:37:03 SYNC-BAT 101 50.5 I
OBELIX 12:37:46 12:37:48 SYNC-BAT 101 50.5 I
OBELIX 12:38:17 12:38:19 SYNC-BAT 101 50.5 I
*** BB019 end of report
```

OBB021 – Emulation Statistics Report

Sample:

```
$DATA15 SHE409 35> OBEY obb021
COMMENT
********************************************************************
COMMENT * *
COMMENT * BB021: List tape emulation activity from statistic files *
COMMENT * *
COMMENT
********************************************************************
LOAD /KEEP 1/ $DATA15.SHE409.BBSETUP $DATA15.SHE409.MACROS
Loaded from $DATA15.SHE409.BBSETUP:
BBSV_ADDR BBSV_PORT BBSV_TCPIP VTC_OBJECT EZX_MAXRETRY
EZX_RETRYDELAY EZX_TIMEOUT
Loaded from $DATA15.SHE409.MACROS:
BB_BPAK_PGM_VERSION BB_041_TIMEOUT
BB_041_DEVICE BB_041_LABELS
...
VIEWT TMFC2
BB054_SHUTDOWN
COMMENT
********************************************************************
COMMENT * STEP 1: Sets the selection parameters *
```

```
COMMENT * for the two next steps, file extraction and report. *
COMMENT * *
COMMENT * By default, the last 24 hour period will be selected. *
COMMENT * *
COMMENT * Two parameters can be forced before calling BB018_DEFAULTS:
*
COMMENT * CUTOFF-TIME hh:mn:ss *
COMMENT * tells when the 24 hours periods end *
COMMENT * default value is the next round hour *
COMMENT * RELATIVE-START-DAY number *
COMMENT * choose the starting 24 hour period relatively to today*
COMMENT * default value is 0 (current period) *
COMMENT
*****************************************************************
CLEAR ALL
COMMENT PARAM CUTOFF-TIME 00:00:00
COMMENT PARAM RELATIVE-START-DAY -1
BB018_DEFAULTS
PARAM CUTOFF-TIME 14:00:00
PARAM RELATIVE-START-DAY 0
PARAM FROM-DATE 2020-11-16
PARAM TO-DATE 2020-11-17
ASSIGN STATS-FILE-REC, STAT2011
COMMENT
*****************************************************************
COMMENT * STEP 2: Extracts an extract file for the following step, *
COMMENT * from the statistic files matching the pattern *
COMMENT * configured in the BackPak domain configuration. *
COMMENT * Set an ASSIGN STATS-FILE-REC to the extract file. *
COMMENT * *
COMMENT * Input PARAM's: *
COMMENT * CUTOFF-TIME hh:mn:ss *
COMMENT * FROM-DATE yyyy-mm-dd *
COMMENT * TO-DATE yyyy-mm-dd *
COMMENT * *
COMMENT  *  Activity  is  selected  from  FROM- DATE  &  CUTOFF- TIME
(included)*
COMMENT * to TO-DATE & CUTOFF-TIME (excluded) *
COMMENT
*****************************************************************
BB030_EXTRACT_STATS EXTRACT_FILE STATEXT
SHE409-BB030 - Extraction of statistic files 2020-11-17 13:40
Stats file names : \ETINIUM.$DATA15.SHE409.STAT%YY%%MM%
Extract file : STATEXT
Selection from : 2020-11-16 14:00:00 to: 2020-11-17 14:00:00
Existing statistic files Records read Records extracted
----------------------- ------------ ------------------
\ETINIUM.$DATA15.SHE409.STAT2010 skipped 0
```

```
\ETINIUM.$DATA15.SHE409.STAT2011 16 10
Total records written: 10
COMMENT
*********************************************************************
COMMENT * STEP 3: Produce report *
COMMENT * from the file specified in ASSIGN STATS-FILE-REC *
COMMENT * *
COMMENT * Input PARAM's: *
COMMENT * CUTOFF-TIME hh:mn:ss *
COMMENT * FROM-DATE yyyy-mm-dd *
COMMENT * TO-DATE yyyy-mm-dd *
COMMENT * *
COMMENT  *  Activity  is  selected  from  FROM- DATE  &  CUTOFF- TIME
(included)*
COMMENT * to TO-DATE & CUTOFF-TIME (excluded) *
COMMENT
*********************************************************************
ENFORM /IN BB021 /
Enform^Plus - T0295H01^AAR - (18JAN12)DATE - TIME : 11/17/2020 -
13:40:28
(C)2005, 2008-2012 Hewlett-Packard Development Company, L.P.
SHE409 -BB021 BackBox emulation activity by data store page 1
From: 2020-11-16 14:00:00 to: 2020-11-17 14:00:00
Data store: DS_WIN1
Start End R Volume Data size Rate Compr En- Se
time time W label MB MB/s ratio cryp ve VTC
-------- -------- - ------ ---------- ------ ------ ---- -- ---------
Start date: 2020-11-16
14:15:25 15:50:25 W RT302 0 0.0 W ETI4KDISK
14:20:42 15:52:10 W RT303 0 0.0 W ETI4KDISK
14:42:13 16:20:23 W RT304 0 0.0 W ETI4KDISK
15:51:48 11:12:52 W RT303 0 0.0 W ETI4KDISK
16:20:01 11:14:02 W RT304 0 0.0 W ETI4KDISK
Start date: 2020-11-17
10:48:27 10:48:50 W RT302 50 4.2 I OBELIX
11:12:30 11:13:01 W RT303 50 3.6 I OBELIX
11:13:39 11:13:58 W RT304 50 4.5 I OBELIX
11:28:27 11:28:41 R RT304 4 0.0 I OBELIX
11:31:18 11:31:28 R RT303 4 4.0 I OBELIX
Virtual tape emulation summary for DS_WIN1
10 volumes loaded
162 MB of transferred data
```

OBB038 – List of Encrypted Volumes

Content of OBB038:

```
$DATA15 QCE409 22> run obb038 *
```

```
BB010 - Extraction of the BackPak catalog to file VOLEXT 2020/11/24
17:31
Selection of volumes matching the label pattern: *
Number records read : 24
Number records extracted : 24
Enform^Plus - T0295H01^ABE - (31JUL18)DATE - TIME : 11/24/2020 -
17:31:15
(C) Copyright 2005-2018 Hewlett-Packard Development Company L.P.
BB038 Encrypted volumes with label matching * 2020-11-24 17:31
Last DSMTC
Volume write or TMF
label date status Encryption key ID
------ ---------- -------- ------------------------------------------
Key manager id : KMVLE
Client type : 5-VLE INTEROPERABILITY
VEWC06 2020/11/23 ASSIGNED NDDC616B3VEWC06DB02B604C6140008_BBBBBBBB_
2011231719
VEWC07 2020/11/24 ASSIGNED NA9038157VEWC07DB02B60BAB710008_BBBBBBBB_
2011241724
VEWC08 2020/11/23 ASSIGNED N9FA3A5E5VEWC08DB02B60DCC550008_BBBBBBBB_
2011231720
VEWC09 2020/11/24 ASSIGNED N534B7400VEWC09DB02BC58ACB90008_BBBBBBBB_
2011241725
VEWC10 2020/11/23 ASSIGNED N85D27352VEWC10DB02BC5E96E40008_BBBBBBBB_
2011231721
VEWC12 2020/11/23 ASSIGNED NF5781C88VEWC12DB02BC61F9120008_BBBBBBBB_
2011231722
VKMN02 2020/11/23 NC4D7D5F8VKMN02DAFC192C31830008_BBBBBBBB_2011231709
VKMN03 2020/11/23 N4C83FDFAVKMN03DAFC192C31C00008_BBBBBBBB_2011231714
VKMN04 2020/11/24 NF27B17AEVKMN04DAFC192CA0040008_BBBBBBBB_2011241432
VKMN05 2020/11/24 N720280FDVKMN05DAFC192D11DC0008_BBBBBBBB_2011241433
VKMN07 2020/11/24 N86CB4F85VKMN07DB16D7F99D520008_BBBBBBBB_2011241721
VKMN08 2020/11/24 N2AEFBF41VKMN08DB16D7FA56E70008_BBBBBBBB_2011241724
VWCE01 2020/11/20 ASSIGNED N81597B53VWCE01DACA284390C50008_BBBBBBBB_
2011202153
VWCE02 2020/11/23 ASSIGNED N4ED6E0CCVWCE02DACA284DD61C0008_BBBBBBBB_
2011231712
VWCE03 2020/11/24 ASSIGNED N1BC83C38VWCE03DACA284FEC800008_BBBBBBBB_
2011241430
VWCE04 2020/11/24 ASSIGNED NB2496751VWCE04DACA28518BC00008_BBBBBBBB_
2011241431
VWCE05 2020/11/24 ASSIGNED NE17C2622VWCE05DACA285337EA0008_BBBBBBBB_
2011241721
17 printed volumes for Key manager KMVLE
End of report BB038
```

OBB039 – List of Virtualizations / Materializations

Sample:

```
2020-11-23 15:45:09 \ETINIUM.$X4N7 ETINET.100.100 5110 SHE409-KRAKEN-
I5110
Starting  MATERIALIZE  session  on  tape  device  PHYDEVICE  Event
time:2020-11-23
15:48:27
2020-11-23 15:45:41 \ETINIUM.$X4N7 ETINET.100.100 5050 SHE409-KRAKEN-
I5050
Materializing virtual volume VMVW01 started successfully Event
time:2020-11-23 15:48:59
2020-11-23 15:45:46 \ETINIUM.$X4N7 ETINET.100.100 5046 SHE409-KRAKEN-
I5046
Materializing  virtual  volume  VMVW01  ended  successfully  Event
time:2020-11-23
15:49:04
2020-11-23 15:46:08 \ETINIUM.$X4N7 ETINET.100.100 5111 SHE409-KRAKEN-
I5111
Ending MATERIALIZE session on tape device PHYDEVICE Event time:2020-
11-23
15:49:26
--------------------------------------------------------------------
2020-11-23 15:58:00 \ETINIUM.$X4N7 ETINET.100.100 5108 SHE409-KRAKEN-
I5108
Starting VIRTUALIZE session on tape device PHYDEVICE Event time:2020-
11-23
16:01:18
2020-11-23 16:00:40 \ETINIUM.$X4N7 ETINET.100.100 5051 SHE409-KRAKEN-
I5051
Virtualizing physical volume VMVW01 started successfully Event
time:2020-11-23 16:03:58
2020-11-23 16:00:53 \ETINIUM.$X4N7 ETINET.100.100 5053 SHE409-KRAKEN-
I5053
Virtualizing  physical  volume  VMVW01  ended  successfully  Event
time:2020-11-23
16:04:11
```

BB030_EXTRACT_STATS Usage

Sample:

```
$DATA15 SHE409 40> run BB030
SHE409- BB030  -  Extraction  of  statistic files  2020-11-17
13:48
Stats file names : \ETINIUM.$DATA15.SHE409.STAT%YY%%MM%
Extract file : SEXTRACT
Selection from : 2020-11-16 14:00:00 to: 2020-11-17 14:00:00
```

```
     Existing statistic files Records read Records extracted
     ---------------------- ------------ ------------------
     \ETINIUM.$DATA15.SHE409.STAT2010 skipped 0
     \ETINIUM.$DATA15.SHE409.STAT2011 16 10
     Total records written: 10
```

OBB055 – Low Level Tape to Tape Copy

Sample:

```
$DATA15 SHE409 34> o obb055
COMMENT ************************************************************
COMMENT Virtualize / materialize volumes
COMMENT using the low-level tape copy program BB055
COMMENT ************************************************************
CLEAR ALL
RESET DEFINE *
DELETE DEFINE =BACKPAK_BBSETUP
ADD DEFINE =BACKPAK_BBSETUP, CLASS MAP, FILE BBSETUP
DELETE DEFINE =TCPIP^PROCESS^NAME
ADD DEFINE =TCPIP^PROCESS^NAME, CLASS MAP, FILE $ZTC0
PARAM BB055TRIGGER OPERATORLOAD
PARAM GROUPID VG_CAT_WIN1
comment PARAM searchnode \remote-node
comment PARAM VOLUMELIST vollist
PARAM INDEVICE $NUM201
PARAM OUTDEVICE $OBEL01
comment PARAM IDLEWAIT 15
comment PARAM TIMEOUT 60
comment PARAM MAXNOWAIT 5
RUN BB055 /NAME/
SHE409-BB055 virtualization is starting 2020-11-23 12:14:25
PARAM BB055TRIGGER OPERATORLOAD
PARAM INDEVICE $NUM201
PARAM OUTDEVICE $OBEL01
PARAM GROUPID VG_CAT_WIN1
PARAM IDLEWAIT 15 minutes
PARAM TIMEOUT 600 seconds
PARAM MAXNOWAIT 5
SHE409- I3486 NSK  tape  virtualization  ready  to  copy  volumes  from
$NUM201 to
$OBEL01. Volume group is VG_CAT_WIN1.
SHE409-I3484 NSK tape virtualization waiting 15 minutes for an input
tape to
be loaded on drive $NUM201.
SHE409- I3485 NSK  tape  virtualization:  input  volume  VWCP01  (labels
BACKUP) is
```

```
loaded. (SHE409-OBK11RT, GEN=1)
Warning 3162 loading VWCP01 - W3162 Domain license will expire on
2020-12-16. I3
023 VWCP01 loaded on $OBEL01.
Waiting 600 seconds for $OBEL01 be loaded ...
Waiting 600 seconds for $NUM201 be un-loaded ...
SHE409-I3487 NSK tape virtualization of volume VWCP01 (labels BACKUP)
successfull. 50 MB data and 12 file-marks copied
SHE409-I3484 NSK tape virtualization waiting 15 minutes for an input
tape to
be loaded on drive $NUM201.
SHE409-I3489 NSK tape virtualization is idle. Stops after waiting 15
minutes
for a tape be loaded on drive $NUM201.
SHE409-I3495 NSK tape virtualization ends. 1 volumes successfully
copied for
50 MB. 0 volumes skipped
SHE409-BB055 virtualization ending 2020-11-23 12:30:49
```

OEMS2 - EMS Messages Display

Sample:

```
$DATA15 SHE409 14> run oems2
20- 11- 17  22:01:23  \ETINIUM.$Z6R9  *ETINET.100.100  003162
SHE409-W3162
Domain license will expire on 2020-12-16.
20- 11- 17  22:05:46  \ETINIUM.$ZSVR  TANDEM.TAPE.H01  000600
$ZSVR: 5133
MOUNT RTAN02 WITH RING
20- 11- 17  22:05:51  \ETINIUM.$ZSVR  TANDEM.TAPE.H01  000648
$ZSVR: MOUNT
OF RTAN02 ACCEPTED
20- 11- 17  22:05:51  \ETINIUM.$ZSVR  TANDEM.TAPE.H01  000638
$ZSVR: STATUS
1504 - RTAN02 TAPE OPENED ON $OBEL01
20- 11- 17  22:05:51  \ETINIUM.$ZSVR  TANDEM.TAPE.H01  000699
$ZSVR: STATUS
1516 - RTAN02 TAPE ON DRIVE 20-11-17 22:07:3
20- 11- 17  22:07:48  \ETINIUM.$ZSVR  TANDEM.TAPE.H01  000659
$ZSVR: STATUS
1512 - RTAN02 TAPE DISMOUNTED FROM DRIVE
$OBEL01
```

OEMS - EMS Message Extraction

Sample:

```
DATA15 SHE409 55> fup copy oems

fup purge emsout
fup /in EMSFUPIN /
emsdist     /name     /     type     printing,     filter
$DATA15.SHE409.EMSFILT2, &
collector $0 textout EMSOUT, &
time 30 Sep 2020 08:00, &
stop 30 Sep 2020 09:50
```

TAPEWR - Performance Test

Sample:

```
$DATA15 SHE409 18> clear all
$DATA15 SHE409 19> delete define =TAPE01
$DATA15 SHE409 20> RESET DEFINE *
$DATA15 SHE409 21> ADD DEFINE =TAPE01, CLASS TAPE, FILEID
testfile, VOLUME RTAN0
2, LABELS ANSI, RETENTION 1
$DATA15 SHE409 22> RUN TAPEWR =TAPE01 56000 500 100 200
TAPEWR
--------
PARAM's in use...
UNLOAD : ON
maxNoWait : 5
BUFFERMODE : ON
BACKBOXVOL : ON
Volume label : RTAN02
Volume group : VG_WIN1
Command line parameters ....
File size to write: 500 MB
Number of Blocks : 9,362
Length of Blocks : 56,000
Varout, minReclen : 100,
maxReclen : 200
Start time : Tue Nov 17 22:05:51 2020
End time : Tue Nov 17 22:07:46 2020
Elapsed time 00: :01.055
Rate : 4.348 MB/sec
```

TAPERD - Performance Test

Sample:

```
$DATA15 SHE409 24> ADD DEFINE =TAPE03, CLASS TAPE, FILEID
testfile, VOLUME RTAN02,LABELS ANSI, USE IN, BLOCKLEN 56000
```

```
$DATA15 SHE409 25> RUN TAPERD =TAPE03 56000
TAPERD
----------
[ NOT VERIFYING DATA ]
Start time Tue Nov 17 22:15:37 2020
End time Tue Nov 17 22:15:45 2020
read blocks = 9362
read records= 0
Total exfer = 499.000 MBytes
Elapsed time 00: :00.008
Rate : 62.375 MB/sec
```

Trace Macros

Sample Report:

```
$DATA15 SHE409 12> LOAD BBSETUP MACROS
Loaded from $DATA15.SHE409.BBSETUP:
BBSV_ADDR BBSV_PORT BBSV_TCPIP VTC_OBJECT EZX_MAXRETRY
EZX_RETRYDELAY EZX_TIMEOUT
Loaded from $DATA15.SHE409.MACROS:
BB_BPAK_PGM_VERSION BB_041_TIMEOUT
BB_041_DEVICE BB_041_LABELS
...
VIEWT TMFC2
BB054_SHUTDOWN
$DATA15 SHE409 13> V SHE409T
$DATA15 SHE409T 14> listt *
TRCZ3H3  18:02:03.6  UpdatePermissions  I3477  Domain  configuration
\ETINIUM.$DATA1
TRCZ3H8 18:02:09.1 GetVolumeList 18 volume(s) listed
TRCZ3H8 18:02:09.3 GetVolumeList 18 volume(s) listed
TRCZ3H8  18:02:09.9 CreateVolume W3162 Domain license will expire on
2020-12-16.
TRCZ3H8 18:03:45.6 GetVolumeList 23 volume(s) listed
TRCZ3JF 18:03:48.8 GetVolumeList 23 volume(s) listed
TRCZ452 18:45:40.2 (unknown)
TRCZ6R8  22:01:19.6  GetVolumeList  E3375  Domain  configuration  has
changed. Confi
TRCZ6R9  22:01:23.3 GetConfig  W3162  Domain  license  will  expire  on
2020-12-16.
TRCZ6TA 22:05:46.5 Load W3162 Domain license will expire on 2020-12-
16. I3023 R
TRCZ6VS 22:07:48.8 EndVolumeOperation RTAN02
9 files browsed, 11 transactions listed.
VIEWT TRCZ3H3
```

Operations samples

OBB017

Sample Report:
```
$DATA15 RUE409 5> o obb017
COMMENT
************************************************************************
COMMENT * BackBox data store cleanup *
COMMENT * *
COMMENT * 1- BB017_FREE_EXPIRED in all data stores, free storage
allocated *
COMMENT * to volumes expired in DSMTC and TMF catalogs *
COMMENT * *
COMMENT * 2- BB023_DEL_BACKEDUP in "Windows files" data stores,
delete backed*
cOMMENT * up files according to the volume group config*
COMMENT * *
COMMENT * 3- BB022_CHECK_SPACE in "Windows files" data stores, *
COMMENT * check the available disk space *
COMMENT *
COMMENT * PARAM BB017IGNORECHECKHDR1 1 (TO BYPASS hdr1 check on NSK)
COMMENT * DEFAULT 0
COMMENT
************************************************************************
LOAD /KEEP 1/ $DATA15.RUE409.BBSETUP $DATA15.RUE409.MACROS
Loaded from $DATA15.RUE409.BBSETUP:
BBSV_ADDR BBSV_PORT BBSV_TCPIP VTC_OBJECT EZX_MAXRETRY
EZX_RETRYDELAY EZX_TIMEOUT
Loaded from $DATA15.RUE409.MACROS:
BB_BPAK_PGM_VERSION BB_041_TIMEOUT
BB_041_DEVICE BB_041_LABELS
...
VIEWT TMFC2
BB054_SHUTDOWN
PARAM BB017IGNORECHECKHDR1 0
BB017_FREE_EXPIRED OUT $S.#BBOX.BB017
W3173 BackBox storage space purge of expired tape volumes. 76 volumes
in catalog
, 2 volumes purged.
BB023_DEL_BACKEDUP STOREID ALL, OUT $S.#BBOX.BB023
<StoreId>ALL</StoreId>
<StoreIdAlias>0</StoreIdAlias>
I3224 BB023: 0 backed up Windows files have been deleted. Deleted
size: 0 bytes
.
```

```
BB022_CHECK_SPACE OUT $S.#BBOX.BB022
I3225 Normal job end.
```

BB017_FREE_EXPIRED

```
RUE409-BB017 Free BackBox expired storage 2020-11-26 16:37
Processing scope : NEW SCRATCH volumes
Minimum size of volumes to purge: 0 KB
Timeout per Delete script run : 5 minutes
List of expired tape volumes that have been freed up:
Label Type Last load Freed up storage Volume group
----- ---- ---------- ---------------- ------------
NCBP02 BACKUP 2020-11-23 BACKUP_NC_F
W3165 Automatic unload of volume NCBP02. Volume was loaded since
2020-1
1-23 19:48:18 on \ETINIUM.$NUM201 that is now free
VWCP03 BACKUP 2020-11-23 0 MB VG_WC_PR
VWCP06 BACKUP 2020-11-23 50 MB VG_WC_PR
76 Volumes in BackBox catalog
39 Volumes not in integrated catalogues such as DSM/TC
37 Volumes in integrated catalogues such as DSM/TC
9 Scratch
26 Assigned
0 Released
2 Other/unknown status
50 MB purged
W3173 BackBox storage space purge of expired tape volumes. 76 volumes
in catalo
RUE409-BB017 for BackBox ends at 2020-11-26 16:37
```

BB023_DEL_BACKEDUP

Sample Report:

```
RUE409-BB023 Delete backed up Windows files 2020-11-26 16:37:28
Execution window from: to: , max duration:
Store id to clean up: ALL
Processing will be interrupted on: No interruption
Grand total
0 volumes for which Windows files have been deleted
0 Windows files deleted
0 MB deleted
RUE409-BB023 ends at 2020-11-26 16:37
```

BB022_CHECK_SPACE

Sample report:

```
RUE409-BB022-A Check disk space in Data stores 2020-11-26 16:37:30
Data store Location Space used (MB) Free space (MB
---------- -------- --------------- --------------
DATASTORE_RUE48
=== Storage pool ===
P: in NUMEROBIS 4,816 110,42
=== Copy pool ===
\\TOUTATIS\DS_TOUTATIS 32,321 5,356,49
Total Storage pool only 4,816 110,42
DATASTORE_WIN
\\NUMEROBIS\DATASTORE_WINSCIP 0 110,42
Total data store 0 110,42
DS_PR
\\NUMEROBIS\DS_PR 558 110,42
Total data store 558 110,42
RUE409-BB022-B  Volume  groups  per  BackBox  data  store  2020-11-26
16:37:34
Data store : DATASTORE_RUE48 (Type WINDISK)
Volume Nbr of Uncompressed Compr. Nbr of SCRATCH Potential size of
group volumes data size(MB) ratio SCRATCH ratio SCRATCH vols (MB)
------ ------- ------------ ----- ------- ----- ----------------
BACKUP_CAT_SALONE_F
2 49 1.00 1 50% 24,966
BACKUP_CPSYNC_NC_F
13 33,788 1.00 n/a n/a n/a
BACKUP_C_F
6 1,493 1.00 1 16% 24,966
BACKUP_NC_F
14 1,875 1.00 n/a n/a n/a
BACKUP_NOCAT_SALONE_F
2 49 1.00 n/a n/a n/a
BRCOM_F
8 2,991 1.00 1 12% 24,971
TMF_F
10 47 1.00 0 0% 0
TMF_SMALL_F
3 140 1.00 0 0% 0
Data store : DATASTORE_WIN (Type WINDISK)
Volume Nbr of Uncompressed Compr. Nbr of SCRATCH Potential size of
group volumes data size(MB) ratio SCRATCH ratio SCRATCH vols (MB)
------ ------- ------------ ----- ------- ----- ----------------
WIN_NC_F
2 124 1.00 n/a n/a n/a
Data store : DS_PR (Type WINDISK)
Volume Nbr of Uncompressed Compr. Nbr of SCRATCH Potential size of
group volumes data size(MB) ratio SCRATCH ratio SCRATCH vols (MB)
------ ------- ------------ ----- ------- ----- ----------------
VG_NC_PR
```

```
8 456 1.00 n/a n/a n/a
VG_WC_PR
8 102 1.00 6 75% 149,795
RUE409-BB022 ends at 2020-11-26 16:37
```

BB004_PASSWORD_UPDATE

Sample report:

```
$DATA15 SHE409 61> o obb004
COMMENT
*************************************************************************
COMMENT * BackBox data store PW update *
COMMENT * *
COMMENT * BB004_DATASTORE_UPDATEPW *
COMMENT * *
COMMENT * PARAM DATASTORE-NAME DataStoreName
COMMENT * PARAM UPDATING-PASSWORD Password
COMMENT *
COMMENT
*************************************************************************

CLEAR ALL

LOAD /KEEP 1/ $DATA15.SHE409.BBSETUP $DATA15.SHE409.MACROS
Loaded from $DATA15.SHE409.BBSETUP:
BBSV_ADDR BBSV_PORT BBSV_TCPIP VTC_OBJECT EZX_MAXRETRY
EZX_RETRYDELAY EZX_TIMEOUT
Loaded from $DATA15.SHE409.MACROS:
BB_BPAK_PGM_VERSION BB_041_TIMEOUT
...
VIEWT TMFC2
BB054_SHUTDOWN
comment replace the WinStore name & the account PW to update
comment in the folloowing PARAMs
PARAM DATASTORE-NAME DS_WIN1
PARAM UPDATING-PASSWORD NewPassword
BB004_DATASTORE_UPDATEPW
=============================================
SHE409-BB004 DataStore DS_WIN1 processing PW encryption & updating
config 202
0-11-18 16:23
SHE409-BB004 DataStore DS_WIN1, password updated 2020-11-18 16:23
I3225 Normal job end.
```

BB004_DATASTORE_VALIDATE_ACC

This macro is used to validate the password that protects the datastore access path.

Sample report:

```
$DATA15 SHE409 67> o obb004b
COMMENT
*********************************************************************
COMMENT * BackBox validate data store account *
COMMENT * *
COMMENT * BB004_DATASTORE_VALIDATE_ACC *
COMMENT * *
COMMENT * PARAM DATASTORE-NAME DataStoreName
COMMENT *
COMMENT
*********************************************************************
CLEAR ALL
LOAD /KEEP 1/ $DATA15.SHE409.BBSETUP $DATA15.SHE409.MACROS
Load ...
PARAM DATASTORE-NAME DS_WIN1
BB004_DATASTORE_VALIDATE_ACC
SHE409- W3077  The  disk  pool  is  missing  in  the  configuration  of
DataStore
DS_QSCOPY.
SHE409- W3077  The  disk  pool  is  missing  in  the  configuration  of
DataStore
DS_QSCOPYPATH.
============== DataStore Account Validation =========================
SHE409-BB004 DataStore DS_WIN1 processing PW Validation 2021-01-12
16:24
====================================================================
E3017 No route defined to DataStore DS_WIN1.
=============DataStore Account Validation End ===================
I0000 process terminates
```

APPENDIX B – EXTERNAL TAPE DEVICE INSTALLATION

⚠️	This section does NOT apply to the Virtualized BackBox.

For materialization and virtualization, physical tape devices must be installed in a VTC and configured in Windows as regular tape devices.
For virtualization, direct connection can be established between a BackBox VTC and an HPE VTS.
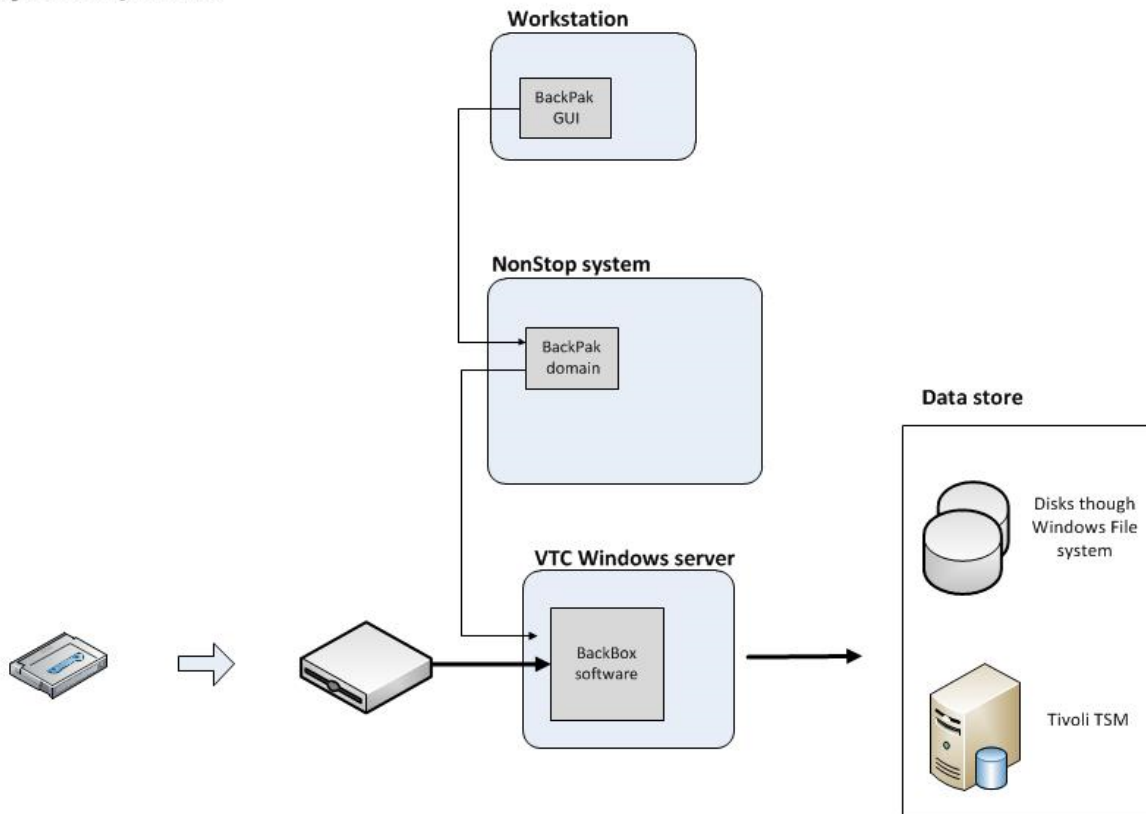See below how to install the external tapes. Once installed, they are configured and operated the same way in the UI.

⚠️	If a restore script is configured, it is assumed that the files will be backed up again by the enterprise backup software when the files are discovered in the new disk location. The Back-Box does not submit the backup script after a **Move from Spare**. If the Data Store is configured for backups through the script, the user has to manually initiate the backup of the moved file.

In a multi VTCs installation, it is possible to dedicate a VTC to the materialization and virtualization, running no tape emulation for NonStop.

## Physical Tape Device Attachment

Workstation

BackPak
GUI

NonStop system

BackPak
domain

VTC Windows server

BackBox
software

Data store

Disks though
Windows File
system

Tivoli TSM

The tape drive must be physically connected to the VTC and the appropriate Windows tape driver must be installed. If there is no Windows driver for the tape drive, the VTC is able to access the legacy drives in raw mode.

Auto-loaders are supported.

Attachment to Another Virtual Tape System
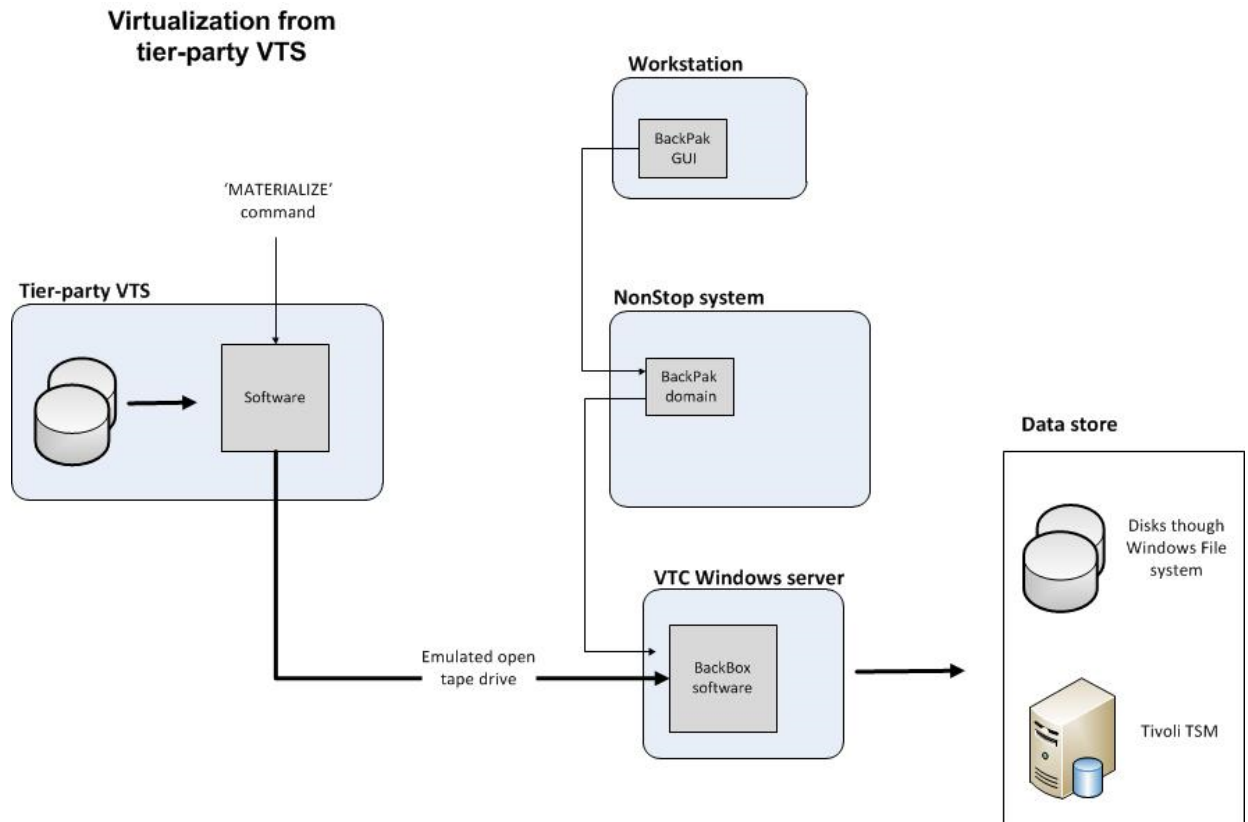
Images of virtual tape volumes can be exchanged directly with a third party Virtual tape unit. The transfer is possible only from the third party to the BackBox system, i.e. for virtualizations. Like the BackBox, other Virtual tape systems are able to materialize/virtualize. In addition, the BackBox VTC is able to provide to the other system a device that appears as a physical tape drive. This link allows a third party virtual tape unit to export its media to be virtualized on the VTC.

To install:

- In the VTC, one FC port is dedicated to the Unix or Windows emulation and one or several tape drives must be configured on this port.
- A cable connects the VTC (target-mode tape controller) to the third party virtual tape unit (host tape controller).
- The tape devices are configured in the third party OS.

VTC Configuration

⚠️ | NonStop devices attached to the VTC should be stopped before the service is restarted.

Update Fiber Ports Configuration

On the VTC Server, start the VTC Management Console and expand the FC category node. Navigate up to the Fiber Port that will be used to connect to the external VTS.

Change the Port type to EXTERN. 8 Devices will automatically be defined.
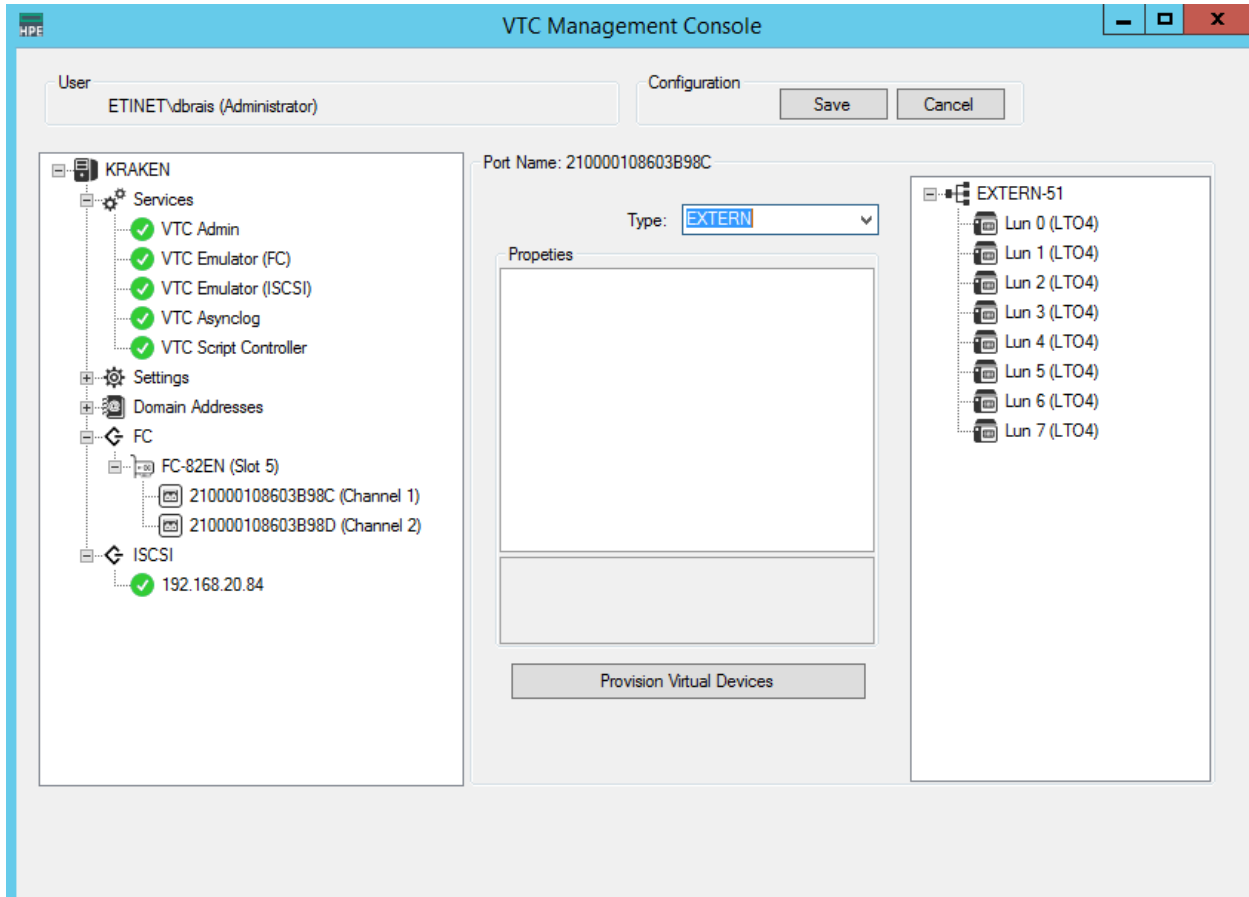
Device emulation can be changed by right-clicking on a specific LUN device or globally by right-clicking on the EXTERN root port. The Emulation type selection box can then be used.
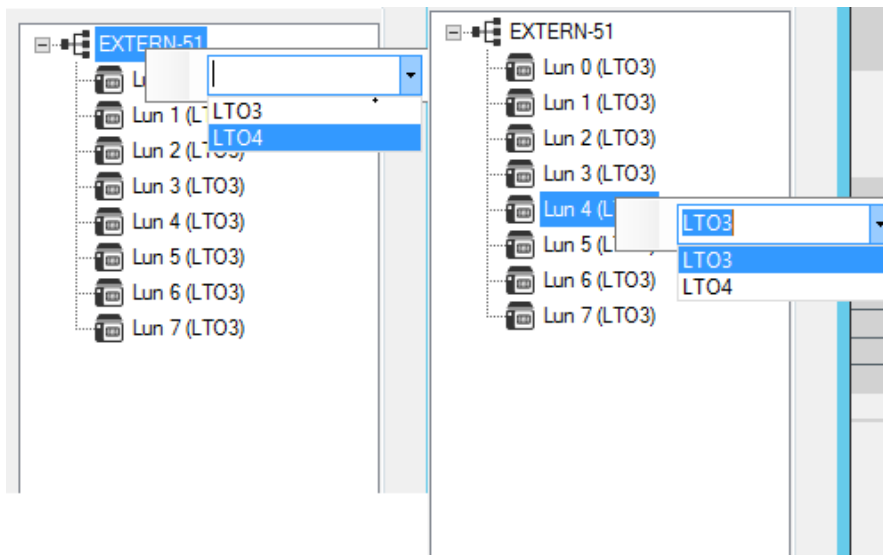
If more or less LUN are needed, use the Provision Virtual Devices dialog box and check or uncheck the LUN number to add or remove from the list. The LUN 0 must always be defined. There are actually no properties that can be set using the EXTERN port type.

When finished, click on the **Save** button and restart the **Services**.

Configuration in the BackPak Domain

For both physical devices and devices emulated by the VTC for another Virtual Tape System, two items must be configured in the Domain configuration through the BackPak UI:

- In VT Controller Advanced Properties, the physical/external tape device(s) must be detected by the VTC and be given a name, i.e. an Alias.
- In Data Store, the VTC that has attached physical/external tape devices, must be a route of the Data Store where virtual volumes will be read or written.

Storage Access in the VTC

The VTC server needs to be prepared to access the Data Store. For example, the IBM Spectrum Protect™ (TSM) API software might have to be installed or the access to remote disk share must be verified.
The access to WINDISK Data Stores can be tested in the BackPak UI on the Storage Admin page, by selecting the VTC with attached external tape as a route to the Data Store.

APPENDIX C – MIGRATION TO BACKBOX

This appendix presents general guidelines for migrating legacy tape storage to BackBox with a focus on the tape media, their content, and their cataloging:

On each site, the migration period requires detailed planning for data in storage, tape catalogs in the NonStop systems and tape drive operations.

NonStop Tape Catalogs

For tape catalogs on NonStop, the BackBox migration functionality is the same for all three catalog types BackBox can access: DSM/TC, TMF and QTOS.

The migration functions (Virtualize Volume, Import from Tape Catalog and the Volume group auto-import feature) work the same way for these three catalog types.

Media Type

BackBox provides emulation for the following media types: CART3480, LTO2 (to mount on LTO3 drives), LTO3, and LTO4, providing a native media type support to all NonStop systems from G06.xx to J06.xx.

If the BackBox media is virtual, the media type is not related to the volume format (except LTO4 which has to be accessed with HPE VLE Encryption) and is not assigned to each volume individually. However, the media type registered in the catalogs DSM/TC and CA must match the emulation type of the tape drive for $ZSVR read/write of a loaded media.

BackBox can manage different media types and device types in a single system and single VTC. It selects the tape drive appropriate to the media type configured in the Volume Group.

During a migration, it might happen that:

- The legacy system uses a media type that is not supported by BackBox (for example, DLTIII).
- An S-Series system that supports CART3480 is replaced by a Blade that does not support CART3480.

In these two cases, the media type of the volume cataloged in DSM/TC or CA must be modified when the volume is moved to the new environment. This change of media type is automatically done by BackPak, in DSM/TC only (not in CA), as part of the three migration functions (**Virtualization**, **Import from Tape Catalog** and the Volume group **auto-import** feature).

This change is reported in EMS by the message #3427: `Media type of volume %s changed from %s to %s in %s %s, to match the configuration of the Volume group %s.`

Short Term Expiration

Short term expiration usually reduces the migration work load. A large part of tape volumes is often written for a short term retention of either 7 or 30 days. It is much more economical to wait for the volumes with short time legacy to expire than to configure them with long time retention settings.

New Tape Labels

Creating BackBox volumes with new labels involves:

- Modifying the backup OBEY files. For DSM/TC, the POOL of the TAPECATALOG define must be modified. (The restore jobs are not affected).
- Running BACKCOPY to move the non-expired data to the BackBox system. The data will be re-cataloged while being copied.

Re-using old tape labels involves:

- Controlling the two storage systems.

	New Tape Labels	Re-use Old Tape Labels
Backup OBEY files	Must be updated (for DSM/TC change the POOL in TAPECATALOG defines) when new tape label is created	No change required
Restore OBEY files	No change required	No change required
Copy of non-expired data to BackBox storage	BACKCOPY Backups and backup content are cataloged twice until the original backup is deleted. Heavy data flow on the NonStop	BackBox virtualization No change in catalogues. Data is moved directly between the storage systems.
Automatic load in the legacy system	Can be kept running for the restores.	Must be stopped. Mount requests to be executed manually in the legacy system.

Available Functionality to Migrate Volumes to BackBox

Migration of ASSIGNED Volumes

The data of these volumes must be converted to the BackBox format to be restored through BackBox. To migrate the tape content:

- Duplicate the content by a NonStop utility to different tape labels in BackBox. Use BACKCOPY for backups, FUP for ANSI tapes.
- Use OBB055 to do a low level cloning with no re-cataloging.

The legacy tape system provides and reads the source tapes as BackBox has written the target tapes. Multi-volume backups might be re-organized in fewer and more BackBox tape volumes, depending on the capacity and compression configured in BackBox.

The new volumes in BackBox must be cataloged again in DSM/TC. For a backup with the CATALOGFILES option, this might considerably increase the size of the DSM/TC database until the old backup is un-cataloged in DSM/TC.

- Virtualize the media to BackBox volumes with the same set of tape labels.

Multi-volume backups are reproduced to the exact same set of tape labels.

This operation is transparent to any tape catalog and what was cataloged is still registered for the same tape labels.

BackBox will register the tape volume in its catalog when the tape data is actually written in the BackBox storage.

Migration of SCRATCH Volumes

SCRATCH Volumes can be migrated only when the same tape labels are to be re-used in BackBox, so that the migration is transparent to existing tape catalogs and to NonStop OBEY files.

Specific functionality allows moving SCRATCH Volumes under the control of BackBox without converting expired data. In the Volume tab, the page Import from Tape Catalog allows to select volumes that are SCRATCH and also populate the BackPak's own catalog. The imported volumes are ready for new backups. As the migration may last several months, some volumes may expire earlier, and they should be ready for reuse before they are virtualized. Auto-import will pick up these specific volumes.

This feature is enabled when the BackBox Volume Group is configured for IN-PROGRESS migration.

When $ZSVR issues a mount request for a SCRATCH volume, BackPak tries to process it even if the volume is unknown in BackPak.

If the requested volume belongs to one of the tape catalogs associated with BackPak Volume Groups configured for "Migration to BackBox" IN-PROGRESS:

- The volume will be automatically registered in BackPak.
- The volume will be loaded for backup and stored as a BackBox virtual media.

Concurrent Operation of Legacy System and BackBox

Two scenarios of concurrent operations are supported; the choice of scenario is configured in the Volume Groups, through the Migration to BackBox parameter.

Migration Feature	Migration None	Migration In Progress	Migration Being Prepared
Auto-import SCRATCH Volumes	No	Yes	No
Automatic load	Yes	Yes	No. Does not prevent a manual load.
Automatic update of the tape DSM/TC TAPEVOLUME entry to match the media type emulated by BackBox	Yes	Yes	No

When there is a migration, the *Migration to BackBox* is usually set to **In Progress**:

1. Switch to using BackBox for all new backups.
2. Assigned volumes data is acquired by BackBox.

During the migration, BackBox executes new backups and restores from recent backups written by Back-Box. For restoring from volumes not yet migrated, the legacy system must still be able to load volumes.

> ⚠️ If a new series of tape labels were created for the BackBox, the data migration is made by BACKCOPY on different labels.

Each backup is cataloged twice in DSM/TC. The possible load automation in the legacy system can be kept running and there would be no likelihood for potential confusion.

> ⚠️ If the same set of volume labels must be re-used by the BackBox system, the data migration is made by BackBox virtualization that does not involve the NonStop tape system.

Each backup is kept cataloged once in DSM/TC. The legacy system must not automatically load volumes that could also be automatically loaded by BackBox.

3. Remove the legacy tape system.

When Migration to BackBox is set to *Being prepared*, the legacy system is still used in the same manner for all NonStop tape applications:

1. Start-up: Nothing changed for backup and restore. Still operated by the legacy system.
2. Data of assigned volumes is acquired by BackBox virtualization.

Each backup is kept cataloged once in DSM/TC. Because of the *Being prepared* status, BackBox will not modify the media type and will not automatically load the volume if $ZSVR issues a mount request.

3. Switch to BackBox for backup and restore, and removal of the legacy tape.

Sample Plan for Migration with Re-Using Existing Cataloged Labels

This can be applied to DSM/TC, TMF and QTOS, with these following special notes for TMF:

⚠️	Re-using existing labels is not possible when TMF has a single pool of virtual volumes. Round-robin should be enabled to help visually distinguish in which tape system the volumes were written (TMFCOM ALTER CATALOG, ROUNDROBIN ON).

Initial Status

The BackPak configuration is assumed to be completed.
The VTCs, the Data store, and the Volume group paired to the DSM/TC, QTOS or TMF catalog are configured.
Be sure the Volume Group is set for **Auto-import**, such as the volumes that expired during the migration period and requested for a new backup would automatically be registered in BackPak and processed by BackPak.
A VTC is equipped with physical tape drives or direct connection to third party VTS to allow virtualization and the cloning of legacy media to BackBox virtual volumes.
In this example, it is assumed that the legacy tape media is physical media, the VTC is equipped with an auto-loader and the tape catalog is set to TMF type.

Step-1: Switch Write Operation to BackBox

- Prevent any new mount requests for backups (TMFCOM ALTER AUDITTRAIL ..., AUDITDUMP OFF).

- Make sure that the legacy tape system will not mount any tape.

- Register in the BackPak domain all volumes that are currently SCRATCH.

  On the BackPak UI > **Volume** > **Import from Tape Catalog**, select the Volume group and ask for registering only SCRATCH Volumes.

- Allow new mount requests for backups (TMFCOM ALTER AUDITTRAIL ..., AUDITDUMP ON).

- Be sure the EMS Extractor is running for the BackPak domain.

  Step-2: Migrate the Non-Expired Tape Volumes.

- Load a set of legacy tapes in the auto-loader.

- Submit the virtualization of the media loaded.

On the BackPak UI >**Volume** > **Virtualize** > enable **Searching in DSM/TC, TMF and QTOS catalogs** > select the VTC that has the auto-loader > select **All tape drives** > select the NonStop node where the catalog is located.

- The Virtualization task reports the processing of each volume in EMS.

- The Virtualization status can be requested from the Virtualize page.

In Step 2, a legacy volume might expire. If a new backup request is issued, BackBox should automatically register it and load it. This special case is reported by the EMS message #3445:

```
Automatically importing the SCRATCH volume %s requested by a backup
and found in the NonStop catalog %s, (volume group: %s).
```

Step-3: Stop Using the Legacy Tape System

- Register the latest legacy volumes that have expired in the BackPak domain.

On BackPak UI > **Volume** > choose **Import from Tape Catalog** > select the Volume group and ask for registering only SCRATCH Volumes

- Verify all the legacy volumes are now in the BackBox system.

Volume summary page can be compared to the number reported by DSM/TC: MEDIACOM INFO TAPEVOLUME *, POOL xyz

- Update the BackPak configuration to disable the Auto-import in all Volume groups.

APPENDIX D - SHARED FILES PERMISSIONS

To set the permissions go to **Server Manager** > **File and Storage Services** > **Shares** and select the store you want to change the permissions for.
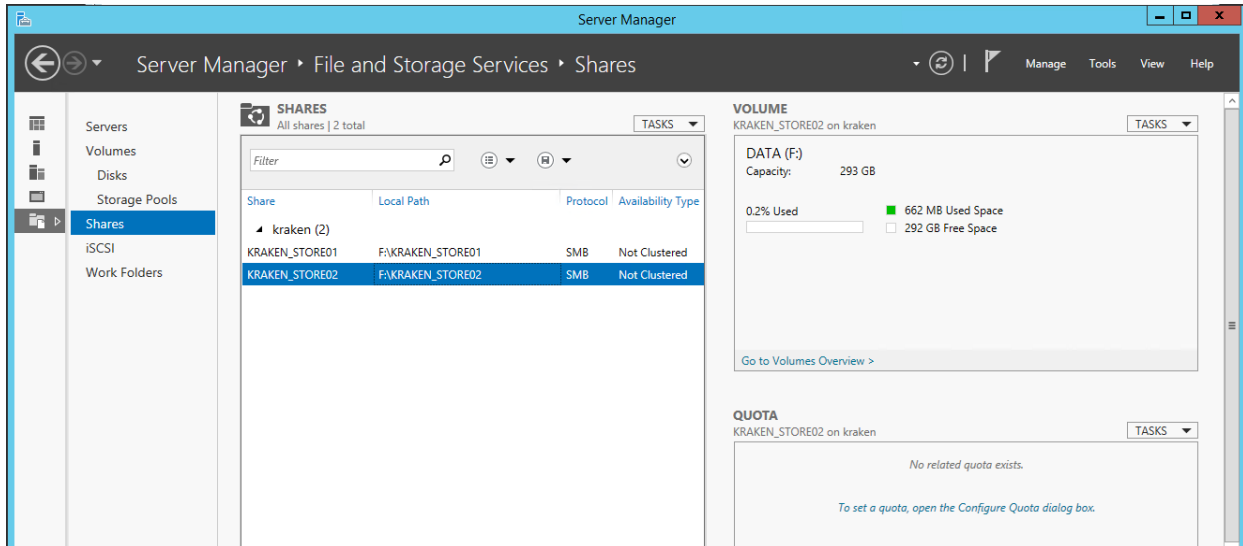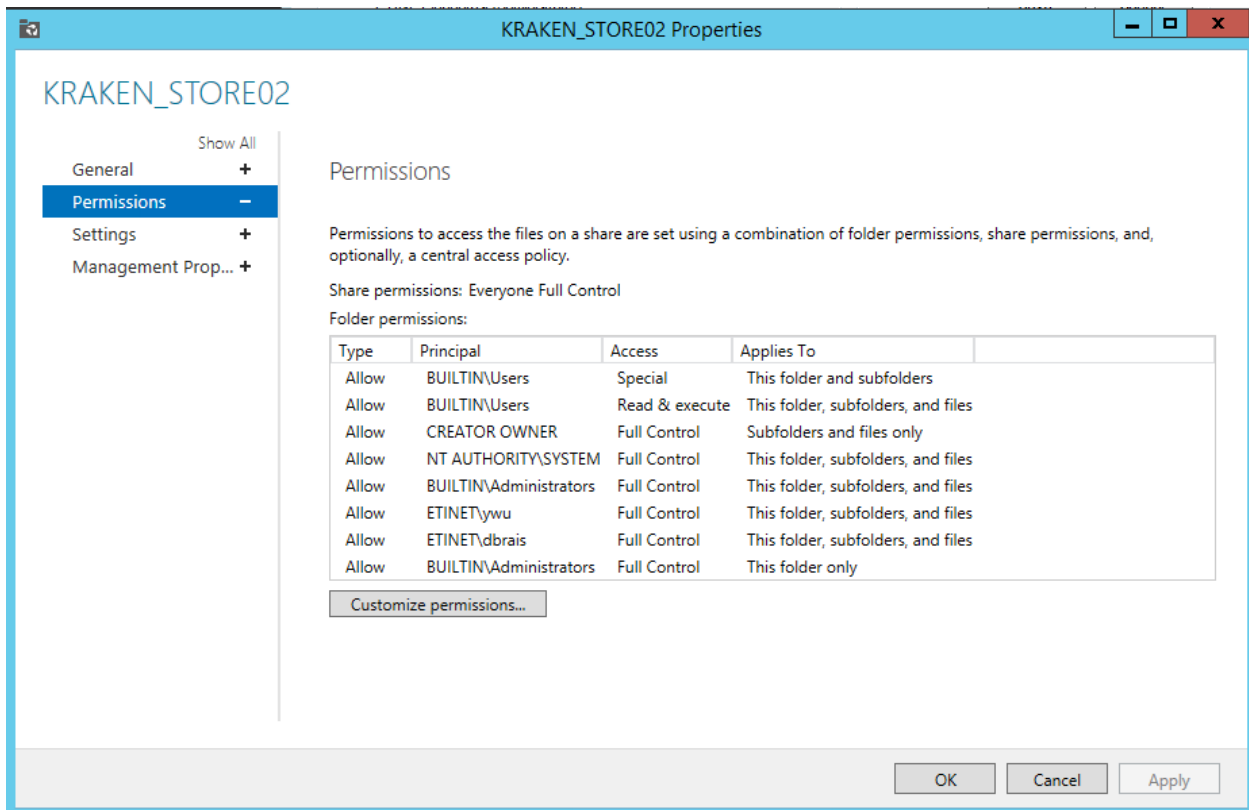

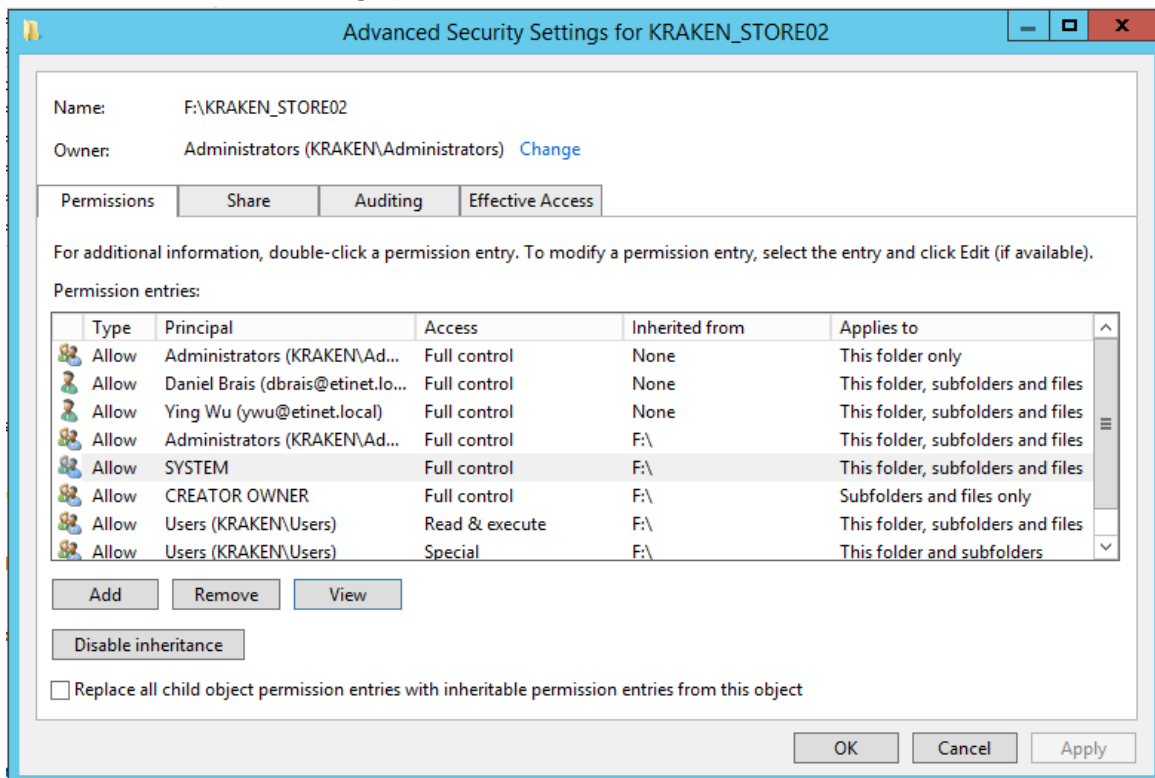Right-click on the selected store and **Properties**.

If the specified location does not exist and you want to create it, go to **TASKS** tab and select **New Share**. Follow the wizard's steps to create a new share.
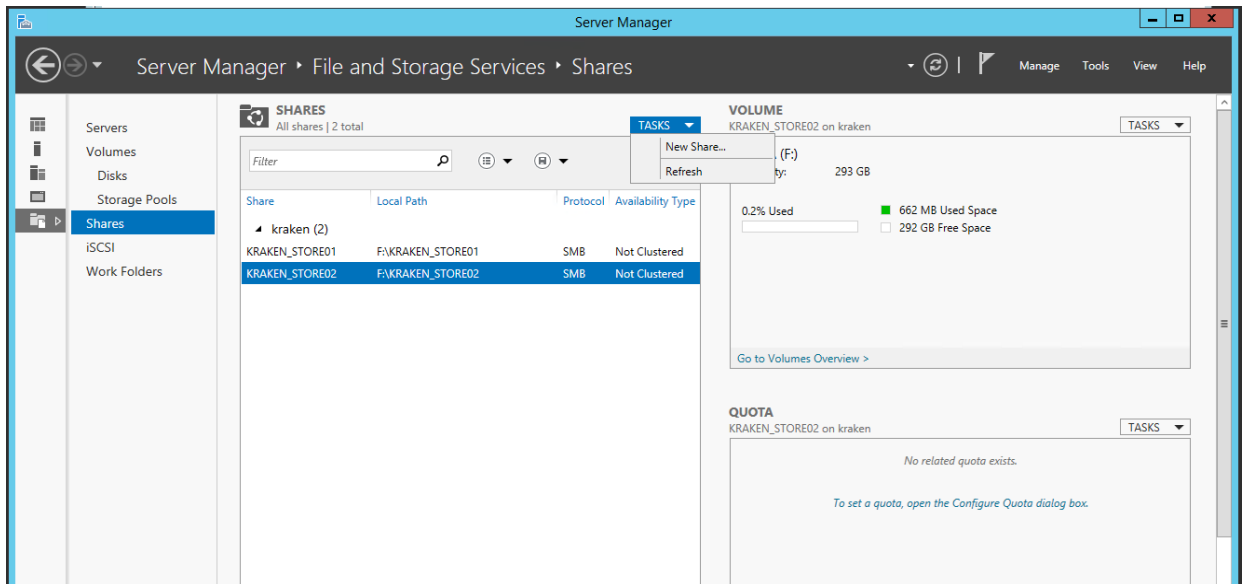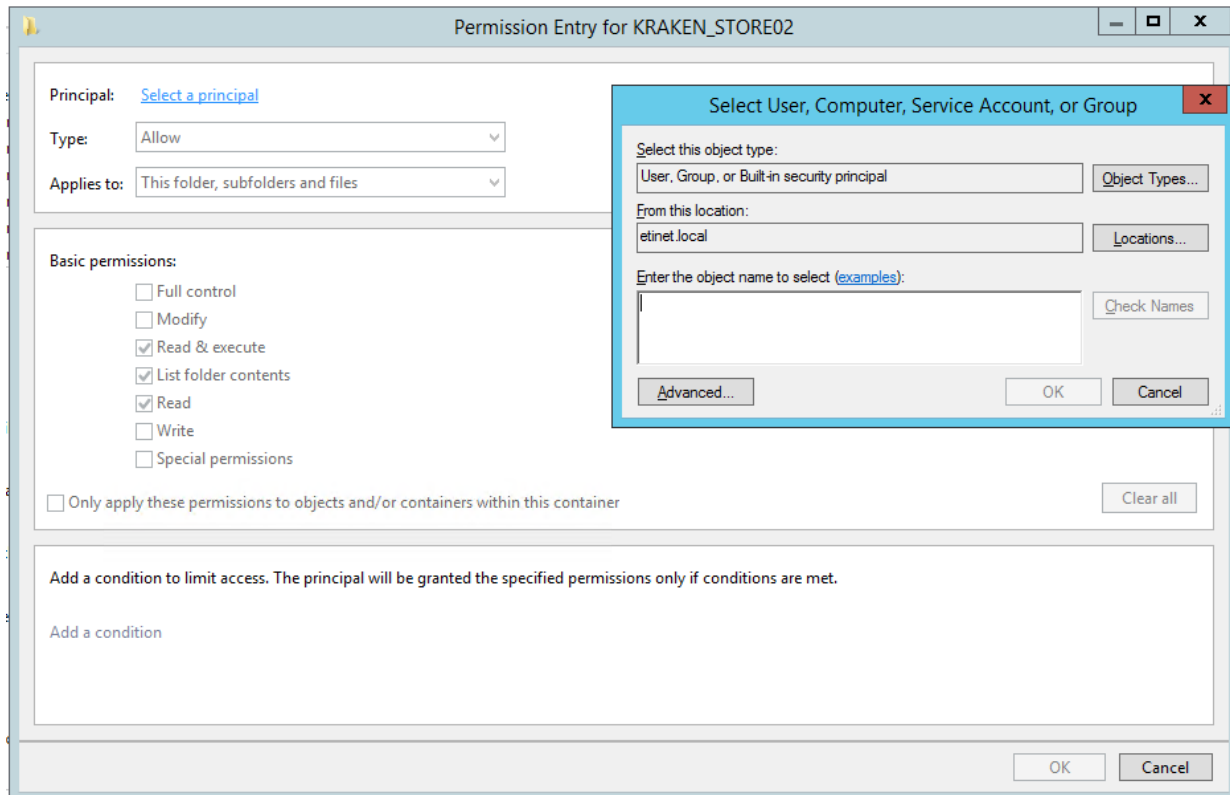

Select the user you want to change the permissions for.

To create a new user and assign permissions for this user click **Add** button.

In the pop-up window, **Select a principal** user to configure.

Once the user is found, all the permission fields become active and the permission leveles can be con-figured for this user. When done with the configuration, click **OK** and then **Apply**.

APPENDIX E – ISCSI CONFIGURATION (ON THE NONSTOP)

To enable the iSCSI option directly on the NonStop you need to add a network (climconfig) interface that would allow to configure iSCSI connection.

Set up the interface on the eth2 connection; specify the ip address, netmask and gateway.

To add the network interface use the commands below:

```
climcmd sclim000 climconfig interface –add eth2
```

```
climcmd sclim001 climconfig interface –add eth2
```

```
climcmd sclim000 climconfig ip –add eth2 –ipaddress 192.168.20.251 –netmask 255.255.255.0
```

```
climcmd sclim001 climconfig ip –add eth2 –ipaddress 192.168.20.252 –netmask 255.255.255.0
```

```
CLIMCMD sclim000 climconfig route –add eth2 –default –gateway 192.168.20.5
```

```
CLIMCMD sclim001 climconfig route –add eth2 –default –gateway 192.168.20.5
```

APPENDIX F – PROCEDURE FOR FILES/FOLDERS OWNERSHIP RECOVERY

When users join the QoreStor server (Embedded in the VTC) into a Windows Domain through VTC Management Console, the machine SID (Security Identifier in Windows environment) of the QoreStor server could be changed and all SIDs of local accounts in the QoreStor server could also be changed along with the SIDs.

In such a case, all virtual volumes owned by these accounts and generated before joining into the Windows Domain cannot be reused after joining the Windows domain.
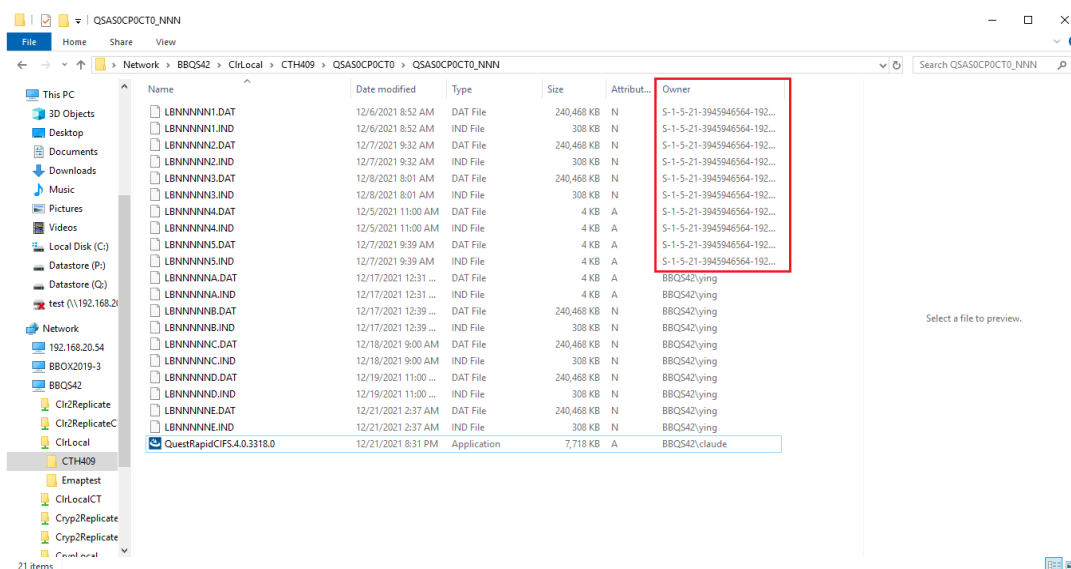
In order to avoid being locked out of the accounts, users need to log into VTC server with Domain Administration accounts (accounts in Domain Admin group).

Once logged into the domain with Administration account, users can change the ownership of the files and folders into valid accounts.

After joining a Windows domain, the SID of the local "administrator" account on the embedded QoreStor server loses the administrative privileges.

To gain access to the inaccessible folders and files, follow the procedure:

1. Log into VTC with Domain Administrative Account.
2. Start **Computer Management** console.
3. Connect this console to QoreStor server.
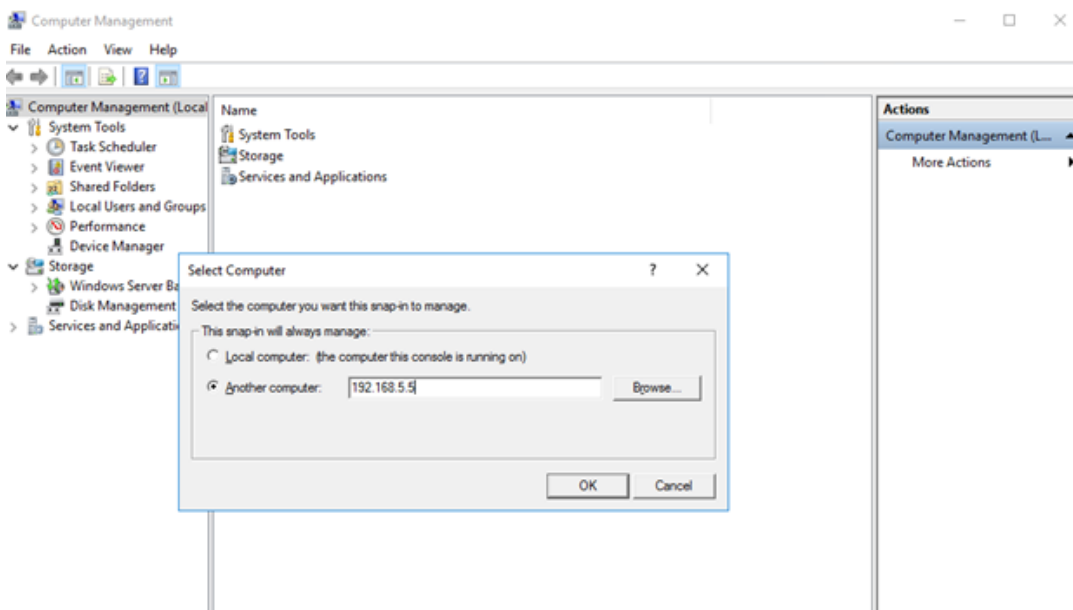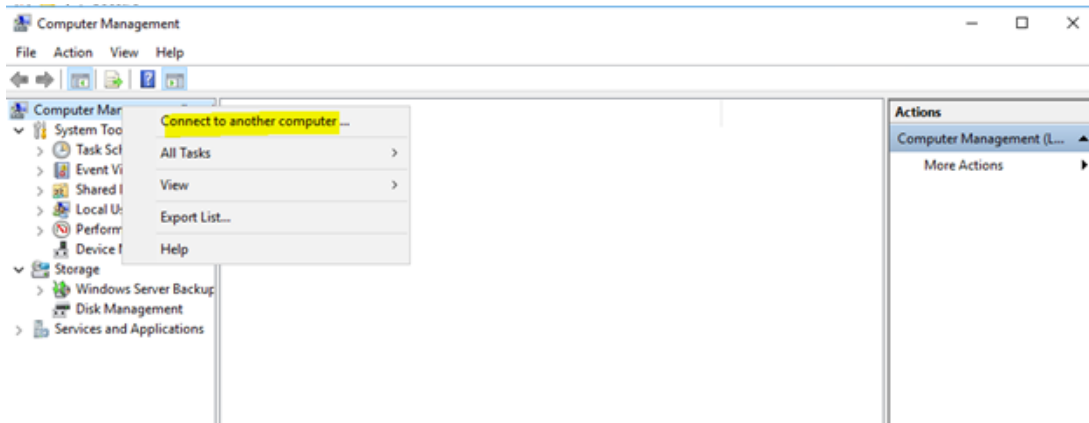
4. Add the "administrator" account of the QoreStor server in "Administrators" group, if it is not there.

⚠	In case the procedure fails and the ownership cannot be recovered, contact ETI-NET support team.

APPENDIX G - REMOVING NONSTOP NODES

Use this procedure to decommission NonStop systems and to remove existing configuration along with any relevant data from BackBox VTC.

To remove existing NonStop nodes:

1. Log in to the BackBox UI for the NonStop node to be deleted.

2. **Volume** > **Volume List** to display the volumes. Check **All**, then select **Delete Checked Volume(s)**.

3. Go to **Configuration** > **Volume Group**, switch to edit mode and then delete any listed Volume Groups.

4. Go to **Configuration** > **Data Store**, switch to edit mode and then delete any listed Data Stores.

5. Go to **Configuration** > **VT Controller**, switch to edit mode and then delete the listed VT Controller.

6. Once the data has been deleted, go to **Configuration** > **NSK Nodes**, switch to edit mode and then click on the **Delete** button to delete the respective NSK node.

7. Log in to the VTC MC Console.

8. Expand the domain address node and right-click on the domain name to be deleted.

9. Delete the domain name.