BackBox© E5.00 User Guide

Abstract

This User Guide document is for BackBox© E5.00

Published: March 2025

Legal Notice

Confidential computer software. Valid license from ETI-NET Inc. required for possession, use or copying.

The information contained herein is subject to change without notice. The only warranties for ETI-NET- products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. ETI-NET shall not be liable for technical or editorial errors or omissions contained herein.

BackBox is registered trademark of ETI-NET Inc.

StoreOnce is a registered trademark of Hewlett Packard Development, L.P.

Microsoft, Windows, and Windows NT are U.S. registered trademarks of Microsoft Corporation. Tivoli

Storage Manager (TSM) is a registered trademark of IBM Corporation.

QTOS is a registered trademark of Quality Software Associates Inc.

All other brand or product names, trademarks or registered trademarks are acknowledged as the property of their respective owners.

This document, as well as the software described in it, is furnished under a License Agreement or Non- Dis-closure Agreement. The software may be used or copied only in accordance with the terms of said Agreement. Use of this manual constitutes acceptance of the terms of the Agreement. No part of this manual may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, and translation to another programming language, for any purpose without the written permission of ETI-NET Inc.

Copyright © 2013, 2025 ETI-NET Inc. All rights reserved.

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.

This present manual is dedicated to the BackBox E5.00 distributed by ETI-NET. For additional information refer to BackBox end user documentation:

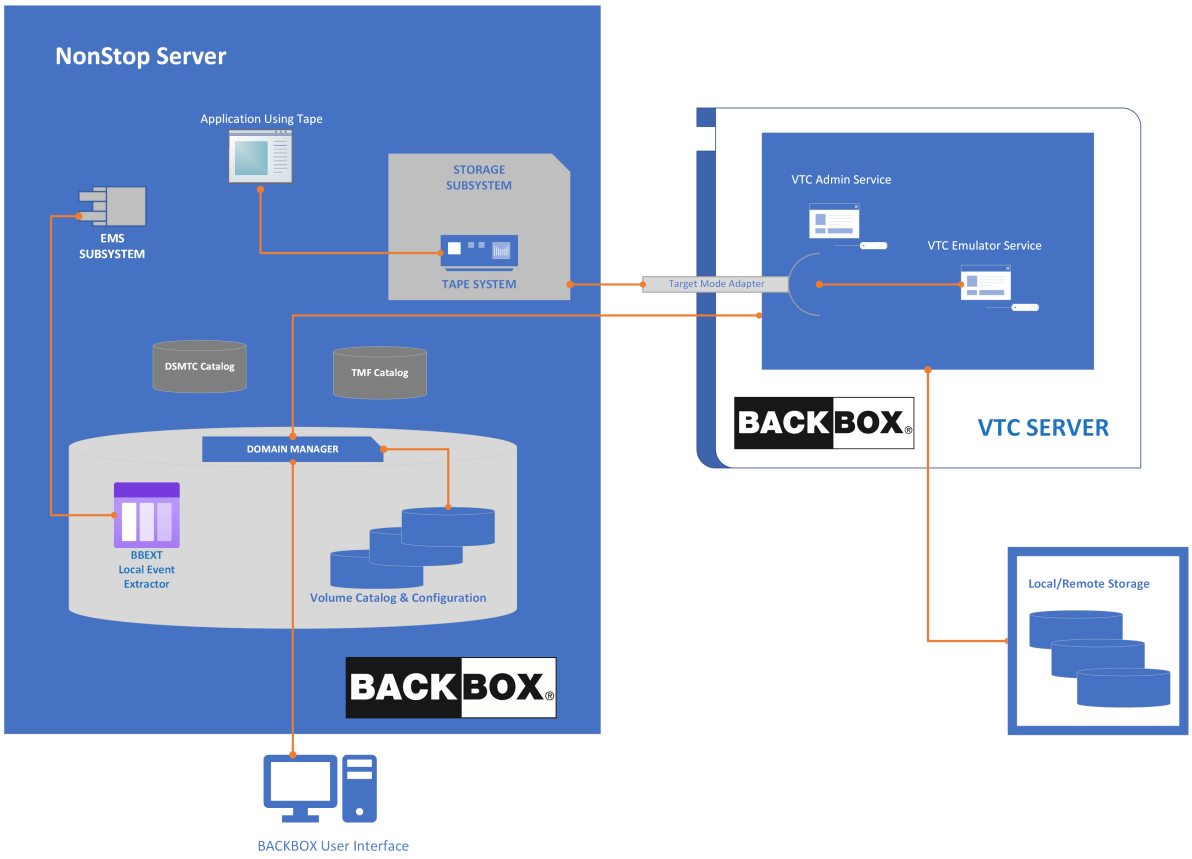
- BackBox Release Notes - Listing the new features, improvements, resolved defects and security fixes
- BackBox User Manual- Configuring and operating BackBox subsystems.
- BackBox Messages Manual and Troubleshooting - List of EMS error messages generated by the BackBox products.
- BackBox Catalog Sync Option - describing a D/R plan by replicating the DSM/TC and BackBox tape catalogs.
- BackBox Virtual BackBox Installation - preparing the virtual Windows server(s) who will act as a Virtual Tape Controller for BackBox iSCSI environment. The virtual BackBox will only work with a virtual NonStop system.
- QoreStor Upgrade Procedure for BackBox - updating QoreStor for BackBox to the latest QoreStor version.

PRODUCT DESCRIPTION

ETI-NET BackBox is a virtual tape solution to connect the NonStop Guardian tape subsystem to external storage facilities.
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 deduplication 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
- BackBox User Interface Client
- Domain Manager
- Event Extractor

A graphical user interface (UI) of BackBox runs on the operator workstation.
The Domain Manager, Event Extractor and User Interface are BackBox components.

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 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.

BACKBOX USER INTERFACE CLIENT

The BackBox graphical user interface is a web-based client application that runs on the operator 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 BackBox 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 BackBox 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 BackBox 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

VTC Required Hardware

Data Rate	Celerity FC HBA Type	NonStop Connectivity Type
8Gbits	FC-8, FC-16, FC-32	G9 Storage CLIM with optional 8 Gbps HBA
16Gbits	FC-16, FC-32	G10 Storage CLIM with FC-16
32Gbits	FC-32	G11 Storage CLIM with FC-32

Contact your ETI-NET representative for detailed server specifications.

VTC Required Software

Windows Server	Release Version
Standard	2022, 2019 or 2016

ETI-NET 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 for vNonStop or G10 Storage CLIM

Software Requirements

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

Expand connectivity between all NSK nodes of the BackBox domain.

The Expand security must allow the Domain Manager to start Guardian utilities on the peripheral nodes. For BackBox 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 NonStop Access Authorizations.

Additional Software

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

⚠	Partial integration is provided for QTOS.

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

OPERATOR WORKSTATION

Hardware Requirements	Software Requirements	Tape Encryption Key Manager
Microsoft Windows x64 computer system with TCP/IP connection to the NonStop system.	Windows 10 Windows 11 Windows 2019 Windows 2022	HP Enterprise Security Key Manager (ESKM)
TCP/IP connection for remote VTC server(s).	Microsoft .NET Framework 4.6.2	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
HPE StoreOnce	4.3.9-2426.20 or earlier
DELL Data Domain + BoostFS	DDOS 7.10.1.15-1078832 CLIENT 7.10.1.10-1058783
Cohesity Data Cloud	6.8.1u5 or later (6.x series) 7.1.1 or later (7.x series)

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 (BackBox catalog and DSM/TC catalog) to a secondary site (see BackBox 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 BackBox 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 autoscratch 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, LTO7 and LTO8 can be used on CLIM base NonStop host supporting LTO6, LTO7 and LTO8 tape drives. These tape drive emulations 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 QoreStor 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 decide whether compression is beneficial 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 deduplication appliance (such as Data Domain), BackBox VTC compression should be disabled. Failure to do so results in poor deduplication ratio.

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.

Encryption by the Storage Subsystem

Encryption provided by the storage or operating system itself is not described in thismanual.
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.

TAPE ENCRYPTION OPTION

This Tape Encryption Option section documents the tape encryption provided by the BackBox software running on VTC servers.
The information provided in this section is useful during the configuration and operation of the tape encryption.
Tape volumes can be encrypted by the BackBox VTC software or by the storage subsystem where the media is written by BackBox.
This section considers only the encryption provided by the BackBox VTC software.
Refer to BackBox Messages Manual and Troubleshootingfor additional information and support.

SUPPORTED OPERATIONAL ENVIRONMENTS

BackBox encryption is available for Windows File System Data Stores and for all NonStop systems supported by BackBox: H06.xx, J06.xx, and L06.xx.
The data is encrypted using IEEE 1619.1 (tape) industry standard algorithms before being sent to the Data Store.
The encryption algorithm uses a 256-bit encryption key stored on an external Key Management Server.
Encryption by BackBox software can be used with anEnterprise 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 in an ESKM the same encryption keys as would a CLIM implementing VLE.

⚠	For storage subsystems that implement data deduplication, such as StoreOnce, BackBox, data encryption avoids the deduplication.

Encryption or compression prevents deduplication algorithms from matching re-occurring data “chunks” which makes deduplication ineffective. For these subsystems, BackBox encryption should be performed only for a subset of the most sensitive volumes in distinct Volume Groups. Otherwise, all volumes should be encrypted by the storage subsystems themselves.

⚠	For QoreStor data stores, Key Manager encryption is not supported.

BACKBOX VTC ENCRYPTION

The BackBox VTC tape emulation performs block level encryption. Block level encryption permits compression of each clear block of data before encrypting it. This improves the utilization of the storage while keeping the data-at-rest secure.
The BackBox tape emulation implements IEEE P1619.1 standard for tape-based encryption using the Advanced Encryption Standard algorithm and the Galois Counter Mode (known as AES-GCM) algorithm.
The AES Encryption algorithm uses a secret key. This key is suitable for block-mode encryption and it has an optional length of 164, 192, and 256 bits. BackBox tape emulation encryption implementation uses a 256-bit key.
The GCM provides an authentication algorithm that allows computing 16 bytes MAC for each tape block encrypted. This algorithm ensures strong authentication and block integrity.
The BackBox tape emulation software encryption can take advantage of the Intel processor AES-NI instruction set (if available) to accelerate execution of the AES algorithm and to reduce the CPU load when encrypting/decrypting data.

KEY MANAGER SERVER

As mentioned above, BackBox tape emulation encryption implementation uses a 256-bit key to encrypt or decrypt data. The key must be secured in a Key Manager server and must be available for the lifetime of the data stored in the virtual media.
The privacy of the data depends on the security of the key. The Key Manager server protects access to keys by allowing only authenticated users. Once both server and user digital certificates are authenticated by a certificate authority (CA), a secure communication channel (using TLS/SSL) is established between the server and the client, making any exchange private.
The Key Manager server can take care of a huge number of keys, which allows sharing key management infrastructure between NonStop systems and other platforms to take advantage of infrastructure investment and minimize management costs. There is no need for a separate infrastructure to generate, store, and protect tape volume keys for BackBox.
BackBox currently supports the following kinds of Key Manager servers:

- The Utimaco Enterprise Security Key Manager (ESKM).

In the BackBox configuration, dependingon the type of client interface with the Key Manager, Key Manager Servers can be defined as distinct logical views with different configurations.
Each view is identified by an arbitrary Key Manager ID used by the BackBox domains. Such a view contains:

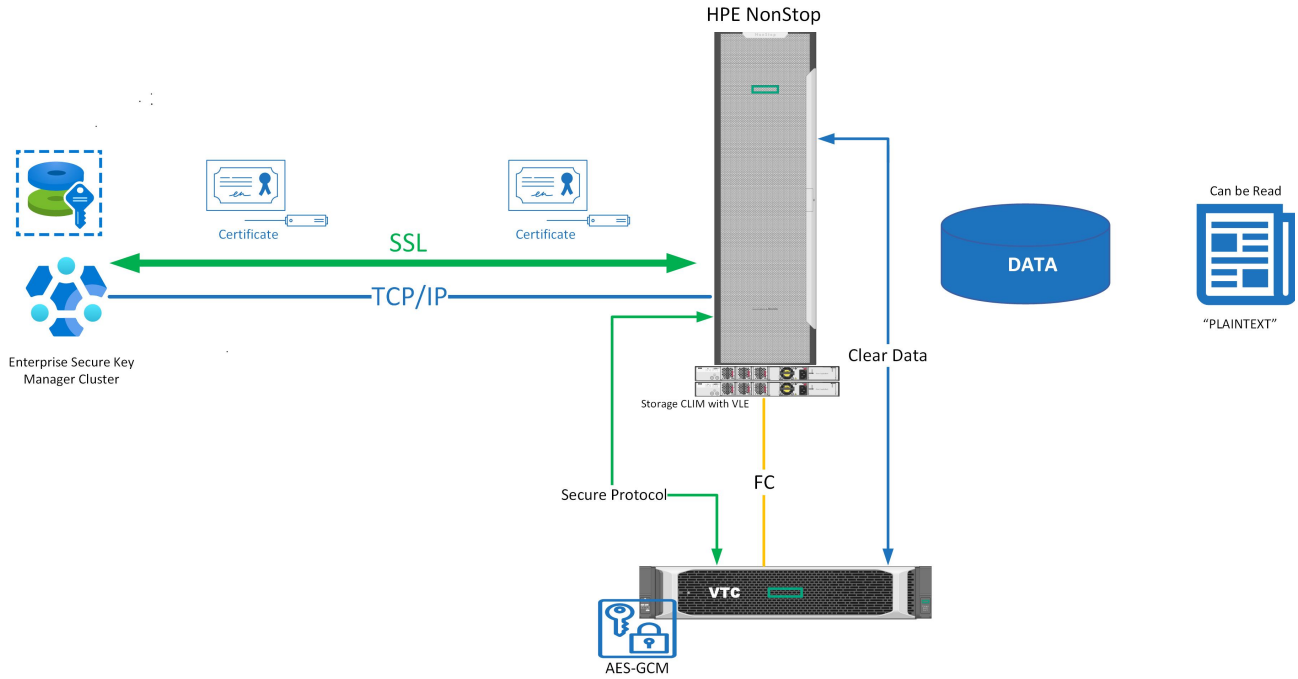
- general information, such as the server type (ESKM)
- the server's associated IP port and address(es)
- common Client Attributes, such as the possible connected Client Type and the Local Group.
- the list of possible clients able to reach the Key Manager server

KEY MANAGER CLIENT

BackBox tape emulation software can interact with Key Management in one way:

- For a VLE setup, the client to the Key Manager is the CLIM (for ESKM only).

VLE SETUP



For NonStop Volume Level Encryption(VLE), the Key Management appliance used is the Enterprise Secure Key Manager (ESKM), which is accessed via Storage CLIMs. This means that only NonStop systems supporting CLIMs (NonStop Blade systems and certain NS-series models) are supported.
The ESKM server generates and stores the keys, usually in a cluster of ESKM servers, replicating the keys on each server. The ESKM clusters can be split across multiple sites for site diversity.
Each Storage CLIM with the VLE option implements an ESKM Client that obtains keys from the ESKM and forwards them to the devices through the T10 SCSI Security Protocol command set that manages Encryption aware tape devices.
The BackBox tape emulation implements the T10 SCSI Security Protocol command set to integrate enterprise-class Key Management appliances. When emulating LTO 4 tape drives, BackBox virtual tape devices notify the CLIM that it can be used for encryption.
In the BackBox configuration, CLIM and LTO 4 tape emulation configured for VLE usage is named VLE-CLIM Client and must be assigned to an ESKM Key Manager ID with Client type set to "VLEINTEROPERABILITY".
All LTO 4 virtual tape devices configured for VLE are dedicated for encryption/decryption purposes. Only LTO 4 media types can be presented to the Storage CLIM and $ZSRV server in VLE encryption mode.
When attaching a VLE-CLIM Client to a Key Manager ID, it is necessary to identify the list of CLIMs that can be used to reach the ESKM server.
Encryption key rotation frequency is based on the VLE key generation policy (KeyPerTape or KeyPerDrive) set in SCF.

VLE Key Generation Policy

When an LTO 4 tape drive is configured as an encryption device, VLE records a Drive Encryption context for it. This context holds information as the MasterKeyName (that identifies the tape drive by the tape drive

identifier and the CLIM number it connects to), the encryption algorithm used by the tape drive, the key size needed by the tape drive, and the key generation policy: KeyPerTape or KeyPerDrive.
To work with VLE, most of the BackBox encryption configuration consists of making LTO 4 tape drives available to NonStop systems and enabling VLE in the NonStop environment.

```
STORAGE - Status TAPE \NSBLDE4.$VTE400, ENCRYPTION

Media
  Not present or encryption status unknown



Drive

  MasterKeyName.....N2108001086022114_S066666C1002541

  KeyAlgorithm......GCM-AES
  KeySize...........256
  KeyGenPolicy......KeyPerTape
```

When the KeyPerTape key generation policy is set (via SCF), each tape written by the tape drive will use a unique encryption key. Each time data is rewritten on the media, (when the media state changes from state SCRATCH to SELECT), the tape drive will use a new key to encrypt the data. In this case, the key is automatically renewed and the key is identified by a key name associated with the media. In some situations, such as the need to restore the media's data on a remote NonStop system using another ESKM Cluster, it will be necessary to export the media key in the other ESKM Cluster using the Media Key Name.

```
STORAGE - Status TAPE \NSBLDE4.$VTE400, ENCRYPTION
Media
  KeyName...........N7566B3CCLAB035D873833A969D0008_BBBBBBBB_1911112107

  KeyAlgorithm......GCM-AES
  KeySize...........256


Drive
  MasterKeyName.... N2108001086022114_S066666C1002541
  KeyAlgorithm......GCM-AES
  KeySize...........256
  KeyGenPolicy......KeyPerTape
```

When the KeyPerDrive key generation policy is selected, each tape written by the tape drive will use the current tape drive Encryption Key. Each time media data is rewritten, (when the media state changes from state SCRATCH to SELECT), the tape drive will use the key identified by its Drive context. The key is not
renewed (or changed) automatically. If the user wants to change the drive key, it will be necessary to ALTER the tape drive in SCF using the NEWENCRYPTIONKEY attribute.

```
STORAGE - Status TAPE \NSBLDE4.$VTE400, ENCRYPTION

Media
  Not present or Encryption status unknown



Drive
  MasterKeyName. ... N2108001086022114_S066666C1002541
  KeyName.......... N2108001086022114_2011023101234

  KeyAlgorithm. .... GCM-AES
  KeySize. ......... 256
  KeyGenPolicy. .... KeyPerDrive
```

As with KeyPerTape, when the media's data is rewritten, a Media Key Name is used to identify the key that was used by the tape drive at encryption time. Even in a case where a user renews the Drive Encryption key and changes the drive key context, the Media Key Name will still be available. The key most recently used to write data on each media is retained to facilitate later decryption, regardless of whether the key associated with the drive has been changed some time after the media was written.

```
STORAGE - Status TAPE \NSBLDE4.$VTE400, ENCRYPTION

Media

  KeyName..........N7566B3CCLAB035D873833A969D0008_BBBBBBBB_1911112113
  KeyAlgorithm.....GCM-AES
  KeySize..........256



Drive
  MasterKeyName.... N2108001086022114_S066666C1002541
  KeyName.......... N2108001086022114_2011023101234
```

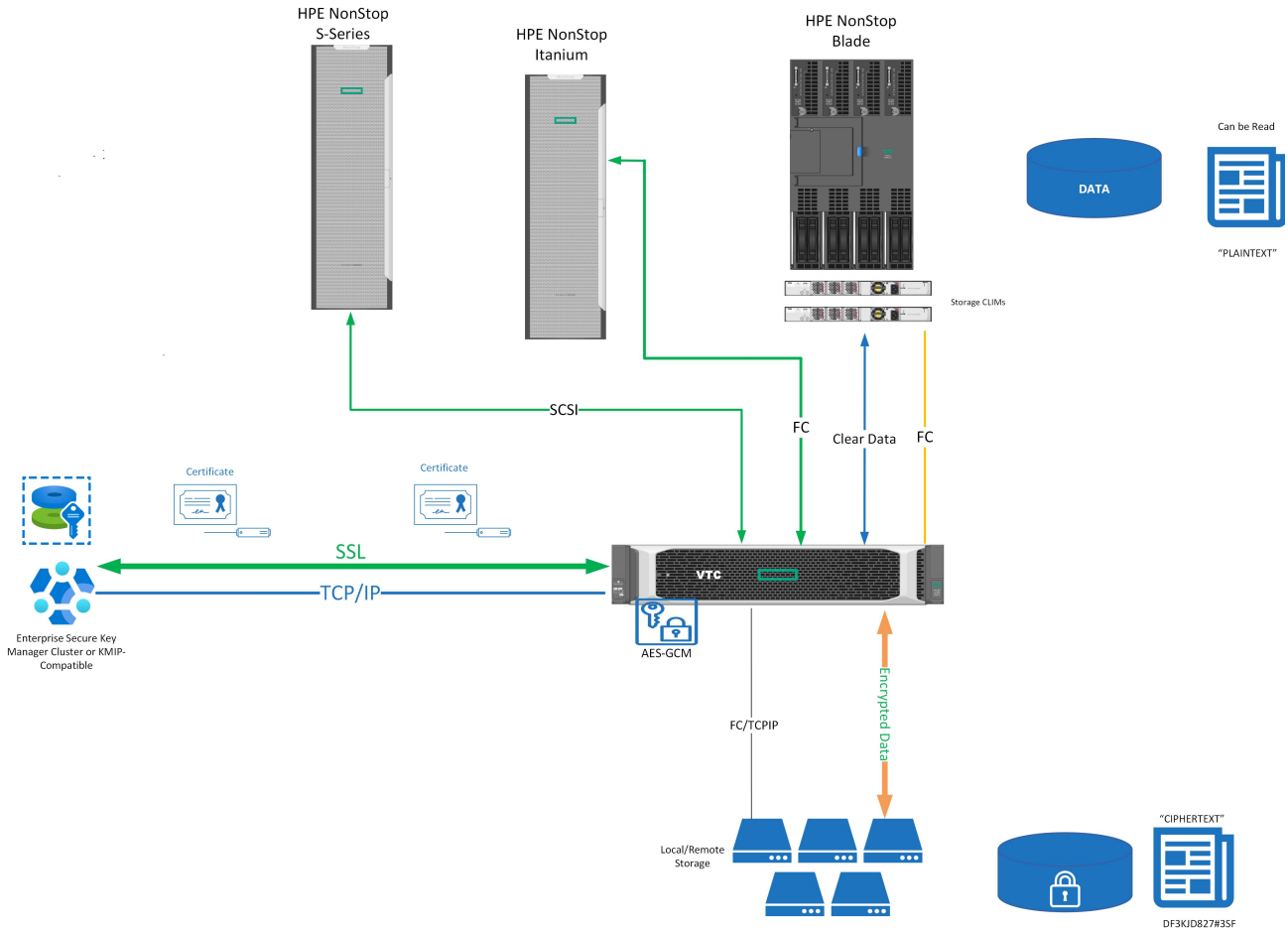
The samples above show examples of drive status of media backup with current Drive key context. Below are examples for the same media after renewal of the drive Encryption key.
Since media is usually written, read and rewritten by different tape drives, a Media Key Name will always be generated to identify the encryption key of the media, regardless of which key generation policy has been used. Key management actions, such as export, delete or query should be performed using the Media Key Name.

```
STORAGE - Status TAPE \NSBLDE4.$VTE400, ENCRYPTION

Media
  KeyName.......... N7566B3CCLAB035D873833A969D0008_BBBBBBBB_1911112113

  KeyAlgorithm..... GCM-AES
  KeySize..........256



Drive

  MasterKeyName.... N2108001086022114_S066666C1002541
  KeyName.......... N2108001086022114_20111118134512

  KeyAlgorithm..... GCM-AES
  KeySize..........256
  KeyGenPolicy..... KeyPerDrive
```

KeyPerTape vs. KeyPerDrive

The nature of the tape media is used to hold different data generations for specific periods of time (retention).
The fact that KeyPerTape policy generates a new key when a virtual tape is rewritten makes its usage more secure.
If a virtual volume were tampered with, only the data on that specific virtual volume would be compromised. The ESKM administrator can delete the key to avoid a security breach. Also, key renewal is performed automatically and doesn't require manual intervention at the TAPE device level: there is no need to STOP and ALTER the device.
The KeyPerDrive policy is less secure, since multiple virtual volumes will all be encrypted using the same key. Having one virtual volume tampered with would be more critical, as data on all virtual volumes encrypted with that key could be compromised. Deleting that key would affect much more data, as none of the other virtual volumes encrypted with that key would be retrievable thereafter.
We highly recommend using the policy with less exposure: KeyPerTape policy.

VTC Client (Non-VLE) Setup



BackBox software includes a key management client to interface with Key Manager server. This allows tape encryption to the whole range of NonStop systems. All tape device types supported by BackBox, CART3480, LTO 3 and LTO 4, can encrypt. VTCs are registered as clients to the Key Manager Server.
In the BackBox configuration, VTC with encryption devices licensed are named VTC Client and can be assigned to an ESKM or a KMIP Key manager ID. For each VTC Client attached, we will need to define information related to the TLS/SSL communication required to connect to the Key Manager server.
When an ESKM Key manage is set to used "VLE INTEROPERABLILITY" Client type,

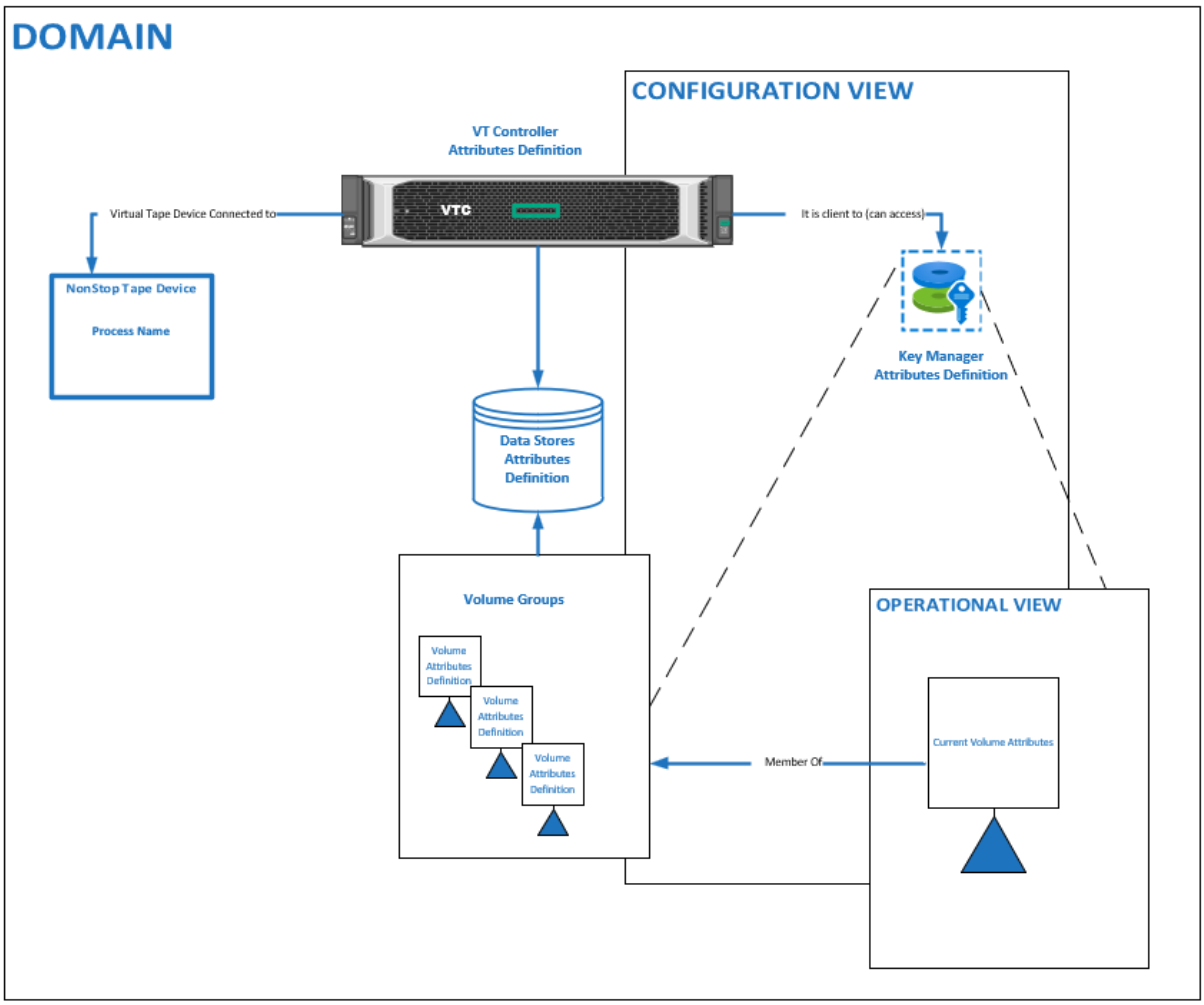
- VLE key naming convention will be used :

NXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX_BBBBBBBB_ZZZZZZZZZZ

- Access to encrypted virtual volume can be made across NonStop node not supporting Storage CLIM and Storage CLIM configure with VLE.
- VTC Client can be used by any available virtual tape drive. Virtual tape drives are not dedicated to encryption.
- Usage of encryption is not restricted to LTO 4 media type. LTO 3 and CART3480 can also be used.
- VTC Client will use KeyPerTape method when requesting a new key even VLE the key generation policy KeyPerDevice is used for VLE managed LTO 4 devices.

A VTC Client can be assigned to an ESKM or KMIP Key manager ID when the Client type is set to "VTC ONLY":

- In this mode, BackBox key naming convention would be used:
- BBOX_XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX_AAAAAAAAAAA
- Access to encrypted virtual volume can be made across any type of NonStop node.
- VTC Client can be used by any available virtual tape drive. Virtual tape drives are not dedicated to encryption (except LTO 4 configured for VLE.)
- Usage of encryption is not restricted to LTO 4 media type. LTO 3 and CART3480 can also be used.
- When data retention date expired for specific volumes, encrypted data still remains on them. A simple way to make sure expired encrypted data can't be recoverable is to delete the encryption key associated to it from the Key Manager server. Doing so, protected data will be secured, even if expired data can be found in several copies (on a DR site, vault in Backup Enterprise, etc...). The VTC client can help automate deletion of encryption key when data has expired. VTC client can request Key Manager server to delete old key when virtual tape volume is SCRATCHED by rewriting data or by freeing expired volumes when running the daily cleanup job (OBB017.)
- It is also possible to virtualize and encrypt data of non-encrypted legacy psychical tape media.
- Each virtual volume will be encrypted with a different key and will be rotate each time the volume is rewritten (same has VLE KeyPerTape.)



A BackBox license key must be installed to allow VTCs encryption.
If the Client uses to the Key Manager, CLIM for VLE, the user must configure the BackBox domain in the same way:

- The encryption is enabled in the Volume Group configuration by choosing an encryption algorithm (AES-GCM 256 bits).
- The Key Manager must be registered under an arbitrary Key Manager ID and all its clients defined.
- The setup must be verified by the Test Function available on the Key Manager configuration page.
- The BackBox license key contains a maximum number of encryption drives concurrently active. The tape workload requiring encryption should be anticipated, especially in the case of a VLE setup where VLE drives cannot be used to write non-encrypted backups.

The Key Manager ID and the encryption algorithm are saved in the BackBox catalog of virtual volumes to know how to decrypt each volume, independently of configuration changes to the Volume Group or to the Key Manager server.
The Key Manager ID is a logical identifier that becomes important when there are more than one operational Key Manager servers on a site and for D/R operations where three duplications are to be managed:

- The replication of encrypted virtual volumes.
- The replication of catalogs (BackBox, DSM/TC and TMF catalogs).

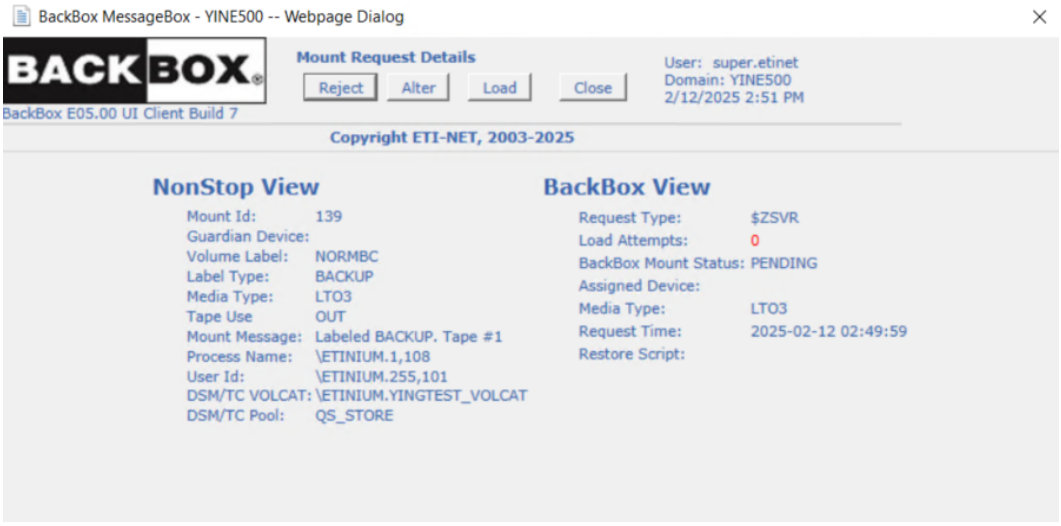
⚠	The Key Manager ID, which is an arbitrary BackBox ID, is part of the BackBox replicated catalog. The Key Manager IDs must be planned from an enterprise point of view.

- The replication of keys from the Key Manager server of the Primary site to the Key Manager server on the Secondary site.

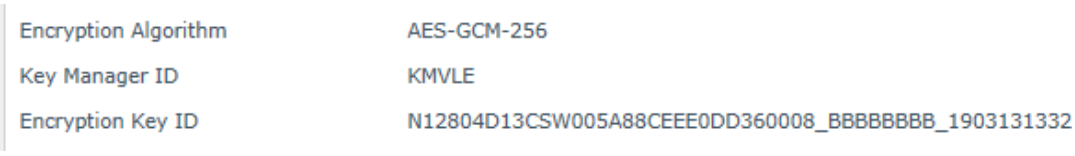
Once the system is configured, the encryption functionality is totally transparent and automated. Once a NonStop tape mount requests to mount a volume from an encrypted Volume Group is recognized, the BackBox Domain will find a free virtual tape drive connected to this NonStop system which allows it to receive the encryption key from the Key Manager server (via the appropriate Key Manager Client) and access the storage location of the virtual volume.
When the virtual device is found, the BackBox Domain will request it in order to load the volume and put it online. Once the volume is online, a request will be generated through a secure TLS/SLL session between the Key Manager server and Client to obtain the Encryption Key (identified by the Encryption Key ID) needed by the virtual tape device to encrypt or decrypt the virtual tape volume data.

⚠	When errors related to encryption happen, any attempt to use the drives will fail with Error 101 (“tape is write-protected”), and a descriptive message should be logged in the EMS. In such a case, refer to BackBox Messages Manual and Troubleshooting and Guardian Procedure Errors and Messages Manual.

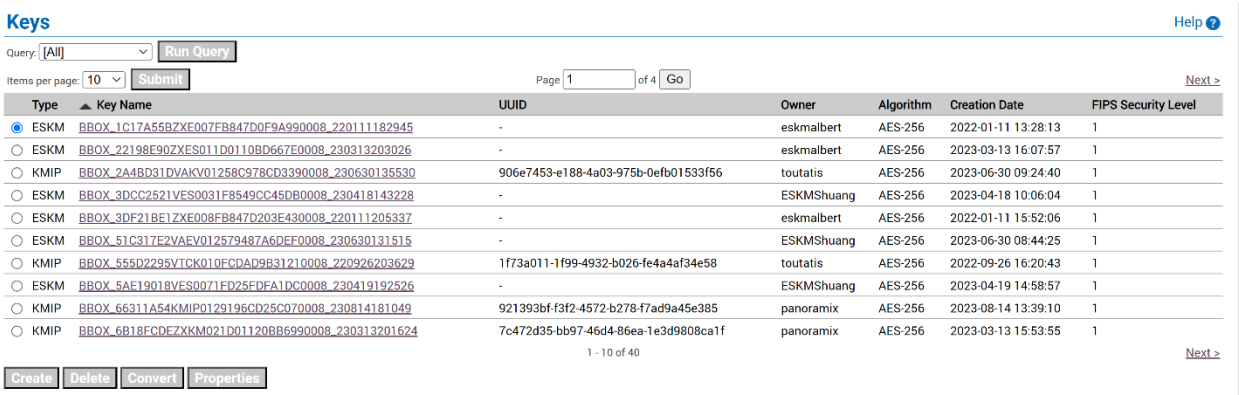
To see the encryption/decryption status while a tape is being written/read: the encryption/decryption status for each drive is displayed on the BackBox UI status page.



For each encrypted volume there is an encryption information section in the Volume Details page of the BackBox UI that shows the last encryption state at the exact moment the volume has been written.



For Key Management purposes, it is recommended to periodically run the batch job OBB038 (list of encrypted volumes) to keep track of encrypted volumes over a specific time period and to verify if the encryption has not been turned off (purposely or accidentally) for volumes that are supposed to be encrypted.
The media identifier is part of the Encryption Key ID: volume names are included in the media identifier. Naming the volume allows the ESKM administrator to carry out searches on key names within the ESKM operation console.



BACKBOX ENCRYPTION CONFIGURATION

Enabling Encryption

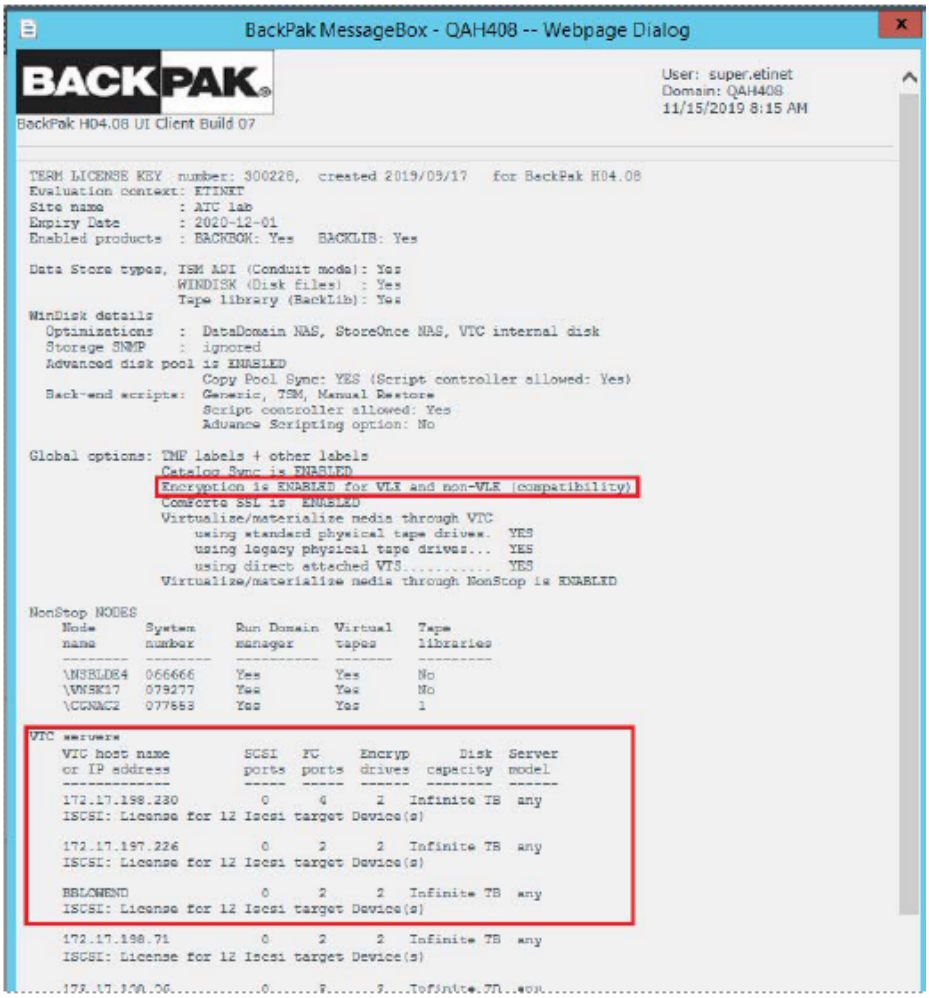
BackBox Tape Encryption is a licensed option. You will have to license virtual tape encryption devices per VTC regardless of the VLE setup. Make sure to specify the quantity of encryption devices (BBENCR) for each VTC server in the license order.

Nonatomic License (License version prior to 4.09)

Without the encryption license option, the Key Manager tab does not appear on the Configuration page and, therefore, the encryption cannot be configured.
The encryption is controlled at two levels in the BackBox license key:

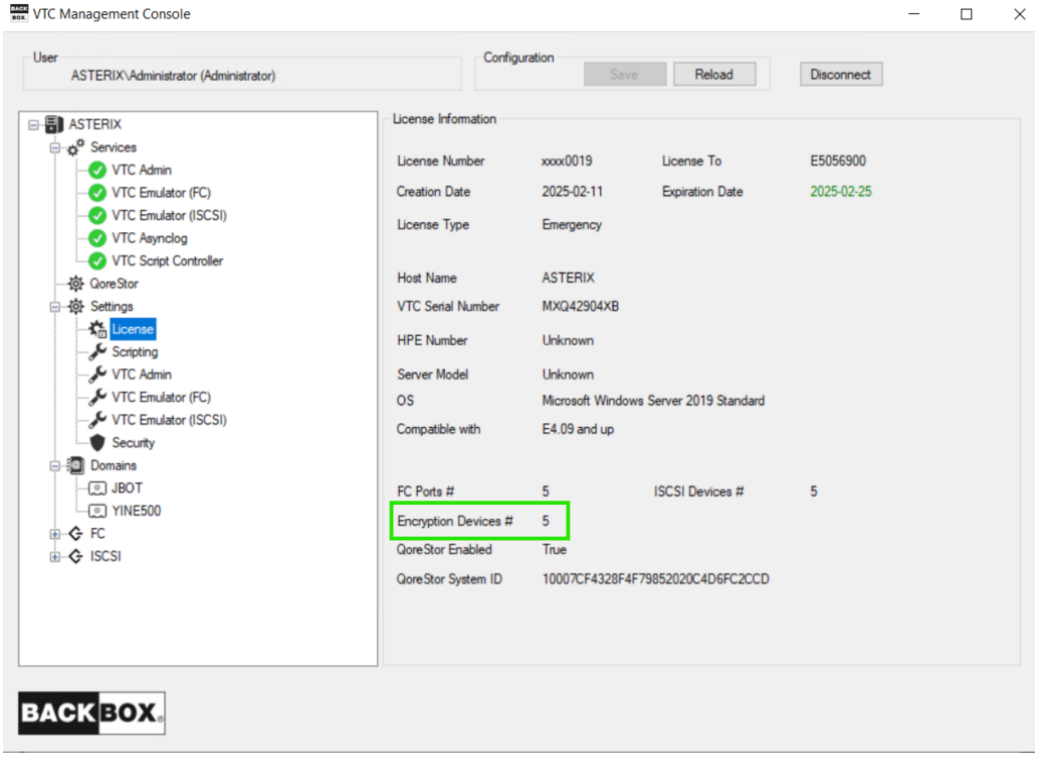
- Global control by the encryption option.
- In each VTC, the maximum number of virtual drives operating concurrently with encryption is limited. This number can be smaller than the actual number of drives when some tape volumes are not to be encrypted.

To verify the license control levels, go to **Configuration > Domain > License Options**



Atomic License (License version 4.09 and later)

For domain license 4.09 and higher, the encryption devices are controlled by VTC license version.
Check the VTC Management Console > **Settings** > **License** for the info regarding the number of encryption devices.



VLE Configuration

Volume Level Encryption requires the creation of a security officer that allows a member of the SUPER group to perform VLE operations and configuration tasks.

For more information about VLE requirements, installation and other product references, see NonStop Volume Level Encryption Guide.

VLE Virtual Tape Drives Topology

- Identify CLIMs that support VLE

The first step is to identify CLIMs supporting encryption, by determining which of them have VLE installed.
If it is not already known, the easiest way to verify that a given CLIM is ready for encryption is by using the SCF command:
`STATUS CLIM $ZZSTO.*, KEYMANAGER`
This command will list all CLIMs that have access to the ESKM Key Manager.

```
1- > status clim $zzsto.*, keymanager

STORAGE - KeyManager Status CLIM \NSBLDE4.$ZZSTO.#S1002531

CLIM not registered with Key Manager
STORAGE - KeyManager Status CLIM \NSBLDE4.$ZZSTO.#S1002533

CLIM not registered with Key Manager

STORAGE - KeyManager Status CLIM \NSBLDE4.$ZZSTO.#S1002541
KeyManager 10.10.10.54  OK

KeyManager 10.10.10.55  OK

STORAGE - KeyManager Status CLIM \NSBLDE4.$ZZSTO.#S1002543

CLIM not registered with Key Manager

STORAGE - KeyManager Status CLIM \NSBLDE4.$ZZSTO.#S1002561

CLIM not registered with Key Manager
```

In this example the only CLIM with VLE Encryption support is S1002541.

Then, for each VLE-supporting CLIM identified in the previous step, display all of the WWN port names available on that specific CLIM by using the TACL command:
`climcmd <clim-name> lunmgr –wwns`

```
$SAS22 ETINET 4> climcmd S1002541 lunmgr --wwns

slot   port   wwn   speed

1   1   5001438001336f40 4 Gbit


1   2   5001438001336f42 4 Gbit


Termination Info: 0
```

- Identify VTC Ports Connected to the VLE-Supporting CLIMs

For each CLIM identified to be used for BackBox VLE virtual tape drives, determine the VTC Server, the FC ports and the tape drives that will be used for VLE.
Log on to the BackBox UI interface and navigate to the VT Controller configuration page. A list of each VTC available port is shown in VTC Ports table. The Host WWN column displays the WWN of the host port connected to the VTC port.

Enabling Virtual Tape Encryption Emulation in a VTC

FC Emulation

The VTC is internally configured by default for LTO 3 media type. To enable the LTO 4 emulation required by VLE, the tape drives must be stopped and reconfigured in SCF, in CLIM, and in VTC.
For a VTC, there might be several entities involved: several BackBox domains, several NonStop nodes, and more than one CLIM per node.

Step	Description
1. Take note of the location (CLIM # and LUN #) of the tape drives to be changed to LTO4	At the TACL prompt: SCF INFO CLIM <clim-id>,DETAIL STORAGE - Detailed Info CLIM \NSBLDE4.$ZZSTO.#C1002561 Configured Devices:

Type	Name	Primary CPU	Backup CPU	Lun
TAPE	$LW2131	0	1	1

Step	Description

TAPE	$LW2132	0	1	2
TAPE	$LW2133	0	1	3
TAPE	$LW2134	0	1	4
TAPE	$G86130	3	0	17
TAPE	$G86131	3	0	18
TAPE	$G86132	3	0	19
TAPE	$G86133	3	0	20
TAPE	$G86140	0	1	29
TAPE	$G86141	1	2	30
TAPE	$G86142	2	3	31
TAPE	$G86143	3	0	32

2. Stop all tape drives emulated by the VTC to update

NonStop, at the SCF command prompt:
RESET TAPE $G8*, FORCE

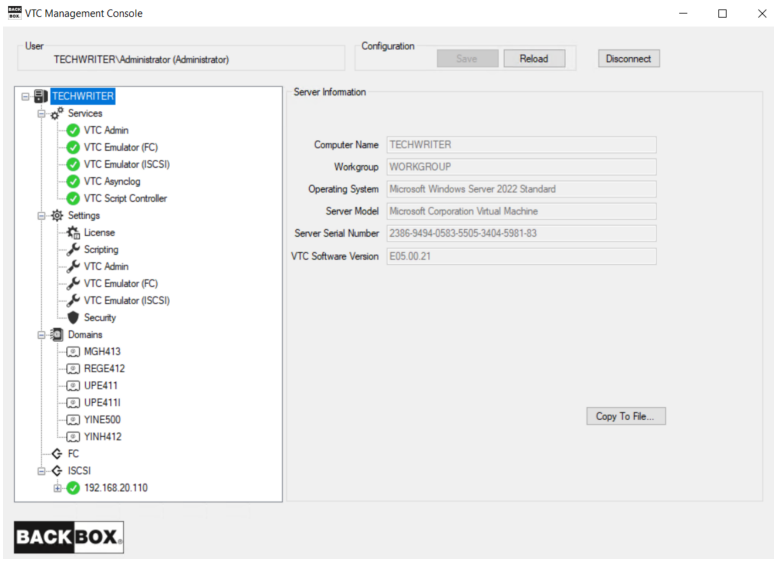
3. Delete the tape drives to change to LTO4 (List in Step 1)

NonStop, at the SCF command prompt:
DELETE TAPE $G86133

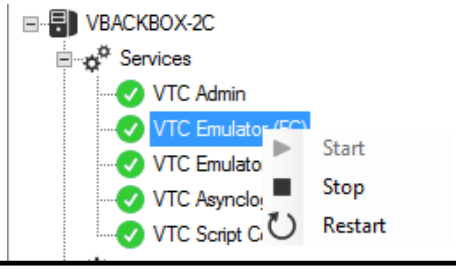
4. Stop the VTC Emulator (FC) Service

In a Remote Desktop session to the VTC

Open the Search dialog and type VTC Management Console and click on the executable to start it.



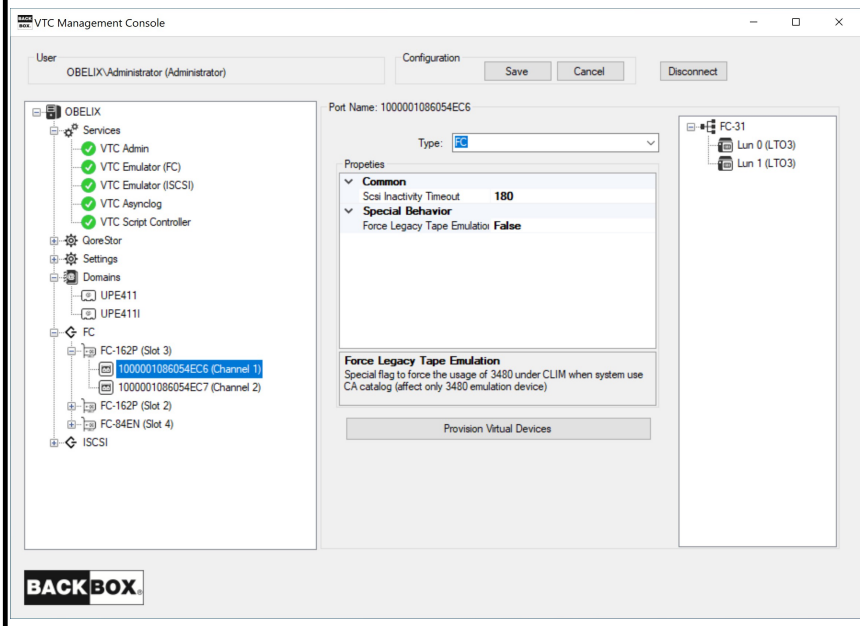
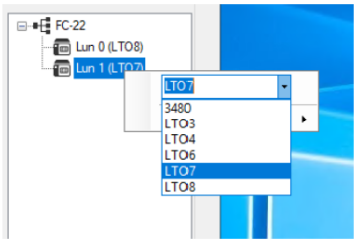
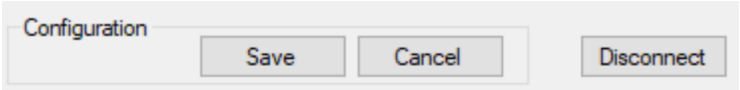
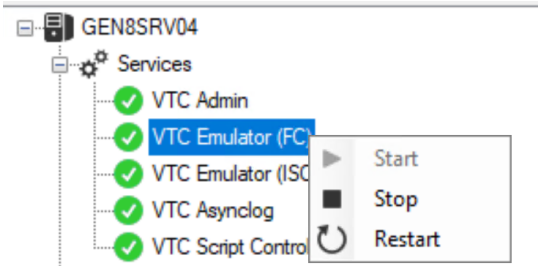
Right-click on the VTV Emulator (FC) of the Services node and click on the Stop action.



5. In the CLIM, remove the entries to change to LTO4 (List in Step 1)

At the TACL prompt:
climcmd C1002561 lunmgr --scan climcmd
C1002561 lunmgr --delete 20

Are you sure you want to delete lun 20 (tape HPE M8505 #BB030FA705)? y
Termination Info: 0

Step	Description
6. Update the VTC internal configuration	Using the VTC Management Console, expand the FC and HBA Card node and click on the identified Port connected to the VLE CLIM.  Replace the emulation type LTO3 by LTO4 or V0505 on the devices that will be VLE.  If all devices are designated to be VLE, right-click on the Port ID node and select the LTOX emulation to change all devices at once. Note: Additional LUN can be added by clicking on the Provision Virtual Devices button. Save changes by clicking on the Save button. 
7. Restart the VTC Emulator FC) Service	Using the VTC Management Console, right-click on the VTC Emulator (FC) of the Services node and click on Start.  If there is a syntax error, the service will stop immediately. If the service stops, check the reason in the Event log: In the MS-Windows menu, Administrative Tools, select Event Viewer > Applications and Services Logs > Virtual Tape Controller.

Step	Description
8. Rescan the CLIM and approve the new LTO4 tape drives	At the TACL prompt: **climcmd C1002561 lunmgr –scan** Termination Info: 0 **climcmd C1002561 lunmgr --approve** OK to assign lun 20 to tape HPE Ultrium4-SCSI #BB030FA705? **y** Termination Info: 0
9. Re-add the LTO4 tape drives in SCF (List in Step 1)	Adjust the SCF command to add the tapedrives, the LUN # might be changed. Then execute the command: **ADD TAPE $G86133, SENDTO STORAGE, &** **PRIMARYCPU 2, BACKUPCPU 3, & CLIM** **S1002531, &** **LUN 20**
10. Restart the tape drives emulated by the VTC	At the SCF command prompt: **START TAPE $<tape-name-pattern>** Check in EMS the messages reporting the tape drives starting. Verify the NonStop systems recognized by the LTO4 media type: **MEDIACOM INFO TAPEDRIVE**

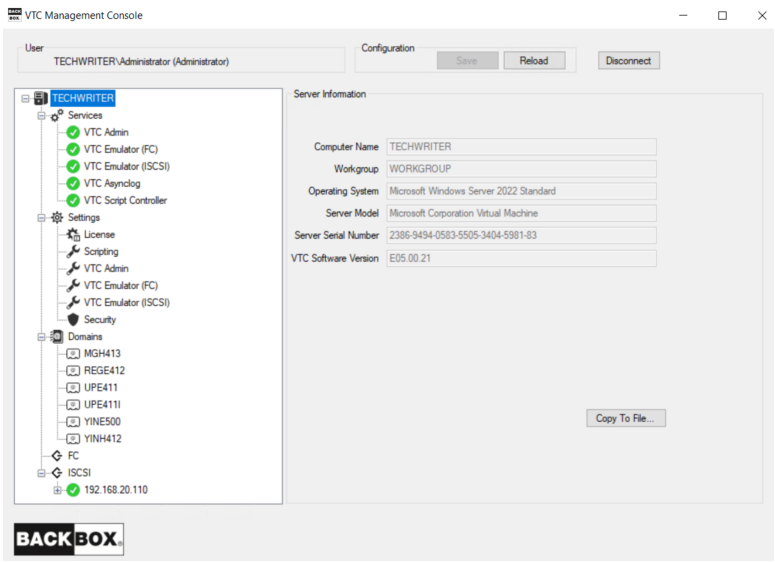
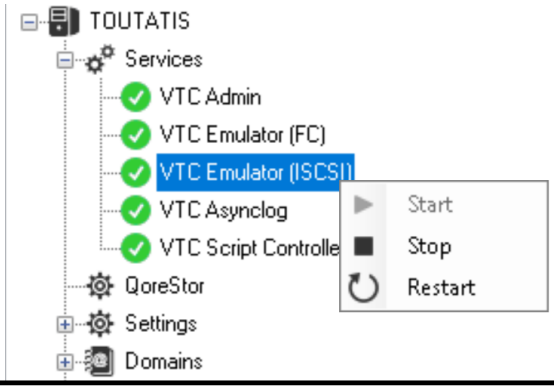
Tape Drive Name	Device Type	NL Check	BLP Check
$G64131	LTO3	OFF	ON
$G64140	LTO4	OFF	ON
$G66130	LTO3	OFF	ON
$G66133	**LTO4**	**OFF**	**ON**
$G66140	LTO4	OFF	ON
$G64141	LTO4	OFF	ON
$G66141	LTO4	OFF	ON

iSCSI Emulation

To enable the iSCSI emulation required by VLE, the tape drives must be stopped and reconfigured in SCF, in CLIM, and in VTC. For a VTC, there might be several entities involved: several BackBox domains, several NonStop nodes, and more than one CLIM per node.

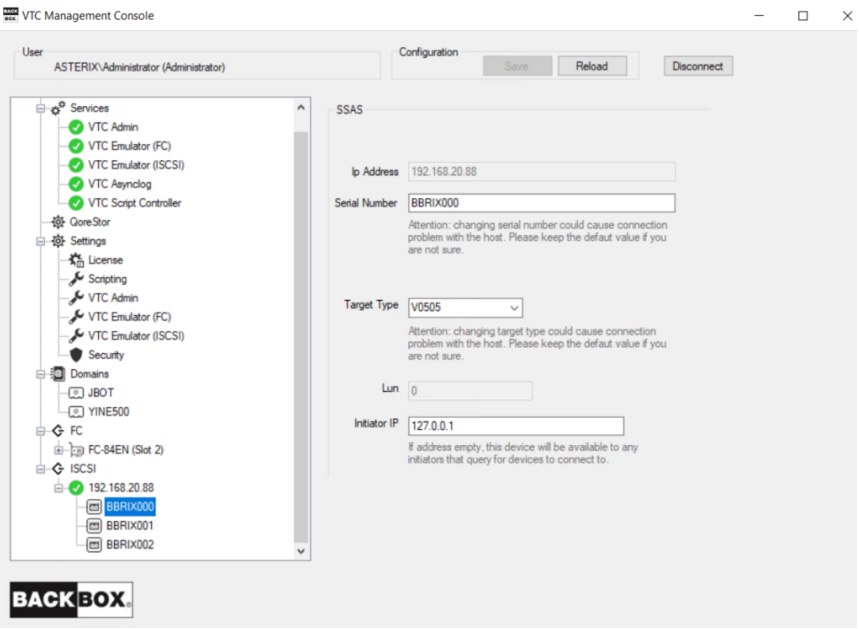
Step	Description
1. Take note of the location (CLIM #) of the tape drives to be changed to iSCSI	At the TACL prompt: SCF INFO CLIM <clim-id>,DETAIL STORAGE - Detailed Info CLIM \NSBLDE4.$ZZSTO.#C1002561 Configured Devices:

Type	Name	Primary CPU	Backup CPU	Lun
TAPE	$LW2131	0	1	1
TAPE	$LW2132	0	1	2
TAPE	$LW2133	0	1	3
TAPE	$LW2134	0	1	4
TAPE	$G86130	3	0	17
TAPE	$G86131	3	0	18
TAPE	$G86132	3	0	19
TAPE	**$G86133**	3	0	20
TAPE	$G86140	0	1	29
TAPE	$G86141	1	2	30
TAPE	$G86142	2	3	31
TAPE	$G86143	3	0	32

Step	Description
2. Stop all tape drives emulated by the VTC to update	NonStop, at the SCF command prompt: **RESET TAPE $G8*, FORCE**
3. Delete the tape drives to change to iSCSI (List in Step 1)	NonStop, at the SCF command prompt: **DELETE TAPE $G86133**
4. Stop the VTC Emulator (iSCSI) Service	In a Remote Desktop session to the VTC Open the Search dialog and type VTC Management Console and click on the executable to start it.  Right-click on the VTV Emulator (iSCSI) of the Services node and click on the **Stop** action. 

5. In the CLIM, remove the entries to change to LTO4 (List in Step 1)	At the TACL prompt:
	`-t`
	or
	`--addiscsitape`
	Ex: `climcmd SCLIM000 lunmgr -t 192.168.30.20`

Step	Description
6. Update the VTC internal configuration	Using the VTC Management Console, expand the iSCSI node and click on the identified Port connected to the VLE CLIM.



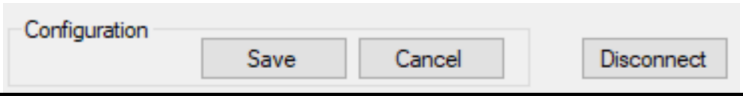
a. Serial Number is the target identifier and shouldn't be modified, as the connection is securely established with the host based on the serial number.

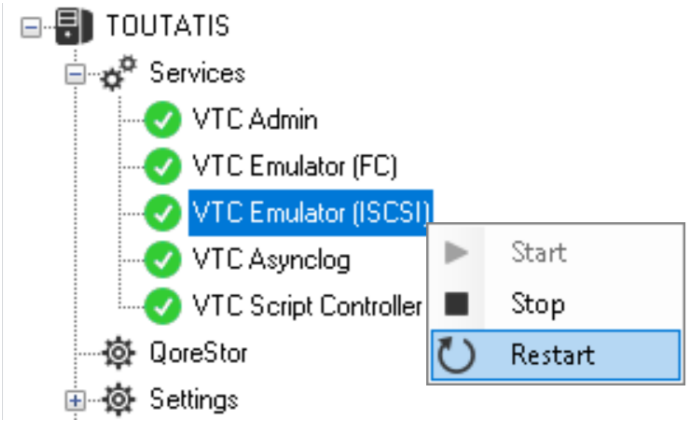
b. Target Type is the emulation tape type to be used for the target (V0505 and/or LTO4).

c. Lun is assigned by default and cannot bechanged, as it's used to provision virtual devices.

d. Initiator IP links the selected target to a specific CLIM. Once linked, the iSCSI device will only answer to the discovery command from that specific storage CLIM. By default, new added device is assigned with a dummy value of 127.0.0.1 that must be changed with the CLIM storage IP address of the target device to be to connected to. The new added device IP address can be left blank to answer to any CLIM storage.

If not updated and left with the default value (127.0.0.1), the target device will not answer to any CLIM storage when attempting to adding iSCSI tape target devices by using the CLIMCMD `--addiscsitape`.
If updated to blank, the target device will answer to any CLIM storage when attempting to adding iSCSI tape target devices by using the CLIMCMD `--addiscsitape`.
If updated to a specific CLIM address IP, the target device will only answer to that specific CLIM storage when attempting to adding iSCSI tape target devices by using the CLIMCMD `--addiscsitape`.



Step	Description
7. Restart the VTC Emulator FC) Service	Using the VTC Management Console, right-click on the VTC Emulator (iSCSI) of the Services node and click on Retart.  If there is a syntax error, the service will stop immediately. If the service stops, check the reason in the Event log: In the MS-Windows menu, Administrative Tools, select Event Viewer > Applications and Services Logs > Virtual Tape Controller.
8. Re-add the LTO4 tape drives in SCF (List in Step 1)	Adjust the SCF command to add the tape drives, the LUN # might be changed. Then execute the command: **ADD TAPE $G86133, SENDTO STORAGE, &** **PRIMARYCPU 2, BACKUPCPU 3, & CLIM** **S1002531, &** **LUN 20**
9. Restart the tape drives emulated by the VTC	At the SCF command prompt: **START TAPE $<tape-name-pattern>** Check in EMS the messages reporting the tape drives starting. Verify the NonStop systems recognized by the LTO4 media type: **MEDIACOM INFO TAPEDRIVE** Tape Drive Name Device Type NL Check BLP Check $G64131 LTO3 OFF ON $G64140 LTO4 OFF ON $G66130 LTO3 OFF ON **$G66133 LTO4 OFF ON** $G66140 LTO4 OFF ON $G64141 LTO4 OFF ON $G66141 LTO4 OFF ON

Enabling VLE on Tapes in SCF

Replacement of FC HBA Card Emulating LTO 4

Should an FC HBA card in a VTC fail, it may need to be replaced. Replacing the HBA of the CLIM connected to it will have the same functional impact as replacing a group of tape drives with new ones. All virtual LTO 4 tape drives emulated using the new HBA will be seen by the CLIM as different tape drives. Also, those tape drives will not, by default, be managed by the VLE for encryption, even if the prior tape drives were all set to encrypt or decrypt data.
Some pre- and post-card-replacement actions will be needed to achieve this task.
Important:
The following activity needs to be carried out by a local system user member of the SAFEGUARD encryption officer group:
Before replacing the HBA:
In SCF, perform the following actions on the affected (associated with the FC Ports of the failed FC HBA) LTO 4 tape drives individually by using the pattern process name (only for virtual tape drives connected to the port that needs to be replaced):

- Stop the tape drive.
- Alter the tape drive with the attribute: KEYGENPOLICY NOENCRYPTION.
- Start the tape drive.
- Status tape drive with attribute: ENCRYPTION, to validate the result.

When done, STOP all tape drives again and replace the failed FC HBA.
After the HBA is replaced, re-activate the key generation policy for the tape drives that use the new HBA.

- Stop the tape drive.
- Alter the tape drive with the attribute: KEYGENPOLICY KEYPERTAPE.
- Start the tape drive.
- Status tape drive with the attribute: ENCRYPTION, to validate the result.

Adding Key Manager in BackBox Configuration

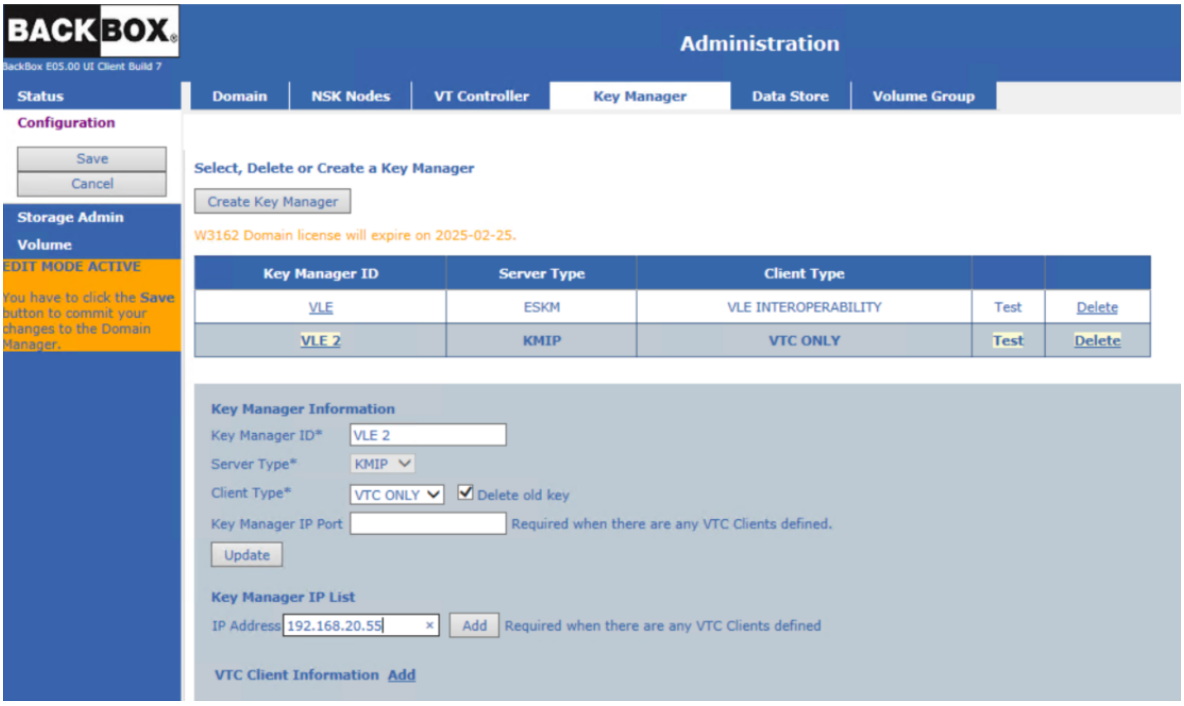
Attach the listed CLIM supporting the VLE to be able to reach the targeted ESKM Key Manager represented by a BackBox Key Manager's configuration entity (Key Manager ID).
Log on to the BackBox UI interface.

- Select the Configuration menu and select the Switch to Edit mode.
- Select the Key Manager tab.
- Select the targeted Key Manager ID.

⚠	A VLE-CLIM Client can be attached to an ESKM Key Manager Type only. If the Key Manager entity doesn't exit, create one.

Click on the Create Key Manager button and fill in the Key Manager information:

- Choose an alias name and type it in the Key Manager ID file.
- Server Type must be set to ESKM.
- Client Type must be set to VLE INTEROPERABILITY.
- Other fields can remain empty or filled in for self-configuration documentation or for future use.



NON-VLE CONFIGURATION

In this setup, the VTC is a client to the Key Manager. To be authenticated by the KeyManager, the VTC presents an account, a password, and a digital certificate signed by a Certificates Authority (most of the time a local one.)
For security reasons, tasks related to the generation, installation and configuration of certificate and authentication elements should be restricted to a Security Authority user.
Since there are many ways to generate a digital certificate and each of them may require specific certificate fields entries depending on Key Manager server used or enterprise security policies restrictions, following procedure would focus on IN and OUT needed to be produced and which one (role) should accomplish it. Method describes to produce requirements should be taken as guidelines and adapted to enterprise reality.

Key Manager Configuration

- VT Controller (VTC) who will be used as client must be identified. Each VTC should be licensed for encryption support (Security Authority user role)
- Supplemental client licenses (1 per VTC identify) should be provisioned at the Key Manager server (KM Administrator role)
- A username with his password (1 per VTC identify) should be create according to the enterprise policy (KM Administrator role.) The VT Controller ID can be a good candidate for username
- All VTC's "username" should be configured as a group on the key manager server (KM Administrator
- role) and allow to:
  - Be able to request key generation
  - Be able to access key owned by VTC group member
  - Be able to delete key owned by VTC group member (if key deletion automation will be enabled for SCRATCH media)

If Key manager server type is ESKM and VTC Client are not intent to be used in collaboration with VLE, a local group named BackBox should be created and VTC's username added to it. If VTC Client are intent to be used in interoperability with VLE for tape, VTC's username should be added to same local group than CLIM (normally local group NonStop).

IMPORTANT: For Client Type VTC ONLY, the ESKM Local Group BackBox is only default suggestion and must be override by the group name configure in the ESKM server configuration else key will not be generated and access denied will be logged in the ESKM audit logs.

VTC Configuration

- For a VTC digital certificate generation activity (for each VTC identified by the Third-Party Security Authority user role):
  - Generate a private key (normally an RSA key) for the Key Manager communication channel according to enterprise security policy (key length 1024 or 2048, passphrase).
  - Generate a certificate request with certificate fields set according to enterprise security policy and Key Manager server specific data (the username needs to be specified in the Common Name field or in another specific certificate field, in the Client IPaddress).
  - Submit the request certificate which is to be signed by the Key Manager Server local Certificate Authority (KM Administrator role).
  - Install the signed certificate file (must be named ClientCert.pem), the private key file (must be named ClientKey.pem), and the Local CA certificate (must be named CACert.pem) to authenticate the Key Manager server, into a specific folder on the local disk of the VTC. Access to these 3 files and to the folder should be restricted to only the Third Party Security Authority user and VTC services (LOCAL SERVICE account).
    Note: The 3 files must be in PEM format.
  - Keep and save (required for BackBox configuration):
    - The Key Manager VTC username.
    - The Key Manager VTC username password.
    - The ClientKey.pem passphrase.
    - The 3 file folder locations.

Generate RSA Key and Certificate Request

Here is an example that can be adapted to the Key Manager server requirement and to the enterprise security policies.
It will use openSSL to generate a 1024-bit RSA key and a certificate request with a username in the Common Name field as a Key Manager ESKM requirement.

1- Download and install an openSSL distribution package.

2- From a command console: `c:\OpenSSL-Win64\bin>openssl req -newkey rsa:1024 -keyout ClientKey.pem -out REQ-ClientCert.pem`

Loading 'screen' into random

state - done Generating a 1024-

```
bit RSA private key
. ..... ++++++
. ..... ++++++
Writing new private key to
'ClientKey.pem'  Enter PEM pass
phrase:
Verifying - Enter PEM pass phrase:
You are about to be asked to enter information that will be
incorporated  into  your  certificate  request.
What you are about to enter is what is called a Distinguished
Name or a DN.  There are quite a few fields but you can leave
some blank
For some fields there will be a
default value,  If you enter '.', the
field will be left blank.

Country  Name  (2 letter  code) [AU]:.
State or Province Name (full name)
[Some-State]:.  Locality  Name  (E.g.  city)
[]:.
Organization Name (E.g. company) [Internet Widgets Pty Ltd]:.
Organizational Unit Name (E.g. section) []:.
Common Name (E.g. YOUR name)
[]:BBOX1  Email Address []:.

Please enter the following 'extra'
attributes  to be sent with your
certificate  request
A challenge password []:.
An optional company name []:.

c:\OpenSSL-Win64\bin>
Please enter the following 'extra'
attributes  to be sent with your
certificate  request
A challenge password []:.
An optional
company name []:.
c:\OpenSSL\bin>
```

Sign Client Certificate and CA Certificate

3- Now that the private key has been generated, a certificate request needs to be sent. Once issued, the certificate has to be signed against a CA. Use a local CA installed on the Key Manager Server. In the command window, display the file containing the certificate request as follows:

```
c:\OpenSSL-Win64\bin>type REQ-ClientCert.pem
```

-----BEGIN CERTIFICATE REQUEST-----

MIIBTzCBuQIBADAQMQ4wDAYDVQQDDAVCQk9YMTCBnzANBgkqhkiG9w0B

AQEFAAOB

jQAwgYkCgYEAwjT4SMRtJyMy2sMt4tn4t+1qurnpru99L4OHZknE6zwOakTkYEmV

YISYvKAte2nRVVejYYGuI2VAisHiF6YkivRQi6nblVNC02fn8B2Zh6BGeNzszWRN

ofpJO0q75O5Ig3Rw9bqmV6wRICuN4klOzW5Zxx25st+5uQ11xMzJzlUCAwEAAaAA

MA0GCSqGSIb3DQEBBQUAA4GBAGkDaoqzBn65p3sebRDxR8zuh7T2eeuDY49/JASr

gvM74S3rzrjfjsx8mEdW8m7x2z6yWvwMMmUcxlDXm869sGIYAnaqK5oWsaYt+Tjj

9TvyUpQePnOfufIwj3+NZnHhw0eMjygEQj6AWjPz4EeE6cGjDAmK6q5qm6JfJ2ac Oq3P

-----END CERTIFICATE REQUEST-----

c:\OpenSSL-Win64\bin>

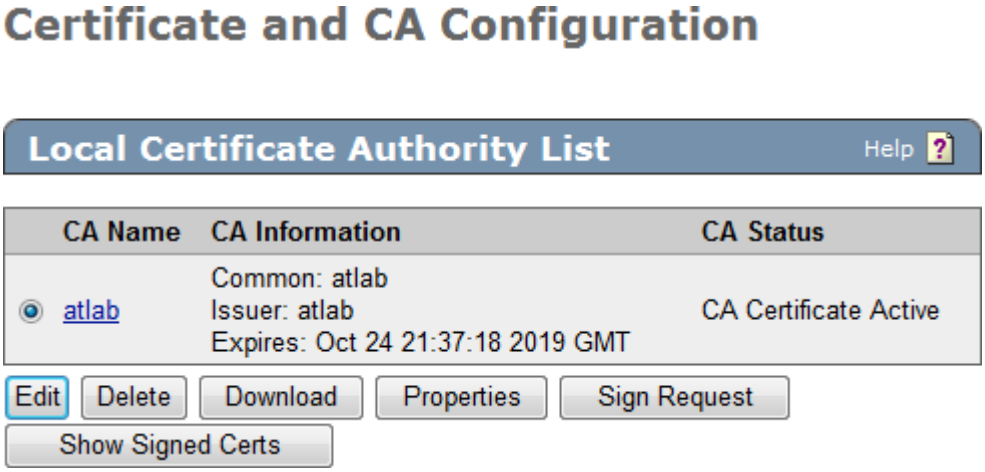
4- Sign the certificate.

A) Select and copy the Client certificate request text from -----BEGIN CERTIFICATE REQUEST---- through ---- END CERTIFICATE REQUEST ----.

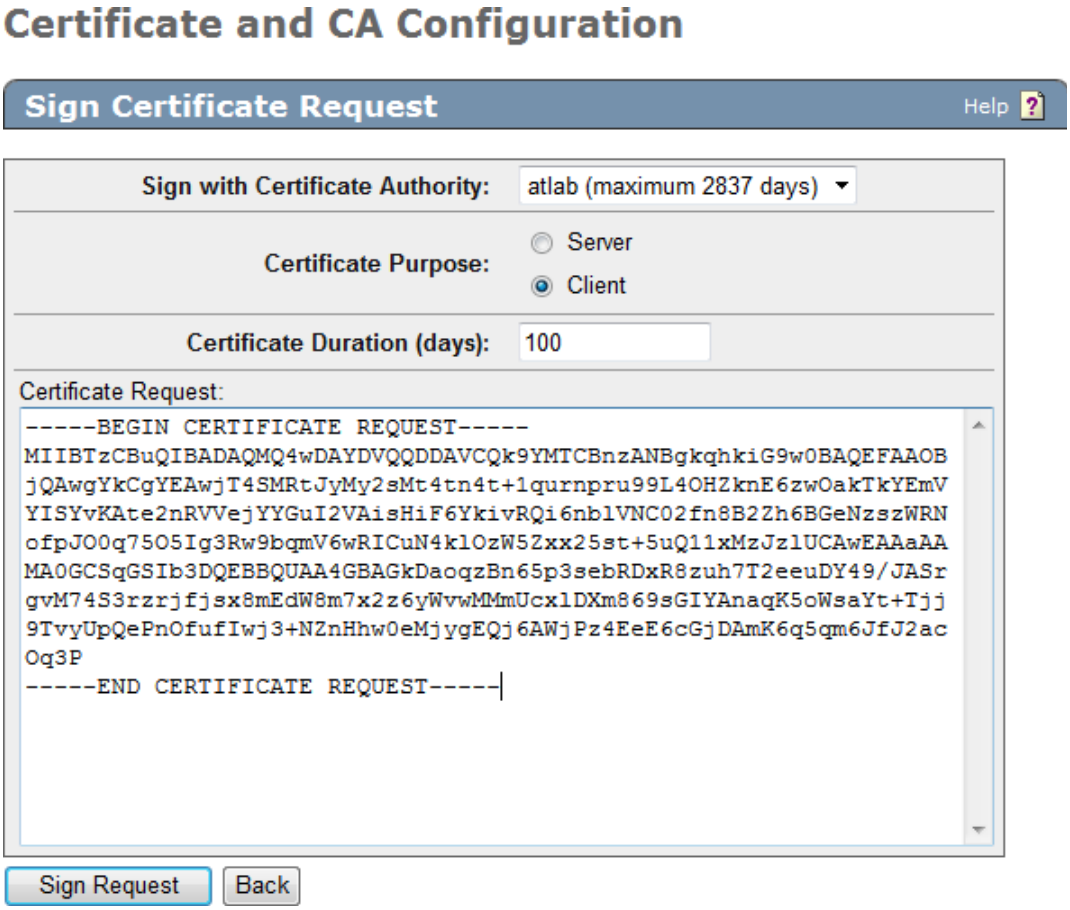
B) Sign Client certificate request with the local CA:

a. Log onto the Enterprise Secure Key Manager UI as admin. On the Security tab, select Local CAs.

b. Select the trusted local CA and click **Sign Request**:

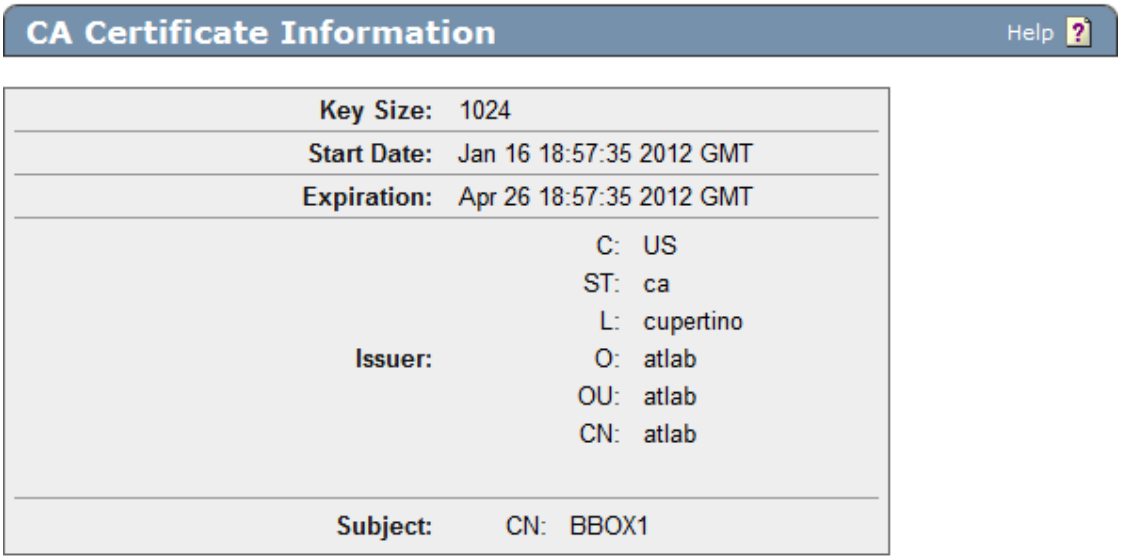


c. Select Client as Certificate Purpose. Paste the copied certificate request into the Certificate Request box.



d. Click Sign Request. The Key Manager signs the Client certificate request with the Local CA and displays the signed Client certificate:

Certificate and CA Configuration



C) Select and copy the signed Client Certificate text from -----BEGIN CERTIFICATE ---------- through -----END CERTIFICATE ---- --. (Or use download).

1. Create a file named ClientCert.pem and paste the signedcertificate containing ..... (or rename the downloaded file).
2. Download the CA certificate and name the file CACert.pem.
3. Move the 3 files: ClientKey.pem, ClientCert.pem and CACert.pem to the designated TSL configuration file locations.
4. The file REQ-ClientCert.pem can be deleted.

Add the Key Manager in the BackBox Configuration

This activity should be accomplished by the (Third Party) Security Authority user. The Security Authority user should have a NonStop user account with enough privilege to modify the BackBox Domain configuration.
Log on to the BackBox UI interface.

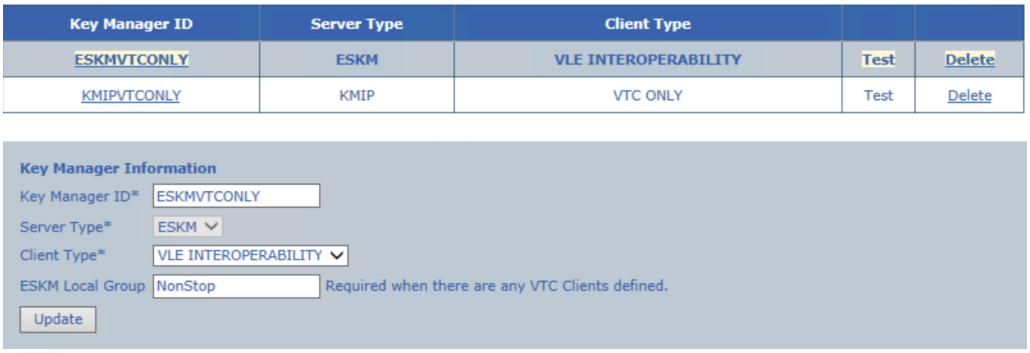
- Select the Configuration menu and select the Switch to Edit mode.
- Select the Key Manager tab.
- Select the targeted Key Manager ID. If the Key Manager entity doesn't exit, you will need to create one first. Click on the Create Key Manager button and fill in Key Manager information:
  - Choose an alias name and type it in the Key Manager ID file.
  - Set the Server Type in accordance with the Key Manager model. (ESKM or KMIP).
  - Set the Client Type according to Client connectivity purpose and Key Manager model. For Server Type

ESKM, the Client type can be either VTC ONLY or VLE INTEROPERABILITY. For Server Type KMIP, Client Type: VTC ONLY.

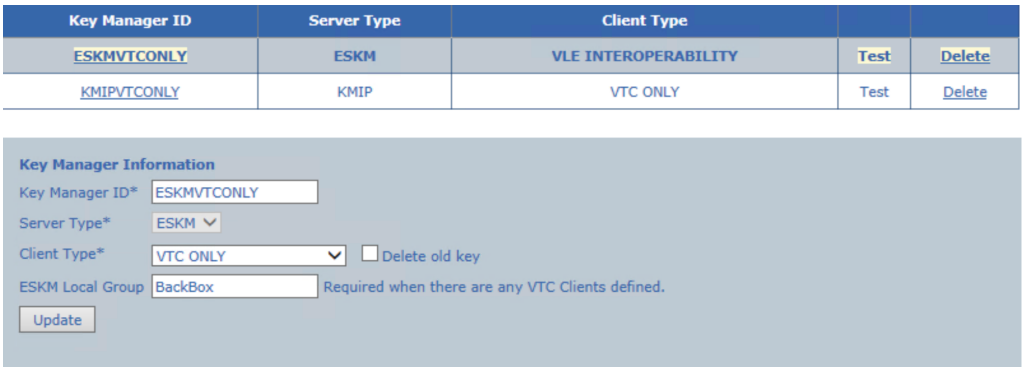
- Enter the Key Manager IP port where the VTC Client can reach the server (KMIP only).
- Add all IP Addresses that the VTC Client can use to reach the server. If a connection fails using the first address, the VTC Client will attempt to connect using the next one, until the list is exhausted (KMIP only).

> Some Key Manager servers, work in cluster mode. IP addresses of each member of the cluster can be added to the list.

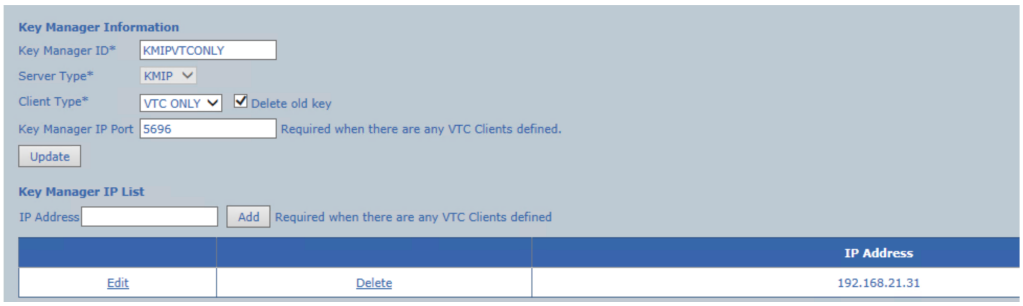
- When Client Type is VTC ONLY, the optional check box Delete old key id is available. This optional field enable/disable automation of deletion of encryption key when data expired.
- When Server Type is ESKM, a supplemental field must be provided (ESKM Local Group.) Enter the Local Group name that the VTC Client is part of. Depending on the Client Type value set, the field will be set with a default name to NonStop (VLE INTEROPERABILITY) to be able to work with NonStop VLE. The value entered could be changed if other group names are used instead of a default name.



ESKM VLE Key Manager Information



ESKM VTC ONLY Key Manager Information

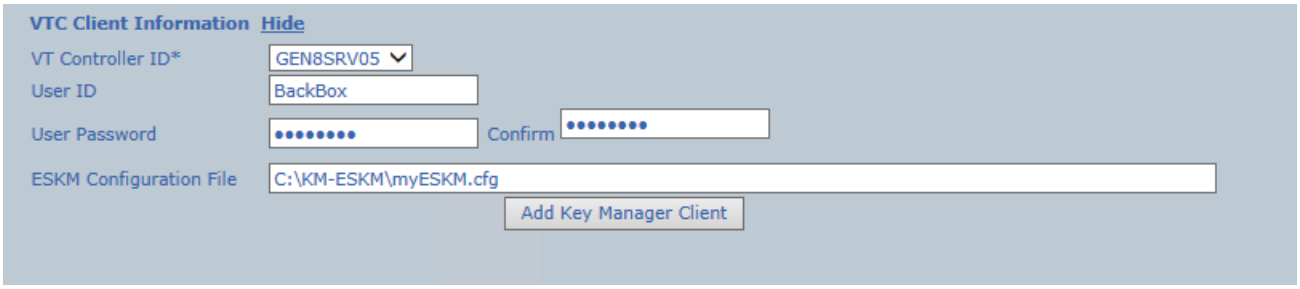


KMIP VTC ONLY Key Manager Information

Add VTC Client Information in the BackBox Key Manager

⚠	You need to have configured Data Store WINDISK with VTC Route to be able to add VTC Client in the Key Manager Configuration.

- ESKM VTC Client (VTC ONLY or VLE INTEROPERABILITY)



Switch to Edit Mode and select the Add link from the VTC Client Information section and:

- Select a VT Controller ID in the drop-down list.
- Attention: Check the displayed number of Encryption Devices: a VTC must be licensed for at least one encryption device to be functional.
- Enter the User ID to be used by the VTC to log in to the Key Manager.
- Key Manage Configuration Info, such as IP address and Port number of the Key Manager) need to be defined
- inside the ESKM Configuration File
- Repeat for all other VTC Clients that need to be attached to the Key Manager ID.
- Click on the Save configuration when done.

User can define the parameters for the communication between the client and the Key Manager server in the ESKM Configuration File IngrianNAE. See the properties below:

ESKM Configuration File

```
#
# NOTE: Do not use quotes when specifying values in
this file. #


#[Version]
# Version of the properties file for the Ingrian
PKCS#11/ICAPI/MSCAPI/.NET # providers.
#
# Do not modify this
property. #
Version=2.4


#[Network
Configuration] #
[NAE Server IP]
# The IP address and port of the NAE
server. #
# Multiple IPs can be specified when load balancing is used. The
port must # be the same on all NAE servers. You can configure up
to three tiers of
# NAE servers. Tiers are numbered 1-3. If all servers in the primary
tier 1 # become unreachable, the client will switch to tier 2. If all
servers
# in tier 2 become unreachable, the client will switch to tier
3. When # using an alternate tier, the client will periodically
try to switch
# back to tier 1 (after Connection_Retry_Interval has
expired). #
# For all tier-aware parameters, the tier is indicated with a
trailing # .n after the parameter name, i.e.
NAE_IP.1=127.0.0.1
# Setting the parameter with no tier sets the default value for all
 tiers. # i.e. Connection_Timeout=600000 sets Connection_Timeout for
all tiers while # Connection_Timeout.1=700000 sets
Connection_Timeout for tier 1.
# A tier-specific setting will
override #
# For NAE_IP, IPs are separated by
colons, e.g., #
192.168.1.10:192.168.1.11:192.168.1.12
#
```

```
NAE_IP=63.80.93.150

# #[Network
Configuration] #
[NAE Server Port]
# NAE_Port is tier-aware
# Do not set the port value to 9443 because this is the port
typically used # to connect to the management console.
NAE_Port=9000

#[Network
Configuration] #
[Protocol]
# The protocol used between the client and the NAE
server. #
# If you are load balancing across multiple NAE servers, the
protocol must # be the same for each server.
# Protocol is
tier-aware. #
# Valid values:
tcp, ssl. #
Default: tcp
#
Recommende
d: ssl #
Protocol=tcp


#[Connection
Configuration] #
[Persistent
Connections]
# Enable or disable persistent
connections. #
# If enabled, the client will use a pool of persistent connections
to the # NAE server. If disabled, a new connection will be created
and then
# closed for each
request. #
# Valid values:
yes, no. #
Default: yes
#
Recommende
d: yes #
Use_Persistent_Connections=yes


#[Connection
Configuration] #
[Connection Pooling]
# The maximum number of connections in the persistent
connection pool. #
# This value is used only when persistent connections are
enabled. # Size_of_Connection_Pool is tier-aware.
#
#
Default
: 300 #
Size_of_Connection_Pool=300


#[Connection
Configuration] #
[Connection Timeout]
# The timeout when connecting to the NAE
server. #
# The timeout is specified in milliseconds. The client will wait
for the # specified number of milliseconds when trying to
connect to each NAE
#
se
rv
er
.
#
# Setting this value to 0 uses the system connect()
timeout. #
# Caution: Setting this value too low may cause connections to
fail when # the NAE servers and/or network are under load. Do
```

```
not change it unless # you really need to.
# Connection_Timeout is
tier-aware. #
#
Default:
60000 #
Connection_Timeout=60000


#[Connection
Configuration] #
[Connection Idle
Timeout]
# The time a connection is allowed to be idle in the
connection pool # before it gets closed automatically by the
client.
#
# The timeout is specified in milliseconds. The client will check
how long # each connection has been idle for. If the time has
passed the value
# specified here, the client will close the connection and remove
it from # the connection pool. To be effective, this setting must
be less than the # Connection Timeout setting in the NAE Server
Settings section in the
# Management Console of the NAE
server. #
# Setting this value to 0 is equivalent to an infinite
timeout. # Connection_Idle_Timeout is tier-aware.
#
# Default:
 600000 #
Connection_Idle_Timeout=60


0000 #[Connection


Configuration]



# [Connection Retry]
# The amount of time to wait before trying to reconnect to a
disabled # server.
#
# The retry interval is specified in milliseconds. If one of the NAE
# servers in a load balanced configuration is not reachable,
the client # will disable this server, and then wait for the
specified number of # milliseconds before trying to connect to
it again.
#
# Setting this value to 0 is equivalent to an infinite retry
interval # (meaning the disabled server will never be brought
back into use). # Connection_Retry_Interval is tier-aware.
#
# Default:
 600000 #
Connection_Retry_Interval=600000


#[Connection
Configuration] #
[Unreachable Server
Retry]
# The amount of time to try establishing a connection if all
servers # in the pool become unreachable.
#
# The retry period is specified in milliseconds. An error is returned
# after the specified period if no server in the pool becomes
reachable. # If logging is enabled, error messages will be
logged to the log file. #
# Setting this value to -1 is equivalent to an infinite retry
period. The # client will keep trying to connect to a server in
the current tier
# until a connection is
established. #
# Setting this value to -1 is not compatible with multi-tier load
# balancing because the load balancer will never switch to the
secondary # or tertiary pools. If multi-tier load balancing is
enabled (i.e., if # NAE_IP[2] is set to one or more IP
addresses) then set this value
```

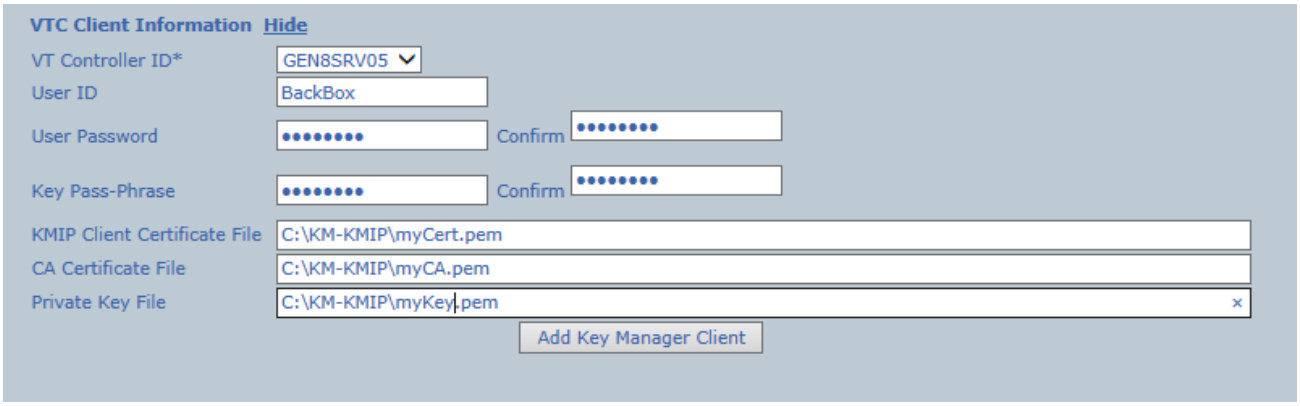
```
# to a number between one and two times the
Connection_Retry_Interval.  #
# Unreachable_Server_Retry_Period is
tier-aware. #
#
Default
:60000 #
Unreachable_Server_Retry_Period=60000

#[Connection Configuration]
#  [Maximum_Server_Retry_Period]
# The total amount of time to spend trying to make connections on
all tiers. # This value only has meaning when using multi-tiered
load balancing.
#
# If this value is set to -1 (try forever), the connection manager
will try # every server on every tier continually, until one
answers.
#
# If set to 0, it is
disabled. #
# If this value is enabled, the connection manager will try to make
connections # for at least Maximum_Server_Retry_Period milliseconds but
will return
# an error if no connection can be made on the tier in
use when # Maximum_Server_Retry_Period expires.
#
# In all cases, the Unreachable_Server_Retry_Period for a given
tier must # expire before the connection manager switches to the
next tier.
#
# Default: 0
(disabled) #
Maximum_Server_Retry_Period=0

#[Connection Configuration]
#  [Cluster_Synchronization_Delay]
# The total amount of time to spend trying to make requests
on keys # go to the same device the key create or latest key
modify went to. #
# A device tries to replicate key information to other
devices in the # cluster after it completes a key create or
modify request.  Until # that replication completes, requests
on the key need to go to the


# device pushing the
replication. #
# If replication fails, the device waits for 30 seconds, then
# tries again.  If three replications fail, the device stops
trying # to replicate data.
#
# The default is 100 seconds: 3 times 30 seconds plus a few extra
# seconds per try for network latency.  For larger clusters
additional # time may be needed.
#
# Disable the function: 0
seconds #
# Default: 100
seconds #
Cluster_Synchronization_Delay=100

#[Connection
Configuration] #
[EdgeSecure Name]
# Name of device or file containing the name of an EdgeSecure
device. #
# The name of an EdgeSecure device is a unique value
assigned # by the administrator to define a single
device.
#
# If the name refers to a readable file, then the first line in
the file # defines the name of an EdgeSecure device.  This
allows all properties # files stored on different platforms to
be the same and still allow
# each platform to refer to a different EdgeSecure
device. #
#
Default
: none #
```

```
#EdgeSecure_Name=


#[SSL/TLS
Configuration] #
[Cipherspec]
# The SSL/TLS protocol and encryption algorithms
to use. #
#  Default  is  "HIGH:!ADH:!DH:!DSA:!EXPORT:RSA+RC4:RSA+3DES:RSA+AES"
# which translates to high-strength RSA key exchange and RC4,
triple DES, # or AES.
# Cipher_Spec is
tier-aware. #
#  Default:
HIGH:!ADH:!DH:!DSA:!EXPORT:RSA+RC4:RSA+3DES:RSA+AES  #
#Cipher_Spec=HIGH:!ADH:!DH:!DSA:!EXPORT:RSA+RC4:RSA+3DE
S:RSA+AES


#[SSL/TLS Configuration]
# [CA Certificate for Server Authentication]
# The CA certificate that signed the NAE server certificate
presented to # clients to establish SSL connections.
#
# If you are using SSL between the client and server, you must
specify a # path to the CA certificate that signed the NAE
server certificate. If # the client cannot validate the
certificate presented by the NAE server,
# the client will not be able to establish an SSL connection with
the NAE # server.
#
# You should provide the path and file name of the CA
certificate. The # path can be absolute or relative to the
application. Do not use quotes # when specifying the path, even
if it contains spaces.
# CA_File is
tier-aware. #
# No
defau
lt. #
CA_File=


#[SSL/TLS
Configuration] #
[Client
Certificate]
# The client certificate to present to the NAE
server. #
# This value is required when client certificate authentication is
enabled # on the NAE server. The certificate must be in PEM
format. If this value # is set, the certificate and private key
must be present even if the NAE # server is not configured to
request a client certificate.
#
# You should provide the path and file name of the client
certificate. The # path can be absolute or relative to the
application. Do not use quotes
# when specifying the path, even if it contains
spaces. # Cert_File is tier-aware.
#
# No
defau
lt. #
Cert_File=


#[SSL/TLS
Configuration] #
[Client  Private
Key]
# The private key associated with the client certificate
specified in # Cert_File.
#
# This value is required when client certificate authentication is
enabled # on the NAE server. The client private key must be in
PEM-encoded PKCS#12 # format. If this value is set, a correctly
formatted key and certificate # must be present.
#
```

```
# You should provide the path and file name of the private key.
The path # can be absolute or relative to the application. Do
not use quotes when # specifying the path, even if it contains
spaces.
# Key_File is
tier-aware. #
# No
defau
lt. #
Key_File=


#[SSL/TLS Configuration]
# [Client Private Key Passphrase]
# The passphrase to unlock the client private key specified in
Key_File. #
# This value is required when client certificate authentication is
enabled # on the NAE server. Since the value is in the clear, this
properties file # must have its permission restricted so that it
can be read only by the
# applications that are to have legitimate
access to it. # Passphrase is tier-aware.
#
# No
defau
lt. #
Passphrase=


#[Logging
Configuration] #
[Log Level]
# The level of logging that will be performed by the
client. #
# The log level determines how verbose your client logs are. You can
# disable logging by selecting NONE; however, it is recommended
that you # set the log level to MEDIUM. A log level of HIGH can
create a very large # log file. Set the log level to HIGH to
troubleshoot  configuration
#
prob
lems
. #
# Valid values:
#     NONE      - nothing is logged
#     LOW       - only essential events are
 logged #       MEDIUM    - some events
are  logged
#     HIGH      - many events are
 logged #
# Default:
 MEDIUM #
Log_Level=MEDIUM


#[logging
configuration] #
[log file]

# the location of the log file the client will
create. #
# you should provide the path and file name of the log file. the
path can # be absolute or relative to the application. do not use
quotes when
# specifying the path, even if it contains
spaces. #
# default: logfile (created in the current
directory) #
Log_File=logfile


#[Logging
Configuration] #
[Log Rotation]
# The log rotation
method. #
# This value specifies how frequently the log file is
rotated. #
# Valid values:
#     Daily     - log file is rotated once a day
#     Size      - log file is rotated when it exceeds
```

```
Log_Size_Limit #
#
Default:
Daily #
Log_Rotation=Daily


#[Logging
Configuration] #
[Log Size]
# The maximum log
file size. #
# If Log_Rotation=Size, the log will be rotated after it
reaches the # specified size. This value is only used when
Log_Rotation=Size.
#
# The size may be specified in bytes, kilobytes (using 'k' or
'K'), or # megabytes (using 'm' or 'M'). One kilobyte is 1024
bytes, and one
# megabyte is 1048576
 bytes. #
#
Default
: 100k #
Log_Size_Limit=100k
```

KMIP VTC Client



Switch to Edit Mode and select the Add link from the VTC Client Information section and:

- Select a VT Controller ID in the drop-down list.
  Attention: Check the displayed number of Encryption Devices: a VTC must be licensed for at least one encryption device to be functional.
- Enter the User ID to be used by the VTC to log in to the Key Manager.
- Enter the Password to be used by the VTC to log in to the Key Manager.
- Enter the Key Pass-phrase required by the VTC to access the private key for the TLS/SSL communication channel with the Key Manager.
- Enter the TLS Configuration File Locations where the digital certificate and private key have been installed. (ClientCert.pem, ClientKey.pem and CACert.pem).
- Repeat for all other VTC Clients that need to be attached to the Key Manager ID.
- Click on the Save configuration when done.

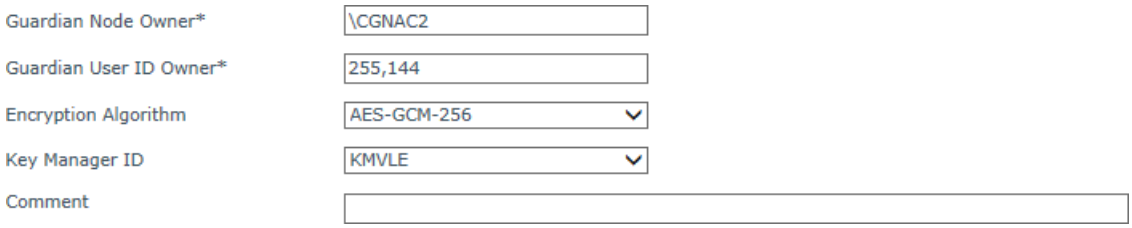
Encryption in a Volume Group

Attention: Toggling encryption ON and OFF affects subsequent usage of the virtual volume member of the Volume Group. To avoid disabling the tape encryption by mistake it is recommended that the number of users who can update the BackBox configuration be kept to a minimum.
Attention: Encrypting data will protect the data from external system access, but it will not protect the access to media from a tape application running in the NonStop. If user segregation needs to be carried out, Control Access from the Volume Group with advanced attributes should be enabled.
Log on to the BackBox UI interface.

- Select the Configuration menu and select the Switch to Edit mode.
- Select the Volume Group tab.
- Select or Create a Volume Group ID.
- In the Class Information:

  - Select the AES-GCM-256 in the Encryption Algorithm drop down list box.

- Select the target Key Manager ID from its drop down list box.



- If the setup is for VLE, the Volume Group Media Type must be LTO 4.

Important: If you already have a Volume Group that you have been using and want to encrypt the content on its media from now on using VLE-CLIM Client, you can simply modify its Media Type to LTO 4.
From that point on, all new uses of SCRATCH volumes in the Volume Group (such as for new backups) will mount as LTO 4 media to be encrypted. Existing ASSIGNED media will also be mounted as LTO 4 and be read by NonStop applications, such as RESTORE, even if not encrypted. If the Volume Group uses the DSM/TC tape catalog, the following MEDIACOM command must be performed on the Pool associated with that Volume Group:

```
MEDIACOM
> ALTER POOL vt-pool-name, TYPE ANY
> ALTER TAPEVOLUME *, POOL vt-pool-name, TYPE LTO 4
```

- Click on the Update Volume Group button at the very bottomof the page.
- Repeat for other required Volume Groups.
- Click on the Save link.

Test BackBox Software Encryption Configuration

Good Practice: Validate encryption configuration before trying to do the real encryption. For a Key Manager ID, the overall configuration and the connectivity to the key server is verified by clicking the Test link on the Configuration Key Manager page.

USER INTERFACE CONFIGURATION FOR TAPE ENCRYPTION

VT Controller

Key Manager

The Key Manager is an external server generating and storing encryption keys; the encryption itself being processed in the BackBox VTC for all configuration types.
The Key Manager must be configured even for VLE Encryption.

- For VLE, the Key Manager configuration is used to control the encryption configuration during Operations and to clearly identify the key server storing the encryption keys.
- For non-VLE Encryption, the Key Manager configuration is also used to identify and secure a network path to the key server.

It is possible to configure more than one Key Manager instance, each describing the server holding the encryption keys for different groups of tape volumes.

ESKM only

- ESKM Configuration File – Path to the NAE properties configuration file that defined Certificate, CA, Private KEY and Passphrase.

KMIP only

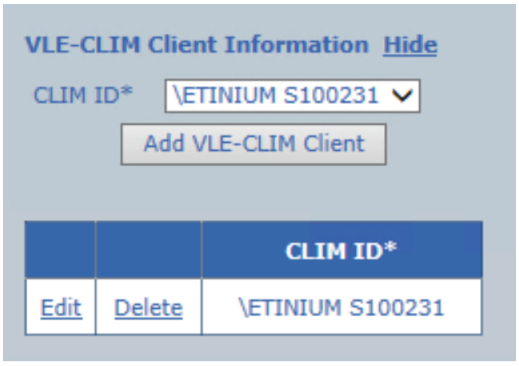
- Key Pass-Phrase - Enter the key passphrase for the private key file and confirm it by re-entering it in the field
- KMIP Client Certificate File – Certificate file used to establish the SSL connection and the Key Manager server (refer to your IT support team to have the file generated)
- CA Certificate File – Enter the CA Certificate File
- Private Key File – Private key file used for the SSL connection between the client and the Key Manager server.

Click 

button at the bottom of the page to finish up the Key manager setting up. Details on the Key Manager setting will be displayed in a table like the one below.

Key Manager – VLE CLIM Clients

When the Encryption keys are managed by the Storage CLIMs for VLE processing, the CLIMs hosting the LTO 4 virtual tape drives must be identified as Clients of the Key Manager in order to identify which Key Manager holds the Encryption key of each volume. The current list of VLE CLIM Clients is presented on the Key Manager page. New CLIMs can be added by clicking on the button Add VLE-CLIM Client.



CLIM ID: Select a CLIM in the selection list. The selection list is based on information queried from the host during the VTC configuration of tape drives in the BackBox Domain. The list of proposed CLIMs is limited to those associated with a tape drive of the BackBox Domain, defined as LTO 4, and enabled for VLE by SCF.
If the proposed list is empty or unexpected, check that the tape devices are enabled for VLE in SCF, and refresh the host information in the VTC configuration page of the involved VTCs by the link Update devices based on the probe result from the VTC and all hosts.
The Key Manager connectivity should be tested before testing actual virtual tape Encryption, in any case of Encryption setup – including HPE VLE.
The Key Manager page is shown in the list of configured Key Managers, and the Test link is available when the Configuration tab is in the Browse mode.
The Test will execute several verifications and show the resulting report in a new window.

- The connectivity of all VTC Clients to the Key Manager, will be tested by a query to the Key Manager for its identification and for each of the IP addresses configured for the Key Manager.
- All VTCs in the domain having LTO 4 devices, will be tested to check if the LTO 4 devices are connected to a CLIM recognized as a VLE CLIM Client to the Key Manager.
- The LTO 4 drives must be started to allow BackBox to check the host WWN and compare it to the VLE CLIM Client configuration. If there is a match, the connectivity to the Key Manager from the CLIM will be assumed.
- The domain configuration will then be analyzed to:
  - Detect the Volume Groups using the Key Manager ID.
  - Verify that the VTC routed to the corresponding Data Stores, have the connectivity to the Key Manager.
  - Verify that the VTCs have the Encryption license option for at least one drive.

Key Manager – Test Report
Only those VTCs that actually receive messages, will be shown in the Key Manager Test Report. For each VTC, there can be three sections:

- A section VTC Client showing the report generated by the VTC.
- The report is green for success, orange for any warning not preventing connectivity, and red for a complete lack of connectivity.
- A section VLE-CLIM Client showing a report of counts of FC LTO 4 drives per port and connected host WWN. The report is green for success, orange if no LTO 4 drive is currently connected to a recognized CLIM, and red for a complete lack of connectivity.
- A list of messages pertaining to the VTC.

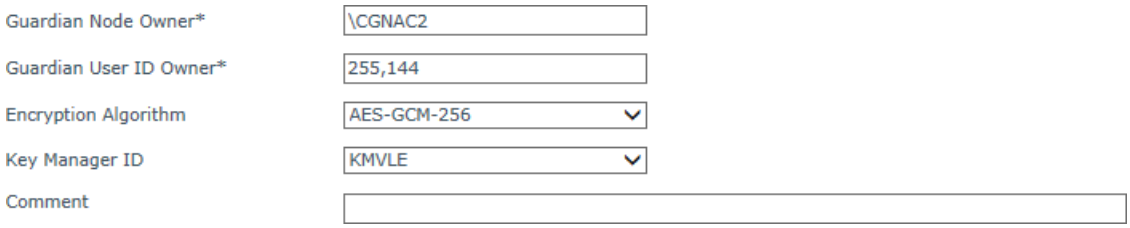
The messages are explained in the BackBox Messages Manual and Troubleshooting
Three Test report samples are presented after the common underlying VTC configuration below, with each sample showing its specific Key Manager configuration page and the associated Test report page:

Volume Group

Encryption

For all setups, the Encryption must be enabled in the Class Information

- Select the AES-GCM-256 in the Encryption Algorithm drop down list box.
- Select the target Key Manager ID from its drop down list box.



A change in this setup will affect further backups, not the restore of backups already written.
If the catalogs (BackBox, DSM/TC and TMF) are replicated on a DR site, it should be noted that the Key Manager ID registered for each volume, will be replicated. Also, the Key Manager IDs of both Primary and Secondary sites must be planned globally.

VLE Setup

For encryption with VLE, the Volume Group Media Type must be LTO 4.

If there is a Volume Group that you have been using, and from now on, you want to encrypt the content of its media using the VLE-CLIM Client, you can simply modify its Media Type to become LTO.
4. From that point on, all new uses of SCRATCH volumes in the Volume Group (such as for new backups) will mount as LTO 4 media to be Encrypted. Existing ASSIGNED media will also be mounted as LTO 4 and be read by NonStop applications, such as RESTORE, even if not encrypted. If the Volume Group uses the DSM/TC tape catalog, the following MEDIACOM command must be performed on the Pool associated with that Volume Group:

```
MEDIACOM
> ALTER POOL vt-pool-name, TYPE ANY
> ALTER TAPEVOLUME *, POOL vt-pool-name, TYPE LTO 4
```

Report OBB038 – List of Encrypted Volumes

OBB038 lists the Encrypted volumes whose label matches a volume label pattern.

Syntax:

```
RUN OBB038 label-pattern
```

Where label-pattern is a specific label or a simple pattern ending by *, ex:

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

Content of OBB038:

```
?tacl macro
COMMENT
**********************************************
******* COMMENT * Extract VOLEXT from
the BackBox catalog                *
COMMENT * and list Encrypted volumes
                                   *
COMMENT  *  One  positional  parameter:  pattern  of
labels          to          select*          COMMENT
**************************************************     RUN
BB010 %1%
```

```
        COMMENT*****************************************
        **************  COMMENT BB038: List the
        BackBox Encrypted volumes * COMMENT
                                  *
        COMMENT Note: The Tandem ENFORM
        reporting tool is required * COMMENT
        ***********************************************
        ****** ASSIGN VOLEXT-REC, VOLEXT
        PARAM LABELS
        %1%
        ENFORM /IN
        BB038/
Sample:

        BB038  Encrypted volumes with label matching *2022-10-24 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  2022/10/27  ASSIGNED  BBOX_21F5BD27VE1001D68095D44B400008_111027202410
        VE1015  2022/10/27  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.	

Volume

Volume Details

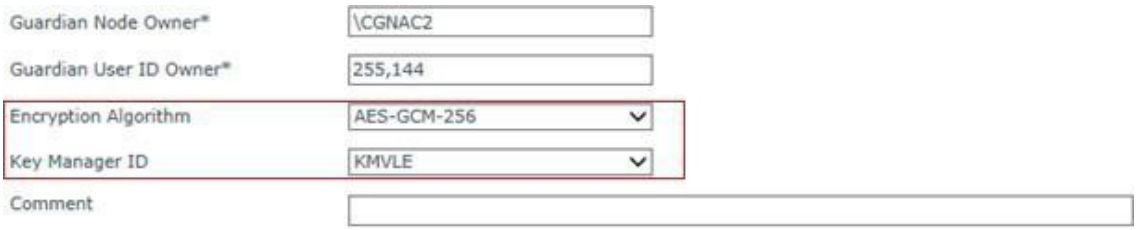
The Encryption state of each volume is registered. The ID of the volume specific key in the Key Manager is included for support to access this key through the Key Manager user interface.

Encryption Algorithm	AES-GCM-256
Key Manager ID	KMVLE
Encryption Key ID	N12804D13CSW005A88CEEE0DD360008_BBBBBBBB_1903131332

Volume Edition

The Encryption attributes of a volume can be updated. Example of use case:

- Volumes manually registered in a Restricted Data store accessing the images of volumes written encrypted in a different environment not linked by the BackBox catalog replication.



Encryption related elements

- Encryption Algorithm (value AES-GCM-256 or None).
  In the case used above, changing None to AES-GCM-256 will enable the decryption when reading the tape volume.
- Key Manager ID: Appears only when the encryption is enabled and is mandatory in thiscase.

This ID names the Key Manager, configured in the current BackBox domain, and this will provide the encryption context for accessing the tape volume.

LARGEBLOCKs SUPPORT

From L17.08 onward, 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.

To MATERIALIZE/VIRTUALIZE physical volume when LARGEBLOCKs are used, set the BLOCK SIZE of physical drive to 1024 KB in the VT Controller Advanced Properties configuration page.

BARE-METAL BACKUP AND RESTORE

⚠	Bare-Metal is a special technique used for both backup and restore that bypasses the NonStop operating system and its basic tape subsystems.

Bare-Metal refers to the re-installation from scratch of a NonStop system that has been corrupted or compromised.

Some NonStop customers are concerned that they will miss their recovery window goal if a major problem corrupts the NonStop operating system to such extent that the system will have to be reinstalled from scratch (Bare-Metal).

The Bare-Metal Backup & Restore procedures are designed to reduce system recovery time-windows.

The purpose of this procedure is to create a disk image backup of the configured basic system and to provide a tool capable of restoring on empty disks, bypassing the NonStop operating system and all its basic tape subsystems.

For more details about the Bare-Metal Back and Restore procedure see Appendix H - Bare-Metal Backup and Restore

STORAGE CLIM

HPE NonStop servers are not directly connected to disk and tape storage devices. To connect to disk and tape devices HPE NonStop servers use storage-CLIMs as interconnection controllers.

Although directly connected to the peripherals, storage-CLIMs are only used as specialized co- processors for I/O in order to reduce the load on the NonStop processors. The drivers controlling the peripherals (tapeIOP) are the ones running on the NonStop processors.

DOMAIN MANAGER

To use BackBox and its capabilities, a domain manager has to be installed on the NonStop.

Domain manager acts as a virtual operator to mount the virtual media.

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 enough 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 BackBox 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 SECUIRTY

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 pass- word 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. This way, the Data Store password is automatically updated by BB004 macro process.

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:

1. Schedule regular backups by the enterprise backup client.
2. 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.

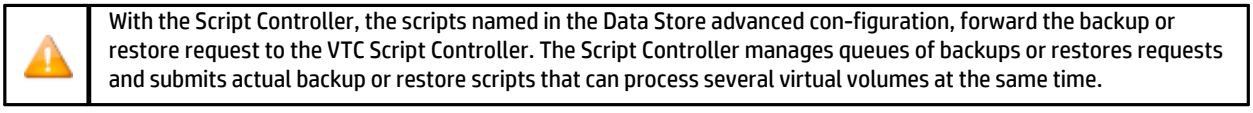
Scripting Facilities

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.



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 con- current 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.

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.
- 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.

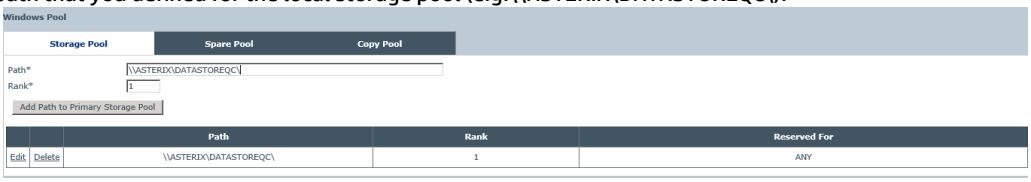
Use the following example for Copy Pool Sync set up:

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

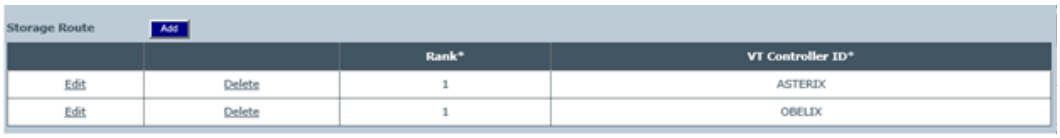
\\ASTERIX\DATASTOREQC\ on the local storage pool

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

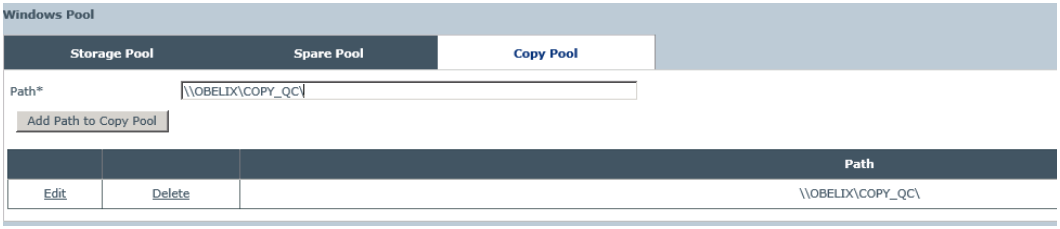
1. To set up the Storage Pool:
   a. Log in as user with Configuration Editable permissions. Go to Configuration > Data Store > click on the Data Store ID where your storage pool has been created and click Switch to Edit Mode.
   b. Scroll down to Windows Pool section and select Storage Pool. In the Path* field put the name of the path that you defined for the local storage pool (e.g.\\ASTERIX\DATASTOREQC\).



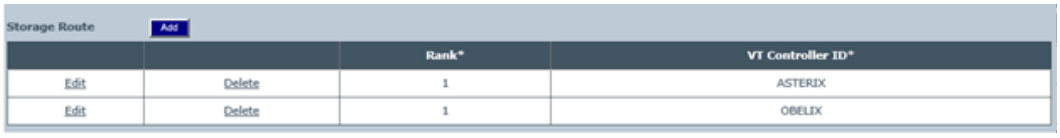
   c. Scroll down to Storage Route section and add one storage route for the local machine (e.g. ASTERIX) and one storage route for the remote machine (e.g. OBELIX).



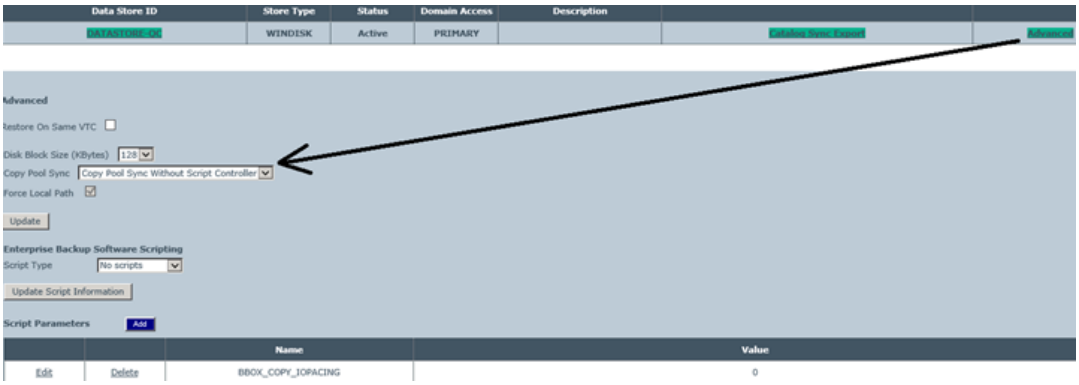
2. To set up the Copy Pool:
   a. In the Windows Pool section, click on Copy Pool and in the Path* field put the name of the path that you defined for the copy pool (e.g. \\OBELIX\COPY_QC\).



   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 check the option for Copy Pool Sync feature, then click Update.



b. Save the configuration

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

To set permissions, see the detailed procedure in the Appendix D - Shared Files Permissions.

VOLUME COLLOCATION

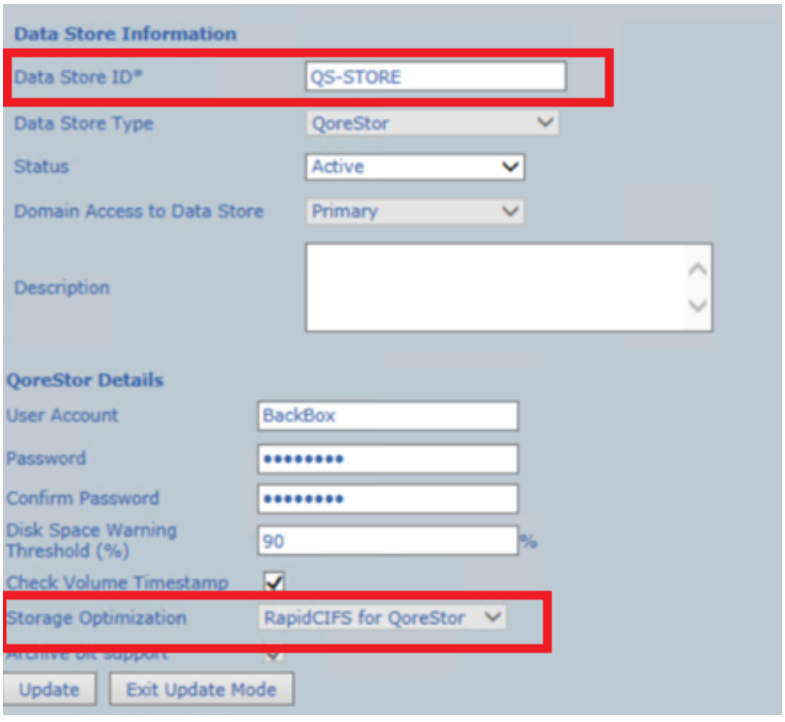
⚠	Volume Collocation applies only to VTC with Data Stores other than QoreStor type or to configure the access to a QoreStor replica in a DR SECONDARY Data Store.

When the Storage Optimization of the Data Store is set as RapidCIFS, 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.

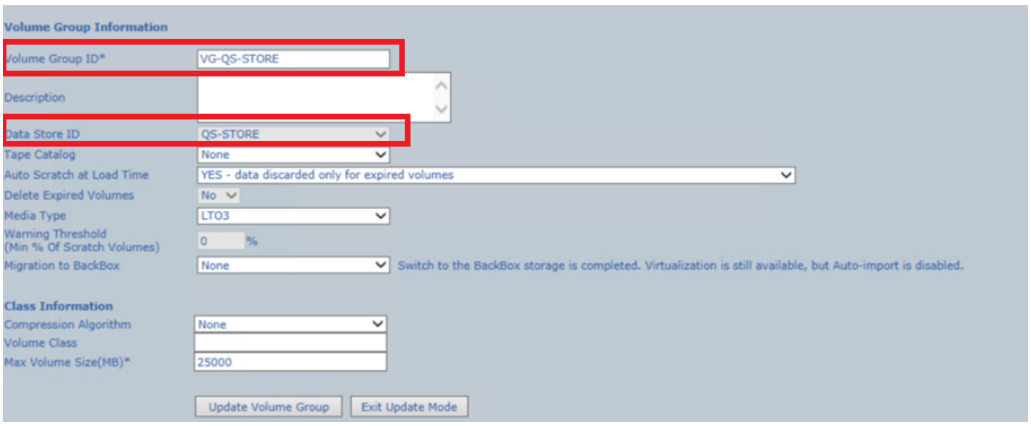
2. Fill out the Data Store Information fields. Select QoreStor as Data Store Type and RapidCIFS for QoreStor for Storage Optimization.



3. Click Add to save the created Data Store.

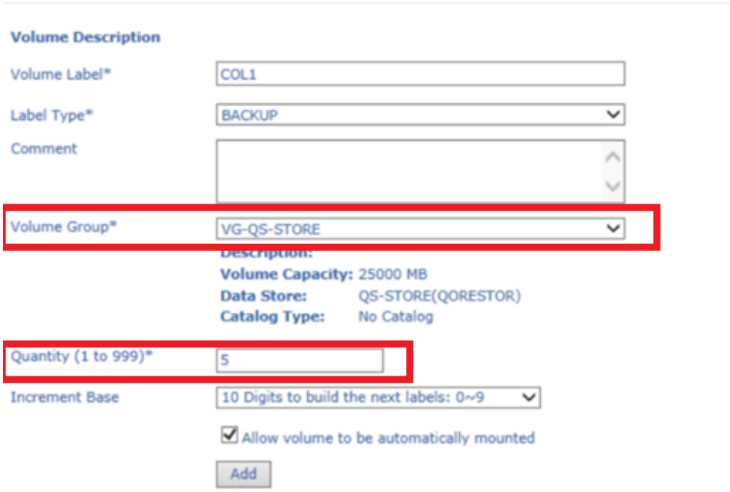
4. Add Path to the Primary Storage Pool and Add Storage Route for the BackBox server. Update the Data Store Information and Save the configuration.

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 you have created before.

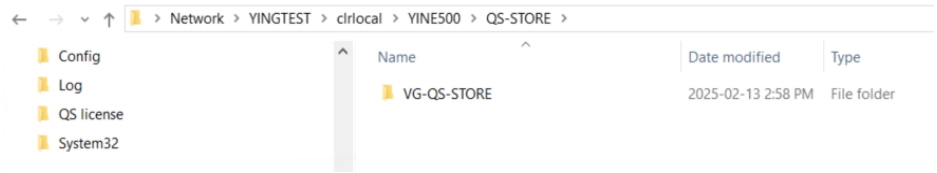


6. Click Add Volume Group and Save the configuration.

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.



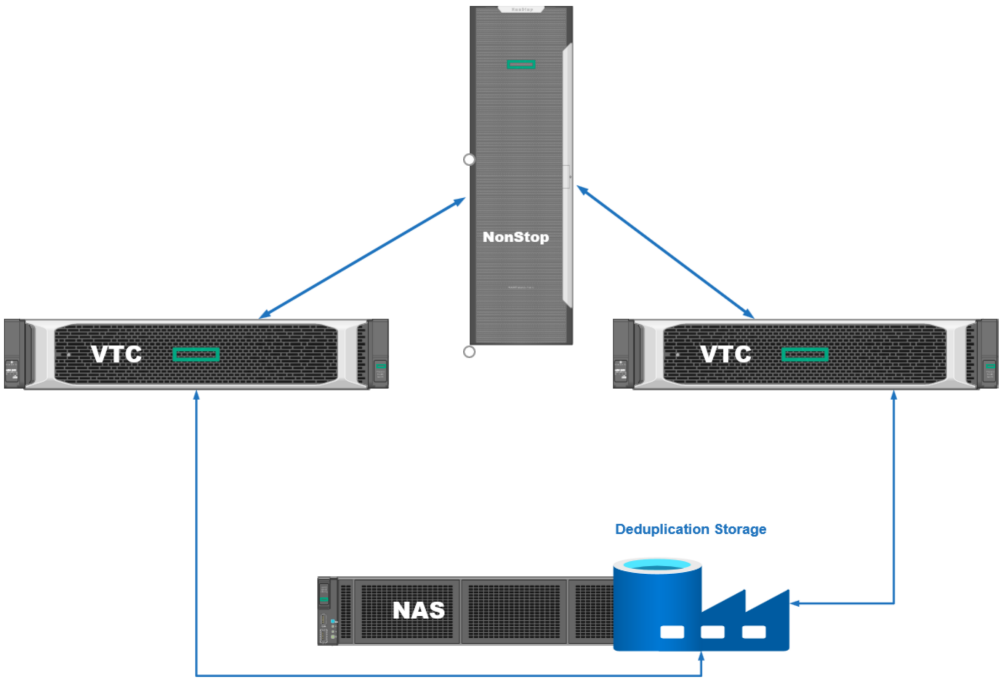
QORESTOR DATA STORE

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.

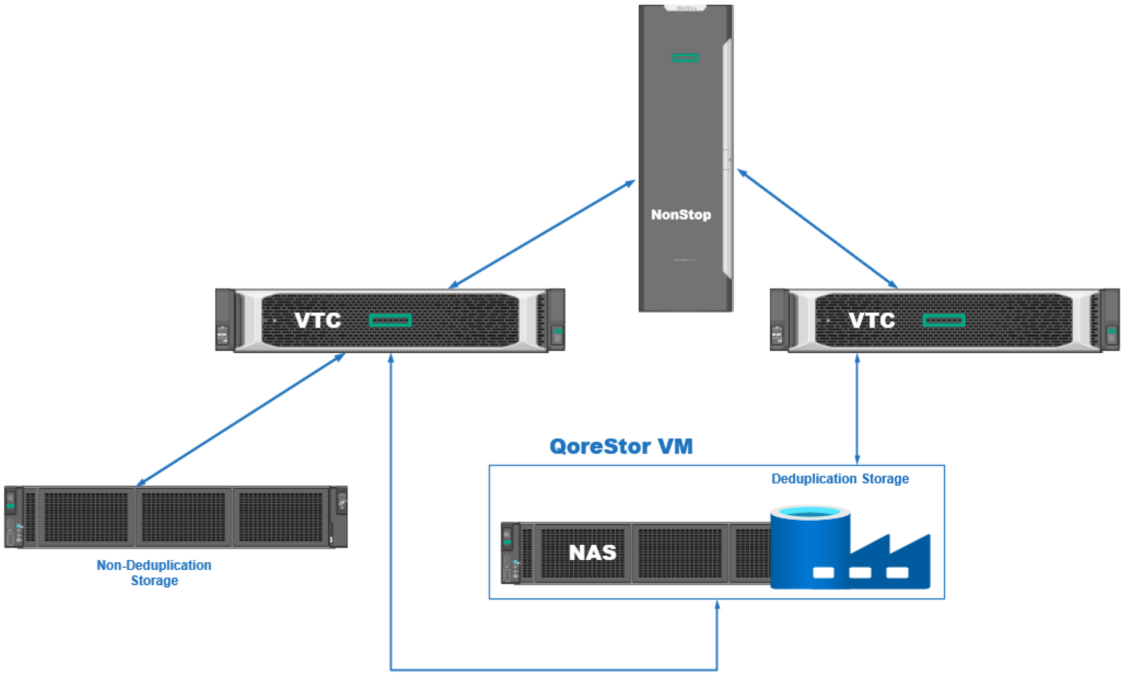
In most cases, a dedicated NAS storage is shared by a pair of VTC connected by FC or iSCSI to a NonStop host (see the diagram below).



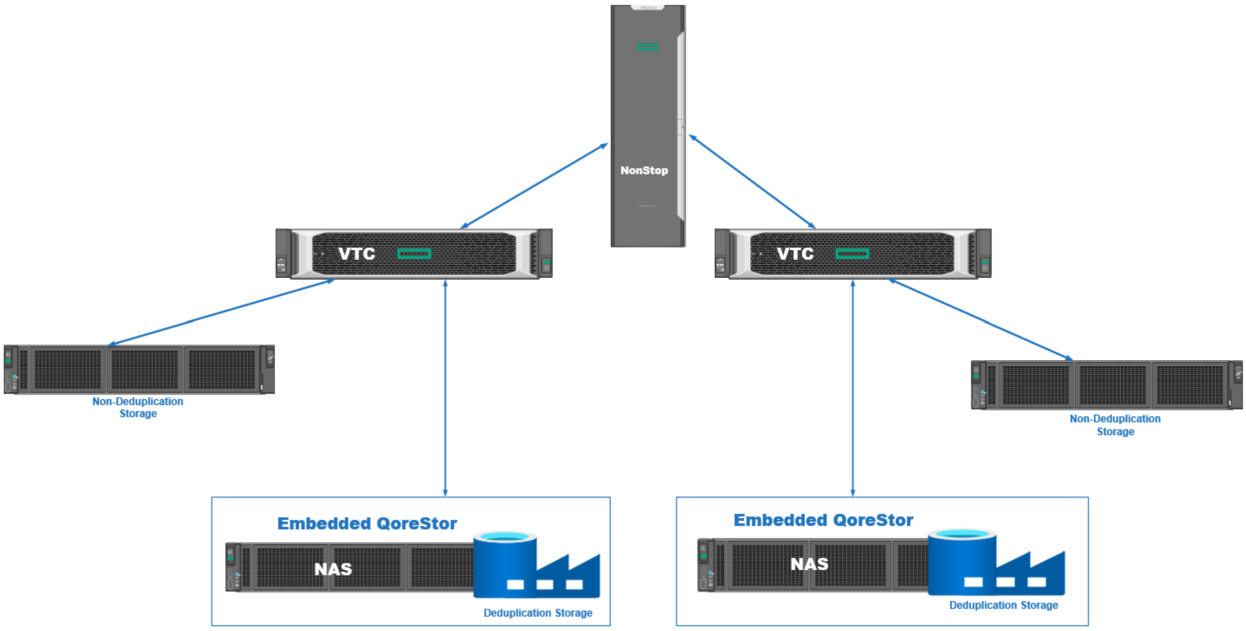
QORESTOR EMBEDDED DATASTORE

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.



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

- an embedded QoreStor
- a corporate QoreStor.

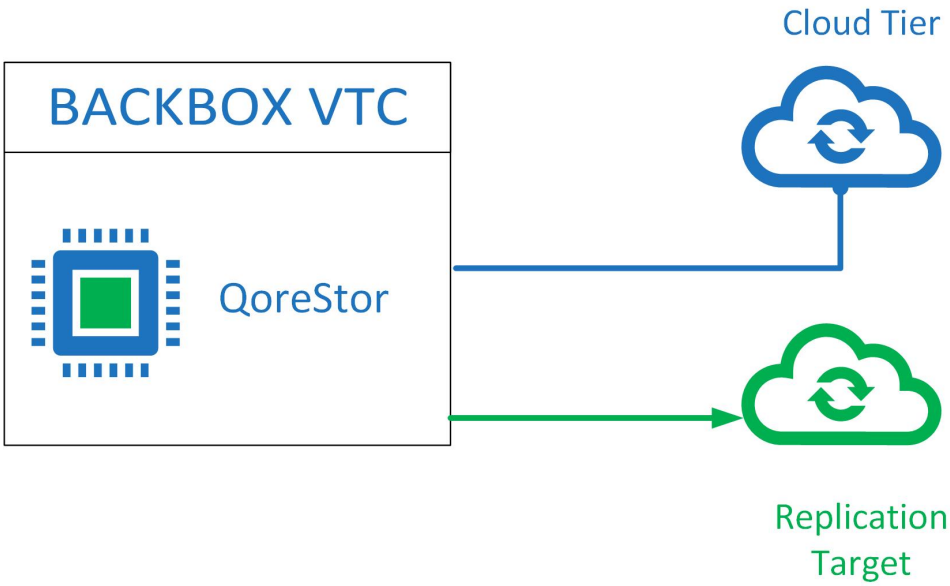
A QoreStor can be used as replication target by multiple sources.

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

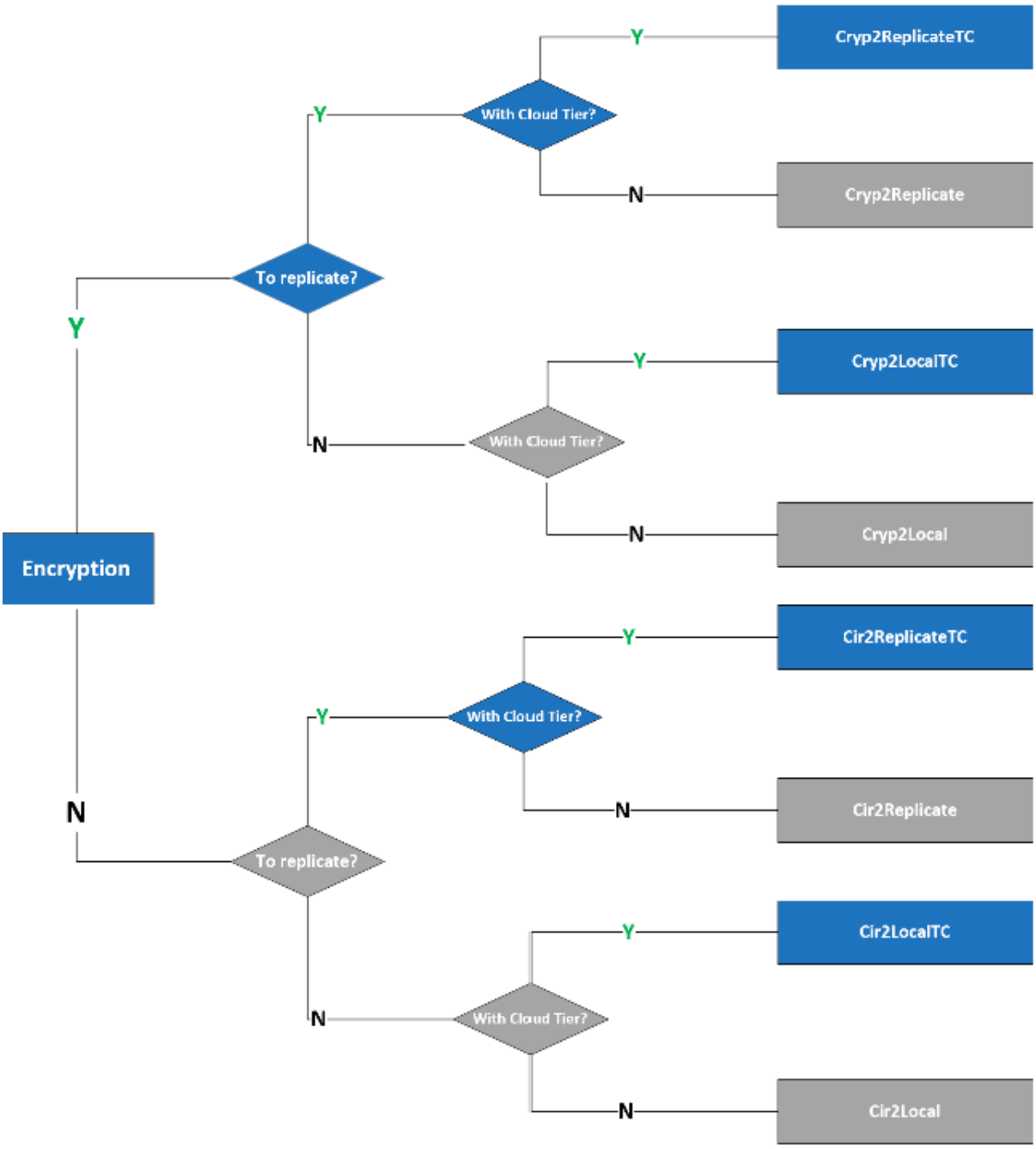
When creating a QoreStor Data Store, different levels of configuration have to be set up (with or without encryption, with or without cloud tiering) in order to establish which QoreStor pre-configured container will be used.

To use Cloud storage expansion, open VTC Management Console to choose the storage Cloud service: AWS S3, Microsoft AZURE, IBM-S3, Google -S3, Backblaze-S3, Wasabi-S3 and S3-Compatible.

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.



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.

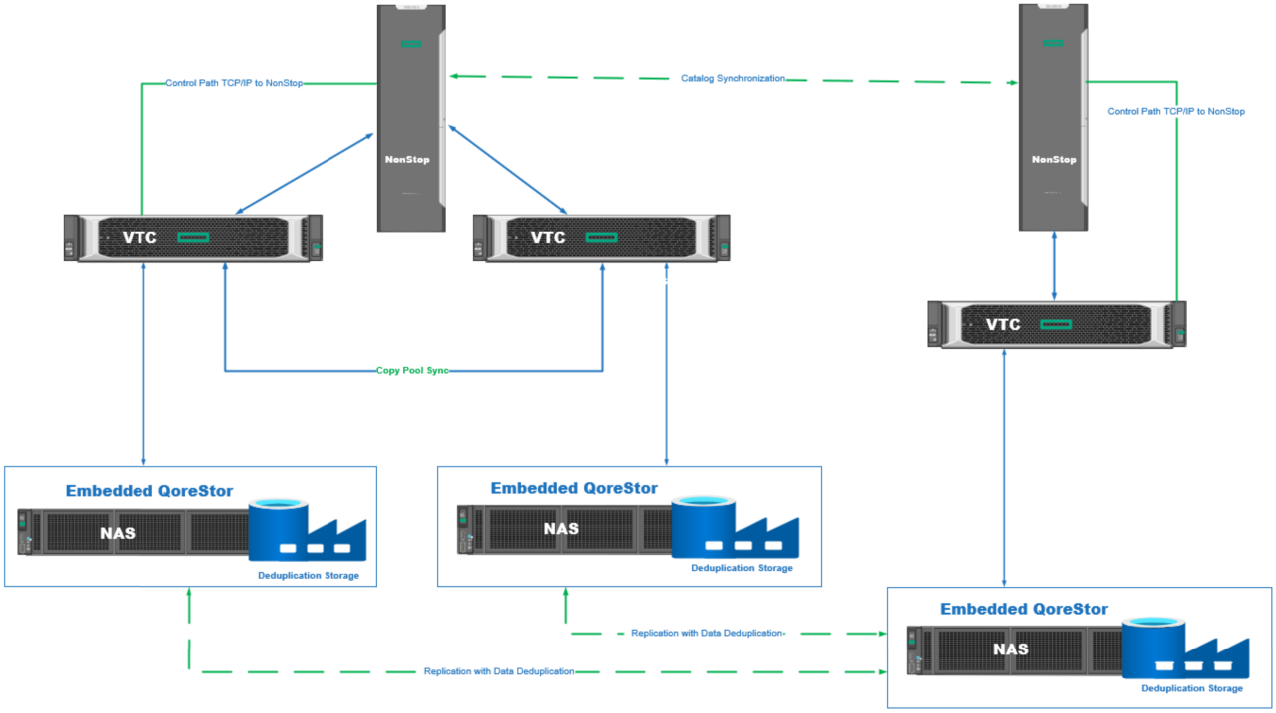
This feature helps identifying tapes below a volume group and setting selective backup policies.

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.



WINDOWS-HOST PHYSICAL STORAGE MONITORING

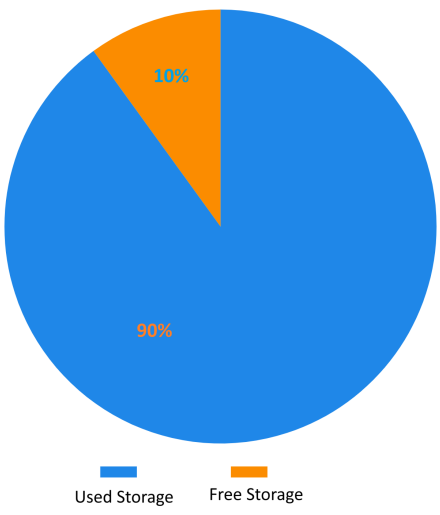
QoreStor physical storage space is monitored to avoid overloading the QoreStor and, therefore, to avoid stopping specific operations due to lack of storage space.

VTC MS monitors the storage and sends a warning message(#6027) when 10% storage capacity has been reached. Yet, replication, copy sync, spare move, migration and backup operations will not be automatically stopped or compromised, even if the warning is flagged.

If no action is taken when warning message is received and the service reaches 5% capacity (error message #6028), the replication, copy sync spare move, migration and backup and backup operations will be stopped in prevention mode. Hence, storage will be tagged as "read-only".

⚠	Restore operations will work without interruptions, even while storage expansion actions are being performed.

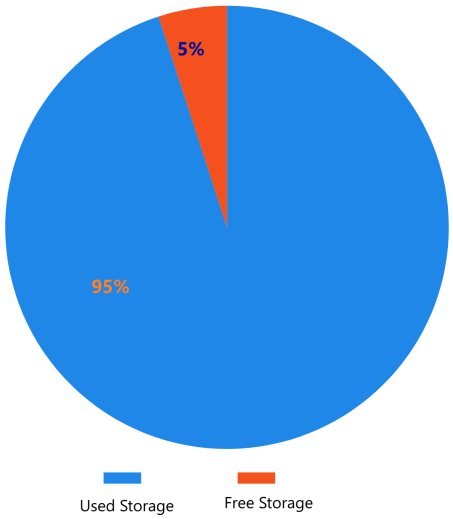
Storage Capacity Threshold Messages



When Windows storage capacity reaches 10% capacity the EMS generates warning message (#6027) output:

```
2025-01-27 21:50                EVENT DETAIL                Page     1   END

 2025-01-27 21:47:58 \INSIDX.$Y7TD ETINET.100.100 6027
 CYNH412-VTC2M2D0R02GM-W6027 There is less than 10% free space left on drive
 X:\. Please free up more space for Qorestor VM running properly. Event
 time:2025-01-27 21:47:52

 Cause:

 Effect:

 Recovery:
```

⚠	Contact your sales representative for physical storage expansion options.



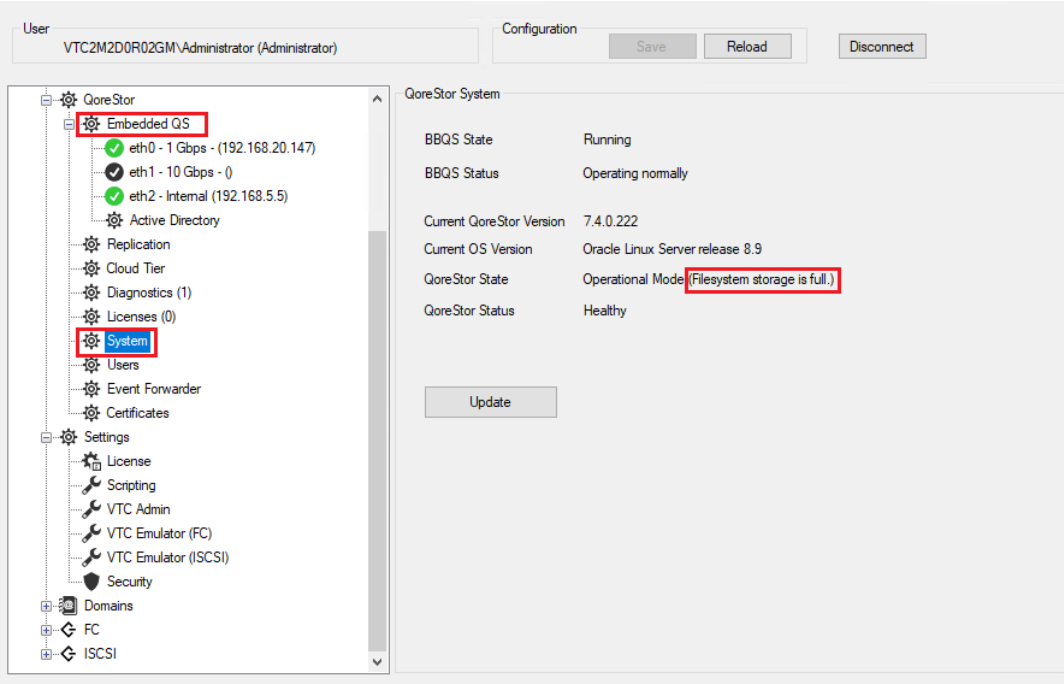
When the storage capacity reaches 5% capacity the EMS generates error message (#6028) output:

```
2025-01-27 23:18                EVENT DETAIL                Page     1   END

 2025-01-27 23:17:45 \INSIDX.$Y8CB ETINET.100.100 6028
 CYNH412-VTC2M2D0R02GM-E6028 There is less than 5% free space left on drive
 X:\. Qorestor VM cannot be used for backup. Event time:2025-01-27 23:17:42

 Cause:

 Effect:

 Recovery:
```

⚠	If storage reaches 5% capacity (error message #6028), the replication, copy sync, spare move, migration and backup operations will be stopped in prevention mode. Hence, storage will be tagged as "read-only".

For details on the above-mentioned warning/error messages, refer to Messages Manual and Troubleshooting.

When physical storage capacity goes below 5% threshold, VTC MC prompts the following error message.



	Contact your sales representative for physical storage expansion options.

For more details on how to manage storage when capacity reaches warning and/or error level, contact ETI-NET Support.

INTERFACES USED WITH QORESTOR

VTCMC

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

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

QORESTOR UI OVERVIEW

The QoreStor UI consists of different sections structured as follows:

- Header panel
- Navigation panel
- Status panel
- Operations panel

Header panel 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 panel with access to the following items:

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

Navigation panel with navigation options for the following action items:

- Dashboard
- Containers
- Local Storage
- Cloud Storage
- Replications
- System
- Diagnostics
- Users
- Events
- Management

Operations panel that displays data and various appropriate dialog related to the chosen navigation option.

Supported software browser versions:

- Mozilla Firefox 67 or later

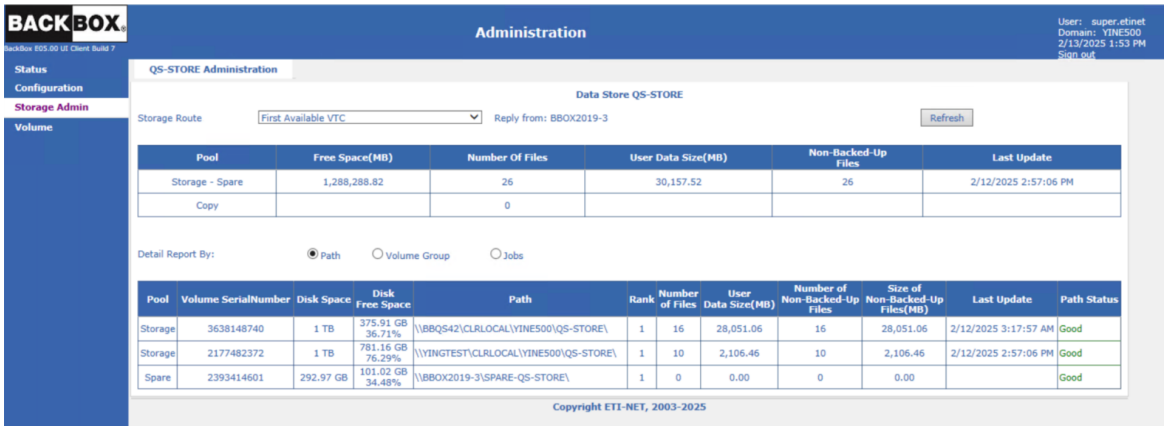
- Microsoft Internet Explorer 11.01
- Microsoft Edge 44 or later
- Google Chrome 75 or later

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:

```
24- 12- 21  20:57:35  \ETINIUM.$Y463  ETINET.100.100  030000
SHE409-BBOX2019-3-I30000 290-QoreStor Repository Cleaner process
stopped as per schedule,

24- 12- 21  20:57:35  \ETINIUM.$Y465  ETINET.100.100  030000
QCH409-BBOX2019-3-I30000 290-QoreStor Repository Cleaner process
stopped as per schedule,

24- 12- 21  20:57:35  \ETINIUM.$Y45X  *ETINET.100.100  010208
SHE409-BBOX2019-3-W10208 VTC license has expired on 2024-12- 16
```

QORESTOR UPDATES

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 VTCManagement 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 deduplication 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 (Cloud Tier) 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 TIVOLI STORAGE MANAGER (TSM) 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 storagemanagement, 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.

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.

```
        4/27/2024 11:17:25 ANE4991I (Session: 1639, Node: QCMONT)

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

Integrity Check for Written Volume(s)

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

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 (set to NO), the last image of the tape volume is presented to the NonStop host.

For more details on Auto Scratch at Load Time settings and configuration, refer to Data Store and Volume Group.

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 BackBox 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:

TMFtapes

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/TCcatalog. 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 BackBox 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 thedaily 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 BackBox 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, theDomain 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 BackBox 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 POOL
      SET   DEFINE  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 Security Volumes Attributes

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.

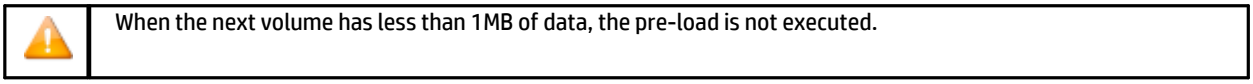
Pre-load applies only to the restore of multi-volume backup sets. It anticipates the next volume load by executing its restore script, while the previous volume is being read by the NonStop.

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.



RESTRICTED DATASTORES

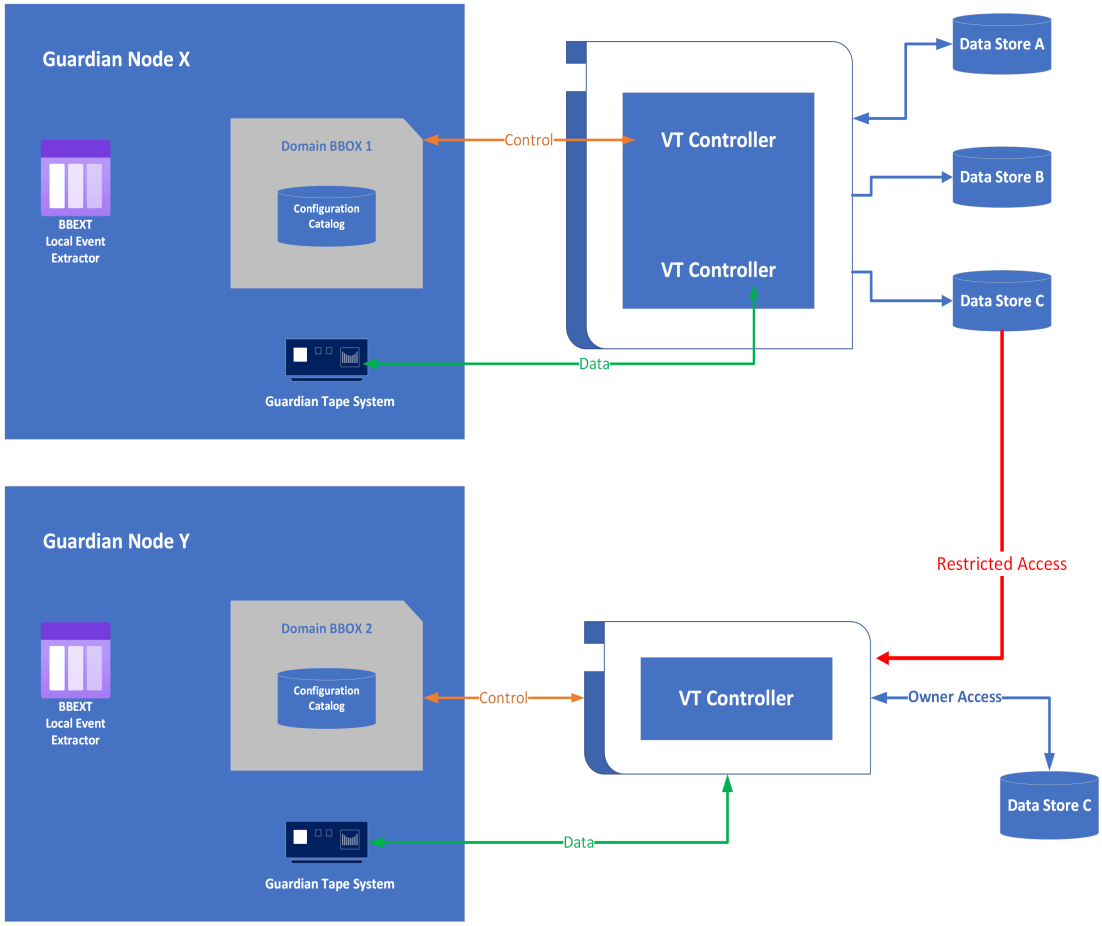
A Restricted Data Store is a view of a Data Store owned by another domain. Restricted Data Store provides read access to virtual volumes owned by another BackBox Domain, most often running on different NSK nodes.

Restricted Data Stores are also a way to manually repopulate the BackBox 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 BackBox domain (Import from tape catalog)
- 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, accessrights 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.

Access Authorizations Notes:

- 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 DataStores. 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 BackBox 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 DATASTORES AND CATALOG REPLICATION

To prepare for disaster recovery, virtual tape volumes must be backed up or replicated. The tape catalogs on NonStop (BackBox 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. BackBox 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, BackBox replicates the entries in the BackBox and DSM/TC catalogs immediately after each backup.

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

The BackBox 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 BackBox 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.

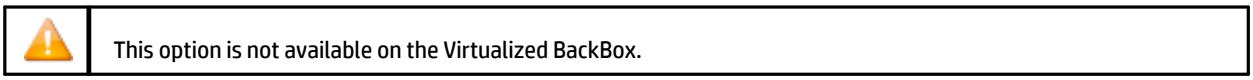
To receive the replicated catalog entries on the secondary site, a Data Store must be configured with SECONDARY domain access in the BackBox Domain on the secondary site.

Refer to the BackBox 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.



CONFIGURATION

The chapter is organized as follows:

Domain Configuration - the main entities defined for a domain configuration.
Special Considerations at Installation - notes on installation procedure
Domain Network - network architecture, structure and port numbers
Tape Catalogs in the NonStop System - tape catalogs and integration
NonStop Access Authorizations - access control to the NonStop resources
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 - reference set for the BBEXT program that automates the tape load.
Procedures for Recovery - backup procedures.

ENTITIES CONFIGURED IN A DOMAIN

The BackBox 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 BackBox 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.
- Key Manager manages the 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 - INSTALLATION

o SPECIFICATIONS FOR MOUNT REQUEST MESSAGES IN EMS

The mount request message issued by $ZSVR in EMS must specify the volume label, in order for BackBox 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.

o RECOMMENDATIONS FOR TAPE DEFINE

The TAPE or TAPECATALOG DEFINE should not specify any tape drive. This will allow BackBox 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.

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

o 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.

VIRTUAL VOLUMES

VIRTUAL VOLUME SIZE

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 import- ant 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 BackBox 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.

VIRTUAL VOLUME MEDIA TYPE

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

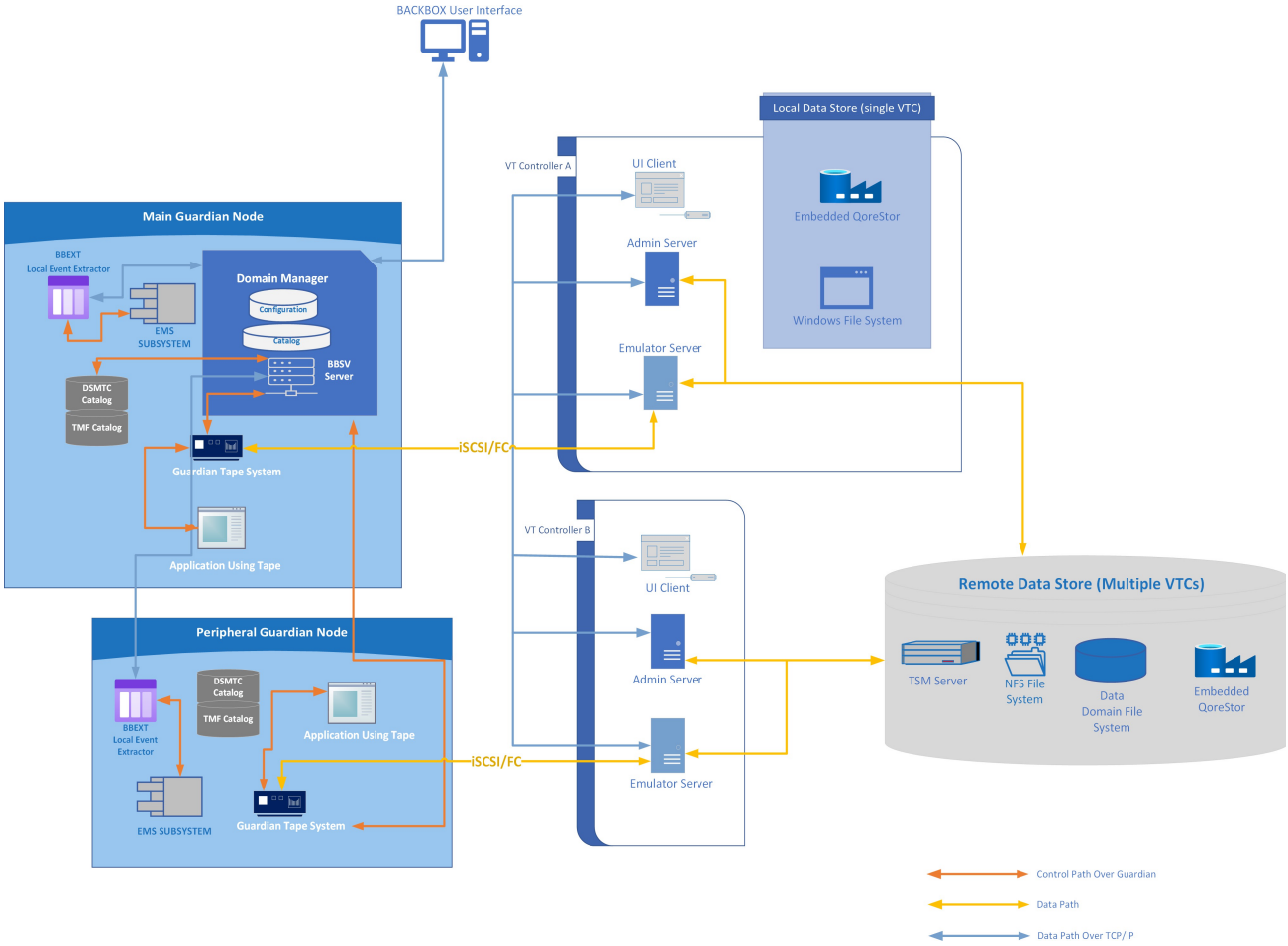
Consider the following when define virtual volumes:

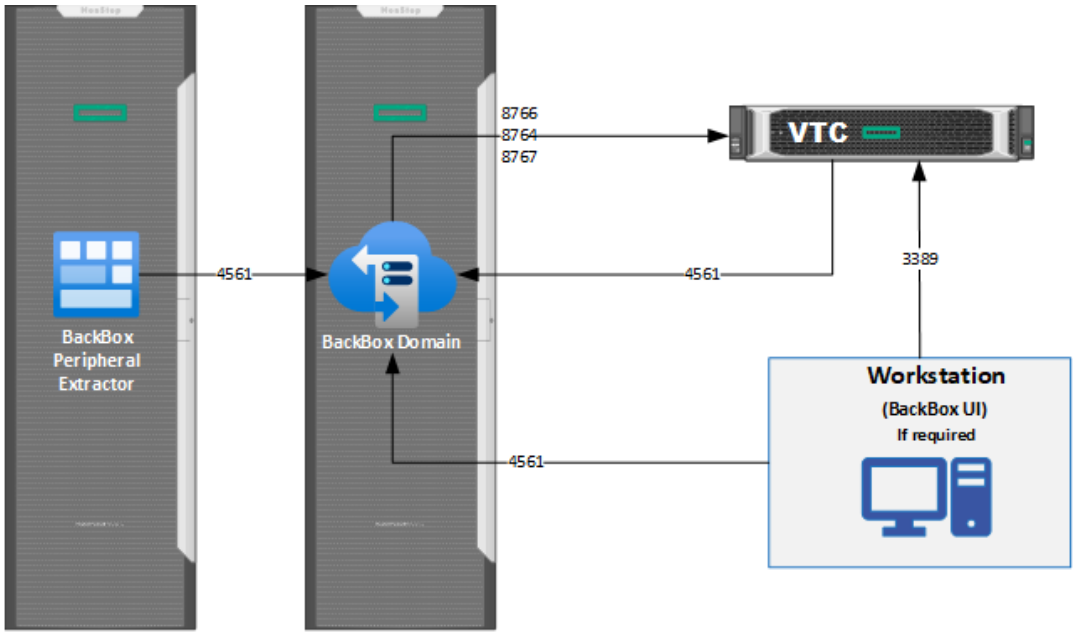
- Each tape drive reports a media type to NonStop host queries.
- DSM/TC (but not TMF) associates a media type with each cataloged volume. When a DSM/TC volume is requested, it will load only on media compatible tape drives.
- Some features are available only on specific tape drive types. For example, when the volume encryption is implemented through HP VLE, only LTO4 tape drives are supported.

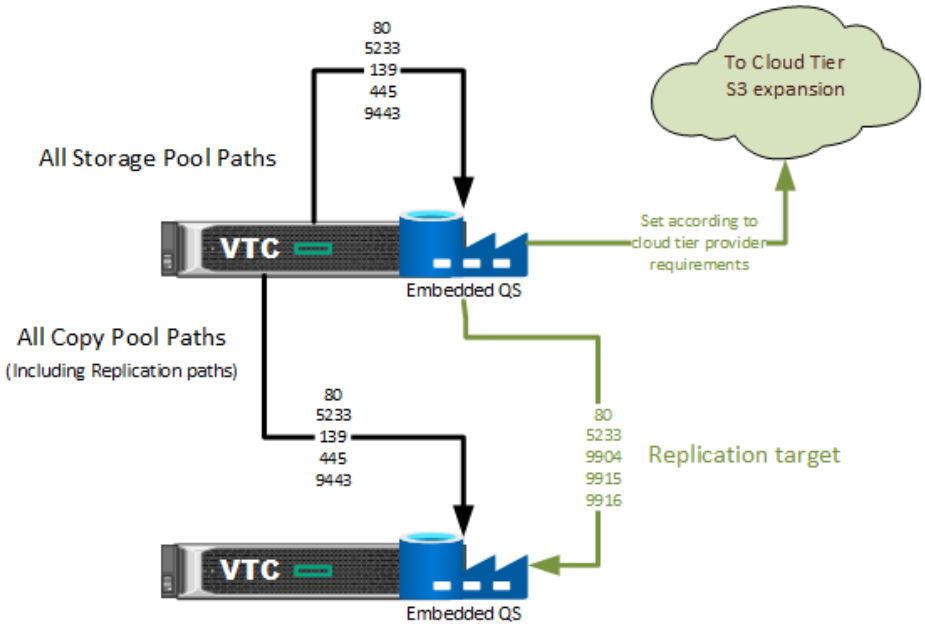
BackBox VTC can emulate these media types:

- CART3480 (for migration)
- LTO2 (for migration)
- LTO3
- LTO4
- LTO6
- LTO7
- LTO8
- V0505 for virtualized BackBox on the Virtualized NonStop

DOMAIN NETWORK


BACKBOX User Interface
Local Data Store (single VTC)
Embedded QoreStor
Windows File System
VT Controller A
UI Client
Admin Server
Emulator Server
Main Guardian Node
BBEXT
Local Event Extractor
Domain Manager
Configuration
Catalog
EMS SUBSYSTEM
BBSV Server
DSMTC Catalog
TMF Catalog
Guardian Tape System
Application Using Tape
iSCSI/FC
VT Controller B
UI Client
Admin Server
Emulator Server
Remote Data Store (Multiple VTCs)
TSM Server
NFS File System
Data Domain File System
Embedded QoreStor
Peripheral Guardian Node
BBEXT
Local Event Extractor
DSMTC Catalog
TMF Catalog
Application Using Tape
EMS SUBSYSTEM
Guardian Tape System
iSCSI/FC
Control Path Over Guardian
Data Path
Data Path Over TCP/IP





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

NONSTOP NODES PER BACKBOX DOMAIN

A domain is defined by:

1. A main node that hoststhe 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 BackBox 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).

VTCS PER DOMAIN

For fault tolerance reasons we recommend that two or more VTCs be attached to each NonStop node(s). Several BackBox 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 BackBox 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.

⚠	If the UI is separately installed on another instance than the VTC MC, go to UI > Preferences and set up the SSL protocol manually to match the VTC MC settings. For more info see SSL Setup.
⚠	The SSL Protocols selection field is disabled if the UI and the VTC are installed on the same server. In this case, SSL should be enabled through the VTC management console. For more info see section Settings>Security in the VTC Management Console.

TCP/IP TRAFFIC PORT CONFIGURATIONS

Client	Server (Inbound Rule)	Standard Port	Protocol	Protection
Product Mandatory Firewall Rules				
Workstation (UI Client)	NonStop (Domain Manager)	4561 Note1	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)- Mandatory only if fiber virtual tape devices are defined.	8764	TCP	TLS Note 2
Nonstop (Domain Manager)	VTC (Administrative Services)	8766	TCP	TLS Note 2
Nonstop (Domain Manager)	VTC (iSCSI Emulator Services) - Mandatory only if virtual iSCSI.	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 needs 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→ It is recommended to use point-to-point Network connectionfor data path protection.

NOTE 5→ TLS needs to be enforced in the Spectrum Protect configuration. See IBM Spectrum Protect documentation on how to enable TLS communication.

NOTE 6→ Port protection depend on certificate and browser policies.

NOTE 7→ RDP port needs 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 each volume separately.

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-cataloged volumes must be associated with the No catalog processing in the Volume Group.

Installation with DSM/TC, TMF

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 Autoscratch, SCRATCH Volumes are removed from storage. They are artificially regenerated as empty volumes, when requested again by a tape application.

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 autoscratch 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.

- In a NonStop system, there is no interaction between tape applications (BACKUP, RESTORE, TMFDR, FUP) and the BackBox processes. The user ID running the tape applications has no impact on the BackBox processes and files.
- Operator actions on the NonStop tape system (TMFCOM, MEDIACOM or SCF) require a user ID in the SUPER group, to add, for example, a TAPEVOLUME in DSM/TC or to reject a MOUNT REQUEST. These actions are frequent in BackBox, therefore all BackBox processes must run in the SUPER group.

At installation:

- An account in the SUPER group (ex: SUPER.BACKBOX represents the installation user), but not SUPER.SUPER, is used to install the BackBox sub-volume.
- 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 Actions Are Initiated

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

Because BBSVs 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.

For versions 4.09 and above only specific users have access to the UI. SUPER.BACKBOX and SUPER.SUPER users are automatically defined for initial configuration.

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 impersonalization).

User Name	Profile
.	Administrator

Since version 4.10 the following have been reintroduced:

- BBSVs 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, uncheck 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, BBSVs 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 BBSVs impersonalization) .
3. Security controlled by BackBox manager and reinforced by Safeguard ACL: without the possibility to use MFA.

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 pro- file. 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.

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.

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-Authentication (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 iscontrolled only by BackBox manager mode. Users permissions will be kept as in the 4.09 version.

	Access to the UI ca be denied even with a valid NonStop User ID/password if the user ID/password are not defined in the User Management page.

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

Examples of predefined 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 BackBox 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 BackBox 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 BackBox 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

BackBox 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 BackBox 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 over- written 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 BackBox 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 BackBox 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 unchecked.

DATASTORES

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.

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. Backup Compression

For normal configuration with a deduplication appliance, such as StoreOnce or Data Domain, the BackBox 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.

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 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 VTCs. 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 man-aged 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 Change

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 BackBox 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.

File Distribution Among Pool Paths

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 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.

IBM Spectrum Protect (TSM) Configuration

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 keywords:

NODENAME

PASSWORD

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

TSM Client Configuration Overview

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-retriesvalue 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 BackBox 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 BackBox 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 BackBox 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).

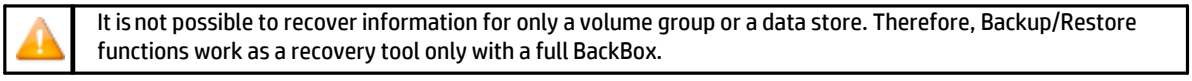
This related data must also be considered:

1. The tape catalog, such as DSM/TC.
2. The configuration of the storage for the Data Stores, such as NAS with deduplication 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 BackBox multi-domain environment, the data and metadata of each domain must be recovered separately. The BackBox Catalog Sync option handles the replication of the volumes metadata for the Back- Box catalog (VOLUME* files) and the DSM/TC catalog. Please refer to the BackBox 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 BackBox domain.

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



SSL SETUP

This section describes the SSL enabling procedure on the BackBox control path, i.e. on the TCP/IP connections between the BackBox components.

Depending on the BackBox component, the provider of the SSL library is different.

Platform	BackBox component	SSL product
NonStop	Domain manager, EMS Extractor, BBCMD & BB053 utilities	OpenSSL
MS-Windows	UI, High-level services	Schannel
MS-Windows	VTC low-level services such as the tape emulator	Schannel

Schannel Security Service Provider (SSP) is a part of Windows Server components that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) Internet standard authentication protocols.

Although the SSL configuration to each BackBox component is done in part through the BackBox interface, each SSL provider supplies its own documentation and configuration tools.

https://learn.microsoft.com/en-us/windows/win32/com/schannel Managing Microsoft

Certificate Services and SSL

ENABLING SSL

BackBox can run with or without SSL.

The default configuration is no SSL. SSL must be either enabled in all components, or disabled in all components:

- of a BackBox domain
- of a VTC (that can be shared by several domains)

SSL is best enabled as the final step of establishing the BackBox management layer:

1. After all components have been successfully installed and made sure that they communicate through TCP/IP, i.e. when the BackBox UI is able to report the internal configuration of all VTCs (UI tab Configuration > VT Controller).
2. Before or after the tape emulation has been configured. It is recommended to first configure the BackBox tape emulation.

SSL CONFIGURATION

Any SSL configuration in BackBox depends on the Certificate Authority, on how the servers and client certificates are produced and transferred, on the chosen encryption algorithms, and on other security options.

The certificates provided with BackBox initial installation should be replaced with the customer's own certificates, based on the security guidelines and polices in place. For more details, see Appendix B - Certificate Store and Appendix C - Certificates Upgrade on Nonstop.

This manual includes a section that document how SSL can be enabled for each BackBox component. It also identifies the tools to configure the local SSL library.

There are two complementary tools to configure SSL:

- The local BackBox component, which accepts the essential parameters.
- The local SSL library, which provides its own specific configuration tool.

ENABLE/DISABLE SSL

All permanent processes on all BackBox domain components must be stopped to allow this change to take effect. There must be no tape activity.

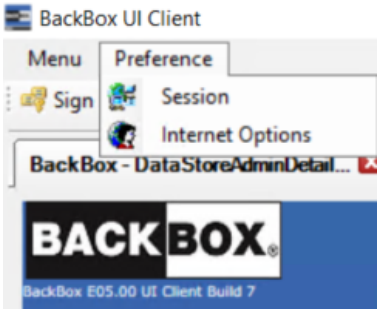
To stop the permanent BackBox processes perform the following actions in order:

1. Stop the BackBox activity.
2. Stop the virtual tapes in SCF.
3. Stop the Windows services in VTCs.
4. Stop the NonStop BackBox processes.

SSL IN THE UI

SSL must be enabled in all installations of the BackBox UI. To enable the SSL:

1. Go to **Preference> Session**.



SSL IN THE NONSTOP

To install SSL, the user should:

1. Generate and transfer certificates to the NonStop, if you don't want to use the ones included in the installation package.
2. Stop all BackBox programs.

Stop all BackBox Programs

⚠	If you are running the EMS Extractor program BBEXT as a permanent process, you need to stop it first in SCF. Example: `TACL> SCF ABORT PROCESS $ZZKRN.#BBOXEXT`

Use the macro BB054_SHUTDOWN to stop all BackBox programs of a given domain before enabling SSL:

```
VOLUME <BackBox-domain-installation-sub-volume> LOAD /KEEP 1/ MACROS BBSETUP
BB054_SHUTDOWN
```

BB054_SHUTDOWN is preferably used over TACL STOP, as it stops the programs by sending an IPC message to the processes, rather than by executing TACL STOP.

⚠	It will also stop the EMS Extractor program BBEXT, if EMS Extractor program BBEXT is not a permanent process.

Alternatively, when BB054_SHUTDOWN does not work:

```
VOLUME <BackBox-domain-installation-sub-volume> STATUS
*, PROG *
```

And after verification:

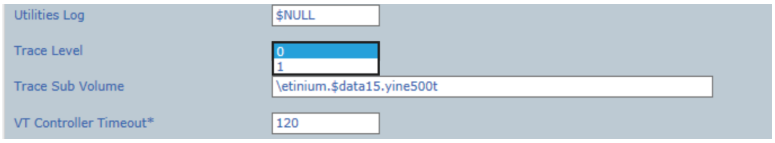
```
STATUS *, PROG *, STOP
```

Enabling /Disabling SSL

Enabled SSL in SSLCFG - file content (TLSv1.2 enabled):

```
servkeypass test
servkey <backBox-domain-installation-sub-volume>.NSKDER servcert <backBox-domain-
installation-sub-volume>.NSKCRT cacerts <backBox-domain-installation-sub-volume>.VTCCRT
RANDOMDELAY 1
MINVERSION TLSv1.2
USESSL 1
TRACELEVEL 0
```

If TRACELEVEL needs to be set to "1", go to BackBox UI and set the Domain Trace to "1": **Configuration > Domain** > Switch to Edit Mode > Trace Level



Setting the Domain `Trace Level` to "1" will trigger the SSL `Trace Level` "1".

Disabled SSL in SSLCFG- file content:

```
servkeypass test
servkey <backBox-domain-installation-sub-volume>.NSKDER servcert <backBox-domain-
installation-sub-volume>.NSKCRT cacerts <backBox-domain-installation-sub-volume>.VTCCRT
RANDOMDELAY 1
MINVERSION TLSv1.2
USESSL 0
TRACELEVEL 0
```

When SSL option is reset (ON to OFF, or OFF to ON), stop all progress files and the EMS Extractor in SSLCFG file.

```
> status *, prog bbsv, stop.
> stop Extractor
```

Restart the EMS Extractor after SSL set up has finished.

For <*BackBox-domain-installation-sub-volume*> use your own installation file location. There is no need to configure SSL in the peripheral nodes; just enable the SSL.

To encrypt the SERVKEYPASS run the program BBpscode to make sure that the keypass is not displayed and visible.

TACL command to run for the keypass encryption:

```
run BBpsCode <ServKeyPass to be encrypted for the NonStop SSL certificate>
```

Once the program has been run and the keypass successfully encrypted, you will be prompted with the message:

```
Successfully updated the Encrypted ServerkeyPass
```

Restarting the EMS Extractor BBEXT

Use the startup OBEY file OEXT in the BackBox-domain-installation-sub-volume or the SCF START PROCESS command.

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

Troubleshooting

If the domain manager is set for SSL, but received a non-SSL connection, the following sample message will be displayed in EMS:

```
Error 0x1408F10B in EMS
2024- 07- 22 15:17:07 \ETINIUM.$X0DN ETINET.100.100 3479 GCE401EA- E3479 SSL library
  error
336130315 (= 0x1408F10B) on socket 7 with Server role -.
```

⚠	If the above message and tape mount need to be manually executed, it means that an old non-SSL process of the EMS Extractor BBEXT might be still running. Restart the EMS Extractor BBEXT using the OBEY file or via SCF ABORT/START PROCESS command.

SSL IN THE VTC

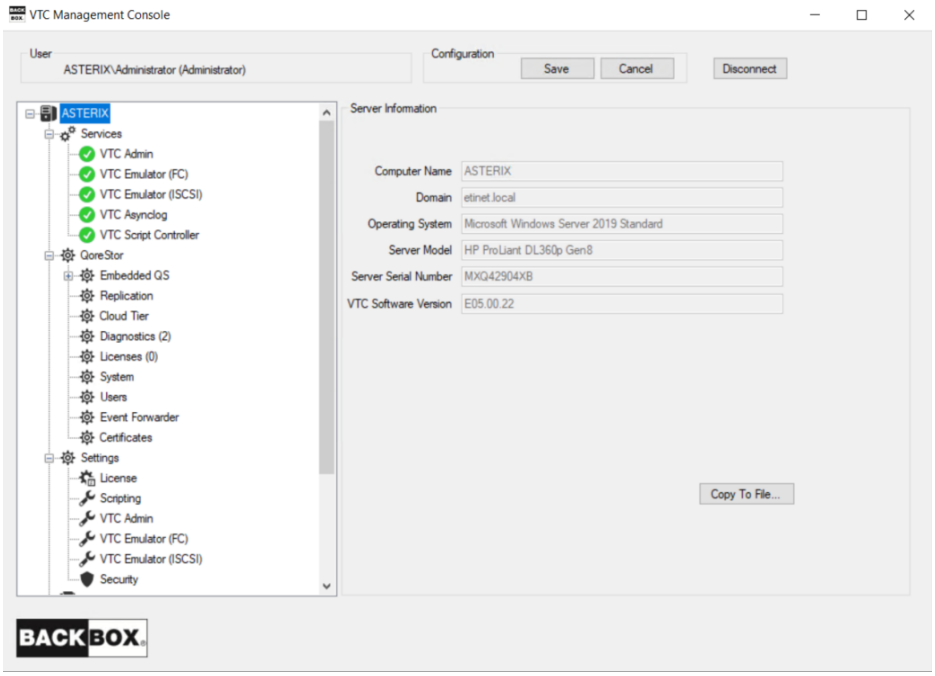
SSL must be enabled or disabled in all installations of the VTC Server.

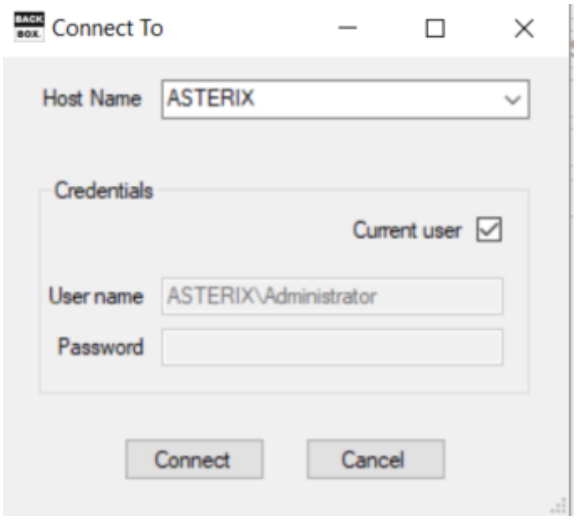
SSL server mode for VTC Server components is implemented using Windows Schannel (Microsoft Secure Channel)..

Enabling /Disabling SSL

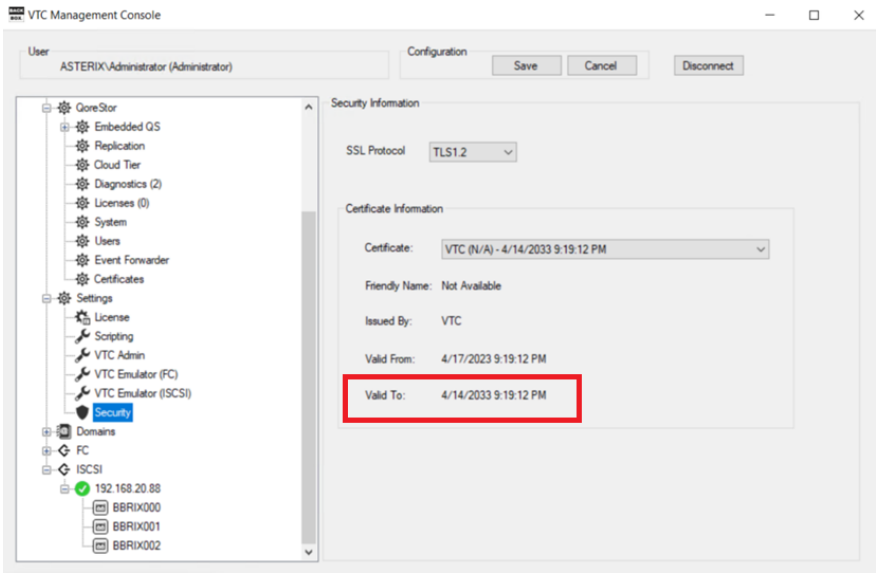
To enable or disable SSL, start an instance of VTC Management Console and access each VTC Server locally or remotely.

On the system where the VTC Management Console interface is installed, open the Search dialog and type VTC Management Console.





Expand the **Settings** node and select the **Security** one. A **Security Information** panel will allow you to enter appropriate TLS/SSL information. When finish, click on the Save button.



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.

⚠	Go to the NonStop to set up the SSL parameters in such a way that the SSL settings are accordingly applied to correctly communicate with the VTC MC. Moreover, if you need to encrypt the servery key pass code, you have to run an encryption program: BBpsCode. For more details, see section Sign In/Out in the User Guide for more information on enabling /disabling SSL.

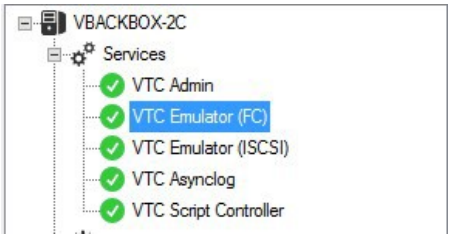
Certificate Information panel displays details about the installed certificate:

- Subject: Name of the certificate
- Issued By: Certificate issuer
- Valid From: Beginning date of the supported certificate
- Valid To: Certificate expiry date

In case of self-signed certificate, add server certificate into the Trust Root Certification Authorities Store. See Add Certificates into Trust Root Certification Authorities in the Appendix A.

⚠	Self-signed certificates distributed with the BackBox application are for test purposes only. ETI-NET is not responsible for the certificate generation and maintenance in BackBox operational environments.

After enabling or disabling SSL protocols in the VTC Server configuration, all VTC services need to be restarted for the changes to take effect. You can restart all service by right-clicking on the Services node and selecting the Restart action. The action will be applied to all services at once.



Troubleshooting

Errors are reported in the VTC Server Virtual Tape Controller Event Viewer log and connections activities are logged into xxTCP/IPSession_n files in the VTC Log Files folder.

BROWSING THE SSL LOG FILES

These files are C text files that can be browsed in TACL by the BackBox macros:

```
LISTT <file-name-pattern>

VIEWT <file-name>
```

DATA ON THE NONSTOP SERVERS

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 BackBox Catalog Sync Option.

A BackBox 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.

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

- The volume owner and access authorizations.
- For a Windows Data Store, the volumes 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, volumes 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 BACKBOX 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 BackBox Domain configuration is changed:

- BACKUP the whole BackBox 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 BackBox Catalog Sync Option is not available, each time the list of virtual volumes is changed:

BACKUP the whole BackBox 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 BackBox 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 BackBox 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 BackBox Catalog Sync Option

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

CONFIGURATION DATA ON EACH VTC 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 IN DATASTORE(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 the VTC MC.

> 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 the 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 labeled volumes:

1. Start the tape application.
2. Wait for the EMS tape mount request to appear on the **Status** page, in the UI.
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 unlabeled volumes:

1. Start the application using a specific tape device.
2. Select a volume from the **Volume List** page.
3. Click the Load button to choose the specific tape device waiting for the volume.
4. Select the tape mode fro IN (Read only) or OUT (Read/Write), depending on the tape application usage and click **Load** to finalize the operation.

Unloading volumes:

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 BackBox 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 Unlabeled Volumes

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 set- tings.

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 - Guardian Tool Samples.

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 BackBox 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	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 Autoscratch 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 2022-08-21 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 2022-07-30 16:45:07 2022-07-30 16:44:59 31
Path: \\BB1\LS_E\LSD3\WIN1
LMW103 2022-08-21 10:32:49 2022-07-30 16:31:33 31
LMW111 2022-08-21 10:37:16 2022-08-21 10:37:03 31
Path: \\happy\lsal\lsd3\win1
LMW106 2022-08-01 14:03:56 2022-07-30 17:08:15 31
LMW107 2022-08-07 18:20:48 2022-08-07 18:20:39 31
LMW112 2022-08-21 10:33:51 2022-08-21 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 2022-08-21 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 2022-08-21 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 A - Guardian Tool Samples.

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 A - Guardian Tools Samples

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.

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.

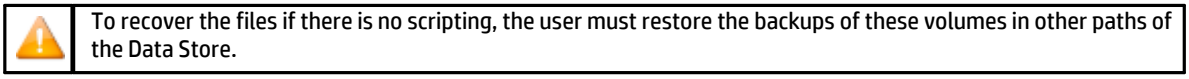
WINDOWS DATA STORE: RECOVERING A DISK PATH

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.

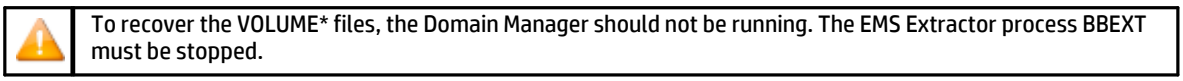
Each time the path in error is accessed, an error message will be logged to EMS.



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 BACKBOX CATALOG

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



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 BackBox 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 BackBox 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 BACKBOX NONSTOP ENVIRONMENT

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

1. The BackBox software.
2. The static BackBox 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 BackBox. An up-to-date catalog is required to make all BackBox 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 BackBox installation sub-volume including the VOLUME* files.
2. Check that the BackBox 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 BackBox 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 BackBox software from an ETI-NET distribution package.
- Initialize the BackBox configuration by replacing the default **BBSVCFG** file with the one previously saved or according to the notes taken.
- Enter the list of virtual volumes in RESTRICTED Data Stores.
- 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 BackBox 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 BackBox 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 BackBox installation sub-volume.
3. Recover the TMF and DSMTC catalogs using the procedures documented by HPE. Eventually, use the BackBox Catalog Sync option for the DSM/TC catalog.

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

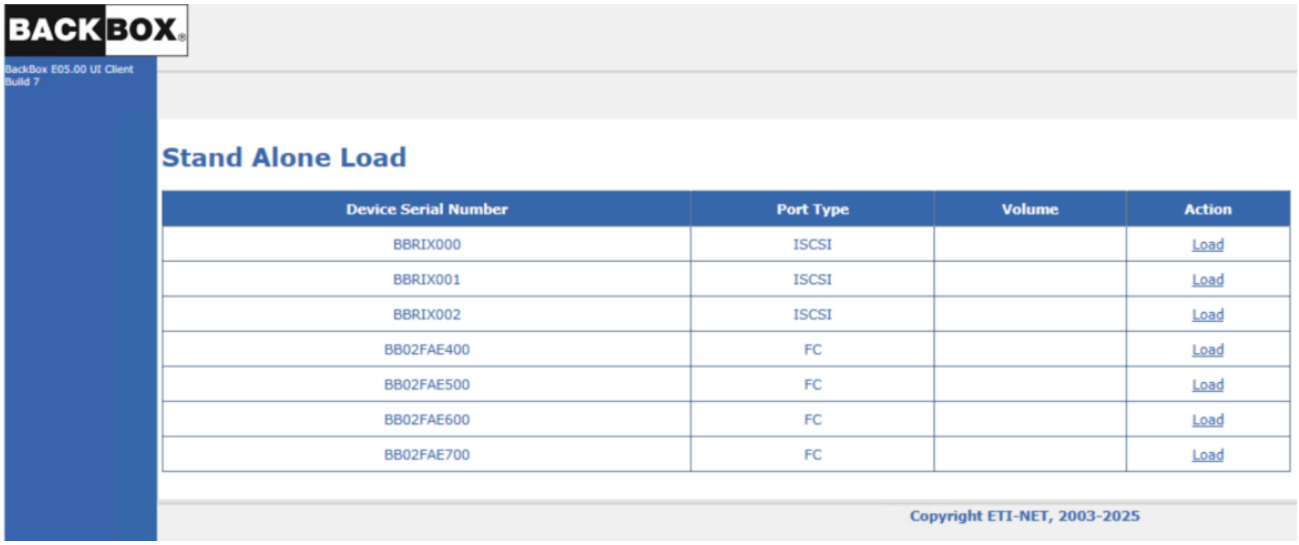
RECOVERY HINTS

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

If load requests are rejected because the timestamps in the BackBox 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 BackBox catalog does not contain entries for volumes requested by RESTORE or RECOVER and no backup of the catalog is available, do the following:



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 BackBox 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 BackBox 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 A - Guardian Tool Samples.

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 BackBox environment as it uses BackBox 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 A - Guardian Tool Samples.

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 avail- able to product support.

Syntax

```
VOLUME <BackBox-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 BackBox trace for the sub-volume configured in the BackBox 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 A - Guardian Tool Samples.

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 BackBox 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 Tool 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 does 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).
[VOLUME-SYNC-ONLY] parameter that allows bypassing cleaning volumes in Data Store.

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

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 Tool 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 Tool 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 BackBox domain. It searches for tape labels registered in:

- The BackBox 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 BackBox domain.
- The QTOS catalogs referred by Volume groups configured in the BackBox 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 BackBox 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 BackBox volumes and the volumes found in tape catalogs. Default value is Yes.

For BB044 sample see BB044 Tape Label Report in the Appendix A - Guardian Tool Samples.

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 A - Guardian Tool Samples.

OBB012 – LIST OF VIRTUAL VOLUMES

OBB012: Lists the virtual volumes registered in the BackBox 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 A - Guardian Tool Samples.

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 A - Guardian Tool Samples.

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 transferred data
```

Report elements:

Start date/time: Time when the load request was accepted by the BackBox Domain Manager.
End time: Time when the volume was unloaded by the VTC.
Volume label: Virtual volume label.
Oper: BackBox 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 BackBox 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 A - Guardian Tool Samples.

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 A - Guardian Tool Samples.

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 transferred data
```

Report elements:

Start date/time: Time when the load request was accepted by the BackBox 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.
Encryp: 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 A - Guardian Tool Samples.

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 A - Guardian Tool Samples.

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.
Encryp: 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 BackBox 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 divided 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 A - Guardian Tool Samples.

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 withOperation_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 labeling new media. All elapsed times are specified in seconds.

Fields have value only for labeled tape volumes used through a TACL TAPE DEFINE.

Report Fields

Field Name	Description	Sample Value for EMULLOAD	Sample Value for SCRIPTBACKUP
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.		
Domain	Domain name	BPAK	BPAK
Label_pre- fix	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 load the volume	0000001	000000000
Init_time	Elapsed time - from the time VTC is ready to report the tape drive ONLINE, - to the time	0000013	000000000

	VTC detects the 1st data block (i.e. after the processing of tape labels).		
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	000000000000000150
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
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 Con-figuration	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	
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, hasthe 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 A - Guardian Tool Samples.

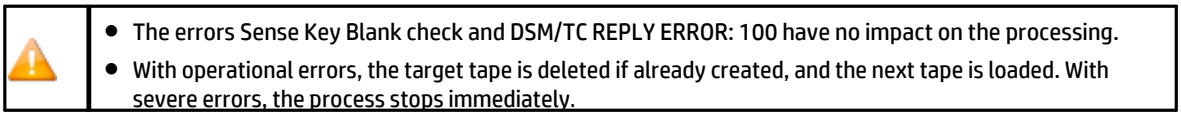
Parameters:

B055TRIGGER 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 needsto 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 A - Guardian Tool Samples.

For an execution Sample, EMS Log see OBB055 - Execution Sample, EMS Log in the Appendix A - Guardian Tool Samples.



- 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 A - Guardian Tool Samples.

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 A - Guardian Tool Samples.

TAPEWR - PERFORMANCE TEST

TAPEWR generates and writes blocks of data to the specified TAPE DEFINE with FORMAT U and LABELANSI.
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 &
minRecordLenInBytes 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 BackBox 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 A - Guardian Tool Samples.

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 A - Guardian Tool Samples.

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)
```

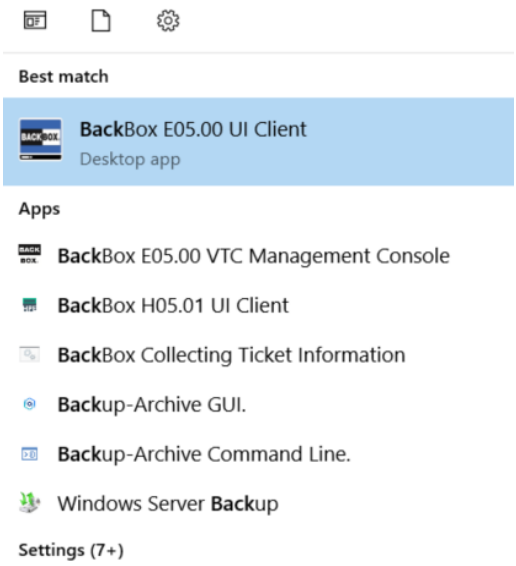
For a trace macro sample see Trace Macros in the Appendix A - Guardian Tool Samples.

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 inAppendix I - VTC Scripting Options.

WINDOWS VTC TOOLS

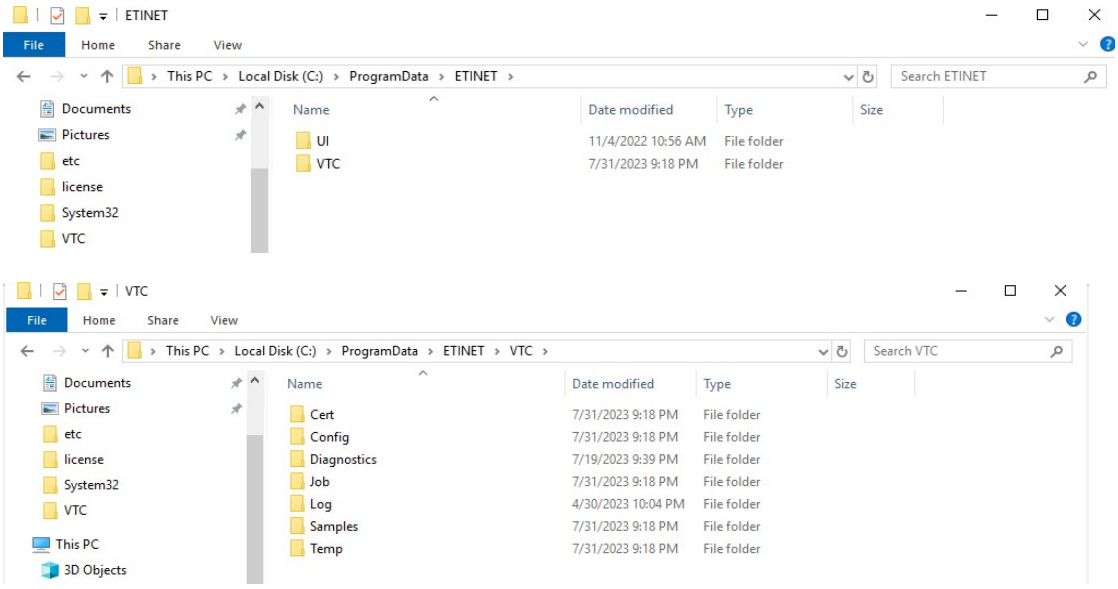
In remote sessions, access VTC Tools via the Windows Search bar, click on Start and type BackBox. All software elements are prefixed by BackBox. The Search dialog window will appear and allow you to choose BackBox version you want to use.



BackBox Collecting Ticket Information gathers the current VTC logs and configuration information in a zip file. See more in BackBox Messages Manual and Troubleshooting.

BackBox 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 field service engineer.

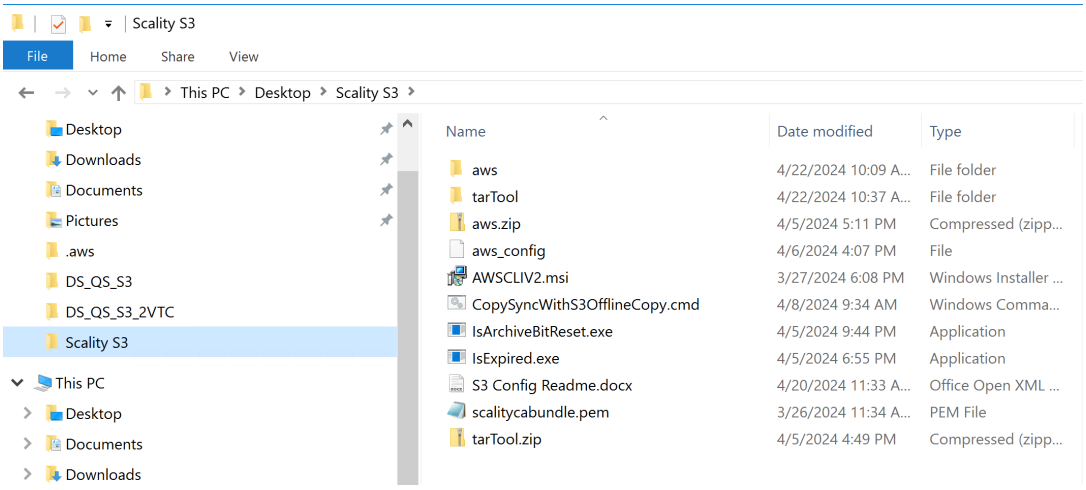
During a support call, a customer might be asked to browse some of these files.



BackBox UI Client is a sub-menu containing the user interface shortcut (UI).

BackBox VTC Management Console starts the console that manages and configures the VTC. See VTC Management Console section.

BackBox Scripts Folder is a customer created folder that contain different script files necessary for various procedures, such as upgrade and/or copysync on the cloud. For more details and examples, see section Offline CopySync with S3 Cloud as Target in APPENDIX I - VTC SCRIPTING OPTIONS.



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 BackBox 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 BackBox UI.

File	Description

CommonServicesCfg.xml	Parameters common for VTC Admin and VTC Emulator (FC) services. Changes are used only when the service is restarted.
BBAdminAppCfg.xml	Parameters for the service VTC Admin. Changes are used only when the service is restarted.
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.
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.
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.

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. Level — Description 1 — Trace management activity does not produce any trace at each block of data 4 — Level 1 + minimal data per data block 8 — Level 4 + data block description 12 — Level 8 + function call and call context description 16 16 — All of the above + debugging values	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

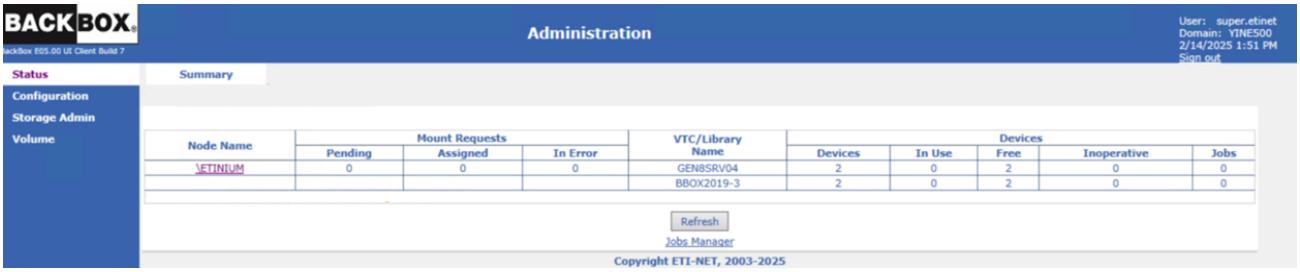
Counter Name	Description
Host Bytes Read/sec	Number of data bytes read per second by a host.
Host Bytes Write/sec	Number of data bytes written per second by a host.
Host Read/sec	Number of reads per second by a host.
Host Write/sec	Number of writes per second by a host.
Host Avg. Bytes/Read	The average 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

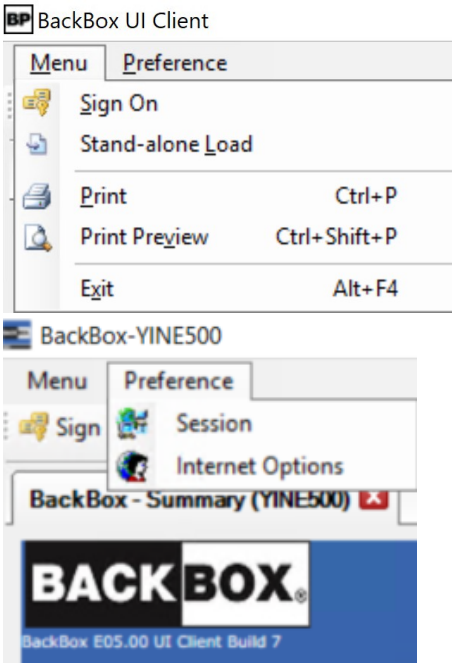
Each page of the user interface contains the following elements:

Windows Title: contains the BackBox 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.



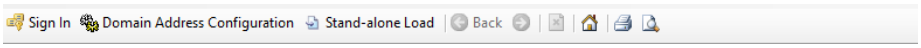
An instance of the BackBox interface can connect to a single Domain at any time.
The domain ID, user ID, and the connecting time are displayed in the page title.

Windows Menus



The menus above are used during the BackBox 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 BackBox 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.

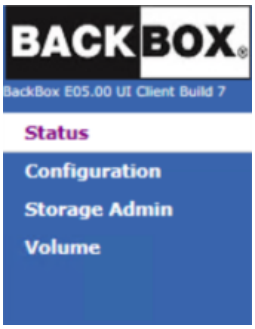
Banner

The Banner is located at the top of each page and displays the BackBox logo and information about the current session.
Below the BackBox 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 islocated 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.

Data Grids

In configuration mode, information is displayed in data grids (except the Domain page).

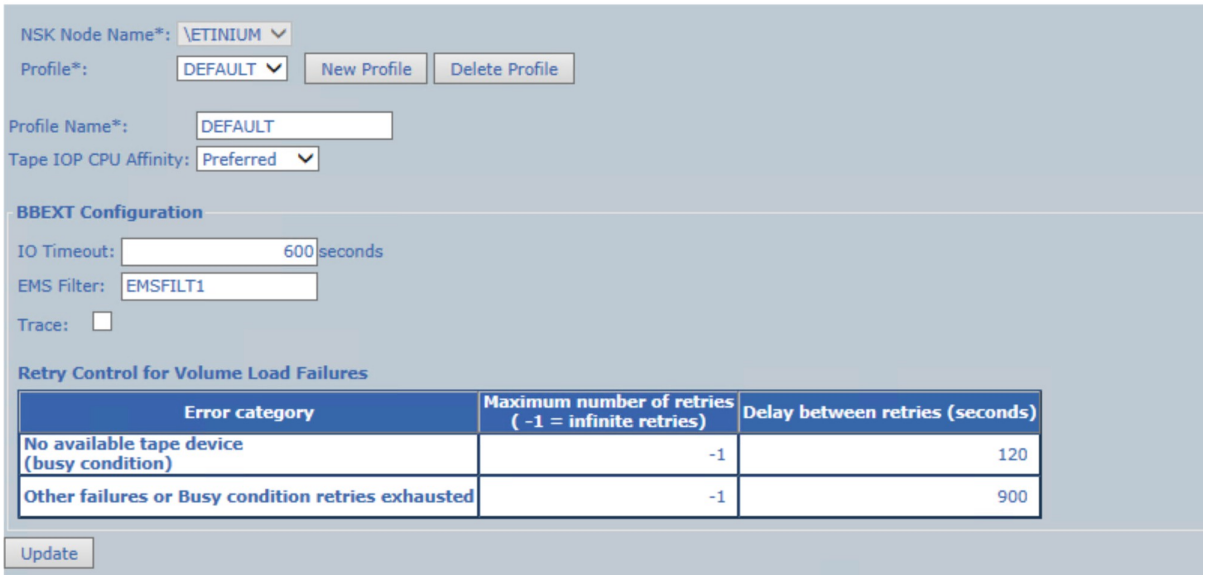
VT Controller ID	Status	Physical Location	TCP/IP Address	Comment	
GEN8SRV04	Enabled		192.168.21.42		Advanced
OBELIX	Enabled		192.168.20.87		Advanced

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).

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
\INSIDX	DEFAULT	Delete



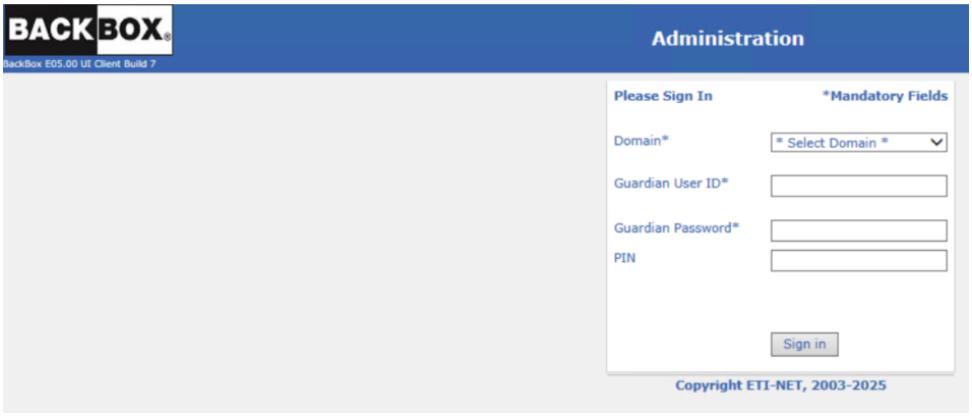
3. Click Save to accept the changes or Cancel if you wish to cancel.

Sign In

A successful sign in to the Domain Manager is required before accessing the BackBox functionalities. To sign in, the user must identify the BackBox 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.

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 inter- face after timeout require a new log-in session. To set a different timeout value (in minutes), use the Menu Preferences session.

Session SSL

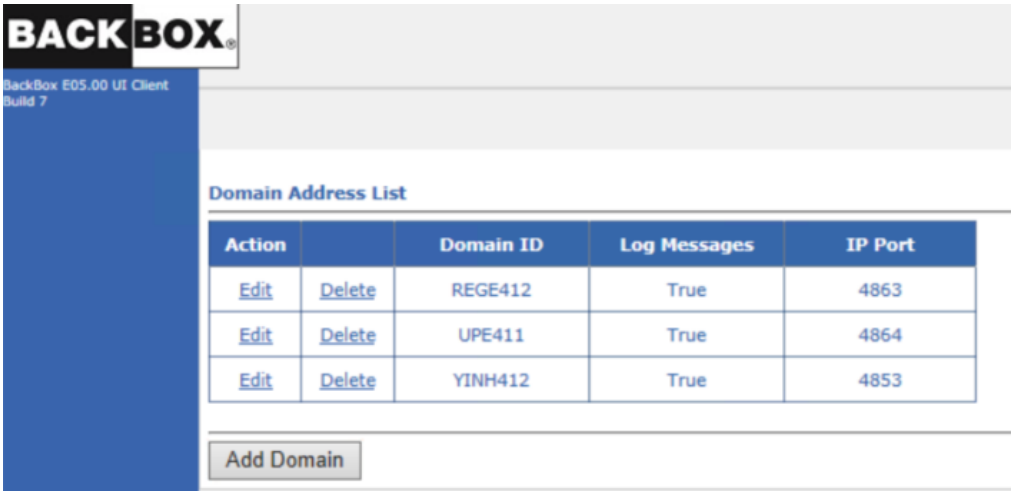
SSL must be enabled/disabled through the UI (**Preference>Session**), along with the other BackBox components. For more info refer to the BackBox SSL Setup manual.

Domain Address Configuration

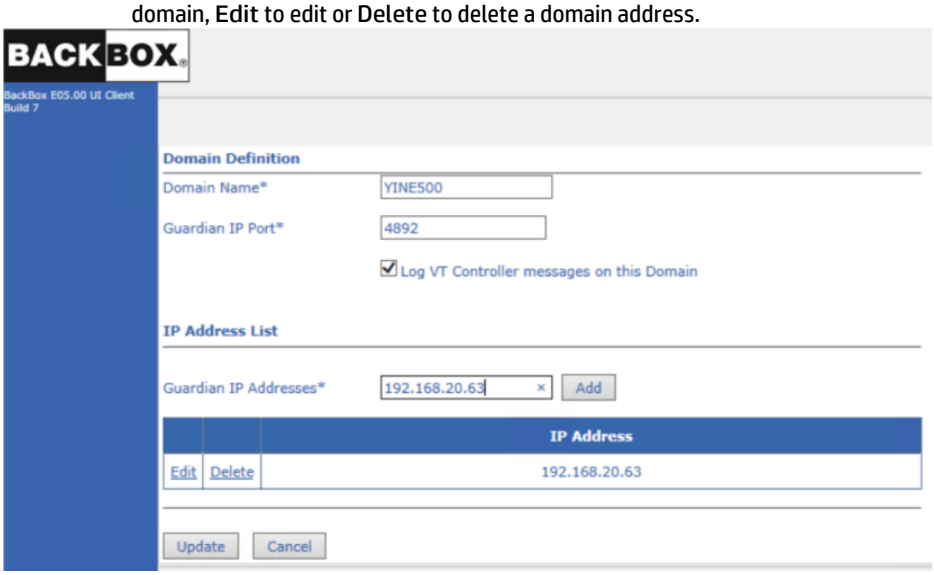
⚠	Domain Address Configuration option is available only when BackBox UI is installed on a workstation.

A domain address identifies a BackBox 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.

Domain address configuration is available for BackBox UI if the VTC is not installed on the same server as the UI.



- When installed on a workstation, in the **Domain Address Configuration** page click **Add Domain** to add a new domain, **Edit** to edit or **Delete** to delete a domain address.



- When BackBox UI is 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

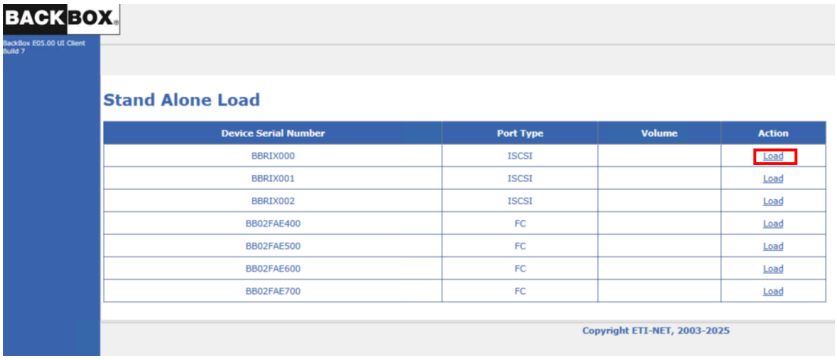
The **Stand Alone Load** allows virtual tape mounting without the Domain Manager when:

- 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 allows stand alone volume loads. The table displayed on the page shows all connected devices listed by serial number.

Elements displayed in the Stand Alone Load table:

Device Serial Number: Serial number of the connected device. The names are consistent with the devices added through VTC MC to either iSCSI or FC

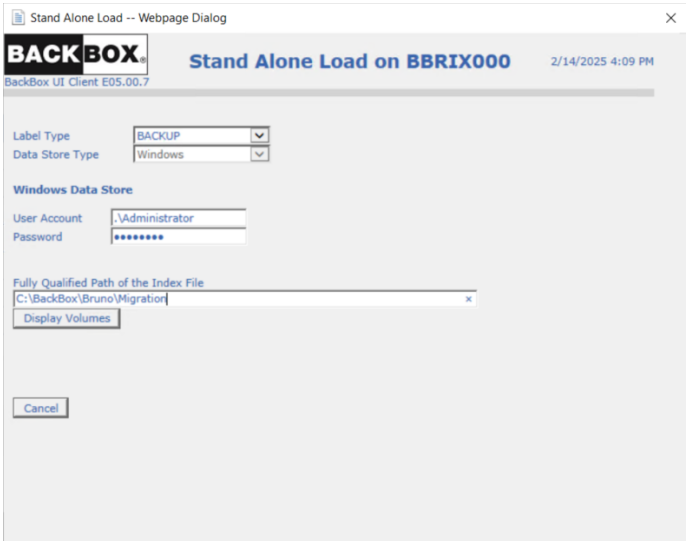
Port Type: iSCSI or FC

Volume: Volume that has been loaded, if any. If the column is empty, no volume is loaded on the device.

Action: Load or Unload, depending on the device status.

To load:

1. Choose the device from the table and click on the Load button - in the Action column - associated with the device to be loaded. In the pop-up window select the appropriate value for each field:



Label Type: Volume label type (values are ANSI, Backup, TMF, IBM or UNLABEL).

Data Storage Type: Windows Data Store is the default value and hard-coded. TSM volumes cannot be used.

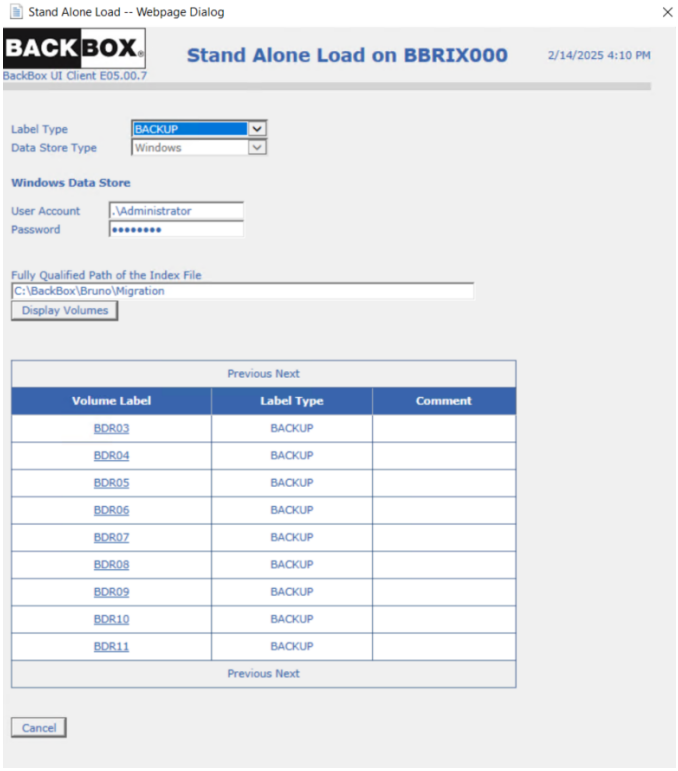
- Input the user account details for the selected Data Store: **User Account** and **Password** (credentials used to access the Windows disk pool).

⚠	Use the assigned credentials for the Data Store to avoid getting access errors.

- Specify the **Fully Qualified Path of the Index File**: name of the path containing the virtual media index file (*.IND file).

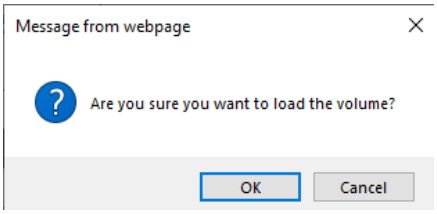
⚠	If the path is not correct, an error message will be generated to let you know that the system cannot find the path specified.

- Click the **Display Volumes** button to open up the table with all volumes associated with the specified index file.



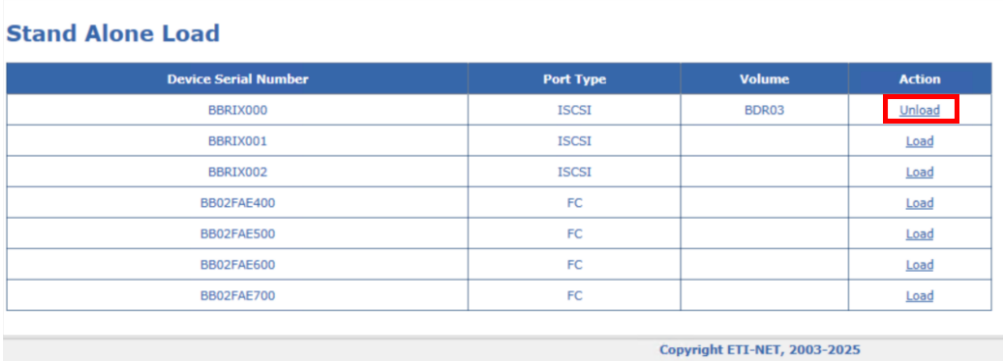
Based on their label, all volumes are listed in the table, along with all comments, if any.

2. Click on any displayed volume label to load it.
3. In the confirmation pop-up window click **OK** to load the volume or **Cancel** to cancel the load.

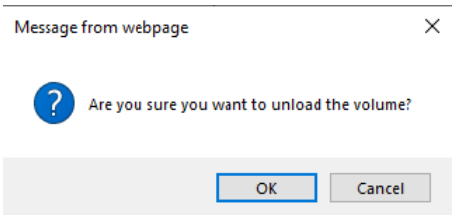


To unload:

1. Click the **Unload** button in the **Action** column. The available volumes to be unloaded are listed in the column **Volume**.



2. In the pop-up window confirm the unload action.



Status Page

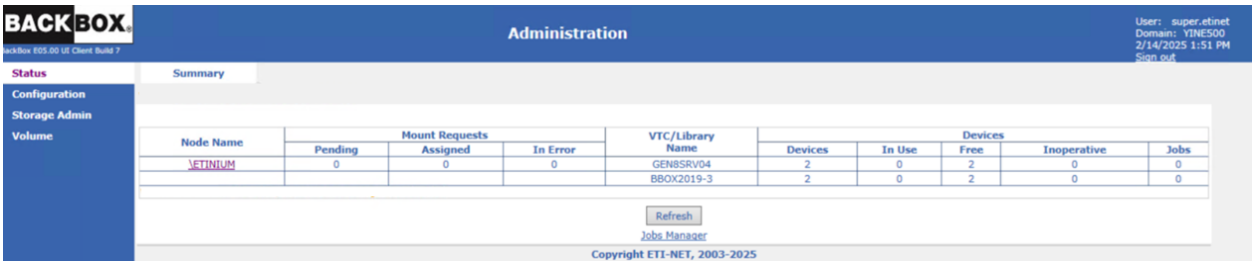
Once logged into BackBox UI, the application opens with the Status Summary page. This page displays the list of NonStop nodes and a summary of current operations.
This Status Summary is an overview of all operations in all nodes included in the domain.

- Click on each device and/or mount for a specific node on the Status for NonStop Node page to see device/mount details.
- The detailed reports can be generated for both NonStop MEDIASRV process and VT Controller(s).

STATUS SUMMARY

This page displays:

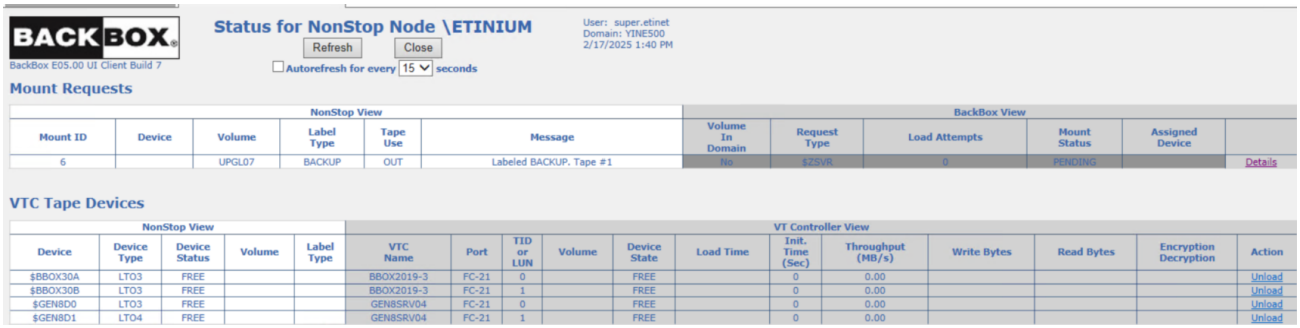
- the list of NonStop nodes with their virtual tape devices
- information related to monitoring current operations
- warnings if the EMS Extractor is not running.
- link to the Job Manager page



⚠	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.

NonStop Node Status

This page shows the detailed operational status for a NonStop node, both from the NonStop and the VTC point-of-view. This page opens up in a separate dedicated tab.



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 BackBox.

- NonStop View - The left part of the table 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.

- BackBox View - The right part of the display shows the attributes of a mount request managed by the BackBox 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.
  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 BackBox for a loaded or loading request.
  Details: Open a mount request detail window.

VTC Tape Devices - list contains all devices that are configured on the current domain.

- NonStop View - The left part of the table 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, LTO3, LTO4, LTO6, LTO7 and LTO8
  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 the table 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.

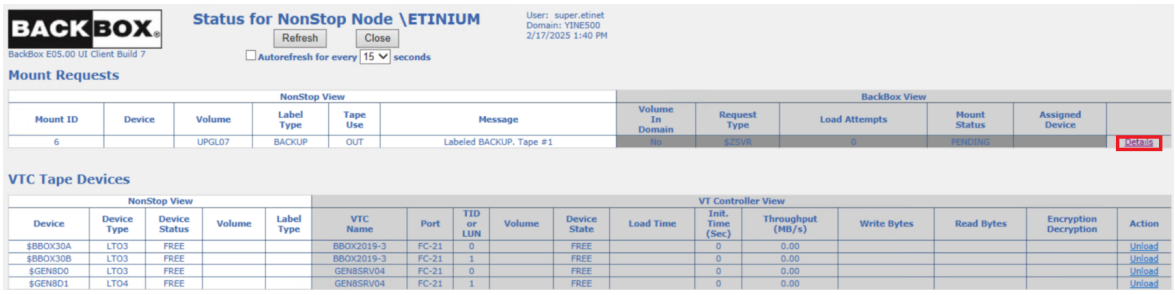
  NOT CONFIGURED - not configured on the VTC.
  ACTIVATED - initial communication received from the NonStop, but SCF START TAPE not received.
  INACTIVE - not polled by the host for three minutes FREE
  - operational and free
  LOADED - internal load completed, reply READY to host polling LOADING - the 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 I/O on a user data block.

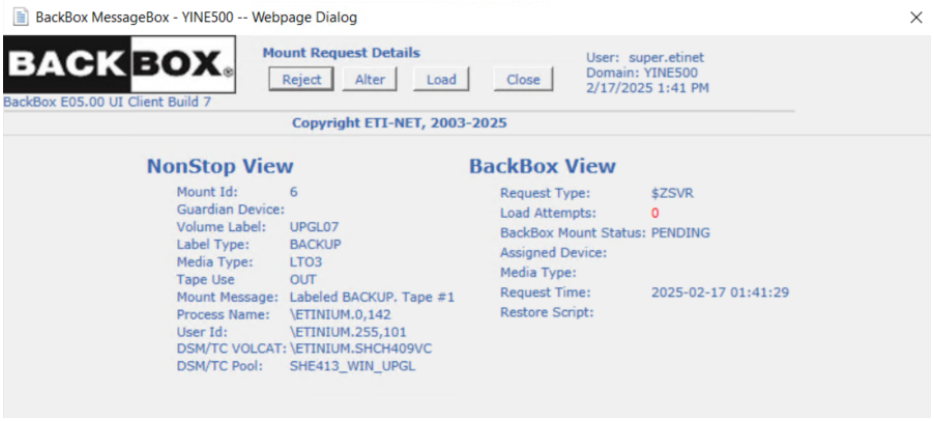
  Throughput (MB/s): Data throughput since the first user data block. Initial time is excluded from computation.
  Write Bytes: Quantity of data written since the volume was loaded. Includes tape labels.
  Read Bytes: Quantity of data read since the volume was loaded. Includes tape labels.

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.

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.



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 the display showsthe 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.

BackBox View

The right part of the display shows the attributes of a mount request managed by the BackBox 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.
BackBox Mount Status: Internal status of the request.
Assigned Device: Device assigned by load processing.

Request Time: Time when the request is known by BackBox.

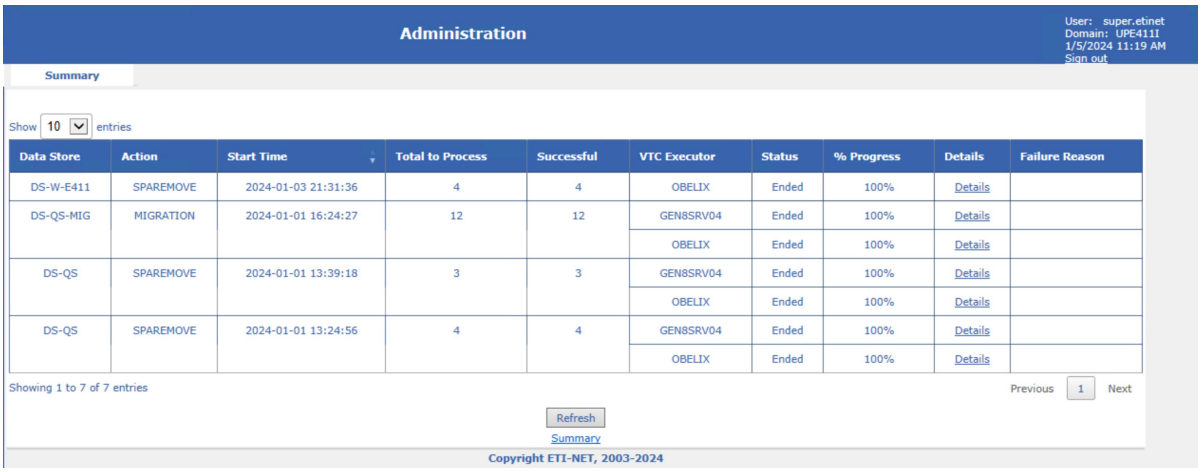
In addition, the page displays the latest message issued by the latest load processing.

Job Manager

Job Manager link displays a list with all the job details currently available for each data store.
The available jobs to be performed are:

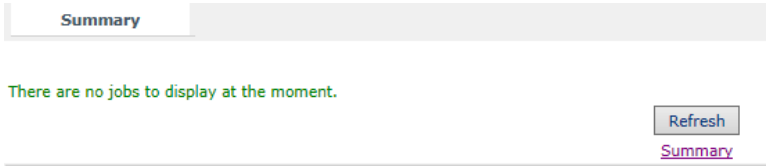
- Migration - when a spare pool defined on data domain has to be migrated. Migration job can be run either with conversion (**Migrate & Convert**) or without (**Migrate As Is**).
- Move Files from Spare Pool - when the main storage is not available, the file system moves temporarily the files into a spare storage. Once the main storage becomes available, **Move Files From Spare Pool** job transfers the files to the main storage.
- **Copy** Sync Uncopied Files - if the files in the storage pool do not match the files of the copy pool (ex. some files are missing from the copy pool), then start the copy sync uncopied files job

On the Job Manager page, the table lists all the jobs (ended, failed, running or suspended), along with the respective job types (COPYSYNC, MIGRATION, SPAREMOVE) under the **Action** column.



Refresh  button - used at any time during or after the process - will update in real time and show the number of successfully processed files for all types of jobs (Migration/Copy Pool Sync/Spare Pool Move).

If no job details are available, the job summary page will display the following message.



You can use the **Job** Manager page to see specific information related to jobs, such as:

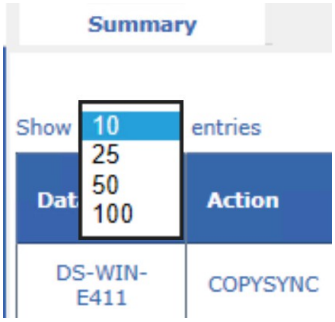
- **Data** Store Name
- Action Type of job that is being executed on the Data Store

Copy Uncopied Files process cannot be started while other processes, such as Migration or Spare Move, are still running.

- 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.
- **Status** Job status (Failed/ Ended/Running/Suspended).
- **Total to Process** - number of files to be processed
- Successful - number of successfully processed files

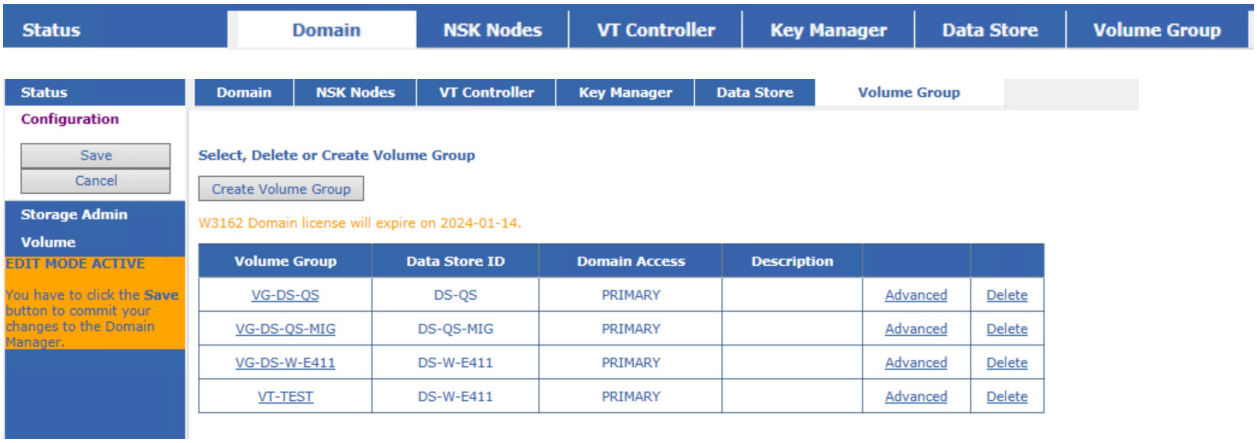
- VTC Executorperforming the job related to the data store
- % Progress - percentage of the job completion while the job is running. If job is completed, it will be shown as Ended with 100% progress rate. If the job is Stopped/Canceled, the job progress will be shown as completed (100%). If the job is Paused, the progress will remain to the current percentage until the job is restarted.When the job finished running, the progress indicated will always be 100%. If Failed, it shows the percentage of the total processed files with percentage rounded value.
- Details about the job
- Failure Reason, if any job failure

Select the number of entries per page if you want to display 10/25/50/100 job entries.



Configuration

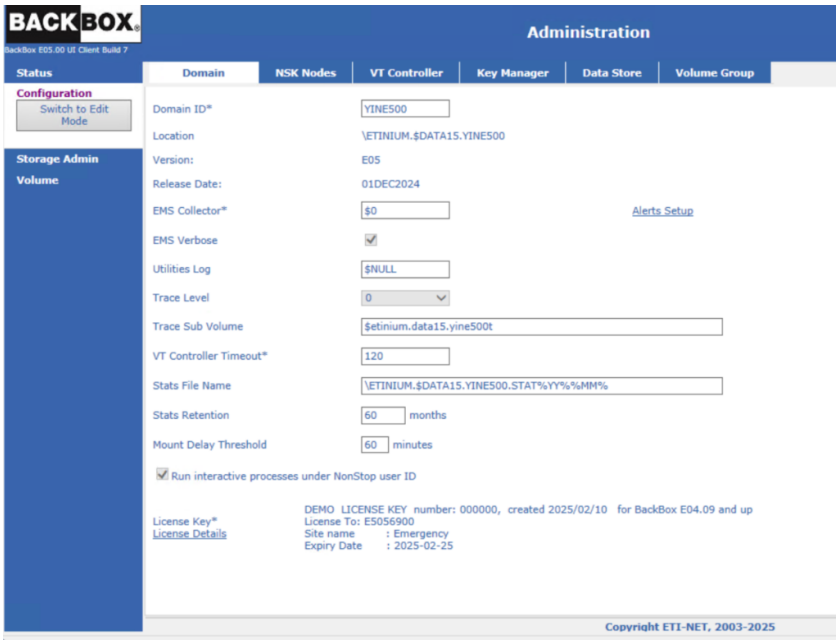
The Configuration tabs allow navigation through the configuration pages. Any configuration change can be updated and then saved, if in edit mode.



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 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 BackBox NonStop component version.

Release Date: Read-only field showing the release date of the BackBox 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 for troubleshoot purposes; 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 %d 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 BackBox 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) sign-on is not supported.

⚠	In order to enable the sign-on 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.

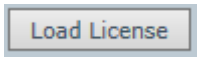
This default setting is **Disabled** : the NonStop user limitations are consistent with the UI user permissions. It doesn't allow the execution of UI commands under the user owning the BBSV program - which must be PROGID. Only SUPER.SUPER and the BBSV owner can change this setting.

License Key*: License key number, along with creation date and the product name, as listed in the license file sent by ETI-NET.

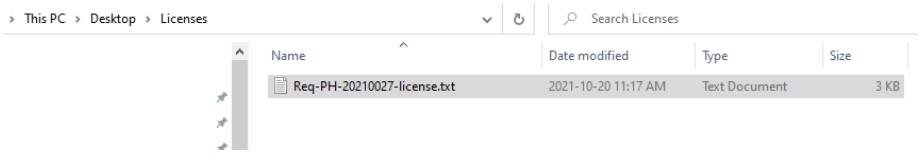
License Options: Link to show available licensed options of the BackBox Domain.

Click on **License Details** to access the details page of your domain license.

To load a license:

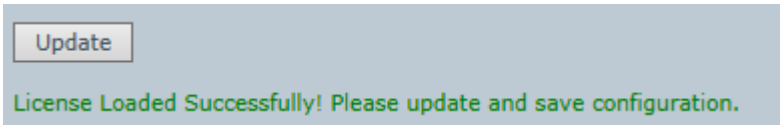
1. **Switch to edit mode** and click on **Load** License 

button at the bottom of the **Domain Configuration** page.
2. Load the file sent by your ETI-NET representative.



3. Click **Update** 

and then Save configuration.



To modify the Domain:

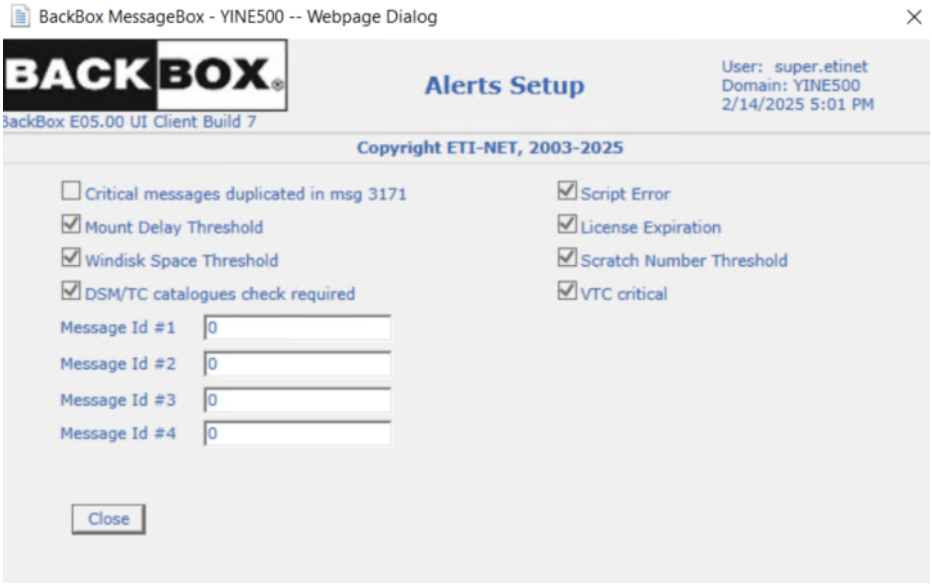
1. Click the **Domain** tab.
2. **Switch to Edit Mode** to change data to specific fields.
3. In **Domain ID** and in other fields, type the changes.
4. Click **Update** to display the new data. In case of invalid data, red error messages are displayed next to the field.

5. Click Save to activate changes.

Alerts Setup

To make the monitoring of critical events easier, some EMS messages generated by BackBox can be highlighted and duplicated by an Alert message tagged with a unique event number.

On the Domain License page, click Alerts Setup link, on the EMS Collector line, to set up various parameters for the alerts.



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 BackBox license is going to expire in the next 7 days (event 3162).

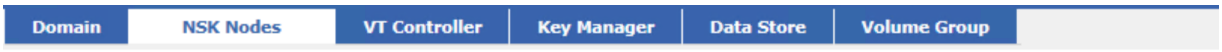
Scratch Number Threshold: Generates an Alert if, during the production of a Volume Group summary report, a Volume Group has less SCRATCH Volumes than the configured threshold (event 3313).

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.



NSK Node Name	Profile
\ETINIUM	DEFAULT
\INSIDX	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. The license file received has to be uploaded on the NonStop in binary mode. See license file content **\ETINIUM.$DATA05.BPAK.BBEXTLIC** in the sample below.

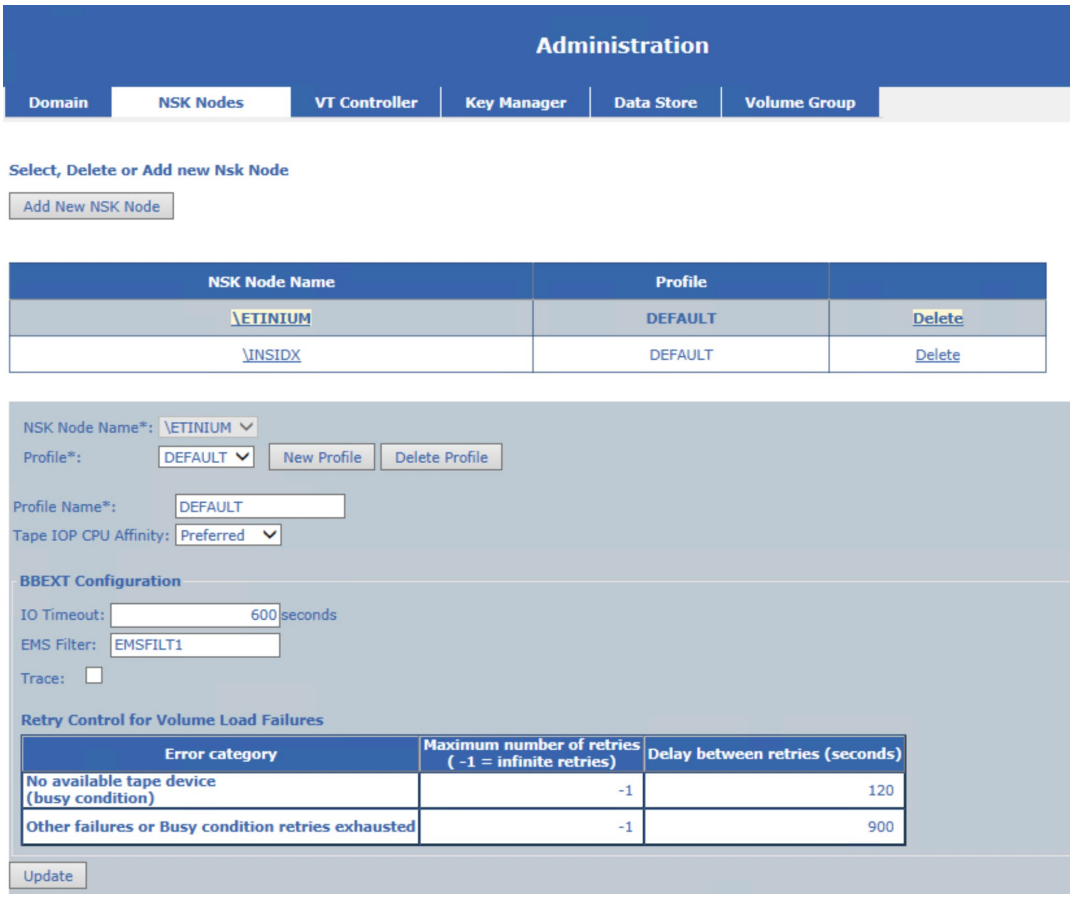
1. Run the Obey file to start the extractor by specifying where the peripheral node license is located (see the sample below).
2. Modify the indicated line in the sample to point at the location of the peripheral node license.

If there is no peripheral node license, the specified line will be ignored by the extractor.

Sample:

```
$DATA15 BBH500 175> fup copy oext
COMMENT ************************************************************
COMMENT start manually the EMS extractor process
COMMENT ************************************************************
CLEAR ALL
RESET DEFINE *
DELETE DEFINE =BackBox_BBSETUP

ADD           DEFINE        =BackBox_  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. BackBox 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.

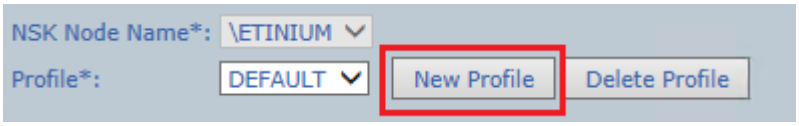
⚠	NSK node deletion is a particular procedure and it should be performed with caution. Refer to Appendix G - Removing NonStop Nodes for details on how to delete an NSK node and data related to the specific node.

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.



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(s):

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.

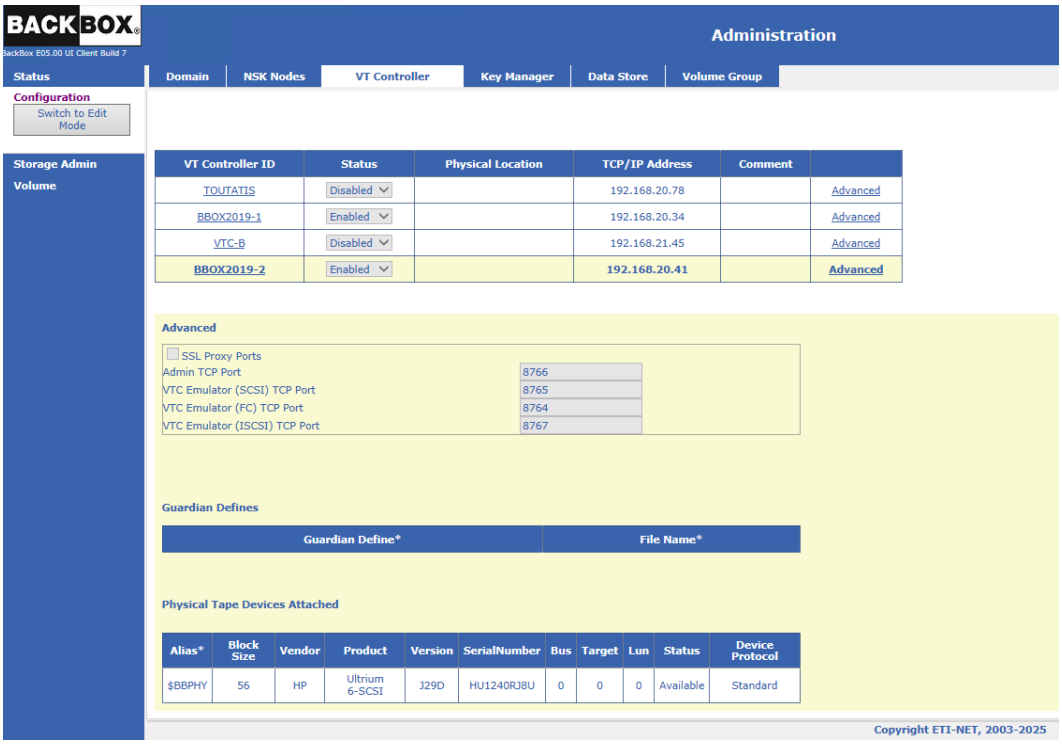
Virtual Tape Controller

The VT Controller page allows to configure the VTC. The configuration of a VTC consists of setting up:

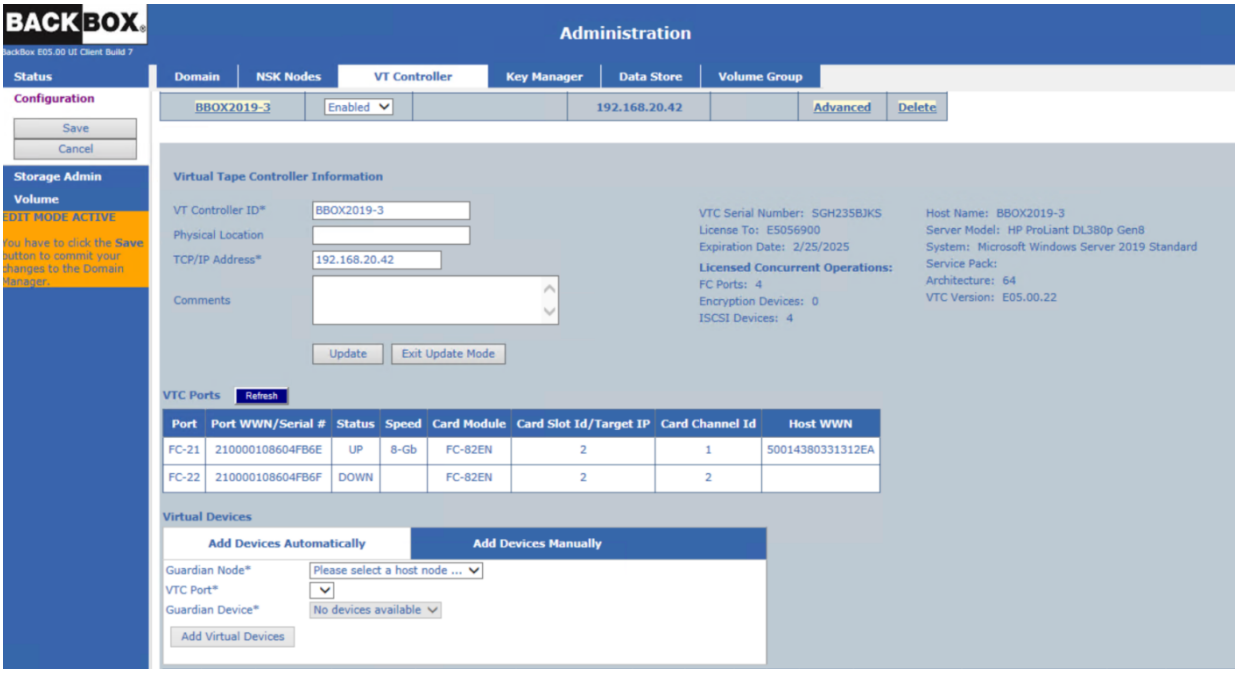
- Its TCP/IP address.
- The definition of operational tape drives. BackBox matches the VTC tape configuration with the one obtained from the CLIM and SCF. The VTC and the host definitions are prerequisites. The VTC must be functional and its virtual tapes must be connected in order to allow the configuration 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 BackBox 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 soft-ware. 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.

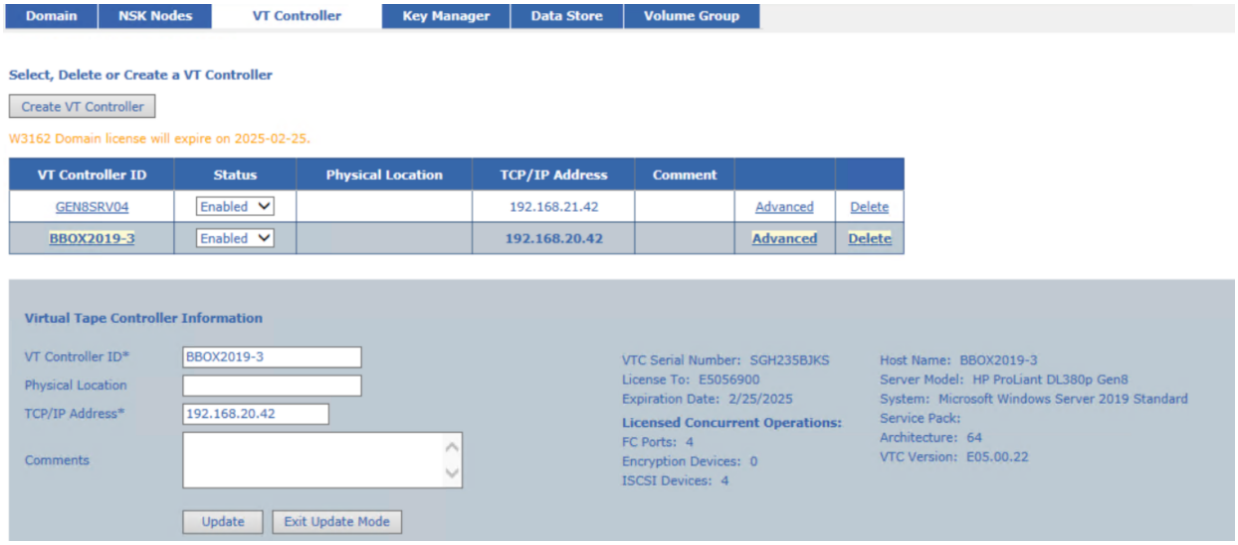
If there is no VTC connected (disabled VTC or the port associated with the configured devices has been removed from the internal

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 BackBox 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



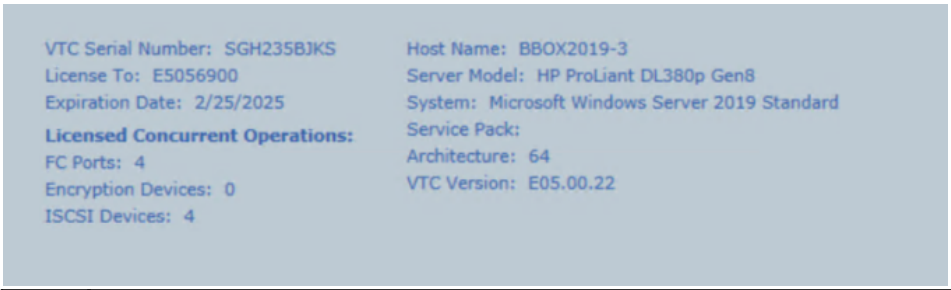
VT Controller ID: Identifies the VTC. It must be unique and cannot be changed once added.
Physical Location: Optional information field that describes where the BackBox unit is physically installed.
TCP/IP Address: TCP/IP address or TCP/IP host name used by the Domain Manager to communicate with the 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 acquired prior to 4.09 release, they have to be replaced by atomic license. Exception: If at least one VTC is using a QoreStor Data Store or running under Windows 2019 server (or later OS edition), all NonStop nodes and VTC nodes must have an atomic license installed on them.



⚠	If License To: does not match on each atomic license (see License Details) an error message will state that there is a conflict between licenses. In such a case, you need to request a change by contacting the ETI-NET 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 fail-over 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 fail-over 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
ISCSI-1							
ISCSI-2							
ISCSI-49	BBLIX300	UP	1Gbps	V0505 ETINET ISCSI V-Tape	192.168.20.87		192.168.20.251
ISCSI-50	BBLIX301	UP	1Gbps	V0505 ETINET ISCSI V-Tape	192.168.20.87		192.168.20.251
FC-21	1000001086054E88	DOWN		FC-162P	2	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. For details on the installation procedure of the iSCSI option see Appendix E - iSCSI Configuration (on the NonStop).

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.

Port	Port WWN/Serial #	Status	Speed	Card Module	Card Slot Id/Target IP	Card Channel Id	Host WWN
ISCSI-1							
ISCSI-2							
ISCSI-49	BBLIX300	UP	1Gbps	V0505 ETINET ISCSI V-Tape	192.168.20.87		192.168.20.251
ISCSI-50	BBLIX301	UP	1Gbps	V0505 ETINET ISCSI V-Tape	192.168.20.87		192.168.20.251
FC-21	1000001086054E88	DOWN		FC-162P	2	1	
FC-22	1000001086054E89	DOWN		FC-162P	2	2	
FC-31	1000001086054EC6	DOWN		FC-162P	3	1	
FC-32	1000001086054EC7	DOWN		FC-162P	3	2	
FC-41	2100001086030EA0	UP	8-Gb	FC-84EN	4	1	50014380331312E8
FC-42	2100001086030EA1	DOWN		FC-84EN	4	2	
FC-43	2100001086030EA2	UP	8-Gb	FC-84EN	4	3	51402EC012415CA4
FC-44	2100001086030EA3	DOWN		FC-84EN	4	4	

Virtual Devices

Add Devices Automatically | Add Devices Manually

Guardian Node* \ETINIUM

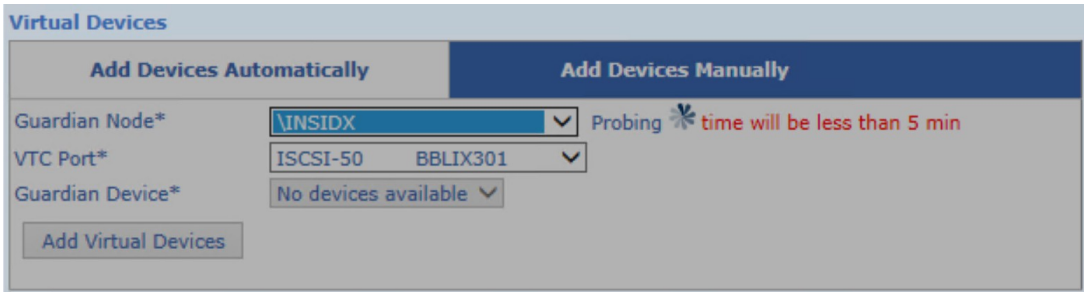
VTC Port* ISCSI-49 BBLIX300

Guardian Device* No devices available

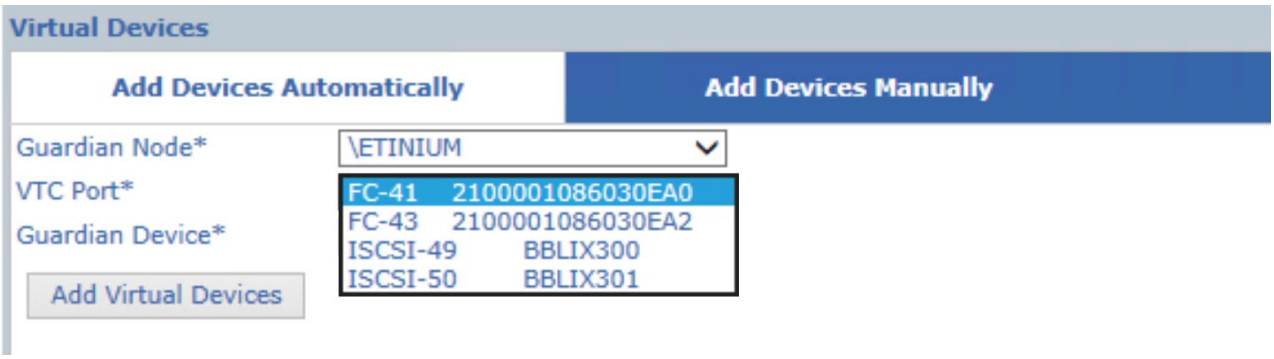
Add Virtual Devices

		Node	Guardian Device	Device Type	Serial Number	Port	Target	Lun	VLE	Explicit Only	Reserved For	Host WWN	Status	Guardian Port
Edit	Delete	\ETINIUM	$OBLI300			ISCSI-01	0	0		False	...			
Edit	Delete	\ETINIUM	$OBLI301			ISCSI-02	0	0		False	...			

Choose the Guardian Node you want to automatically add devices to.

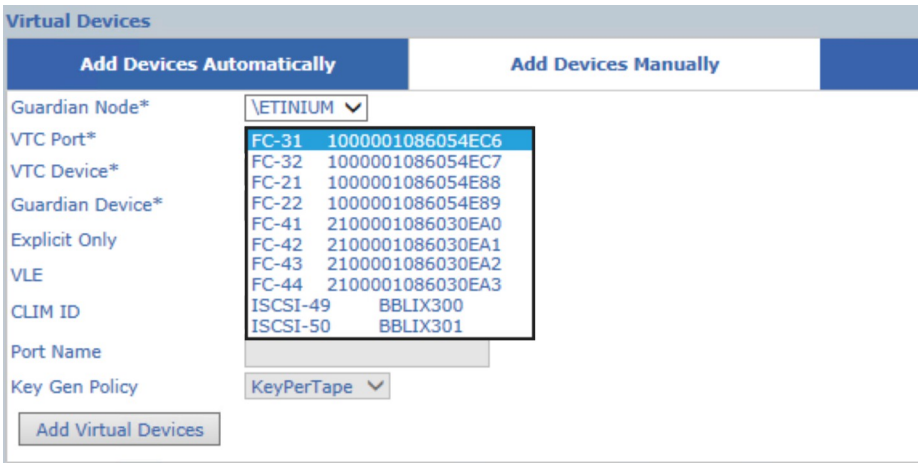


Open the drop-down list for the VTC Port* and choose the appropriate port name. The list contains all Fiber Chanel (FC) and iSCSI devices mapped for the selected Guardian Node.

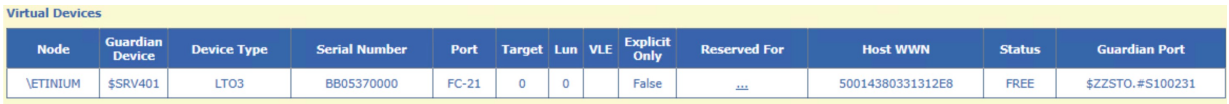


The Add Devices Manually tab allows adding devices by manually mapping Guardian and VTC devices that share the same physical connection (same host port and VTC port).

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 DeviceTarget, and also LUN. The user has to provide the Guardian device name to complete device mapping.



Virtual tapes can be updated or deleted individually in the list of Virtual Drives.

Attributes that can be updated:

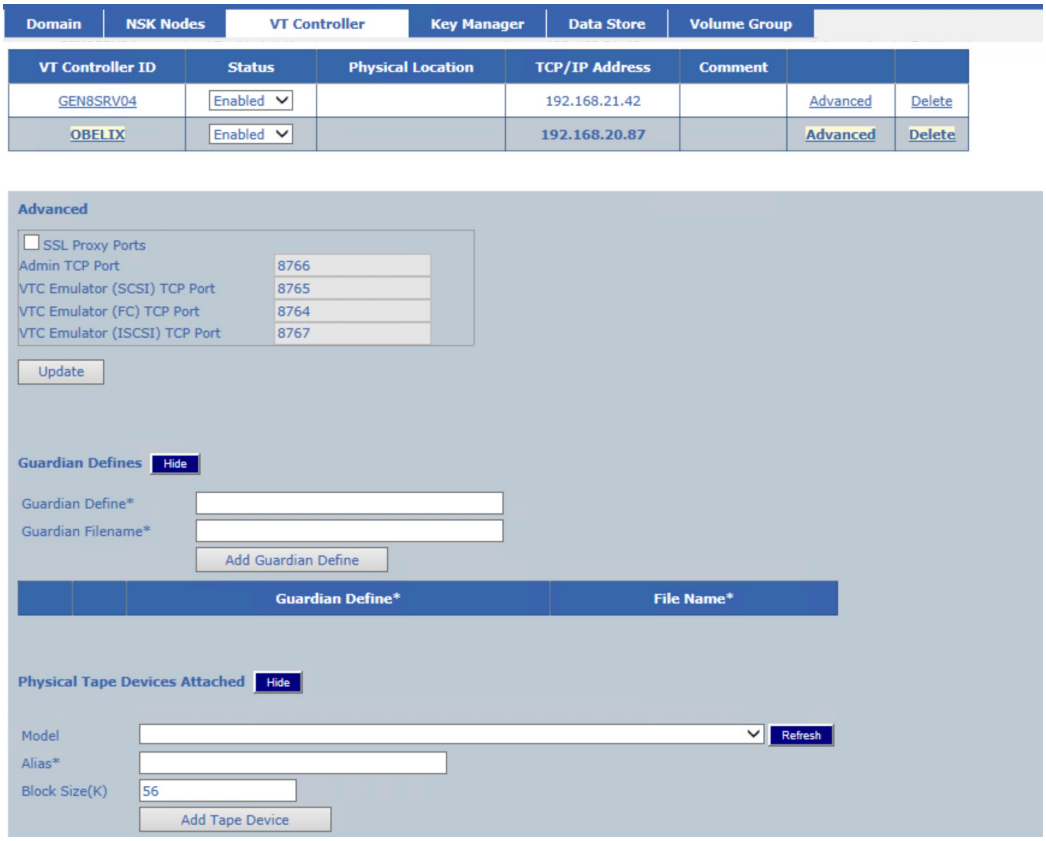
- Node
- Guardian Device
- Device Type
- Serial Number
- Port
- Target
- LUN
- VLE
- Explicit Only
- Reserved For
- Host WWN
- Status
- Guardian Port

Virtual Device Information

Node: Guardian system name.
Guardian Device: Guardian tape device name defined in SCF.

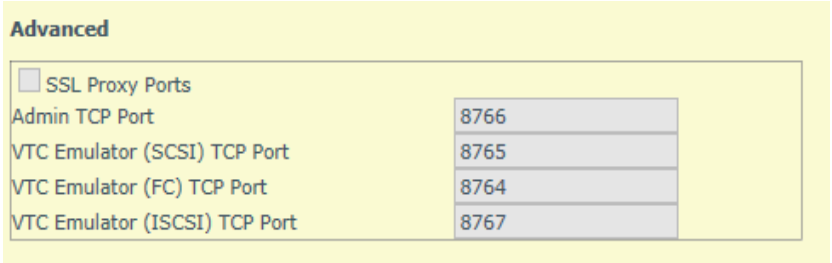
Device Type: Emulation provided by the VTC for this device, CART3480, LT03, LT04, LT06, LT07 or LT08.
Serial Number: Tape device serial number.
Port: Port type (SCSI, FC, BRIDGE) and number.
BRIDGE corresponds to a SCSI physical port of the NonStop; in this case the port number is the FC port number 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 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 the box if SSL tunneling is using the HPE NonStop SSL as proxy port to secure the control path.
The TCP/IP Ports for VTC services might have to be modified if the VTC is reached through the HPE 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 HPE SSL Proxy.

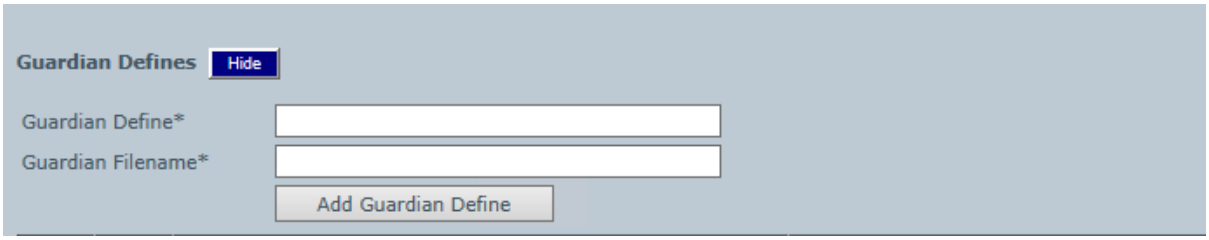
VTC Emulator (SCSI) TCP Port: Port for the VTC SCSI Emulator service. 8765 is required if the VTC is not reached through the HPE SSL Proxy.

VTC Emulator (FC) TCP Port: Port for the VTC FC Emulator service.
8764 is required if VTC is not reached through the HPE 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 BackBox Domain Manager.



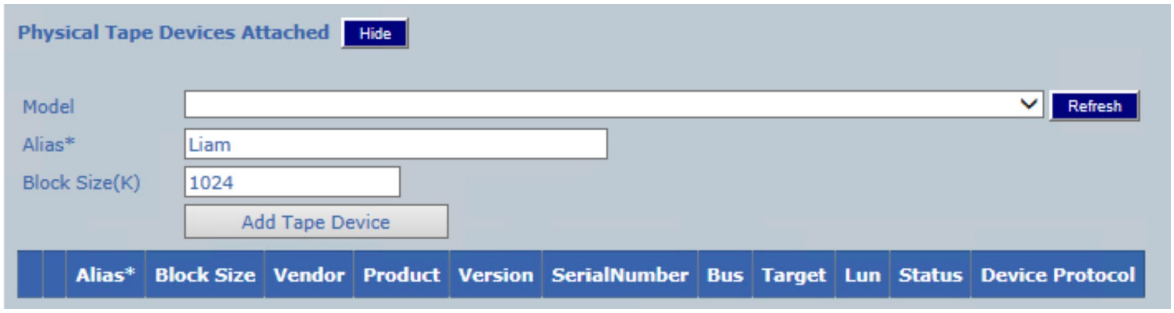
DEFINE is used when the Domain Manager communicates with the VTC. If a DEFINE is specified in this section, all TCP/IP Defines passed by the LISTNER are deleted in the process context, then the TCP/IP Defines configured here are created before accessing the NonStop socket interface.

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.

- To MATERIALIZE/VIRTUALIZE physical volume when LARGEBLOCKs are used, set the BLOCK SIZE of physical drive to 1024 KB in the VT Controller Advanced Properties configuration page.

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.

Key Manager

The Key Manager is an external server generating and storing encryption keys; the encryption itself being processed in the BackBox VTC for all configuration types. For more details, refer to Tape Encryption Option manual.
The Key Manager must be configured even for VLE Encryption.

- For VLE, the Key Manager configuration is used to control the encryption configuration during Operations and to clearly identify the key server storing the encryption keys.
- For non-VLE Encryption, the Key Manager configuration is also used to identify and secure a network path to the key server.

It is possible to configure more than one Key Manager instance, each describing the server holding the encryption keys for different groups of tape volumes.

In the domain configuration:

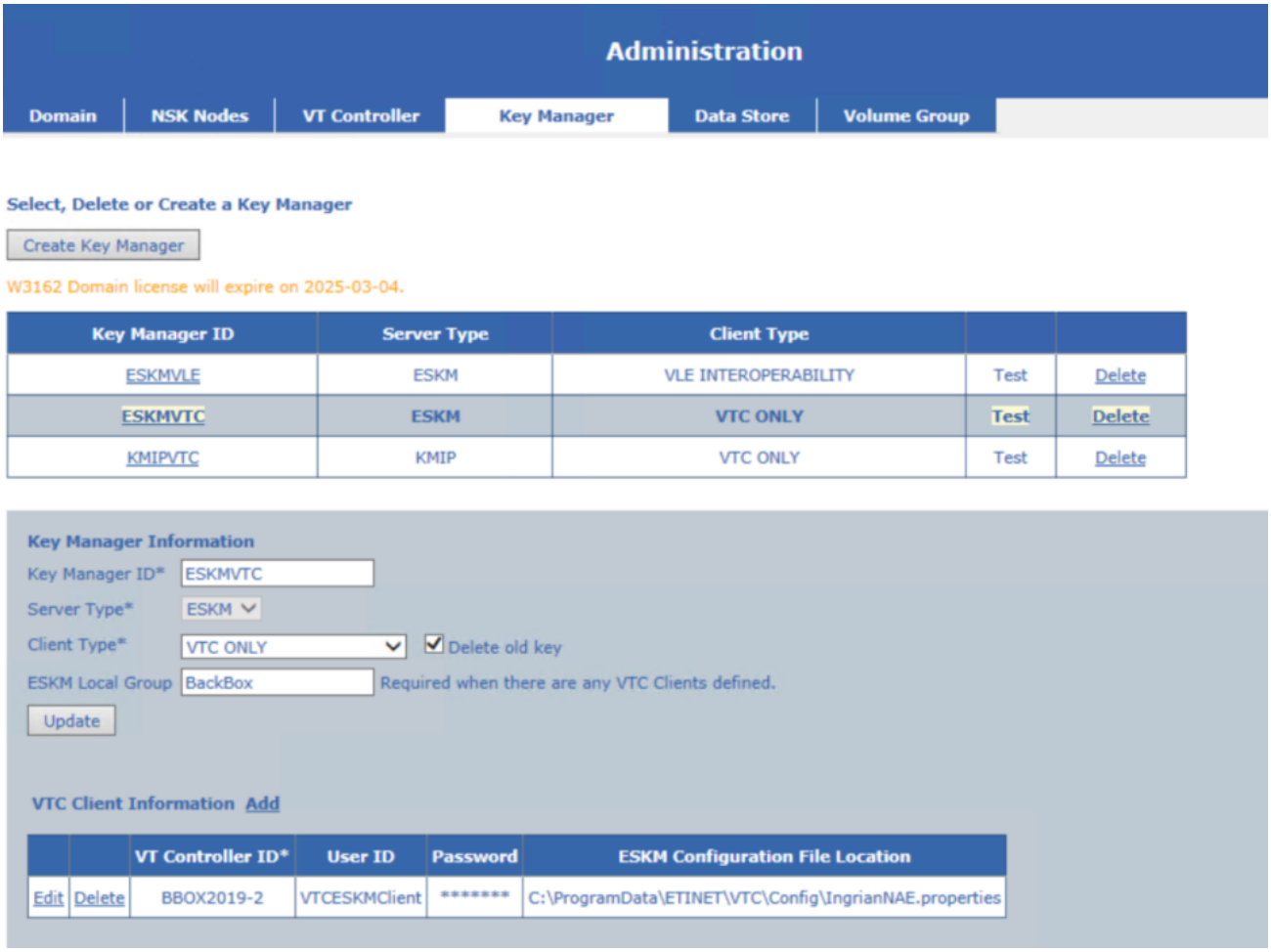
The encryption is enabled in the Volume Group configuration by the attributes Encryption Algorithm and Key Manager ID.

Each Key Manager is configured by:

- A general common set of attributes, such as the Key Manager ID, the Key Manager server type, and its TCP/IP address for the VTC Clients.
- A VTC client to the Key manager for each VTC that will have to connect directly to the Key manager for encrypting/decrypting during tape drive emulation.
- A VLE-CLIM Client to the Key Manager for each CLIM that will connect to an ESKM Key Manager for VLE processing.

The only role of this VLE-CLIM configuration is to detect the connected CLIM during VLE processing and thereby clearly record which ESKM holds the encryption key for each encrypted volume.
When all involved components are configured, the encryption functionality must be verified before an actual test of an encrypted backup. The Test link of this BackBox Key Manager page will verify the domain configuration and the connectivity to the Key Manager and CLIMs. The Test link is disabled when Configuration is in Edit Mode.

The Delete link removes a Key Manager and all its Clients. The deletion will be rejected when the Key Manager ID is referred by a Volume Group or by any virtual volume that was encrypted with a key provided by this Key Manager.



ESKM Local group: To enter when VTC clients will be configured for an ESKM. The group is defined in the ESKM to authorize several clients to share encryption keys. “NonStop” is a common value when VLE (ESKM only).

Update

Click button to have Key Manager Information changed be saved in memory.
IP address(es): used to communicate with the Key Manager server. Add an IP address for each Key Manager

server. Click Add button to add the IP address t the list. You can modify the existing IP address by editing it from the table.

- VT Controller ID – specify the VTC ID (select from the list the appropriate Key Manager client that communicates with the Key Manager server)
- User ID - ID of the account to connect to the key manager server
- User Password – Enter account password and confirm it by re-entering it in the field

ESKM only

- ESKM Configuration File – Path to the NAE properties configuration file that defined Certificate, CA, Private KEY and Pass-phrase.

KMIP only

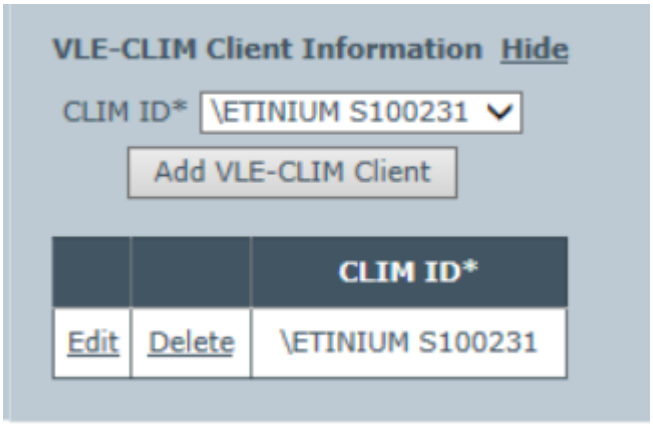
- Key Pass-Phrase - Enter the key passphrase for the private key file and confirm it by re-entering it in the field
- KMIP Client Certificate File – Certificate file used to establish the SSL connection and the Key Manager server (refer to your IT support team to have the file generated)
- CA Certificate File – Enter the CA Certificate File
- Private Key File – Private key file used for the SSL connection between the client and the Key Manager server.

Click Add Key Manager Client button at the bottom of the page to finish up the Key manager setting up. Details on the Key Manager setting will be displayed in a table like the one below.

		VT Controller ID*	User ID	Password	Key Passphrase	KMIP Client Certificate File	KMIP VTC Private Key File	KMIP CA Certificate File
Edit	Delete	VTC_MONTREAL	toutatis	*******	*******	D:\Cert\eskmca.pem	D:\Cert\toutatis.pem	D:\Cert\toutatis.pem

Key Manager – VLE CLIM Clients

When the Encryption keys are managed by the Storage CLIMs for VLE processing, the CLIMs hosting the LTO 4 virtual tape drives must be identified as Clients of the Key Manager in order to identify which Key Manager holds the Encryption key of each volume. The current list of VLE CLIM Clients is presented on the Key Manager page. New CLIMs can be added by clicking on the button Add VLE-CLIM Client.



CLIM ID: Select a CLIM in the selection list. The selection list is based on information queried from the host during the VTC configuration of tape drives in the BackBox Domain. The list of proposed CLIMs is limited to those associated with a tape drive of the BackBox Domain, defined as LTO 4, and enabled for VLE by SCF.
If the proposed list is empty or unexpected, check that the tape devices are enabled for VLE in SCF, and refresh the host information in the VTC configuration page of the involved VTCs by the link Update devices based on the probe result from the VTC and all hosts.
The Key Manager connectivity should be tested before testing actual virtual tape Encryption, in any case of Encryption setup – including HPE VLE.
The Key Manager page is shown in the list of configured Key Managers, and the Test link is available when the Configuration tab is in the Browse mode.
The Test will execute several verification tests and show the resulting report in a new window.

- The connectivity of all VTC Clients to the Key Manager, will be tested by a query to the Key Manager for its identification and for each of the IP addresses configured for the Key Manager.
- All VTCs in the domain having LTO 4 devices, will be tested to check if the LTO 4 devices are connected to a CLIM recognized as a VLE CLIM Client to the Key Manager.
- The LTO 4 drives must be started to allow BackBox to check the host WWN and compare it to the VLE CLIM Client configuration. If there is a match, the connectivity to the Key Manager from the CLIM will be assumed.

- The domain configuration will then be analyzed to:
    - Detect the Volume Groups using the Key Manager ID.
    - Verify that the VTC routed to the corresponding Data Stores, have the connectivity to the Key Manager.
    - Verify that the VTCs have the Encryption license option for at least one drive.

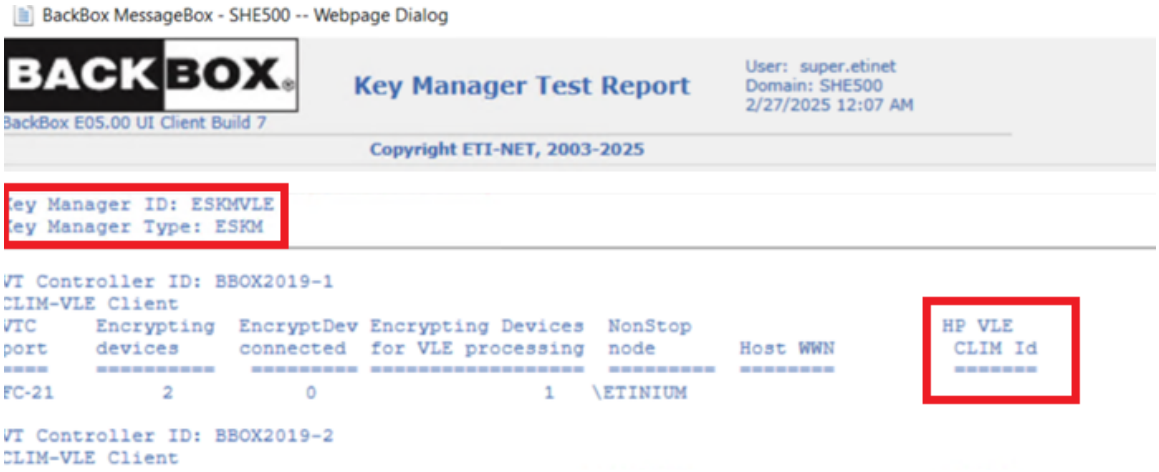
Key Manager – Test Report

Only those VTCs that actually receive messages, will be shown in the Key Manager Test Report. For each VTC, there can be three sections:

- A section VTC Client showing the report generated by the VTC.
- The report is green for success, orange for any warning not preventing connectivity, and red for a complete lack of connectivity.
- A section VLE-CLIM Client showing a report of counts of FC LTO 4 drives per port and connected host WWN. The report is green for success, orange if no LTO 4 drive is currently connected to a recognized CLIM, and red for a complete lack of connectivity.
- A list of messages pertaining to the VTC.

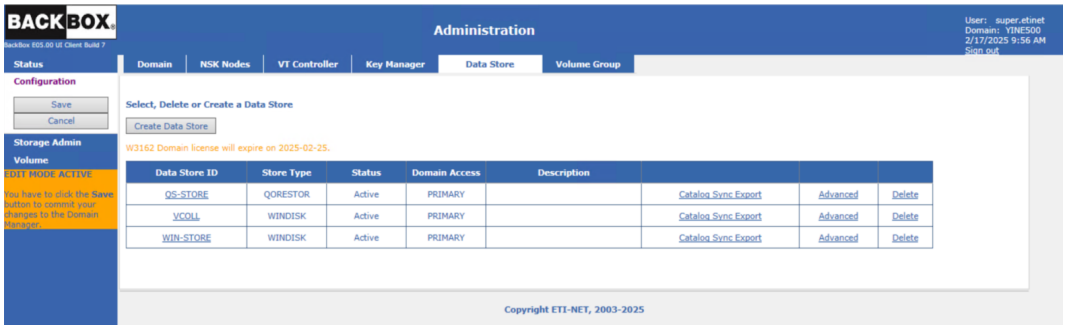
The messages are explained in the BackBox Messages Manual and Troubleshooting

Three Test report samples are presented after the common underlying VTC configuration below, with each sample showing its specific Key Manager configuration page and the associated Test report page:

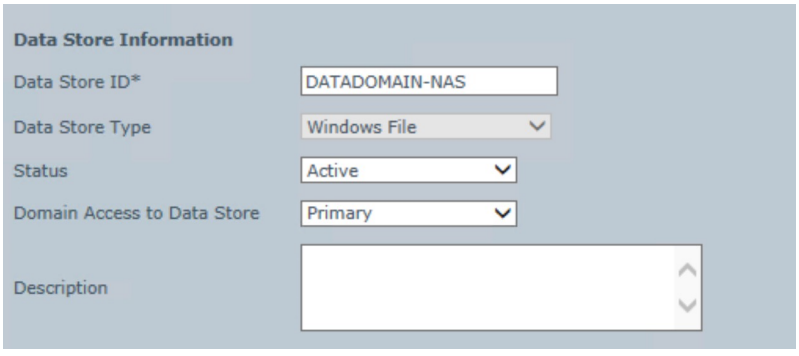


Data Store

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 is available to add a new data store.



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.

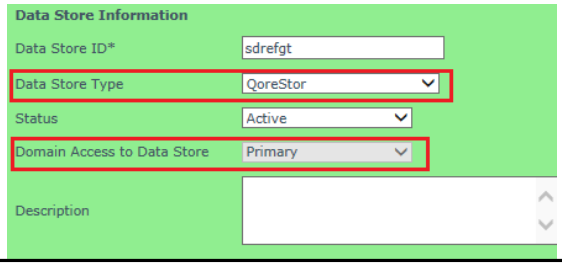
- ACTIVE: Default, no restriction to volume operations.
- INACTIVE: Tape volumes cannot be loaded to be read or written. Automatic operations such as the free-up of expired storage are disabled. As an exception, catalog Export/Import functions (Catalog Sync) are still active.

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 BackBox, and DSM/TC tape catalogs. The domain has a read-only view of the Data Store and cannot execute backups.

> For QoreStor DataStores, domain access to data store is by default set to **Primary** and it cannot be modified to **Secondary** or **Restricted**.
>
> 
>

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.

- 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 BackBox catalog.

Description: Optional user description.

DATA STORE TYPES

There are 2 data store family types, based on the network file-sharing protocol:

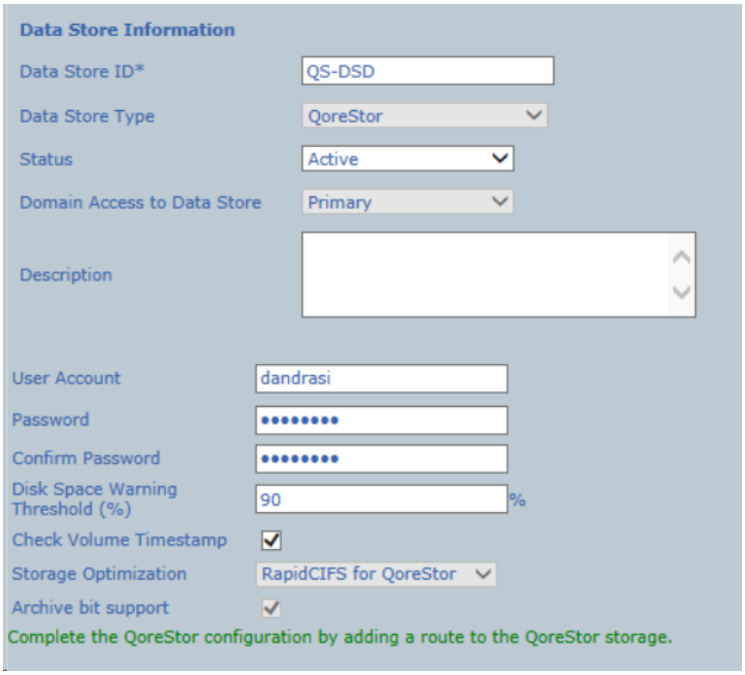
- CIFS
- API

CIFS-based Data Stores	API-based Data Stores
QoreStor	IBM TSM
Windows Files	

CIFS-BASED DATA STORES

QoreStor Data Stores

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.



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.
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.

⚠	For QoreStor DataStores, User Account names cannot be Administrator, admin or monitor. Only alphanumeric (letter and/or digit) values are allowed as names for users. For more details about QoreStor users see Users in VTC MC section.

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 can- not be modified. For QoreStor Polices and QoreStor Pool should be set through QoreStor Data Store Configuration Wizard by clicking on Add.

Once you click the Add button, the DataStore Configuration Wizard opens up at the bottom of the page.

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.

If you want to use encryption at rest, check the box and click Step 2 button to go to the next step.

Check the QoreStor Replication box if you plan on using inter-VTC replication or don't check anything and click Step 3 button to go to the next option.

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.

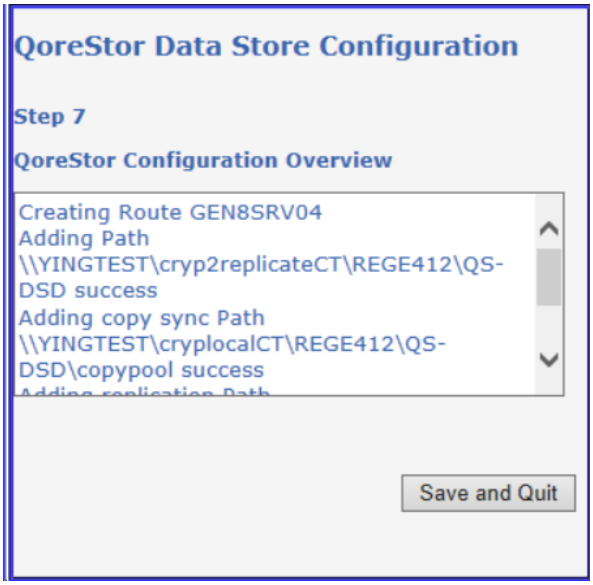
Check the **Cloud Tier** box if you want to enable Cloud Tiering option. Go to the next wizard option.

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 this 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. You can add multiple routes, but you need to click Add Route after each selection.

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.

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).

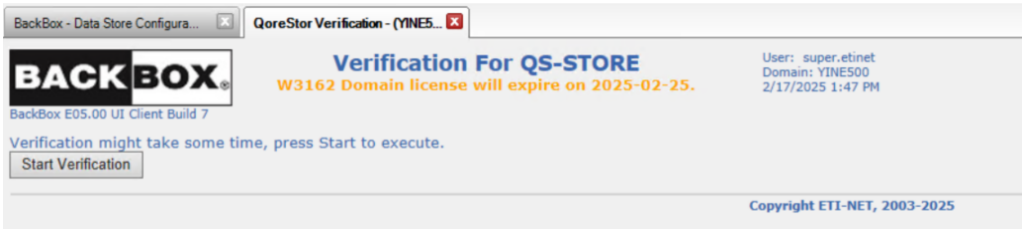


Click Save and Quit to save your configuration or Quit to quit the wizard.

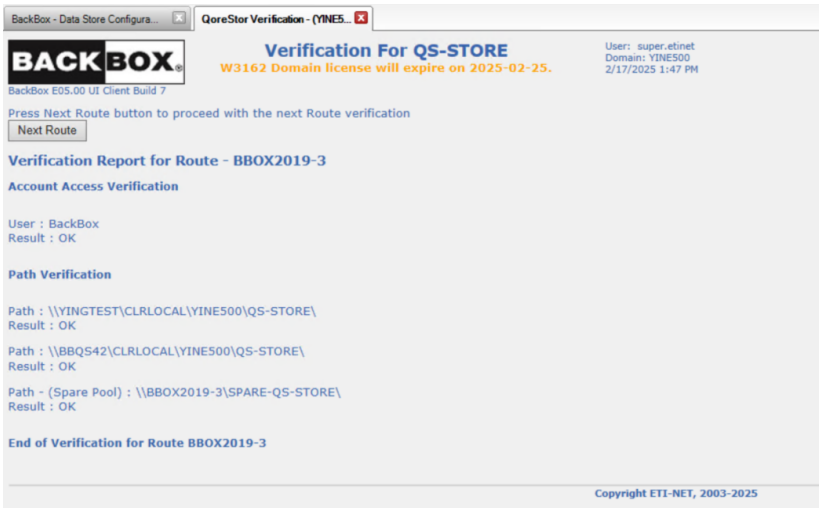
Click on 

to run a verification process on the QoreStor Storage route(s). In the newly opened window start the verification process by clicking on 

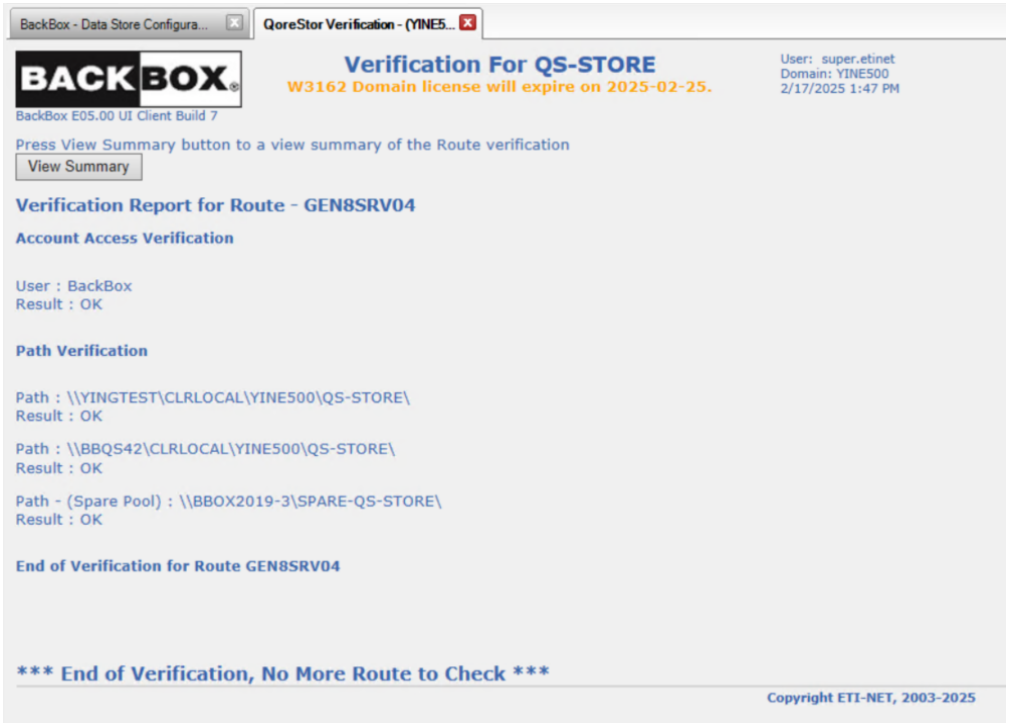
.



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.



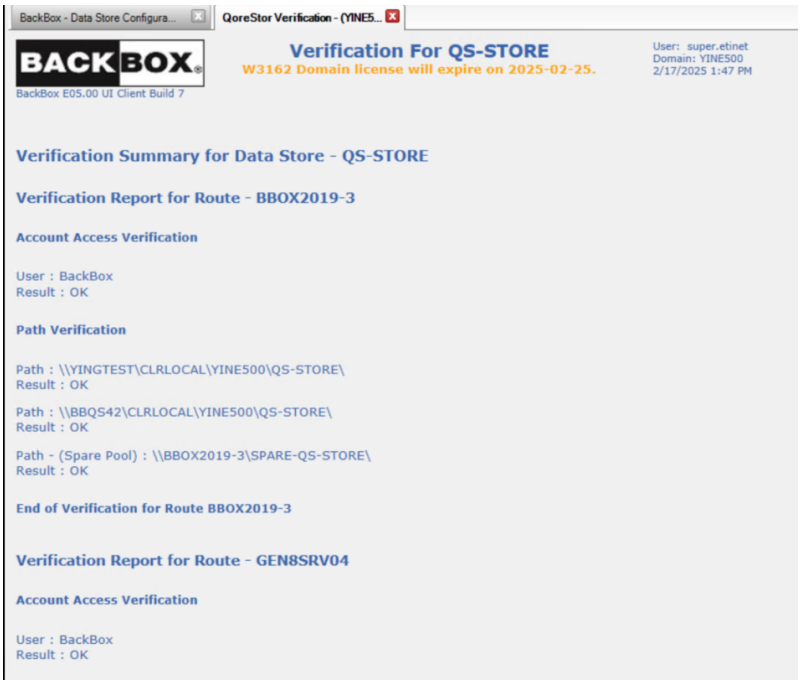
If there is another route to be verified, click Next Route to verify it.



If you have more than one route, click Next Route to display the verification report for the next route.

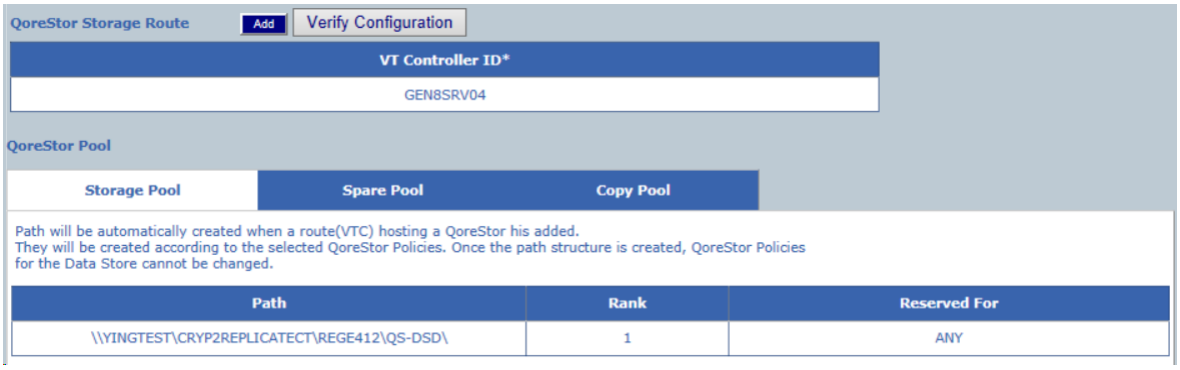
Click on 

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.

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. The bottom panel will display info on QoreStor Policies, details, QoreStorStorage Route and QoreStor pool. The bottom of the Data Store Information panel will display all QoreStor related data store details:

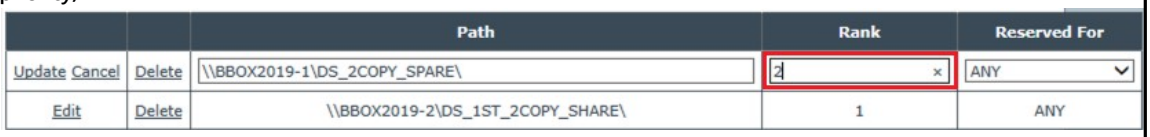


The policies configured with the wizard are listed, check-marked if active, and grayed-out; they cannot be modified even if you switch to edit mode. QoreStor Storage Route indicates the main storage route to the server. QoreStor Pool indicates the paths for each StoragePool, Spare Pool and Copy Pool. 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.

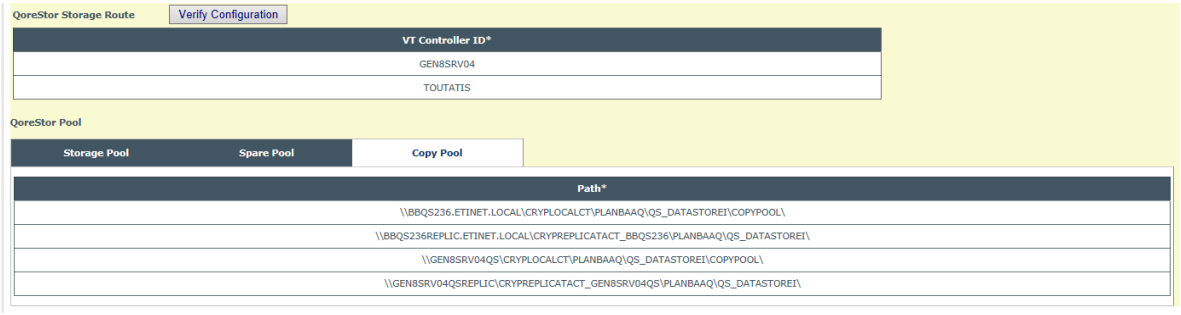
Path: The path name where virtual volumes will be stored. Each path must be a fully qualified Network Share entered as a UNC path (e.g. \\SVR1\BBOX\STORE1).

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 unavailability. To force-use that specific path, choose a rank value from 1 to 99 (rank 1 corresponds to the highest priority).

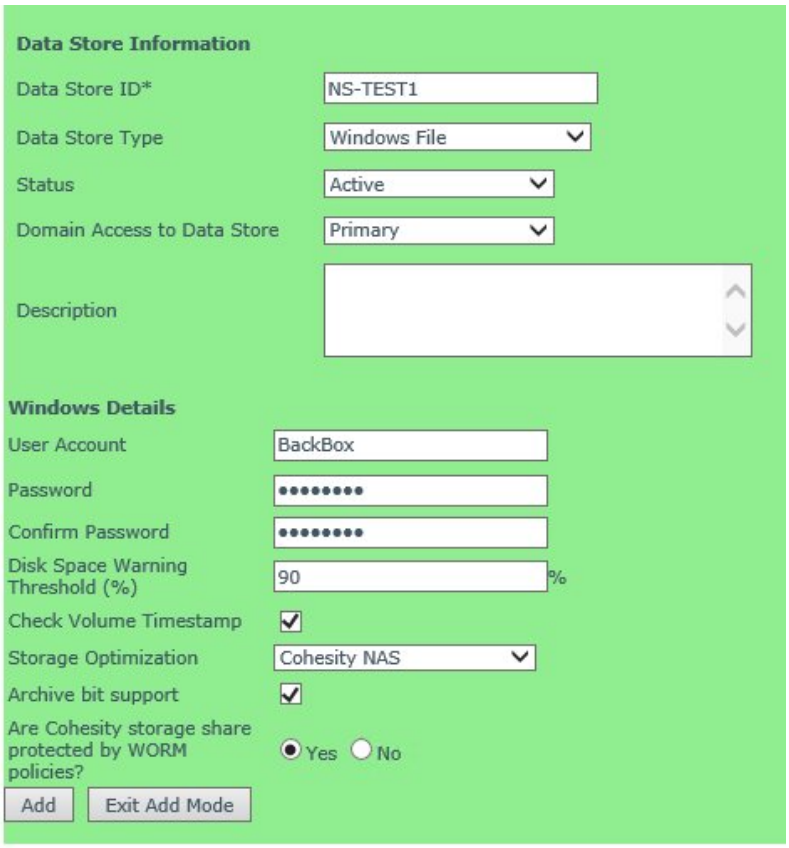


Reserved For: Allows entering a Volume class for which the path will be dedicated.



The copy pool sync path spare as well automatically created, based on the two routes (added with the Wizard) for each embedded QoreStor appliance.

Windows File Data Store



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, they can implement it by scripting with BB004 on Tandem side.

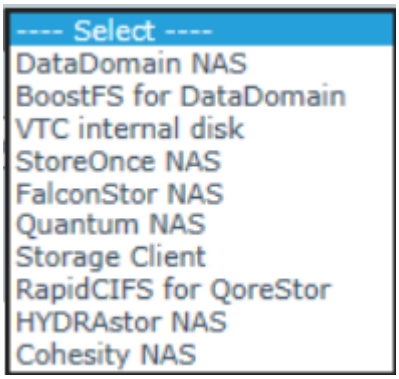
Disk Space Warning Threshold (%): This parameter is used by the NonStop TACL macro BB022_CHECK_SPACE to check the total free space available in all Windows Data Stores. When the space occupied on disk is higher than this threshold, the EMS message 3217 is issued by the daily job OBB017.

⚠	If the 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 dis-able 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.

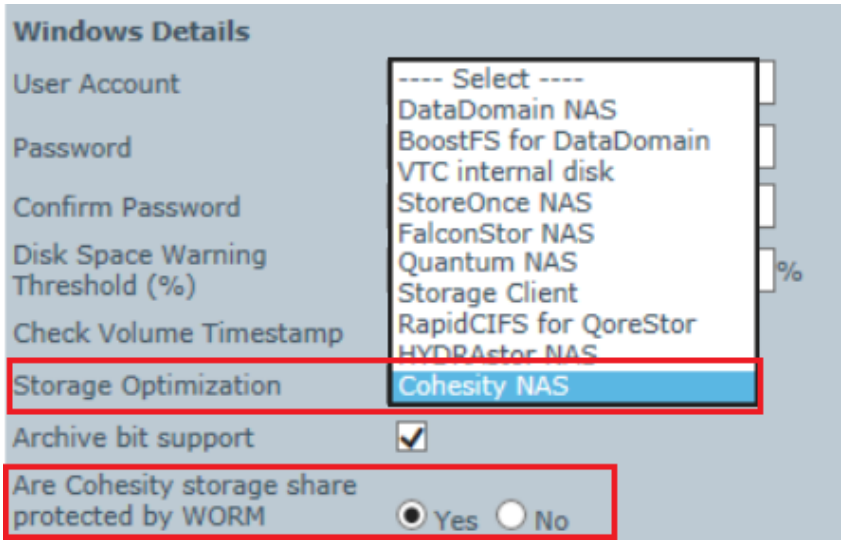
Storage Optimization: This selects a deduplication engine. Depending on the client storage, data store could be optimized with BoostFS for DataDomain, RapidCIFS for QoreStor, DataDomain NAS, StoreOnce NAS, VTC internal disk, FalconStor NAS, Quantum NAS, Cohesity, HYDRAstor NAS, etc.



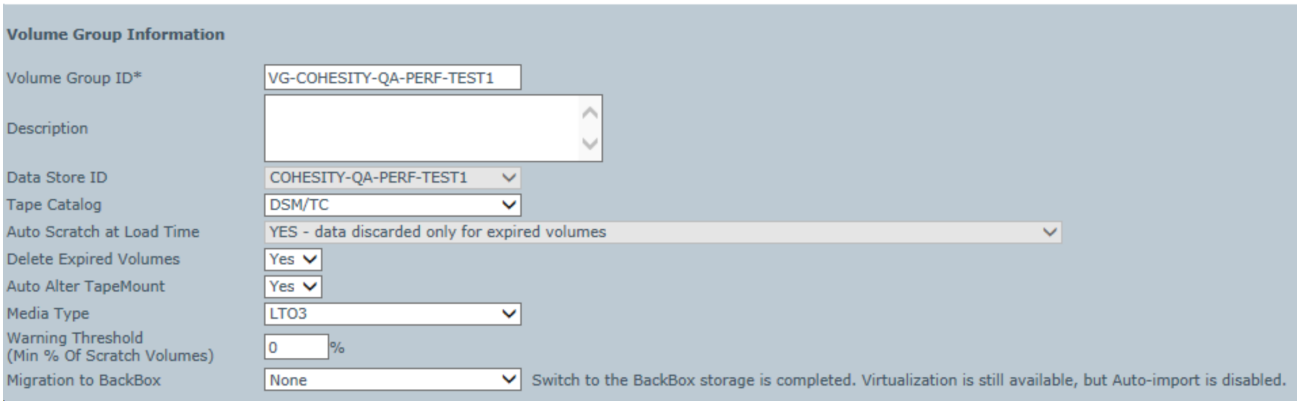
⚠	When running a backup with RapidCIFS optimization, the volume groups (NOC, CAT, TMF, etc.) sub-folders are automatically created within the data store folder. Ex: \\192.168.20.153\QA_Container\VG_NOCAT, \ \\192.168.20.153\QA_Container\VG_CAT

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.

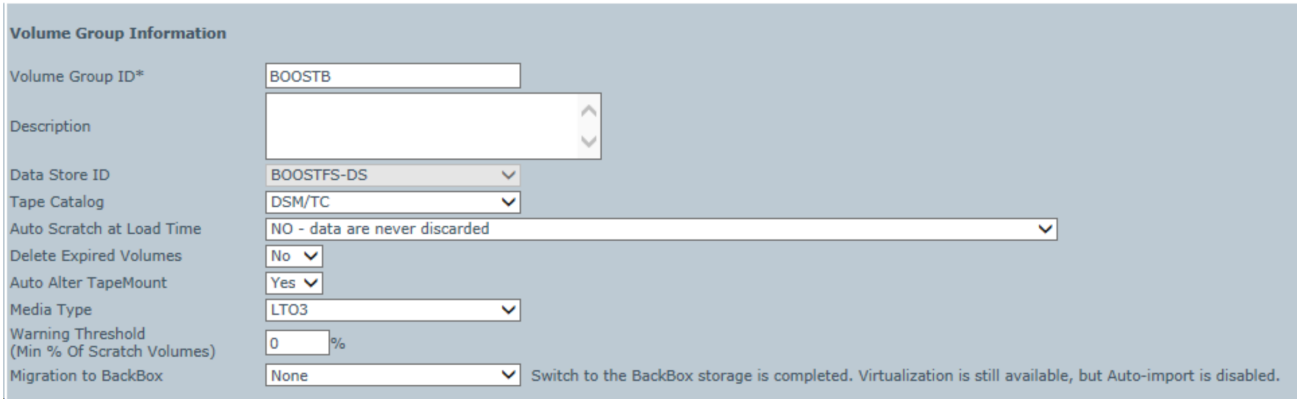
WORM Compatibility: Option active only for DataDomain NAS, BoostFS for DataDomain and Cohesity NAS.



- If yes, all volume groups belonging to the selected data store will have Auto Scratch at Load Time field restricted to YES, meaning that data will be discarded only for expired volumes. This specific configuration forces the auto-scratch function: expired volume data is purged.



- If no, data deletion will be processed according to the auto-scratch policies configured by the user.



⚠	Auto Scratch at Load Time - default value YES. The content of expired virtual volumes is deleted at load time. Auto Scratch at Load Time - set to NO. The content of expired virtual volumes will not be deleted at load time. For more details on Auto Scratch at Load Time function, see Volume Group, Volume Group Information.

WINDOWS POOL

This section permits adding or modifying apath for storing Windows files in three different pools:

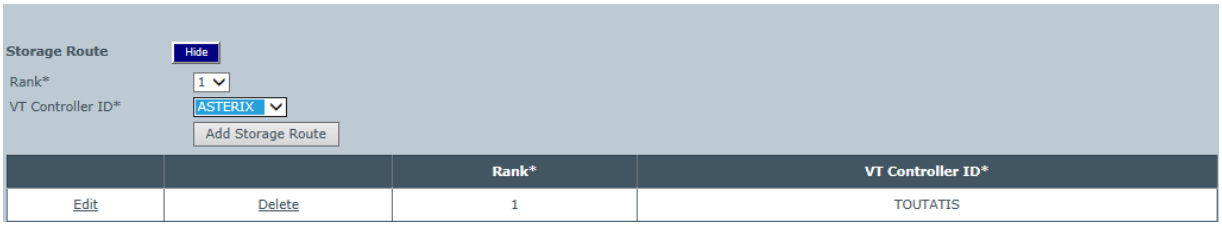
Storage pool is the normal pool.
Spare pool is an emergency pool for writing new backups when the Storage pool is not available.
Copy pool is assumed to contain a copy of the files in the Storage pool and it's used only for a restore when the volume is not found in the Storage pool. Files are either copied via the Copy Sync Pool option (provided with the customer installation)or copied independently of the BackBox.

⚠	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. 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). When the data store has only one route (hence, it can be accessed by only one VTC), the path name can also be 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

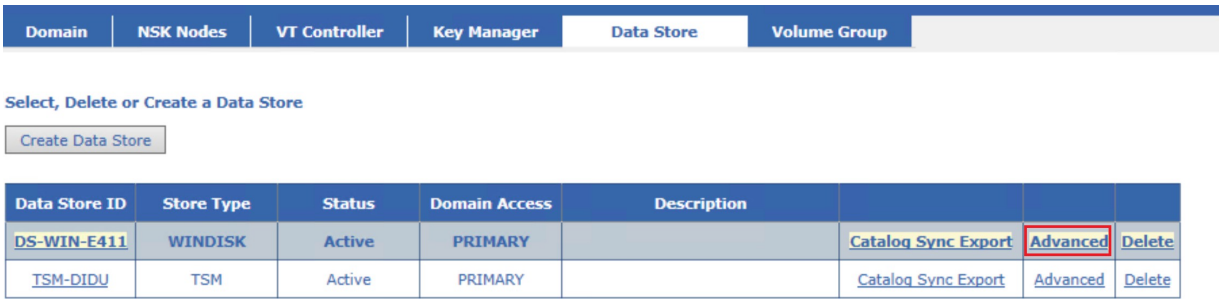


This section lists all VTCs with access to the storage.

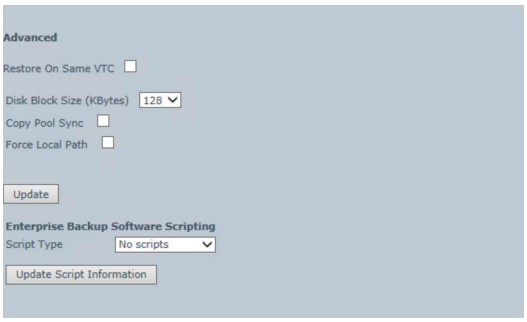
Rank: Indicates the route priority. The highest priority is 1.
VT Controller ID: Identifies the VTC connected to the selected Data Store.

QoreStor/Windows File Data Stores - Advanced Properties

Select the Data Store ID in the Data Store table and click Advanced.



At the bottom of the page, advanced details and options are displayed for the selected data store.

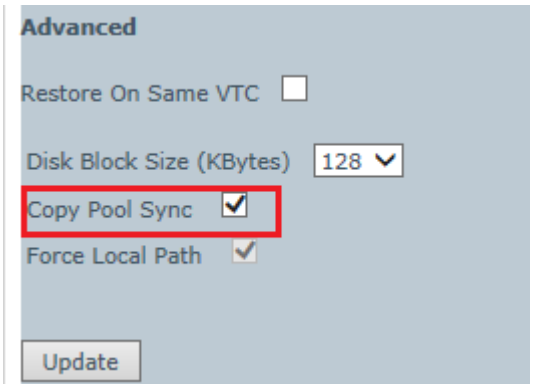


Restore on Same VTC: When checked, and when the TAPE DEFINE set for restore (USE IN) does not specify a tape device, the volume will be read from a device on the same VTC on which this volume has been initially written. When VTC local storage is used for a Data store (DAS or SAN), it is generally better, 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 I/O 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. CopySync program is submitted via COPYSYNC job, after a performed backup or on demand, through the UI. Enabling this option will automatically restrict and change the Scripting Backup Method to Other Methods (triggered by Enterprise Backup Software), in case of scripting being used for this Data Store.

The implicit backup script (in the scripting section) to be disabled.



Selecting Copy Pool Sync will automatically force the local path, therefore the Force Local Path is grayed-out. 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 indicates to the Copy Pool Sync program the amount of time to wait between two I/O 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.

The Scripting sections differ according to the Scripting type selected. Scripting types are No Script, Generic, TSM and Manual Restore.

Scripts, which are optional, are used to specify a Windows command files to be executed following specific tape events. When a file name is specified, whenever possible, it must be fully qualified and it must be copied in each VTC in the same location.

The scripting section also includes Script Parameters (for more details on script parameters refer to Appendix K - Scripts Guidelines) list of users and predefined Windows environmental parameters that will be passed to the scripts (according to the scripting type selected).

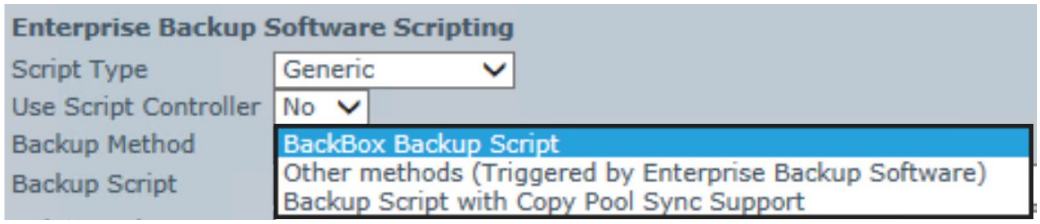
These parameters are passed as Windows environment variables to the shell executing the script, in addition to the parameters generated by the VTC to identify the files to process in the script.

To add a parameter simply click the Add button when in edit mode and enter the required information. The following is a description of the Scripting section by Scripting type:) list of users and predefined Windows environmental parameters that will be passed to the scripts (according to the scripting type selected).

These parameters are 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 process in the script. To add a parameter simply click the add button when in edit mode and enter the required information.

Enterprise Backup Software Scripting: Optionally specify Windows command files to be executed fol- lowing specific tape events. For more info refer to Scripting/Background Migration on Tapes and Appendix J - Script Guidelines.

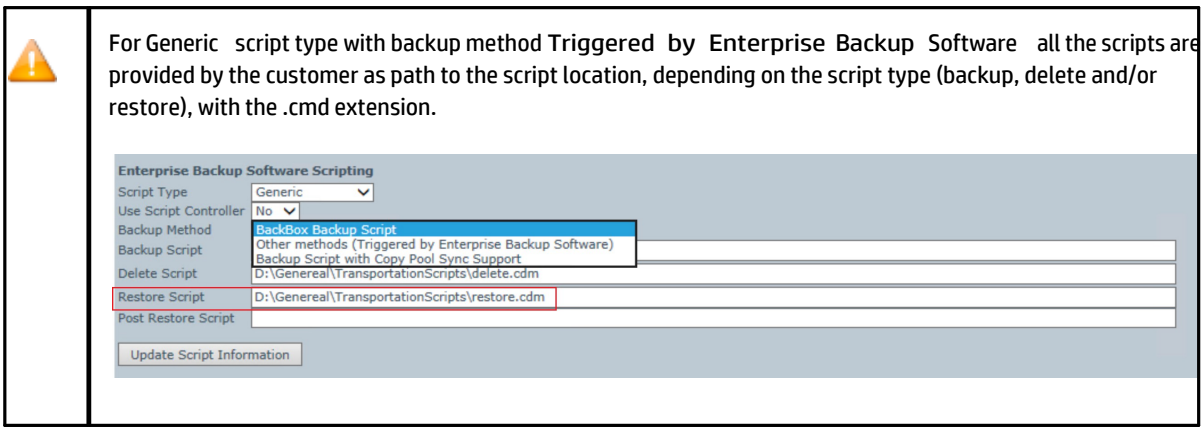
- For Manual Restore, the backup method is hard-coded and it istriggered by the Enterprise Backup Software.
- For Generic script type, the following fields are available:
  Backup Method: available options are BackBox Backup Script (the script provided by BackBox), Other methods (Triggered by Enterprise Backup Software) or Backup Script with Copy Pool Sync Support.



Use Script Controller: To enable or disable the script controller, contact the support team.

⚠	Backup Method: Only Other Method is available if Copy Pool Sync option is active.

Backup Script: command file to be executed after a volume unload. Not available when Copy Pool Sync is active.

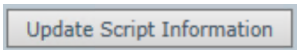


Restore Script: command file to be executed at volume load, when a virtual media cannot be found on the Data Store.
Delete Script: command file to be executed after a volume has been deleted.
Post Restore Script: command file to be executed after a volume requiring the RESTORE script and mounted for input (USE IN) has been unloaded.
Script Parameters: They are optional and user-defined. Named parameters that will be passed on to the scripts. 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.

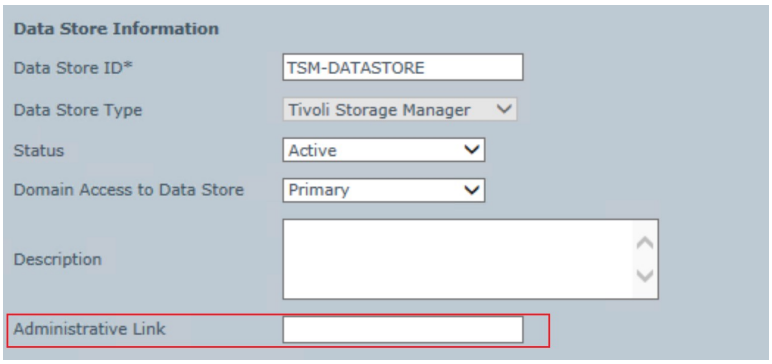
Name: The name of the parameter. Do not specify the % sign after or before the name.

Value: The value of the parameter. Refer to section Appendix J - Script Types for more information.

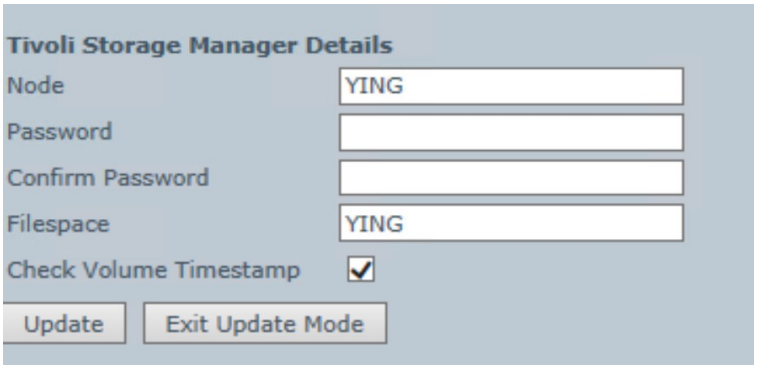
Click  button to save the scripting information.

API-BASED DATA STORES

IBM Spectrum Protect (Tivoli Storage Manager - TSM) Data Store



Data Store Information panel is similar to the other types of data stores, with the addition of an Administrative Link, available only for IBM Spectrum Protect TSM.
Administrative Link: Optional URL of an administrative client for the Data Store.



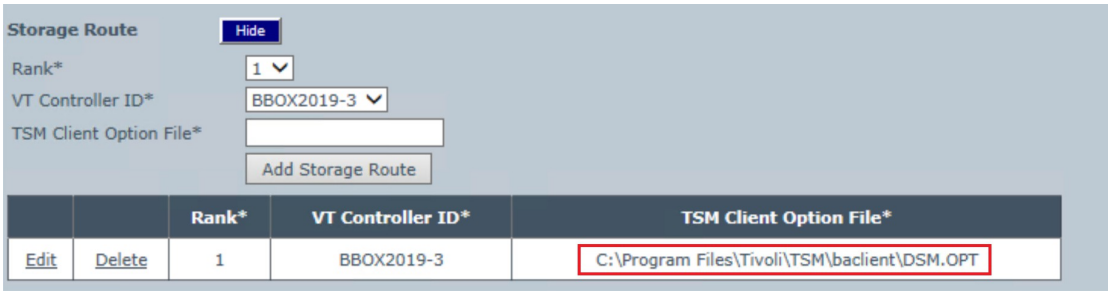
Node: IBM Spectrum Protect (TSM) node name used by the VT Controller to log in to the IBM Spectrum Protect (TSM) Server. This node must be created by a IBM Spectrum Protect (TSM) administrator.If omitted, the IBM Spectrum Protect (TSM) client configuration file (dsm.opt) must contain the node name and 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.

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.

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 FileSpaces.

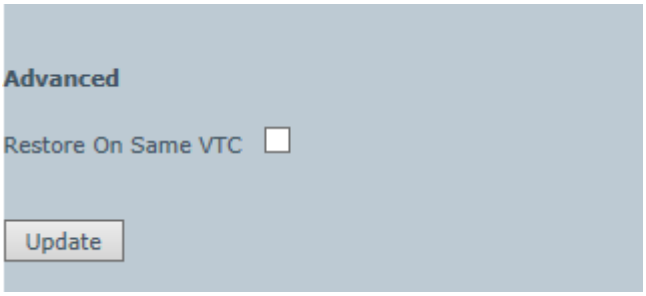
Storage Routes



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.
TSM Client Option File*: .OPT file, specific to TSM, provided by the client. Specify the location of the file, as in the example above.

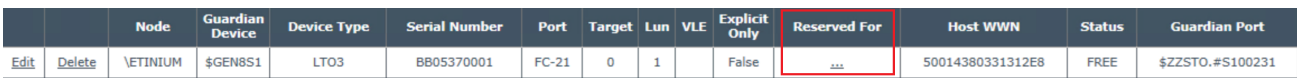
IBM Spectrum Protect (Tivoli Storage Manager - TSM) Data Store - Advanced Properties



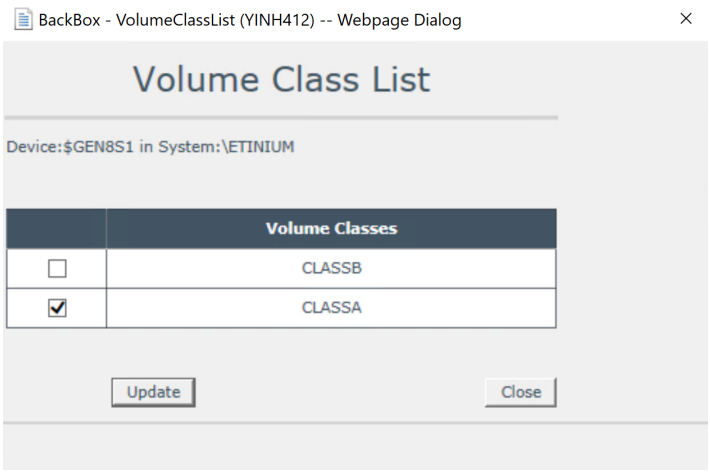
Restore on Same VTC: When checked, and when the TAPE DEFINE set for restore (USE IN) does not specify a tape device, the volume will be read from a device on the same VTC on which this volume has been initially written.

VT Controller Device Reservations

The Volume Class List page is opened when the Reserved For link of the VT Controller page is clicked.



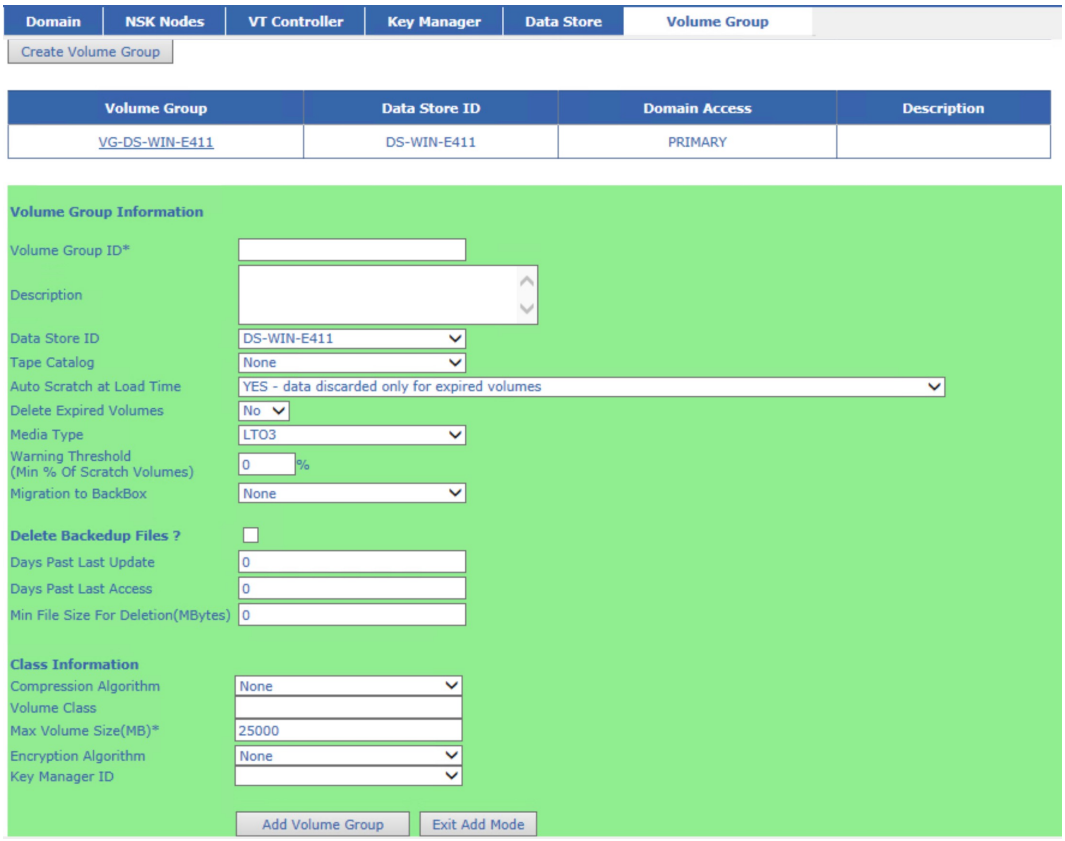
The pop-up window lists the volume classes configured in Volume Groups and permits device reservation for one or several volume classes.



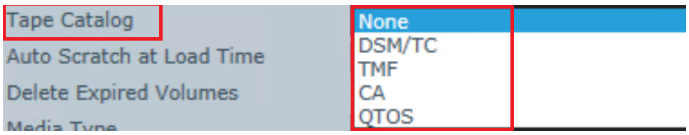
Device: Identifies the device.
Volume Class: Shows the volume class list. Check the classes for which the device must be reserved. If no class is checked, the device is available to volumes belonging to any volume class.
Select the class to reserve it for the specified device.
Click **Update**.

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.



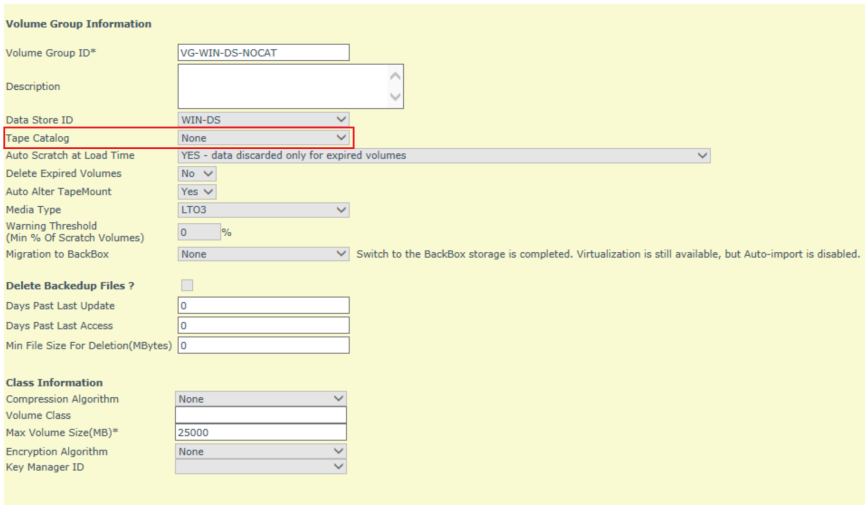
The page layout and the page elements vary according to the Data Store. The example above is for a group associated to a DSM/TC pool and a Primary Data Store.
The Advanced properties are common to all Volume Groups and documented at the end of this section. For Windows files data stores, the page layout varies depending on the catalog type.



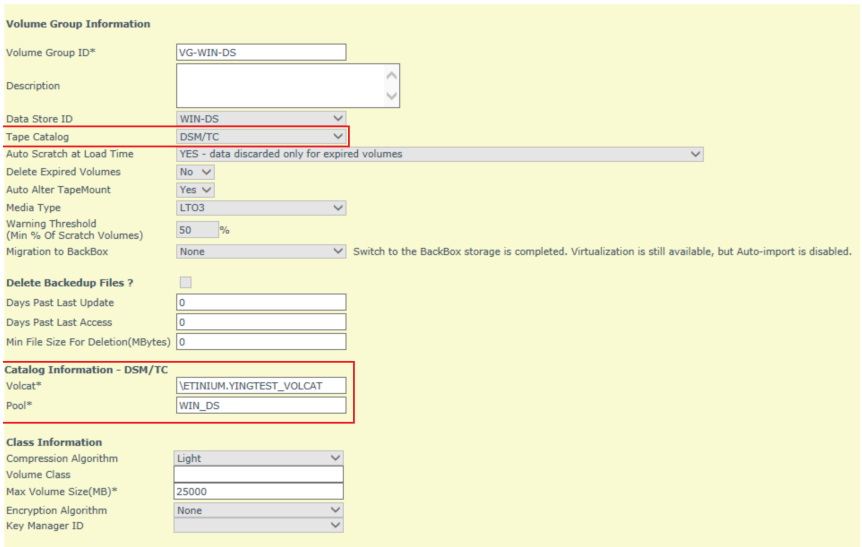
Windows files - DSM/TC catalog
Windows files - QTOS catalog
Windows files - TMF catalog

For IBM Spectrum Protect (TSM) data stores, the same catalogs are possible - although only the DSM/TC layout is presented below.

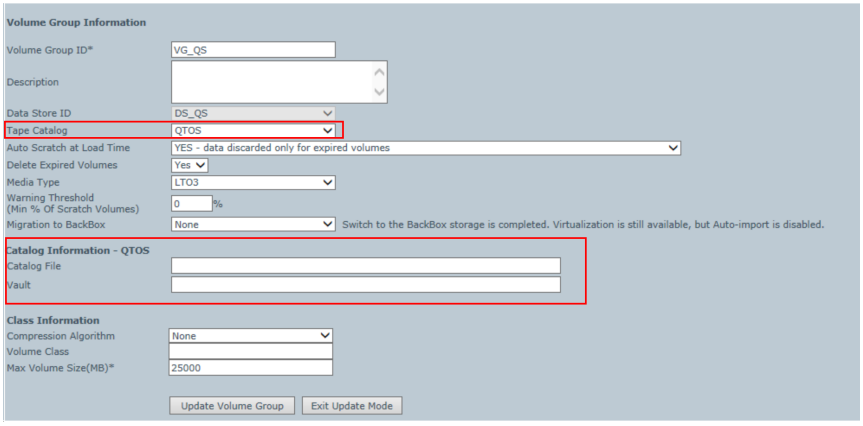
Volume Group Windows Files - No Tape Catalog



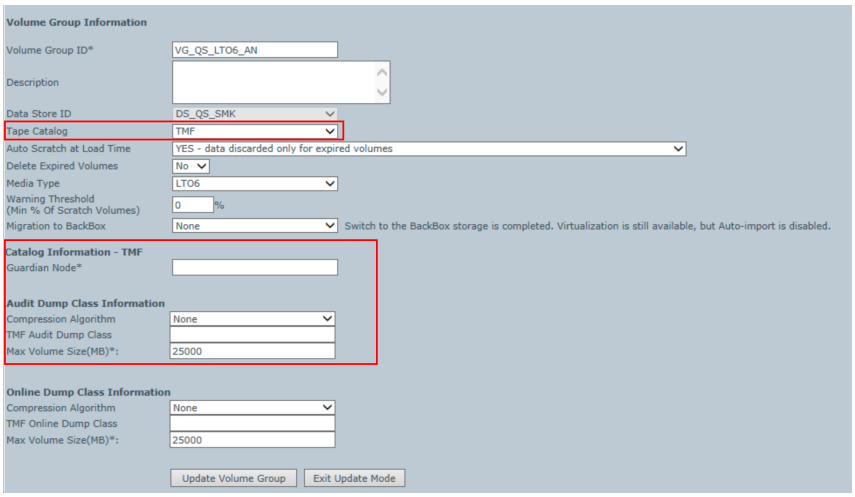
Volume Group Windows Files - DSM/TC Catalog



Volume Group Windows Files - QTOS Catalog



Volume Group Windows Files - TMF 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 or QTOS).

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 BackBox.

- If **WORM Compatibility** is enabled (set to **YES**) - the **AutoScratch at Load Time** option is grayed-out, hence not available for the selected volume group - for the data store where the volume group has been created (option available only for BoostFS for DataDomain, RapidCIFS for QoreStor and Cohesity NAS), data will be discarded only for expired volumes. This specific configuration forces the auto-scratch function: expired volume data is purged.
- If **WORM** Compatibility is disabled (set to **NO**) the AutoScratch at Load Time function doesn't allow data to be automatically discarded, hence data deletion can be set up according to the data purging policies.

⚠	Auto Scratch at Load Time - default value **YES**. The content of expired virtual volumes is deleted at load time. Auto Scratch at Load Time - set to **NO**. The content of expired virtual volumes will not be deleted at load time.

⚠	For QTOS and CA catalogs, there is no expiry test when auto-scratch is enabled. 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).

⚠	If Delete Expired Volumes is set to **No**, the spare move tapes will not be moved, as they are already expired and they cannot be moved or deleted.

	If Delete Expired Volumes is set to Yes, the spare move tapes will be deleted or moved by the end of the day, according to the daily clean-up schedule. In order to delete these tapes before the scheduled time, use OBB017 and perform the action manually.

Auto Alter TapeMount: Mount the tape by automatically asking DSM/TC to substitute another scratch tape from the same pool as the tape to be altered.

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, BackBox 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 BackBox Volume Group and vice-versa.
Filecat: Indicates the DSM/TC file catalog where the tape files and disk files are written by the BackBox 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 BackBox 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 Appendix I - VTC Scripting Options.

- 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.

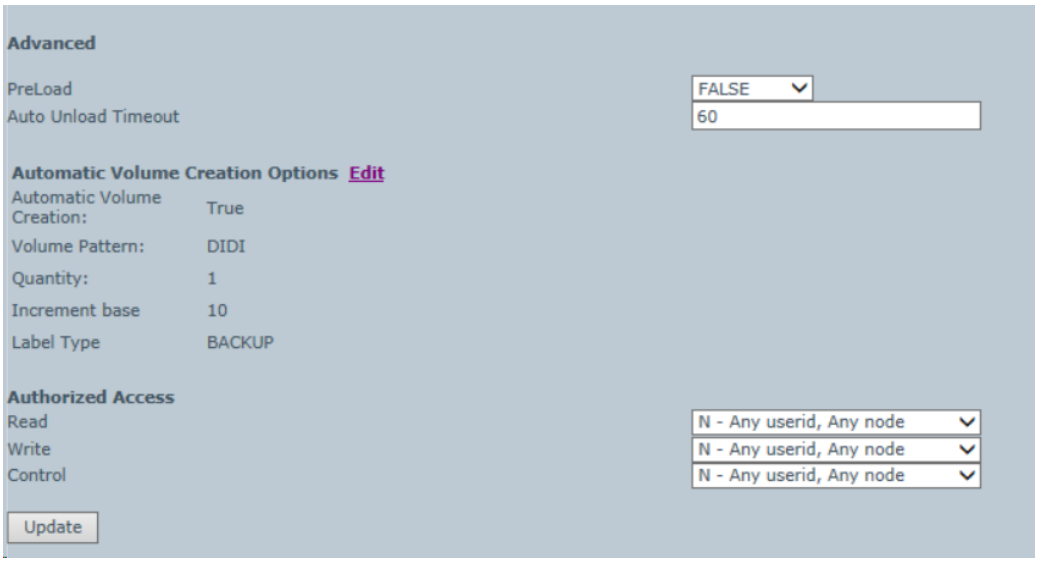
TMF Online Dump Class: This class will be assigned to all volumes in this group.
Max Volume Size (MB): Indicates the maximum capacity (compressed data in megabytes) of the virtual volumes.

Volume Class Information for IBM Spectrum Protect TSM (non TMF)

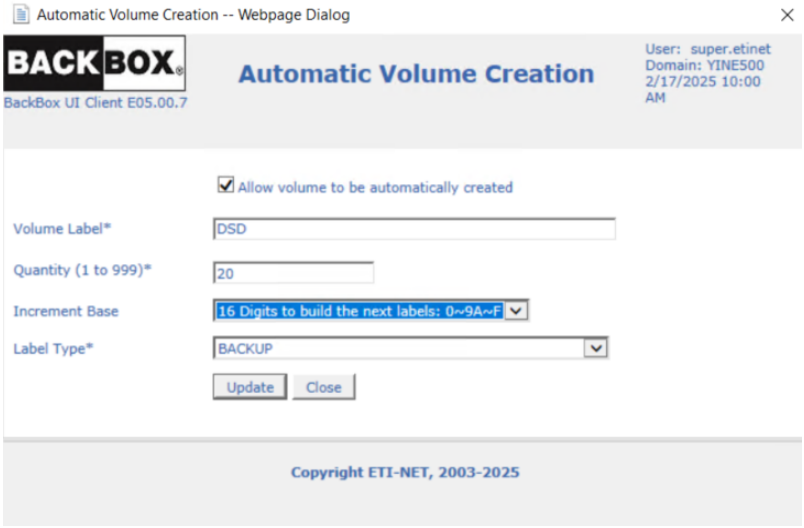
The following fields available when Tape Catalog is not set to TMF and the Data Store type is IBM Spectrum Protect (TSM).

Volume Class: BackBox 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

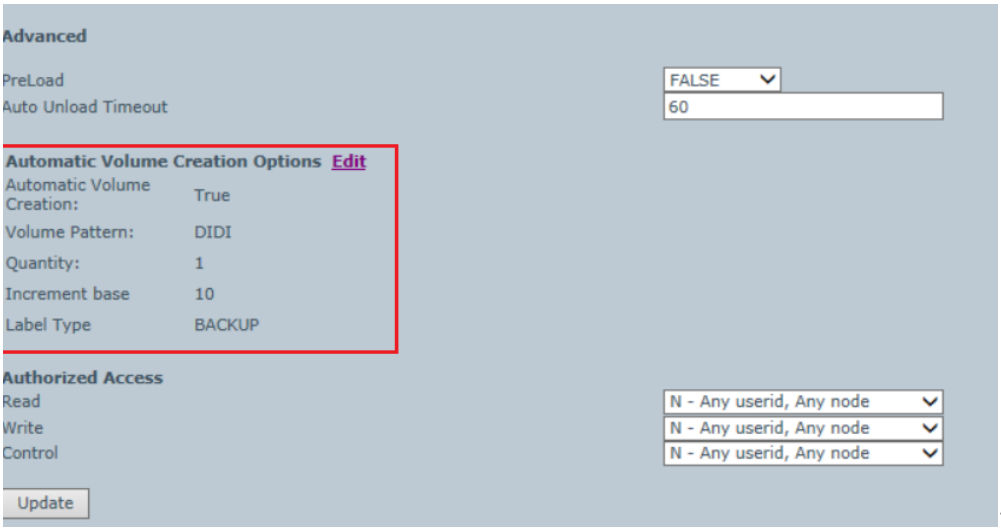


PreLoad: Enabling PreLoad can be useful for the NonStop restore/recover of multi-volume tape files, when a restore script must be executed before the volume can be read by the NonStop. When PreLoad is enabled, the load of the next volume is anticipated (and the restore script initiated) while the previous 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 Volume Creation Options: Click **Edit** to automatically create 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.



Make sure the Volume Label* is alpha-numeric 6 digits long (for example, ABCDEF or YYY000) and the Quantity (1 to 999)* is not

negative or 0. An error message will be displayed if the field values are not valid.
Once updated, the information displayed under Automatic Volume Creation Options will reflect the changes that have been updated.



11

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 BackBox 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 BackBox catalog.

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.

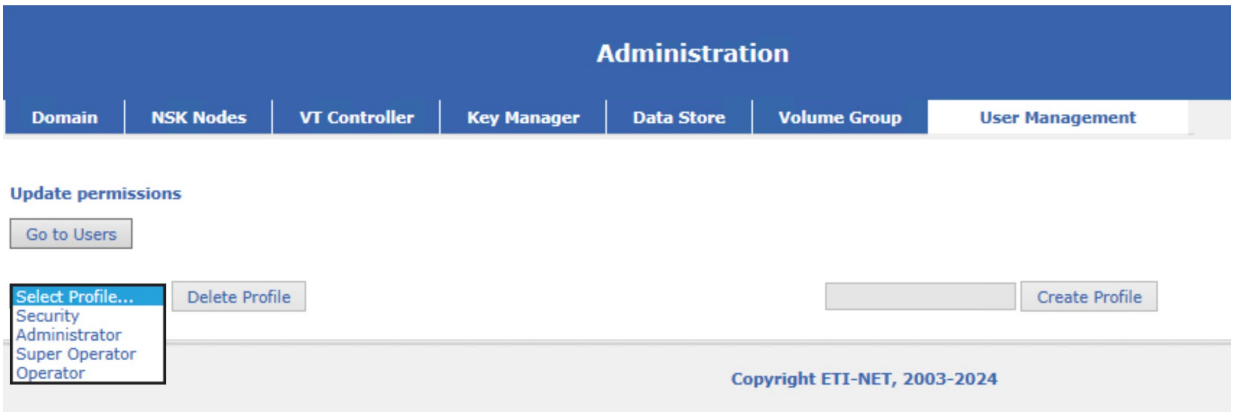
After the initial installation, there are two (2) user profiles automatically predefined: Super.Super and Super.x, where "x" stands for the domain installation owner. Ex: Super.Oper orSuper.QC

⚠	Super.Super user type is not displayed on the UI, as it's a user with full access per- missions and it cannot be managed through the interface.

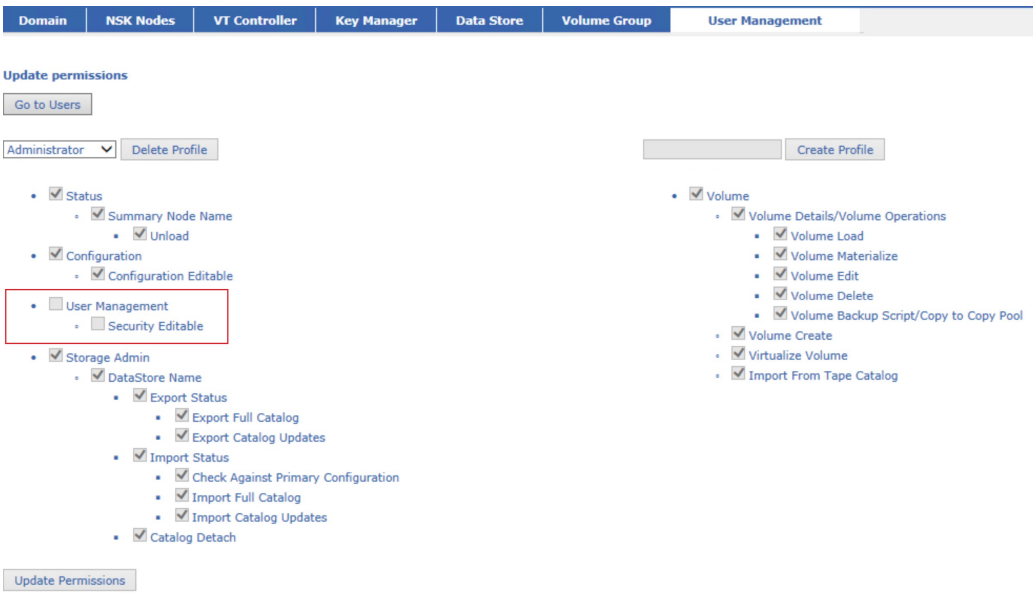
After a fresh install, the default users (Super.Super and Super.X) have the following User Management capabilities:

- Super.Super: administrator permissions with user management capabilities
- Super.X: administrator permissions without user management capabilities

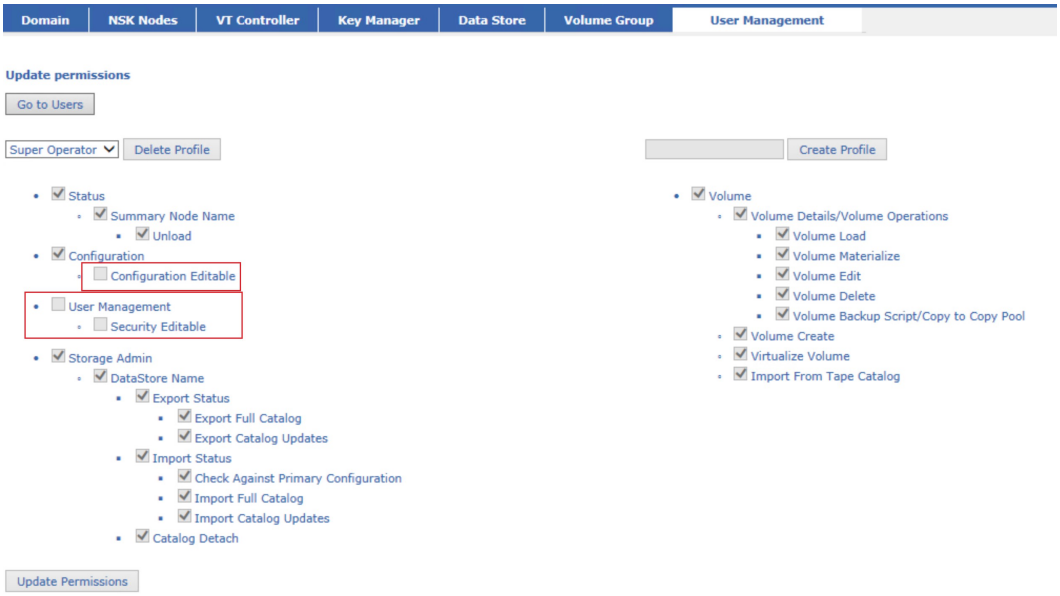
The available default profiles to assign users to are: **Administrator**, **Super Operator**, **Operator** and **Security**.



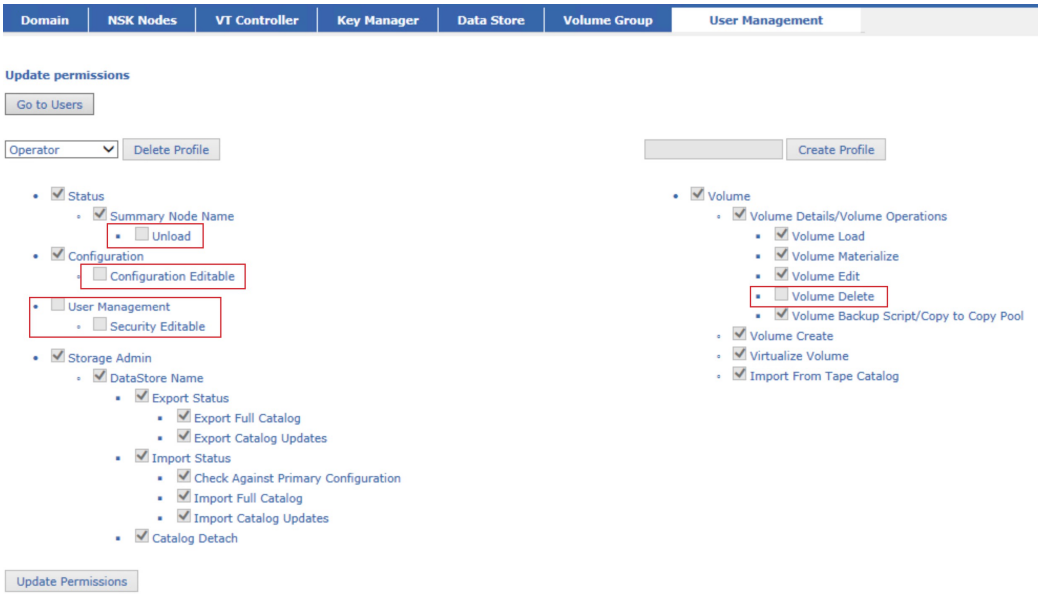
Administrator permissions: full access to all options, except user management



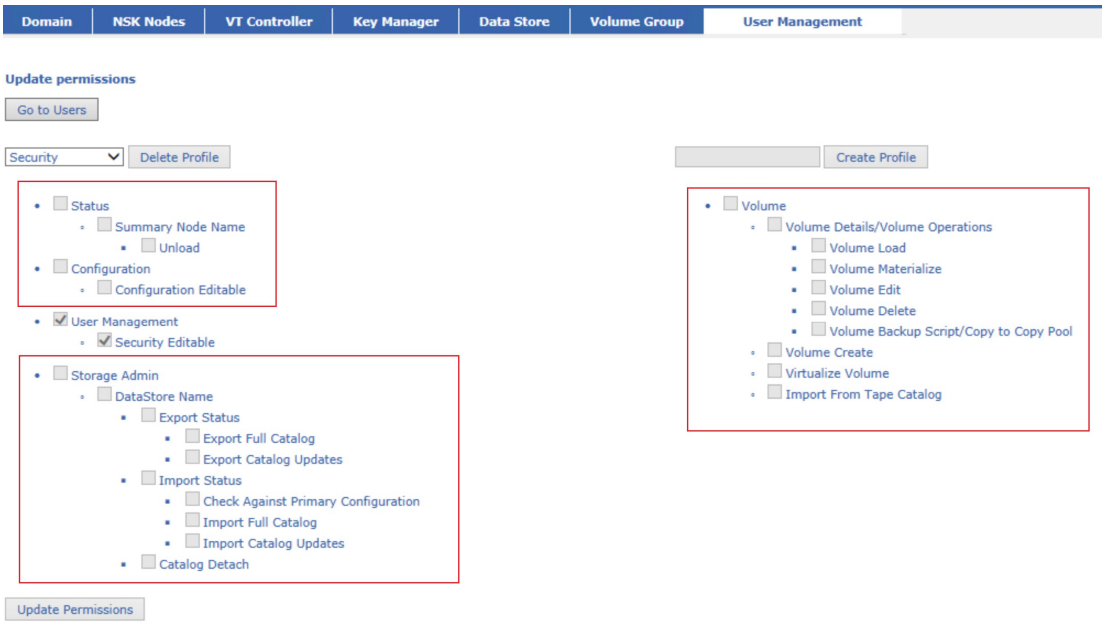
Super Operator permissions: Does not have access to Configuration Editable and User Management - Security Editable options.



Operator permissions: Does not have access to Configuration Editable, User Management - Security Editable, Unload Device and Volume Delete options.



Security permissions: access to User Management-Editable Security page ONLY; can create, delete and edit any customized-profile user.



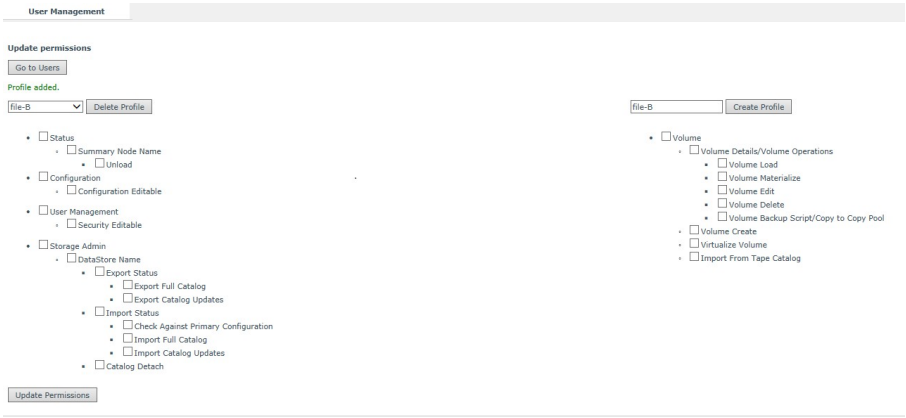
To edit users, profiles and/or permissions, click Switch to Edit Mode.

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.

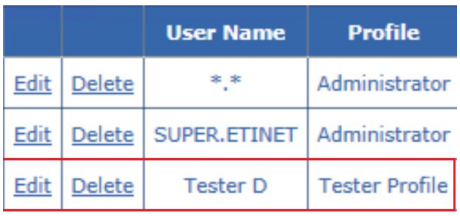
To create a new profile:

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.

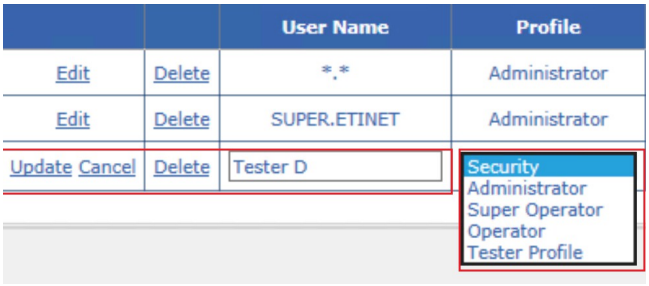


5. Once the profile has been created, you can assign users to it. Go to User Management page and add new user. Give the user a name and select the user to be assigned to the profile you just created. Click Add User to add it to the list.

6. The new user is listed under the user name.



7. You can edit the user name and the profile the user is assigned to by clicking on the Edit button.



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.

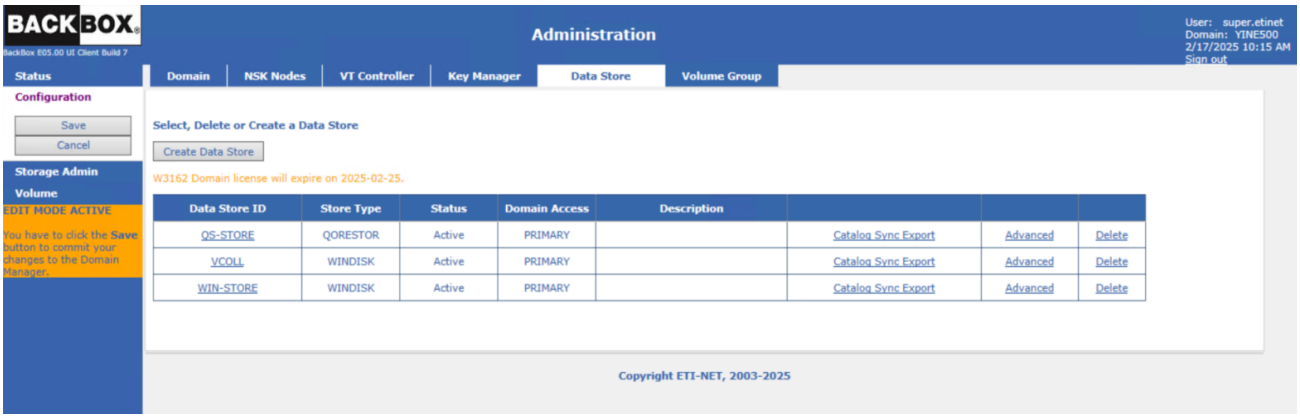
⚠	Profiles with users assigned to them cannot be deleted. An error message will state to delete the users before deleting the profile.
⚠	Default profile permissions cannot be modified.
⚠	No more than 3 custom profiles can be created.

If you are signed in with a security profile, you can assign aprofile 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.

Storage Admin

The Storage Admin page displays a list of the configured Data Stores.



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- Box Catalog Sync Option manual. This link is present only if the BackBox 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 BackBox Domain.

Running Jobs: Displays the jobs currently running on the Data Store (Spare Move, Migration, Copy Sync). 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 BackBox 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 BackBox 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 BackBox catalog (not considering the volumes in storage and DSM/TC), the complete scenario of moving a Data Store from a BackBox 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 RESTRICTED to PRIMARY to allow regular operations including backups.

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.

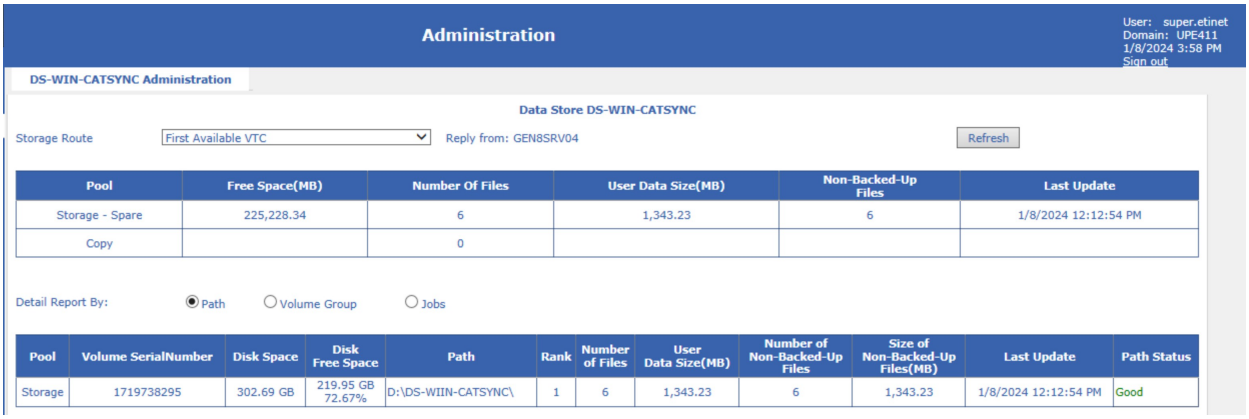
Windows Files Administration

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 Enterprisebackup softwareare not included.



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

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 sub-directories.

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.

Backup all non-backed-up files and **Copy Sync Uncopied Files** links may be available while normal operation in progress. Nonetheless, no other operation can be started.

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 if 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.

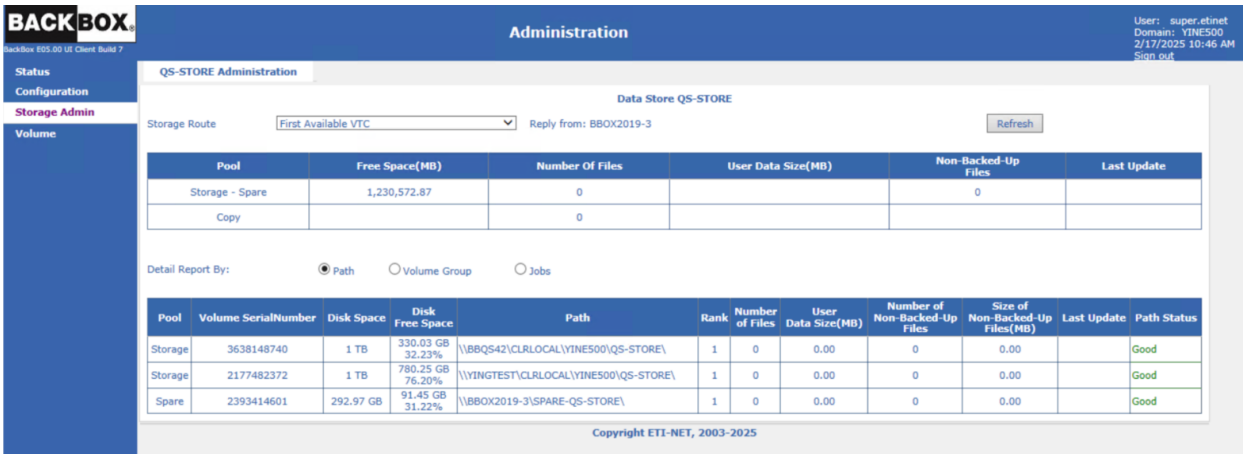
The moving task in the VTC reports its startup and end in EMS, and potential errors.

```
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 BackBox 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.



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.

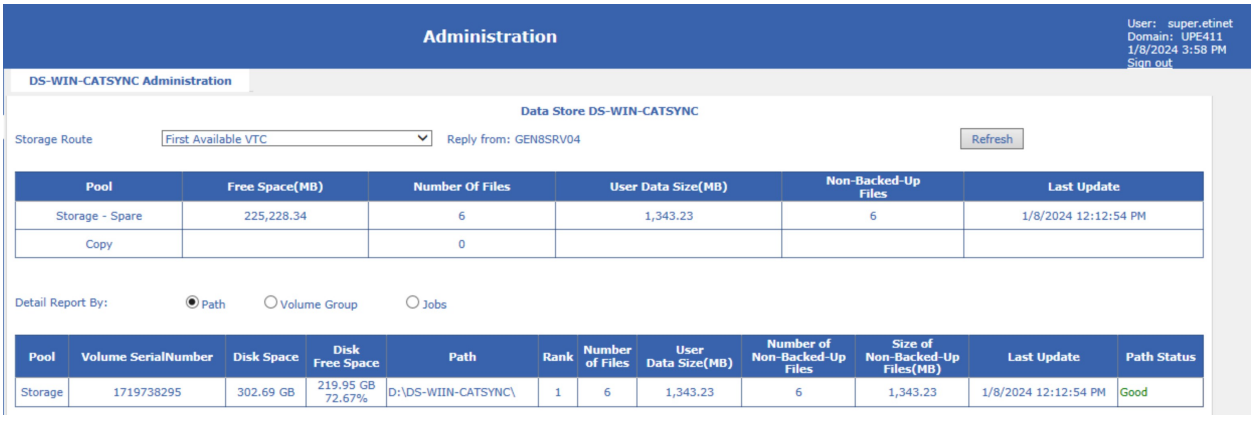
User Data Size(MB): Used space with value given in MB (megabytes)

Number of Non-Backed-Up Files: Total number of files that haven't been backed-up.

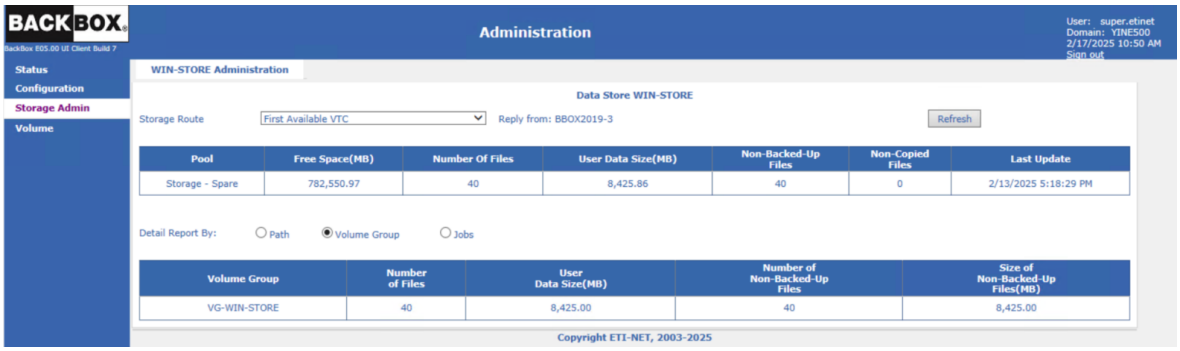
Size of Non-backed-up Files (MB): Total size of non-backed-up files with value given in MB (mega- bytes).

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.



Detail Report by Volume Group



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.

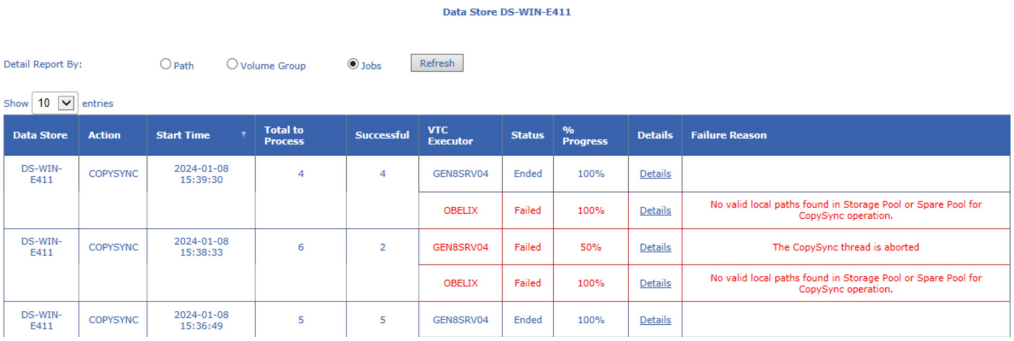
Number of Files: Number of Windows files in the path.

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 (mega- bytes).

Detail Report by Job



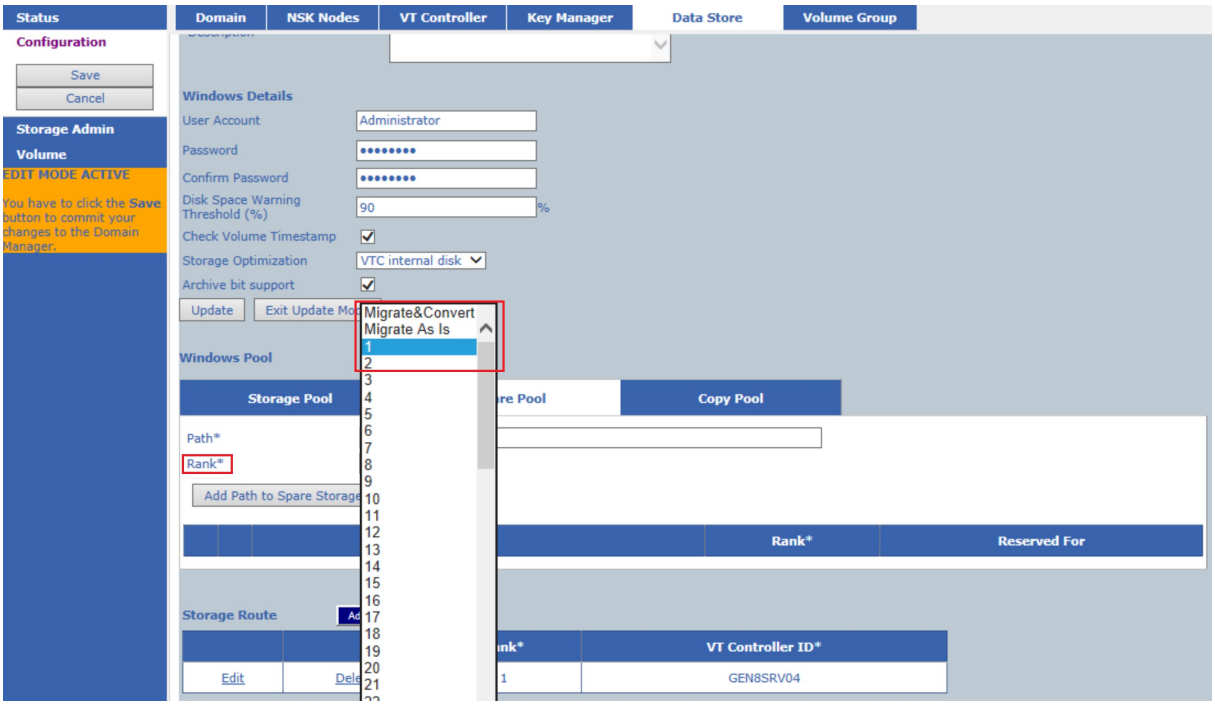
The Jobs page will display various details on the jobs executed for the specific Data Store.

Job Types

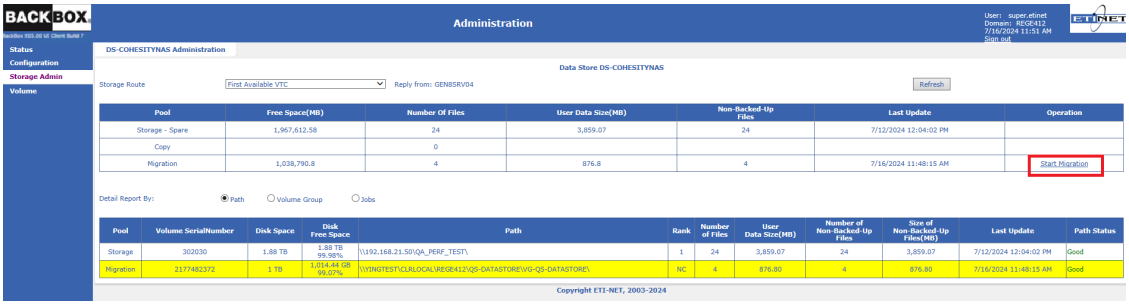
- Migration

To migrate a spare pool:

1. On BackBox UI go to Configuration>Data Store> Switch to Edit Mode.
2. Choose the Data Store.
3. Select in the Information panel Spare Pool.
4. In the Rank* drop-down list select either Migrate As Is or Migrate&Convert.



5. Save the configuration.
6. Go to the Storage Admin page and in the Operation column click on the Start Migration link to start the migration job.



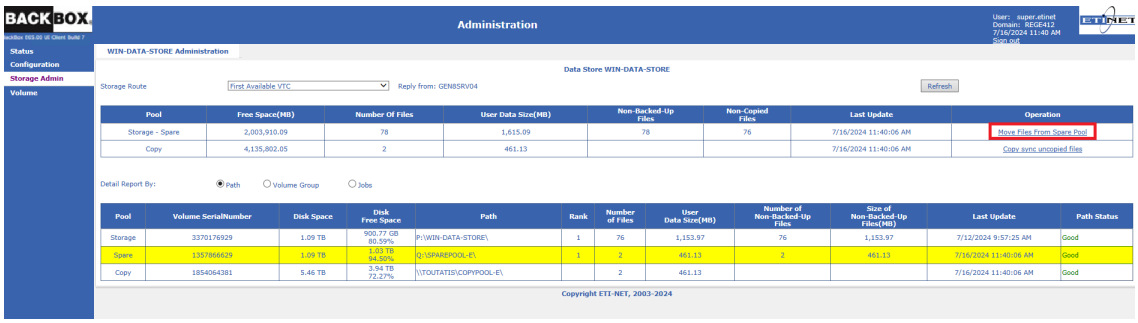
Details: Click on the link provided in the job list to open a new page with information on the job performed or running.

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.

- **Move Files from Spare Pool**

To move files from the spare pool:

1. On BackBox UI go to **Configuration**>Storage Admin.
2. Select the Data Store to be moved to the main storage and click the link **Move Files From Spare Pool** in the Operation column to start the job.



⚠	If **Delete Expired Volumes** is set to **No** in the **Volume Group** configuration page, the spare move tapes will not be moved, as they are already expired and they can- not be moved or deleted. If **Delete Expired Volumes** is set to **Yes** in the **Volume Group** configuration page, the spare move tapes will be deleted or moved by the end of the day, according to the daily clean-up schedule. In order to delete these tapes before the scheduled time, use OBB017 and perform the action manually.

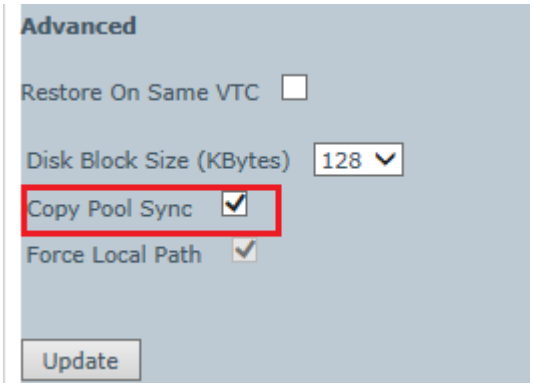
Details: Click on the link provided in the job list to open a new page with information on the job performed or running.

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.

- **Copy Sync Uncopied Files** - If the files in the storage pool do not match the files of the copy pool (ex. some files are missing from the copy pool), then start the copy sync uncopied files job.

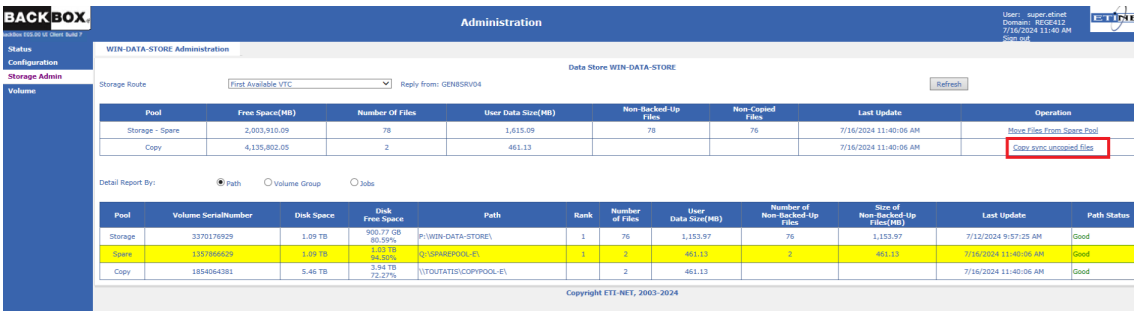
To copy sync uncopied files:

1. Set up Copy Sync Uncopied Files: go to **Configuration**>Data Store> Switch to Edit Mode, choose the Data Store and click the Advanced link in the table corresponding to the data store, then check the Copy Pool Sync box.



Click Update the configuration and then Save.

2. On the **Storage Admin** page, for the configured data store, in the **Operation** column click on the Copy Sync Uncopied Files link to start the job.



Details: Click on the link provided in the job list 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.

To display the failed operations only check the radio button ☑Failures Only on the top of the **Job Details** page.

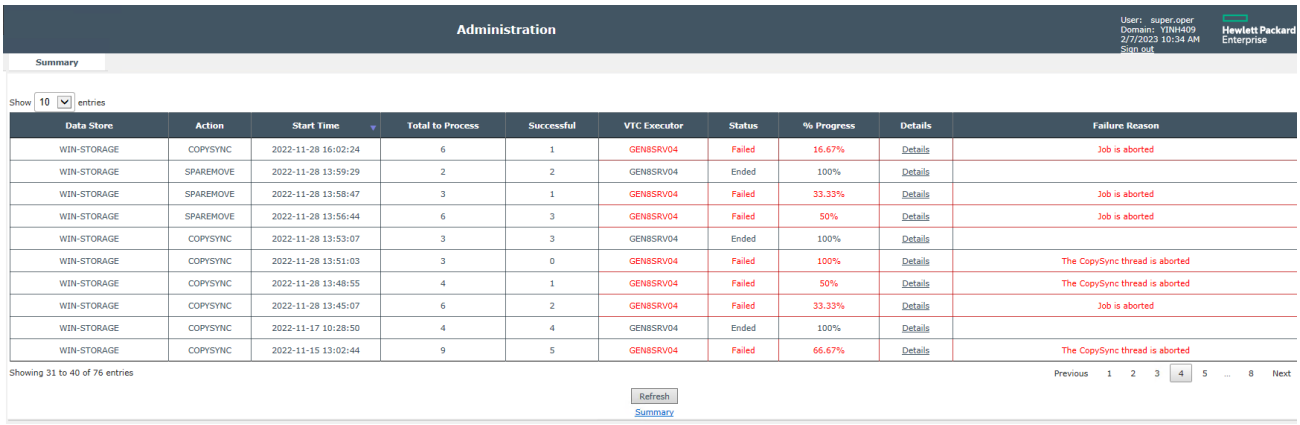
Use the Copy or Save To File buttons at the bottom of the page to save the job details information for future use.

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. Summary There are no jobs to display at the moment. Refresh Summary

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 successfully processed files

VTC Executor: Name of the VTC

Status: Job status depending on the action. It can be **Failed/Ended/Suspended/Running.**

% Progress: Percentage of the job completion while the job is running. If job is completed, it will be shown as **Ended** with 100% progress rate. If the job is **Stopped/Canceled**, the job progress will be shown as completed (100%). If the job is **Paused**, the progress will remain to the current percentage until the job is restarted.

Refresh Refresh button - used at any time during or after the process - will update in real time and show the number of successfully processed files for all types of jobs (Migration/Copy Pool Sync/Spare Pool Move)

When the job finished running, the progress indicated will always be 100%.

If **Failed**, it shows the percentage of the total processed files with percentage rounded value.

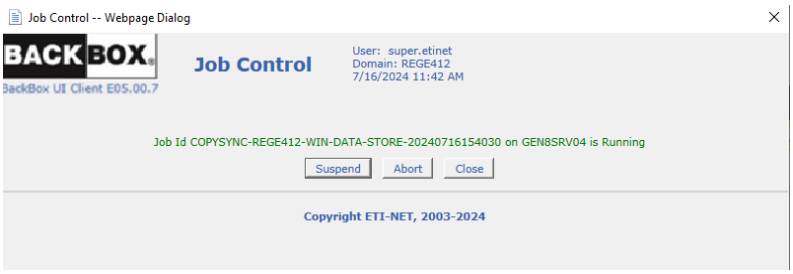
Details: Link to the data store

Failure Reason: In case of a job failure, error message and/or details on the failure reason.

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.

⚠	The Job Control feature is available only while the job is running.

Follow the instructions in the pop-up.



A running job can be suspended or abordted. A suspended job can be resumed or aborted.

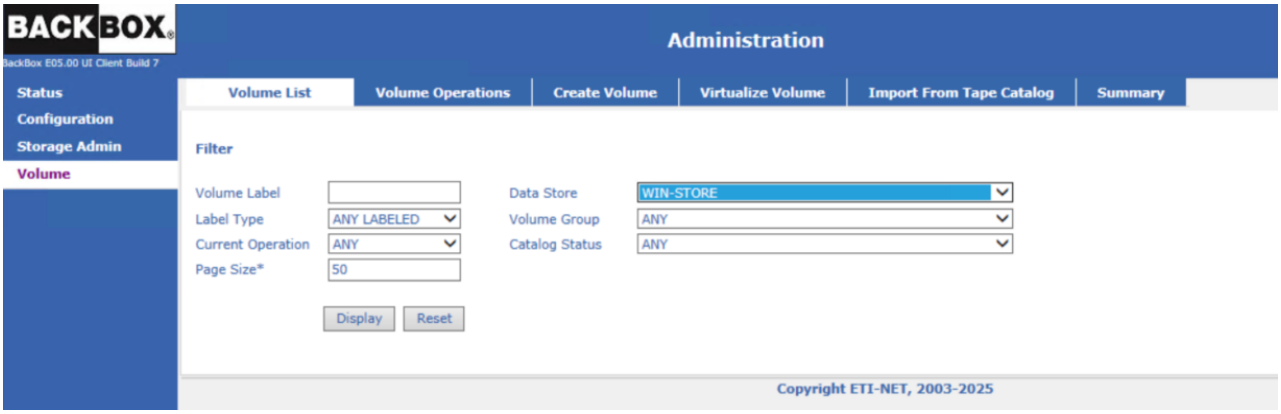
If you choose to change the job status, another pop-up window will prompt you with a message on the change that you just performed.

If the job is aborted, the summary table will list the job status as Failed.

⚠	Jobs details are kept in the log for no longer than 365 days. The older job logs are automatically deleted from the list.

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.

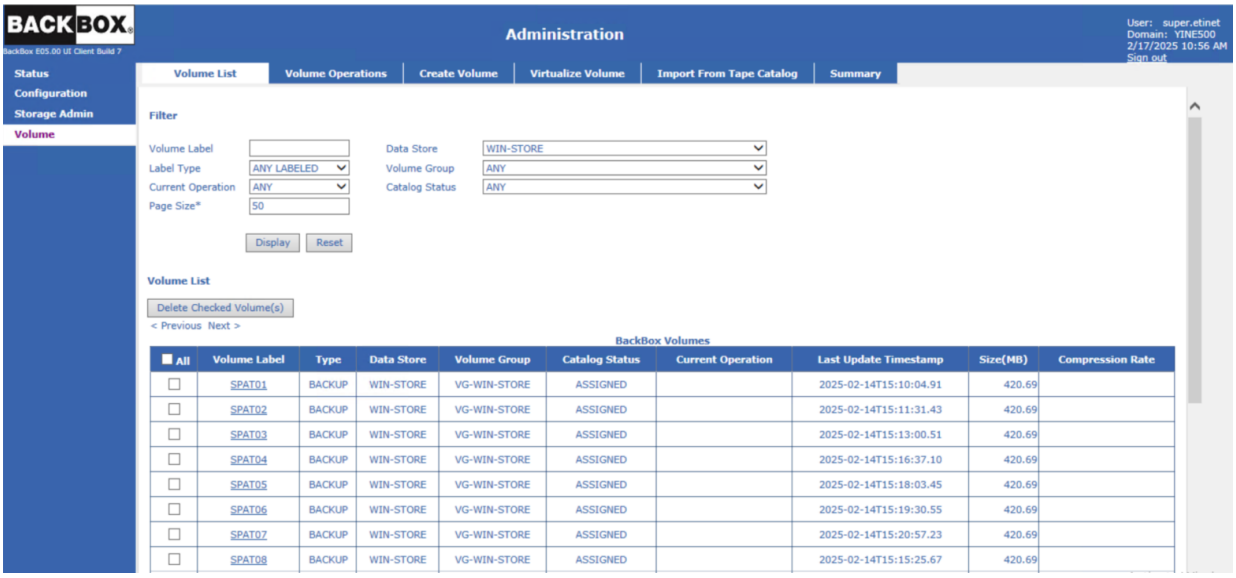
Import From Tape Catalog: Registers in the domain catalog volumes that are already known in a NonStop tape catalog, such as DSM/TC. This function does not move any volume data.

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.
Page Size: Maximum number of results to be displayed on the page. To browse through pages use Previous and Next buttons.
Data Store: Filters volumes based on the data store they belong to.
Volume Group: Filters volumes based on the volume group.
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 Check boxes: 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:

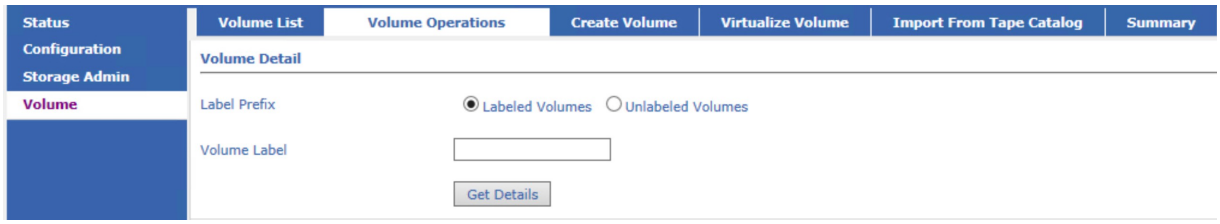
- ASSIGNED
- INCOMPLETE
- SCRATCH
- ANY
- UNKNOWN
- BAD
- RELEASED
- FULL
- SELECTED
- ASSIGNED (Incomplete) - catalog has been assigned by DCM TC, but failed on backup execution
- SCRATCH (Locked) - storage is locked
- SCRATCH (Inaccessible) - storage is inaccessible

☐	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	

When a VOLUME is deleted from the BackBox domain catalog, the entry could remain tagged with the status UNKNOWN (if file deletion failed). Retry to delete the volume later.

Volume Operations

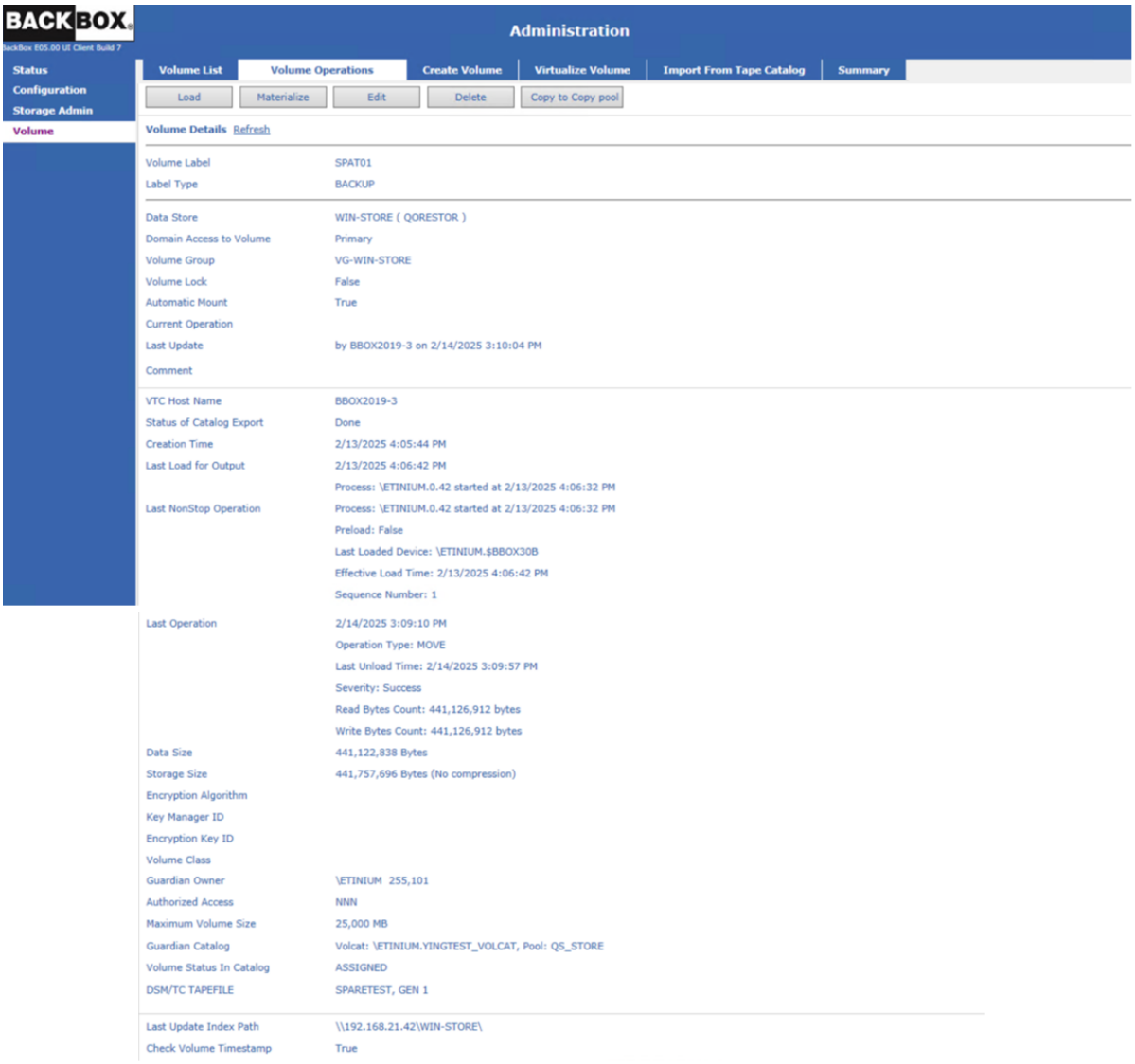
The **Volume Operations** tabbed page allows the user to identify a virtual volume and directly access the volume detail page.



Label Prefix: Indicates whether the volume is labeled or not.
Volume Label: The label of the volume.
Get Details: Link to the Volume Details page.

Volume Details

The Volume Details page displays the info available in the BackBox catalog for a specific virtual volume. The operations available for any volume are Load, Materialize, Edit, Delete, Run Backup Script.



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).

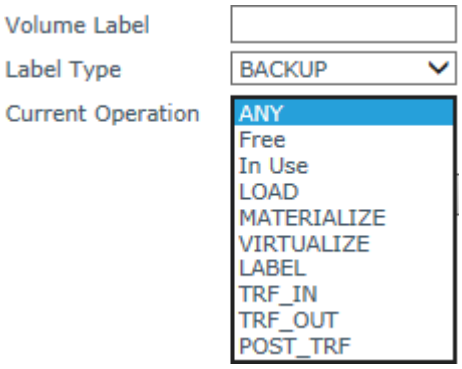
Domain Access to Volume:

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 BackBox 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: BackBox 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.

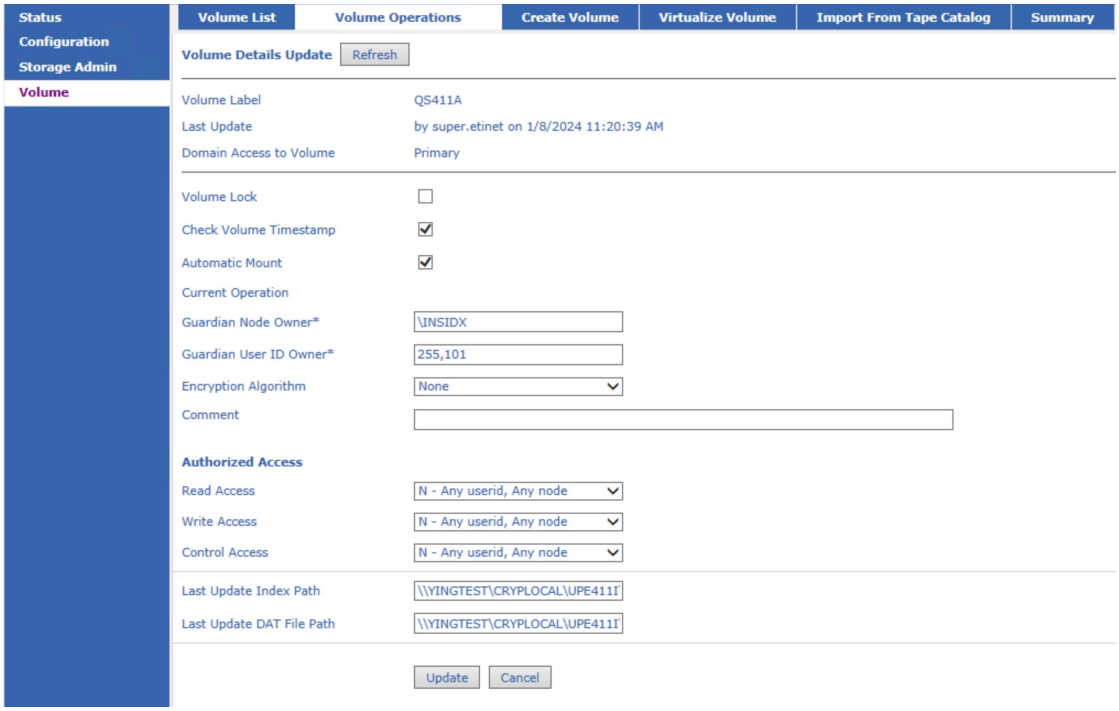
⚠	The expiration is to be interpreted carefully as there may be an override by a third party catalog on the NonStop system ID.

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 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 con- figuration, the VTC compares the volume timestamp stored in the BackBox 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 BackBox 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. It can be updated 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 : It can be updated 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.

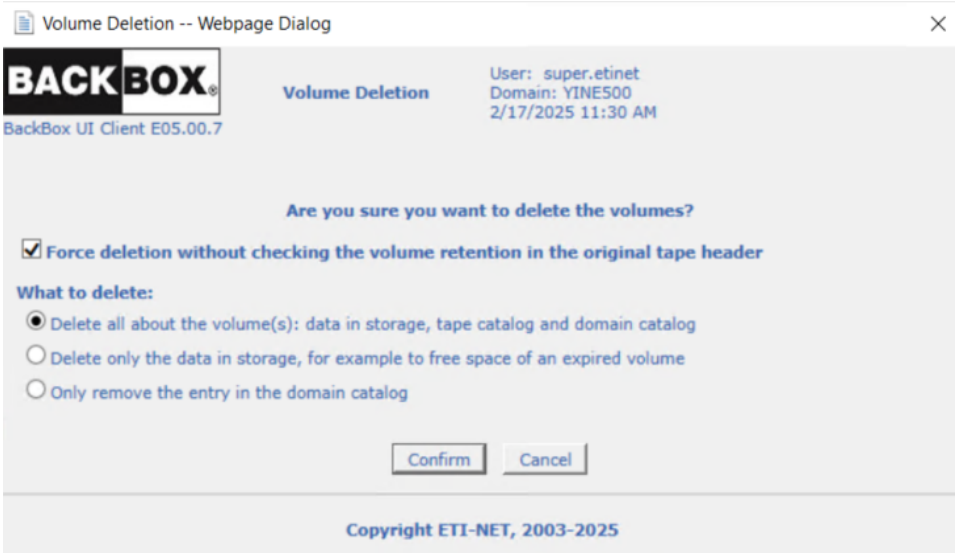
Volume Deletion

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 BackBox domain catalog 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 BackBox 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. BackBox 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 BackBox 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, BackBox 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 BackBox 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 2023-07-22. 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 BackBox 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:

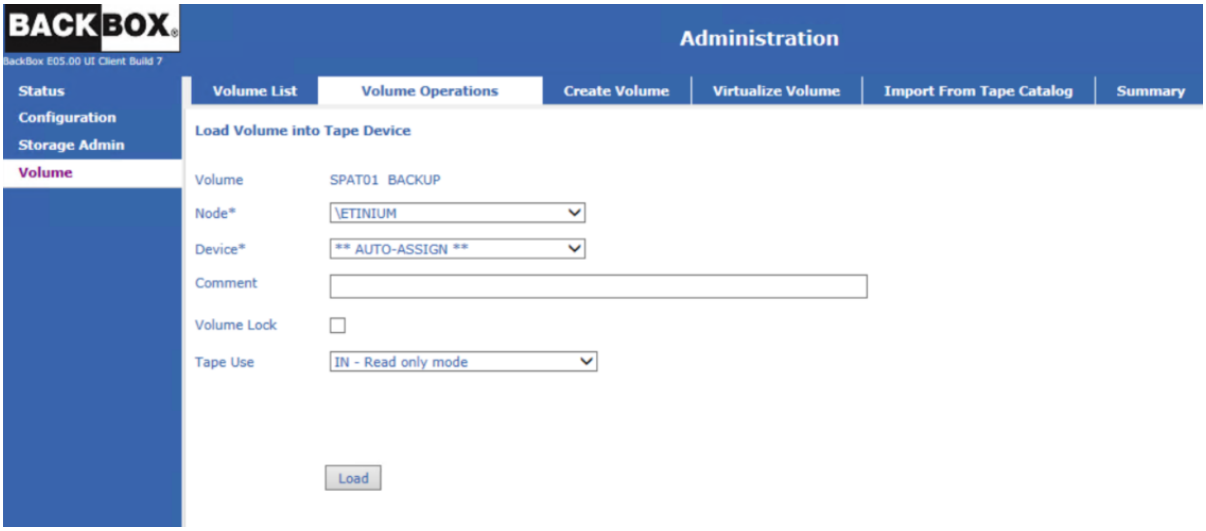
- Delete all about the volume(s), data in storage, tape catalog and domain catalog. This is the default option, where the data, the volume entry in the DSM/TC and in the BackBox domain will be deleted.
- Delete only the data in storage, for example, to free space of an expired volume. The volume will still be available for the next backup and the volume entry in the DSM/TC and BackBox domain are retained.
- 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.

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.

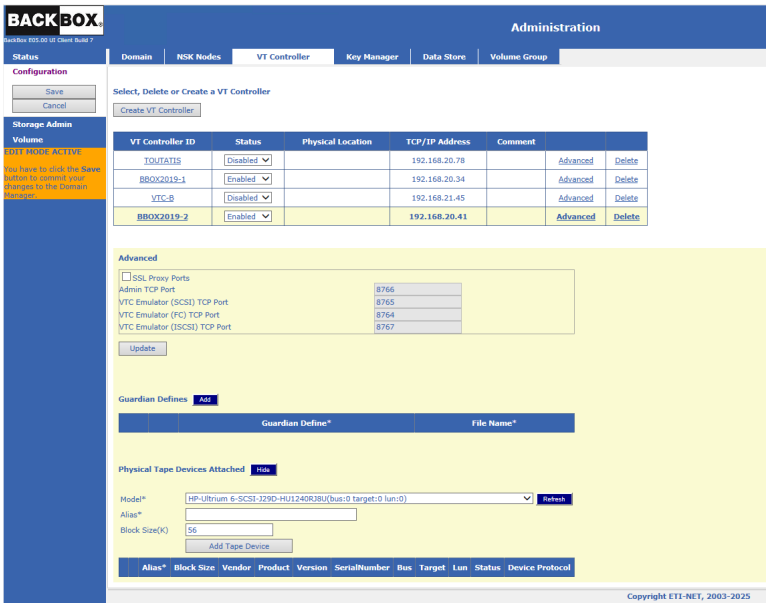


Volume: The volume label and label type to load.
Node: Guardian node of the tape device where to load the volume.
Device: Guardian tape device to load the volume on. If left to AUTO-ASSIGN, the Domain Manager will choose a device.
Comment: Free text kept in the BackBox catalog for the volume.
Volume 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.

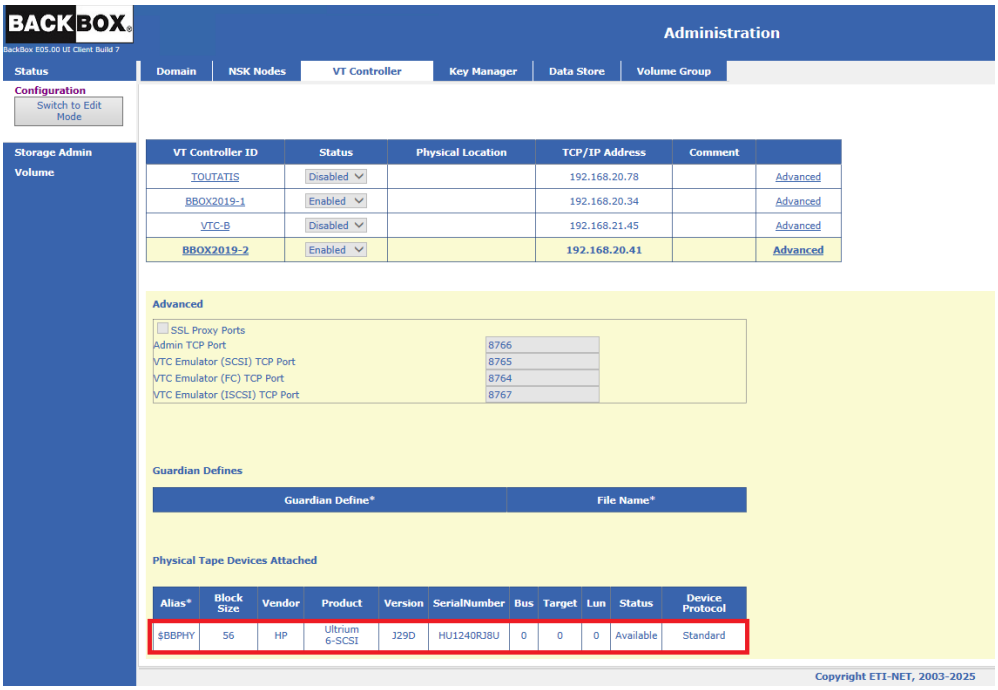
Volume Materialization

The Volume Materialization page is used to clone a single virtual volume to a physical media loaded on a VT Controller

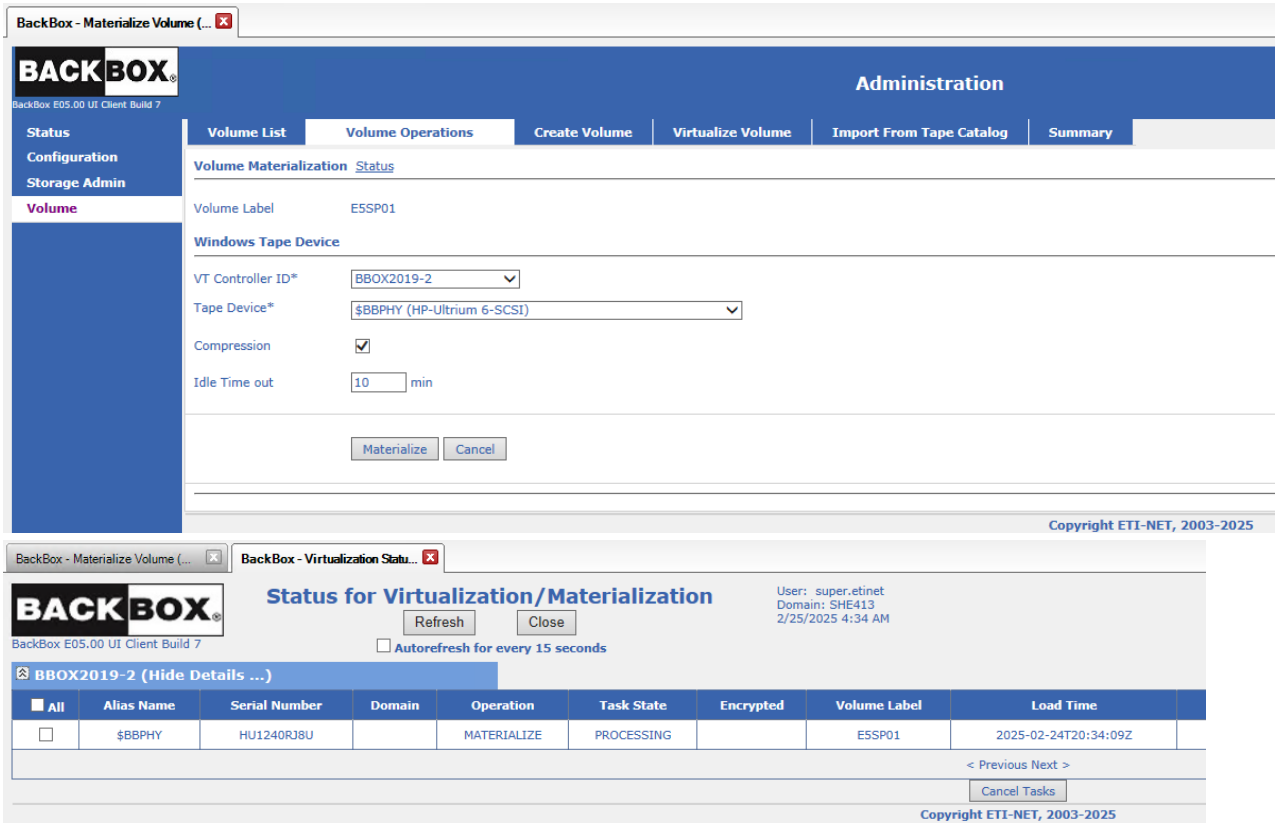
attached drive.
This operation was named "Volume Export" in older BackBox versions.
To attache the physical tape device go to VT Controller page and choose Model*, Alias* and Block Size of the device to be attached.
Click Add Tape Device.



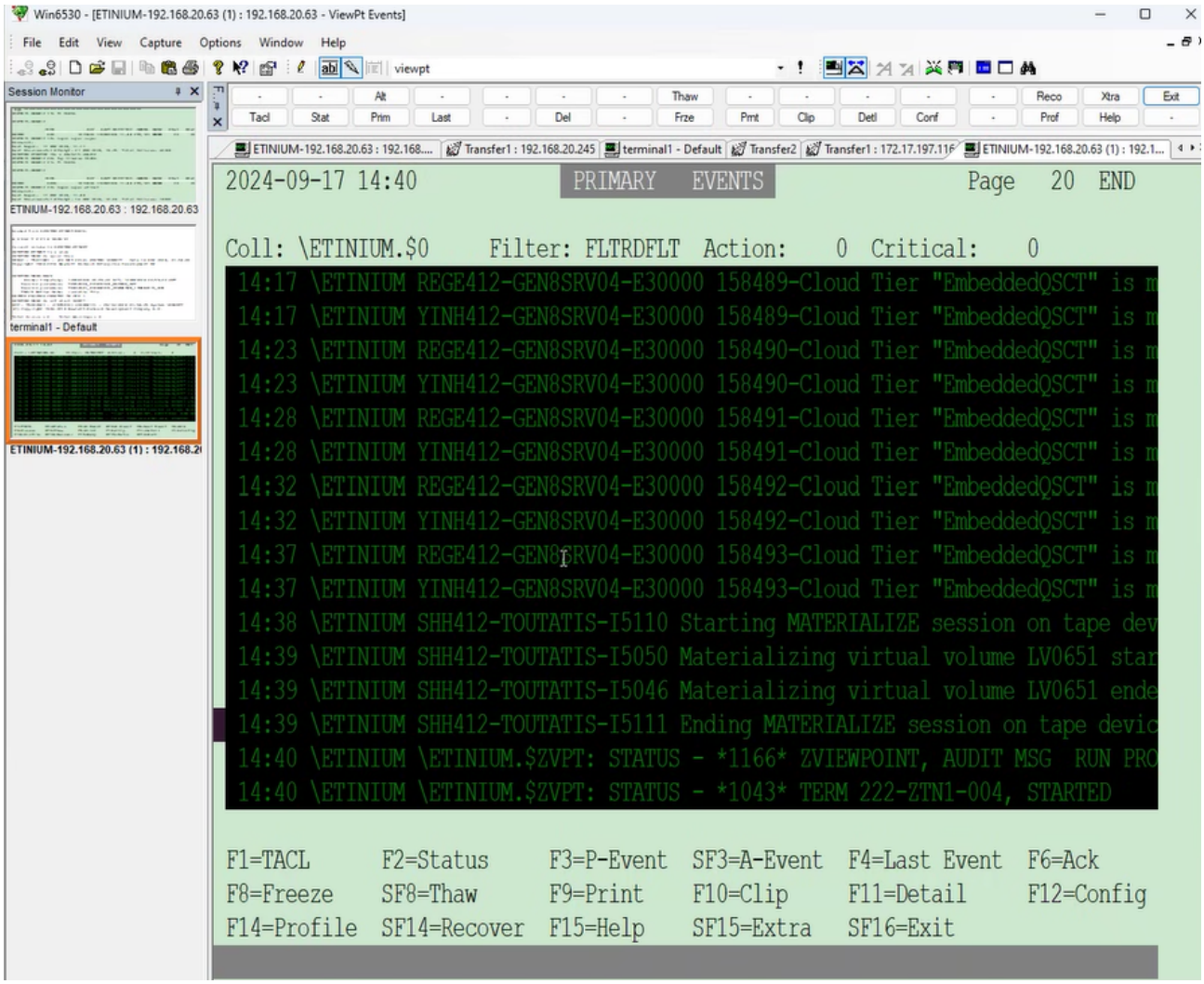
If the physical device is already attached, it will be listed under the VT Controller with details of the device.



The physical media capacity must be able to contain the whole virtual volume. Check Data Size on the volume detail page.

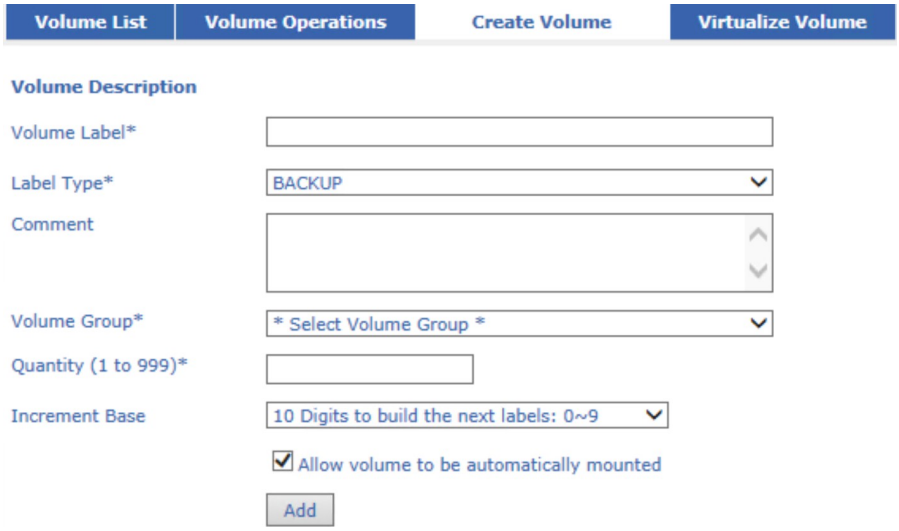


The EMS will report the starting, the ending of the Materialization session and the status of the volume process (e.g. "ended successfully").



Create Volume

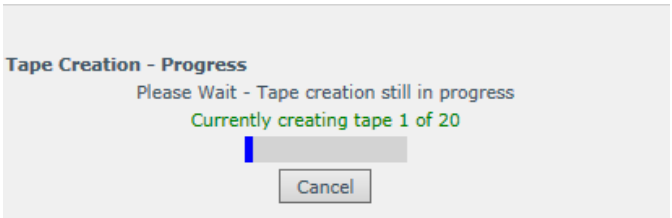
The Create Volume page is used to create new volumes, label them, add them to the library, and catalog them in an external catalog (i.e. DSM/TC or TMF), if needed.



Volume 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 saved 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.

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.



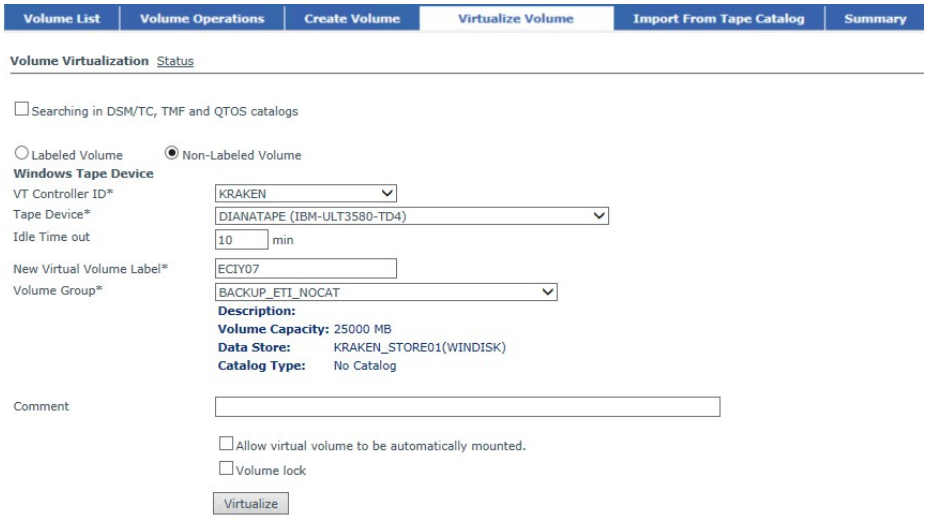
A message is displayed when the process is complete.

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 BackBox 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.

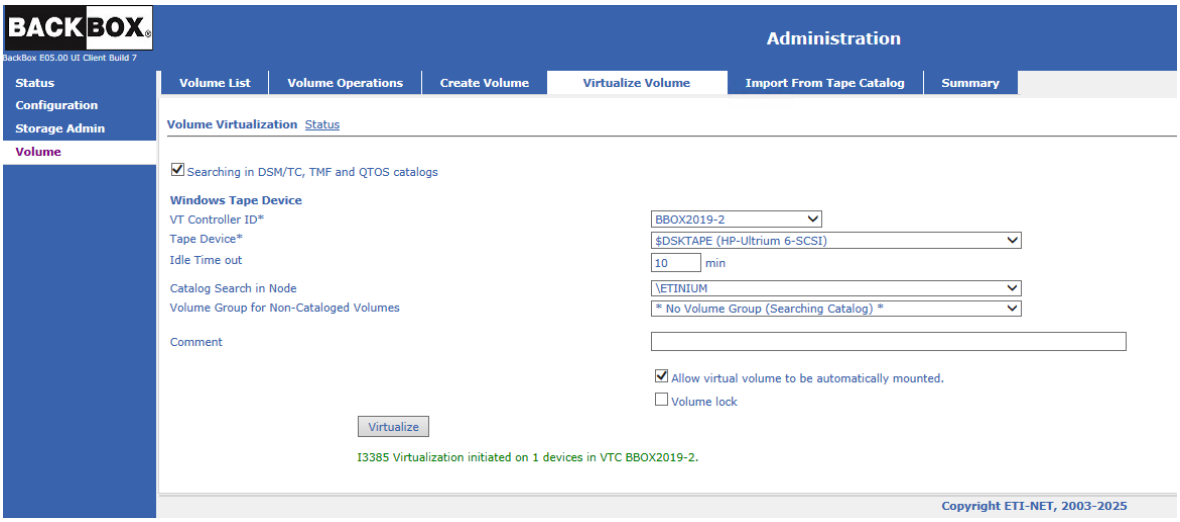
The maximum volume size configured in Volume Groups must be able to contain the entire physical media.
The NonStop tape catalogs associated with the Volume Groups (TMF, DSM/TC or QTOS) are not updated. The media that has to be virtualized must be already cataloged if the Volume Group is associated with a NonStop tape catalog.
A Status page shows the running virtualization-materialization tasks and allows task cancellation at any time.



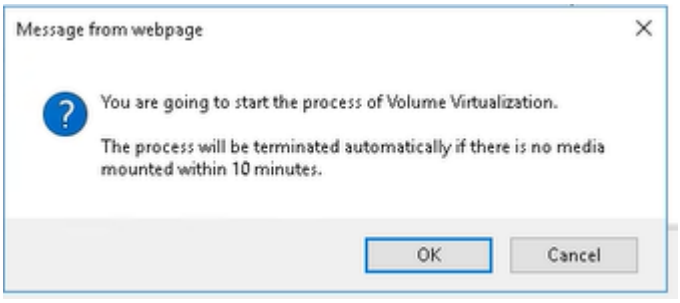
Status: Link to a Status page that will show all virtualizations and materializations on all VTCs that have physical/external tape drives configured.

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 BackBox 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 theBackBox 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 BackBox catalog.



Labeled/Non-Labeled Volume: Type of media to virtualize. If Non-Labeled, the BackBox name for this volume will be requested.
Click **OK** to start the volume virtualization process.



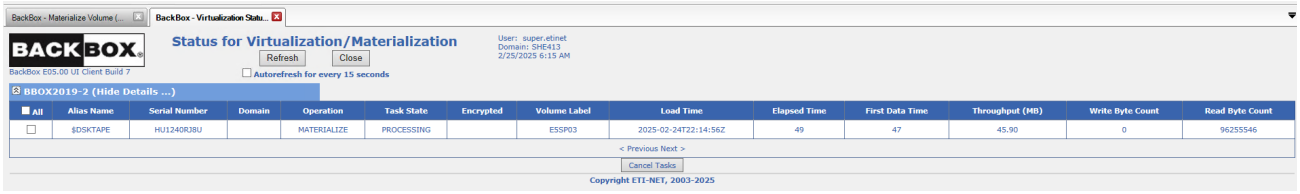
Once the virtualization is started, the UI will show the following messages: `I3385 Virtualization initiated on 1 devices in VTC XXXX.`
Click on **Status** link to see details specific to the volume virtualization:

EMS will report the virtualization starting/ending session and each volume processing status.

```
------------------------------------------------------------------------------
16:53 26FEB25 222,01,1076 SHE413-BBOX2019-2-I5108 Starting VIRTUALIZE session
   on tape device $DSKTAPE Event time:2025-02-26 16:53:22
------------------------------------------------------------------------------
16:56 26FEB25 222,01,1114 SHE413-BBOX2019-2-I5051 Virtualizing physical volume
   E5SP04 started successfully Event time:2025-02-26 16:55:11
------------------------------------------------------------------------------
16:56 26FEB25 222,01,387 SHE413-BBOX2019-2-I5053 Virtualizing physical volume
   E5SP04 ended successfully Event time:2025-02-26 16:55:35
------------------------------------------------------------------------------
16:56 26FEB25 222,01,1114 SHE413-BBOX2019-2-I5109 Ending VIRTUALIZE session on
   tape device $DSKTAPE Event time:2025-02-26 16:55:59
```

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 canceled.
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.

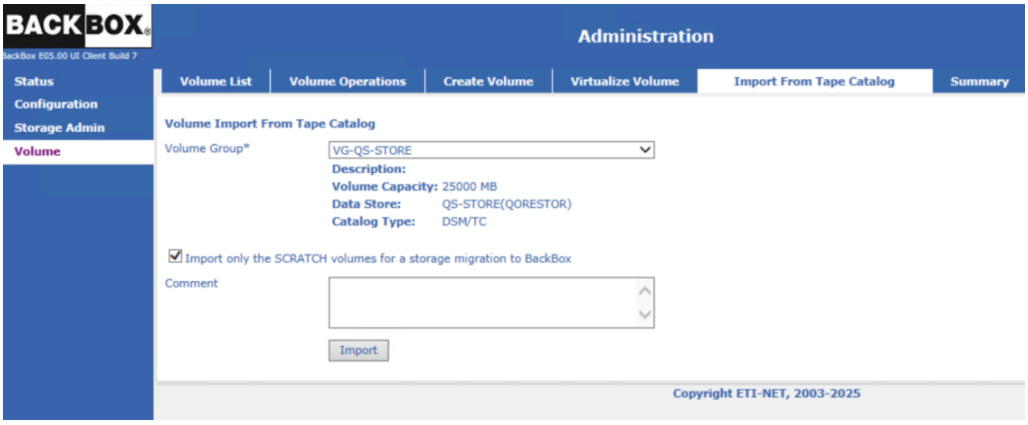
Import From Tape Catalog

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 BackBox catalog.
This procedure is normally used at the beginning of a migration from a legacy storage system to BackBox; 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 BackBox 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 BackBox 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. BackBox 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.

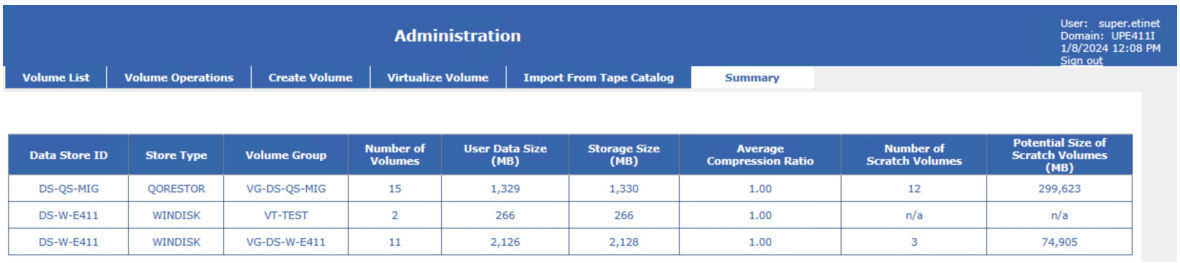
Feedback

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 BackBox, 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.

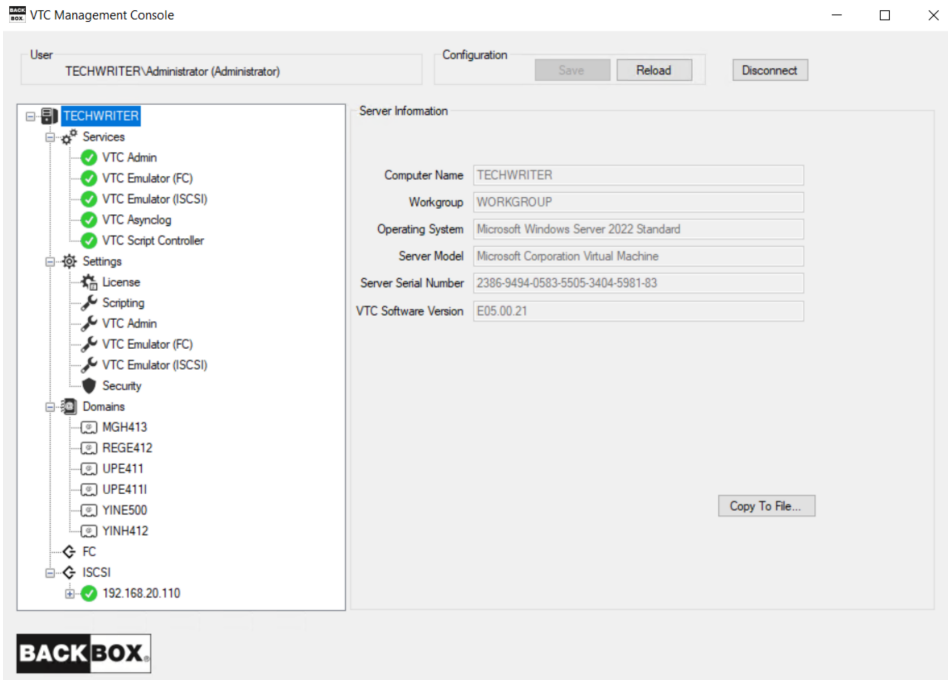


Data Store ID	Store Type	Volume Group	Number of Volumes	User Data Size (MB)	Storage Size (MB)	Average Compression Ratio	Number of Scratch Volumes	Potential Size of Scratch Volumes (MB)
DS-QS-MIG	QORESTOR	VG-DS-QS-MIG	15	1,329	1,330	1.00	12	299,623
DS-W-E411	WINDISK	VT-TEST	2	266	266	1.00	n/a	n/a
DS-W-E411	WINDISK	VG-DS-W-E411	11	2,126	2,128	1.00	3	74,905

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.

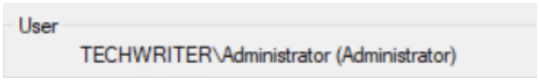
The Summary section displays the following information:
Data Store ID: The Data Store name.
Store Type: The Data Store type (IBM Spectrum Protect TSM or WINDISK).
Volume Group: Volume Group name.
Number of Volumes: Number of volumes in this Volume Group.
User Data Size: The total size of all volumes 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.

VTC MANAGEMENT CONSOLE



Security and Access Rules

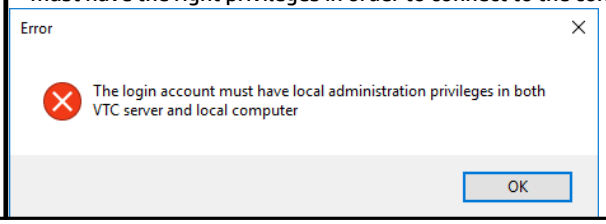
To configure the security and access rules on the VTC server, the VTC Management Console has to be started using an interactive user with permissions to log on to the VTC Server. The VTC Management Console attempts to connect to the local VTC Management Service. The default connected user and their profile are displayed in the user identification box.



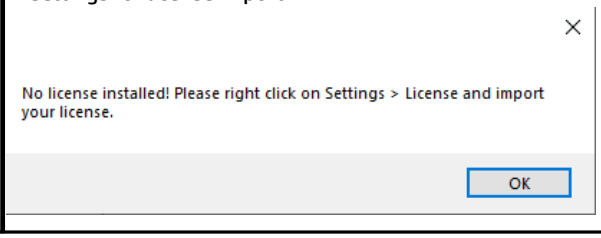
Console Access Restrictions

Some restrictions apply when accessing the VTC Management Console.

Only a local administrator user has access to the VTC Management Console and its functionalities. 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.

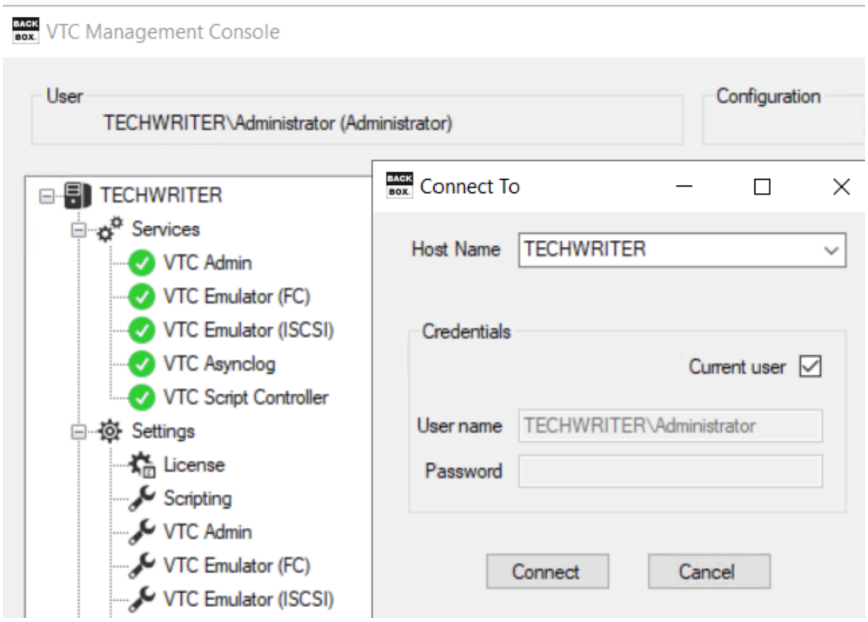


If there is no license installed on the VTC MC, a pop-up message will prompt to let you know about the necessary settings for license import.



Remote VTC Server Administration

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, un-check 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, 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.

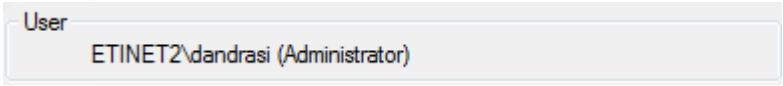
For WORKGROUP deployment, all users accounts for remote administration must be created on each server and must have the same user name and password. To avoid workgroup requirements, it is recommended to use only the domain user to create a local user on the workstation.

⚠	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

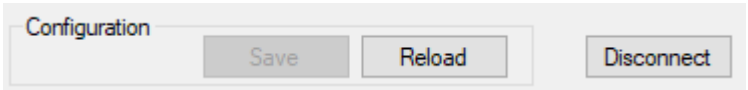
The user interface has four sections:

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.

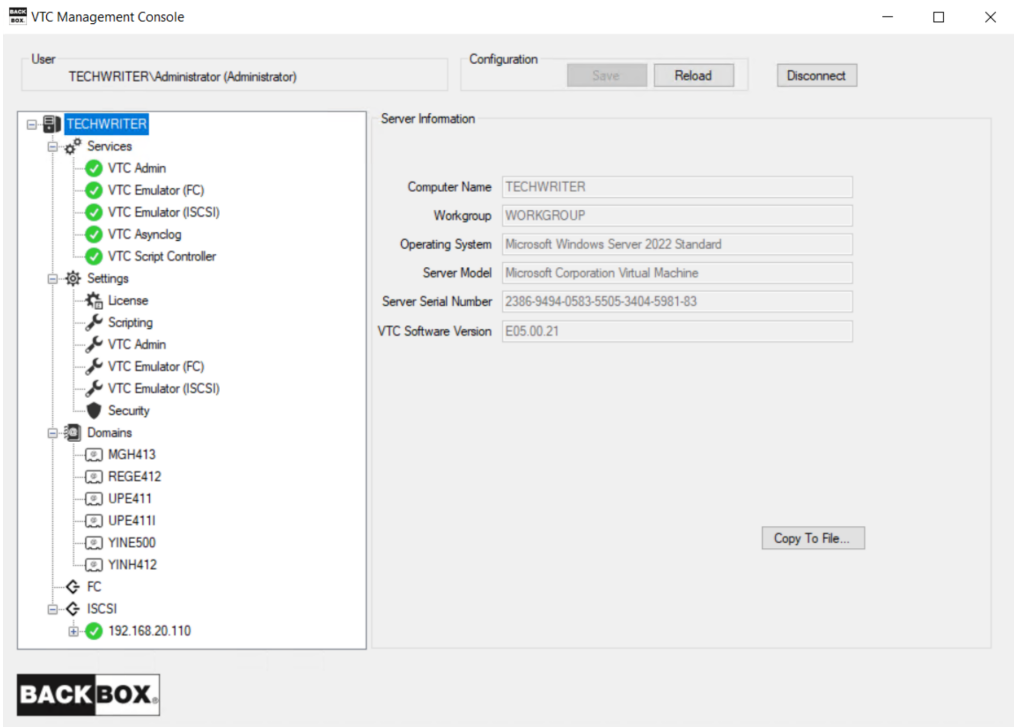
3. Server Tree Nodes Panel (left-side panel)

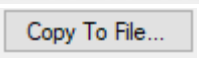
This panel lists the server elements. Nodes can be expanded; they are grouped into different management categories. Right-click on the nodes or elements to see the available actions. If an action is not possible, it appears grayed out.

4. Server Information Panel

When a server is selected, the information displayed on the right side panel is related to that specific server. Not all server nodes have information to display when selected (e.g. Service nodes).

The panel displays details related to the selected server, such as Computer Name, Domain, Operating System, Server Model, Server Serial Number, VTC Software Version and VTC Patch Level, (the patch installed for the VTC version), if any. Contact ETI-NET Support for the latest patch release.



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.

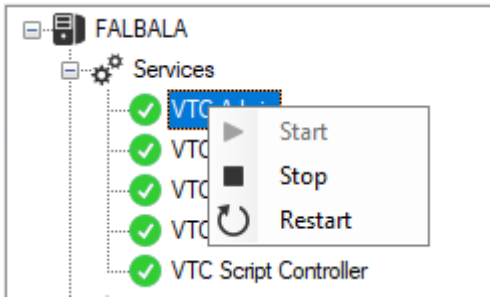
TECHWRITER - Notepad

File Edit Format View Help

```
Computer Name: TECHWRITER
Workgroup: WORKGROUP
Operating System: Microsoft Windows Server 2022 Standard
Server Model: Microsoft Corporation Virtual Machine
Server Serial Number: 2386-9494-0583-5505-3404-5981-83
VTC Software Version: E05.00.21
UUID: C351FC8E-6BA0-4CDD-BB1A-BE8BA197D1D5


License Number: xxxx0017
License Expiration : 2025-02-21T21:05:59.3549978Z
License Creation : 2025-02-07T21:06:32.1533130Z
License To: E5056900
Serial Number: 2386-9494-0583-5505-3404-5981-83
Hpe Number: Unknown
License Type: Emergency
Host Name: TECHWRITER
Release Version: E
Software Version: 4.09
Product: Unknown
Os Version: Microsoft Windows Server 2022 Standard
Number Of FC Ports : 0
Number Of Encryption Devices: 2
Number Of Iscsi Devices: 2
Number Of Devices Per Port : 64
QoreStor Enable: False
QoreStor ID: Unknown
```

Real-time Process Tracking

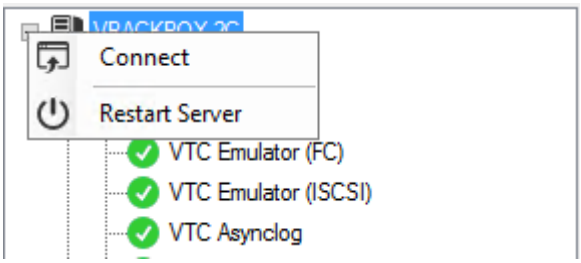
On VTC MC, any background process is real-time tracked. Activate the real-time tracking by clicking on any process button, such as **Start**, **Stop**, **Restart**.



Server Nodes

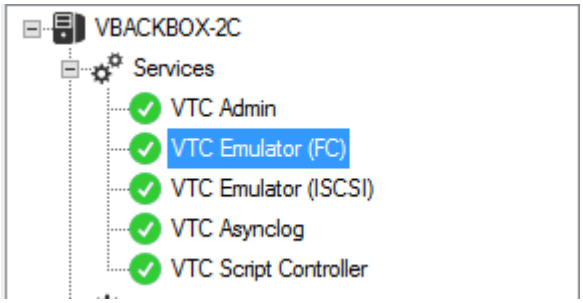
When connected, the **Server Node** is always initialized with the server computer name. Under the **Server Node** there are the four main categories handled by the VTC Management Console: **Services**, **QoreStor**, **Settings**, **Domain Addresses**, and **FC/ISCSI** nodes.

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)**,

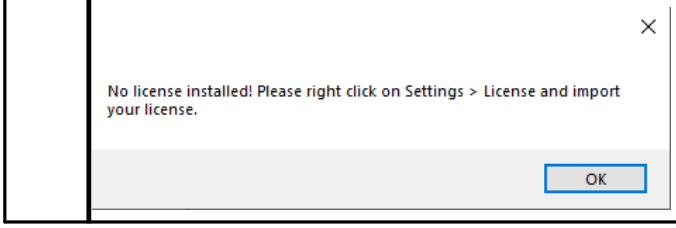
VTC Emulator (ISCSI), VTC Asynclog, VTC Script Controller.When selecting any of the Service categories, there is no related information to be displayed in the right-hand side panel.

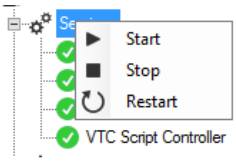


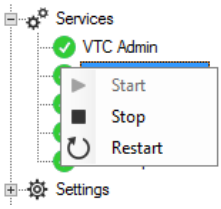
Service states	Description
	Started
	Stopped
	Stopping / Starting

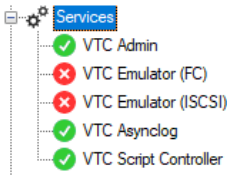
The available actions are activated when right-click on the service: **Start**, **Stop**, **Restart**. If one service is selected, the available actions will be performed at service level, not at server level. The grayed-out actions are not available.

If there is no license installed on the VTC MC and the service is stopped , a pop-up message will prompt to let you know about the necessary settings for license import.





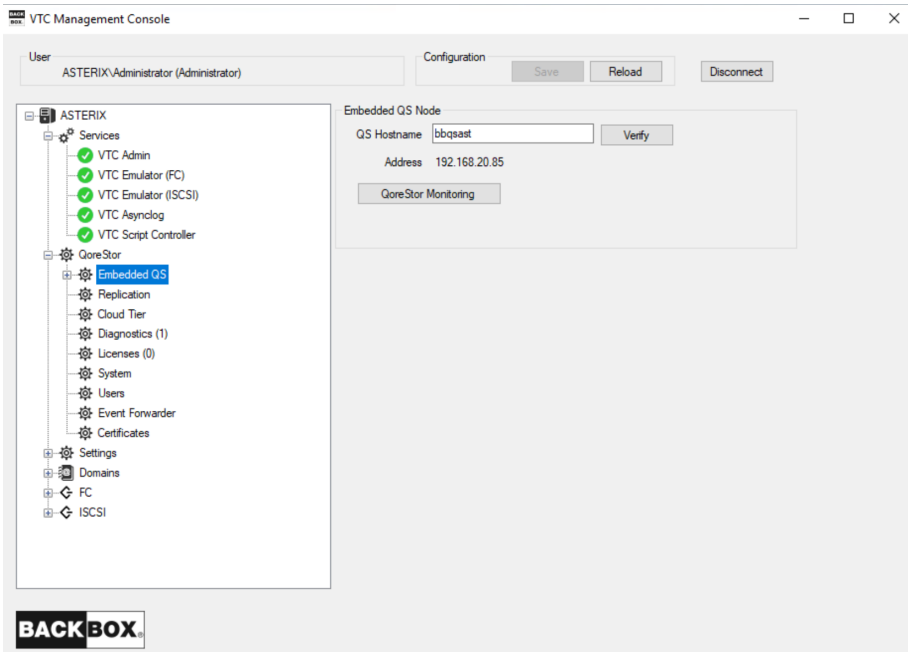




QoreStor

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



⚠	The button QoreStor Monitoring underneath the IP Address will launch the default browser and navigate to the QoreStor user interface.

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 disabledFor embedded QoreStor there are some connection settings that need to be configured:

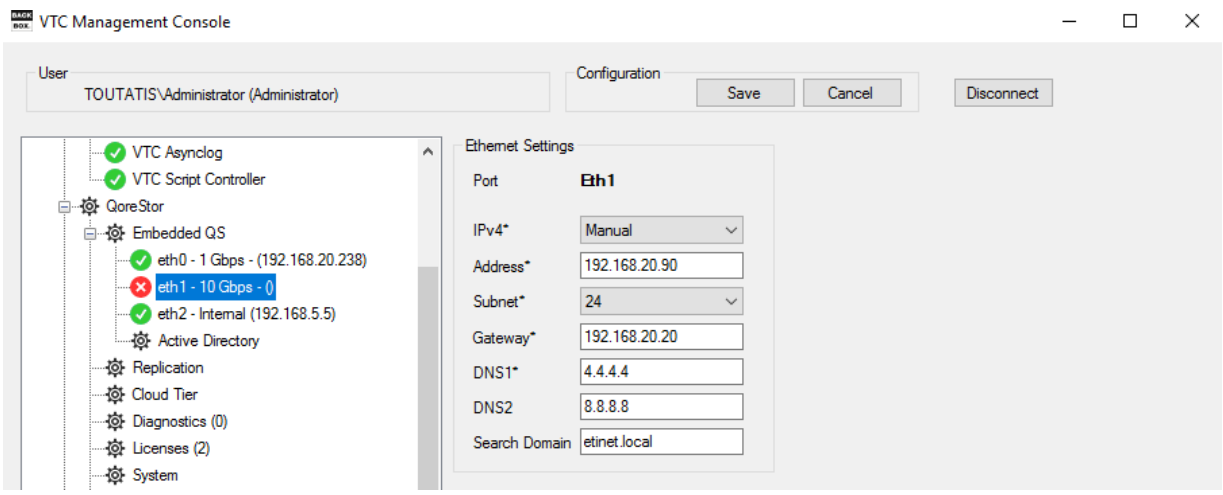
- To configure ethx Automatic

a. Change IPv4 setting.
b. If Automatic, nothing else to change and click on Save to save.
c. If Disabled, 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

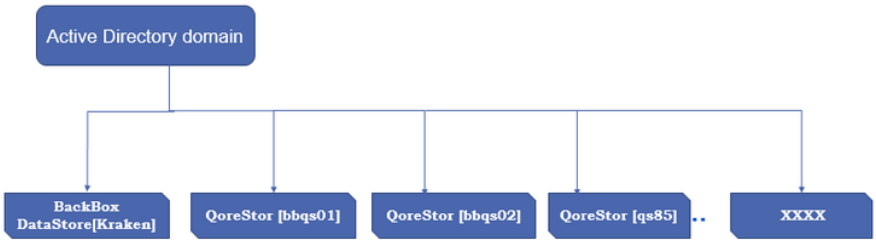
a. Change IPv4 setting to manual.
b. Enter the address.
c. Select Subnet (ex: Subnet=24). For eth0 make sure to use Subnet value in Windows format, otherwise an Invalid subnet mask message is generated and the value is not accepted. For more details on the valid subnet values see Microsoft Network Classes.
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.

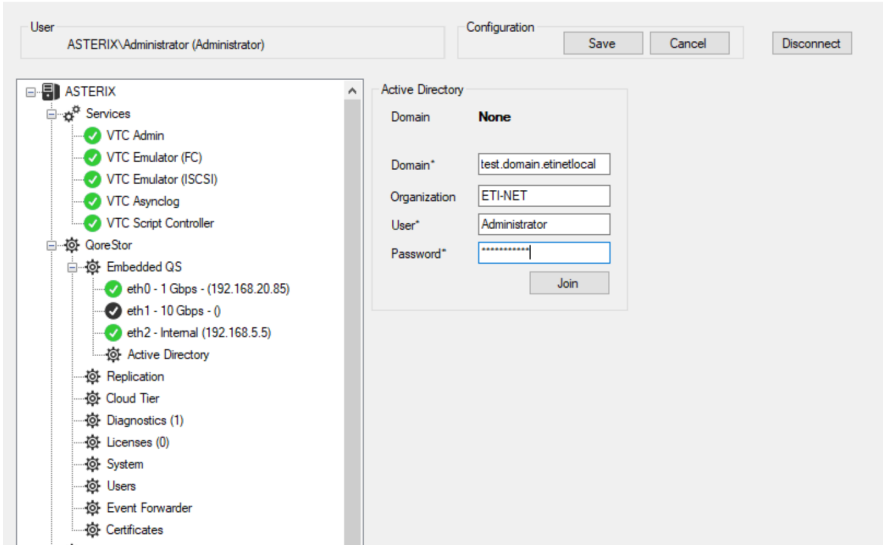
⚠	Default user for CIFS access is BackBox, with default password StOr@ge!

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.

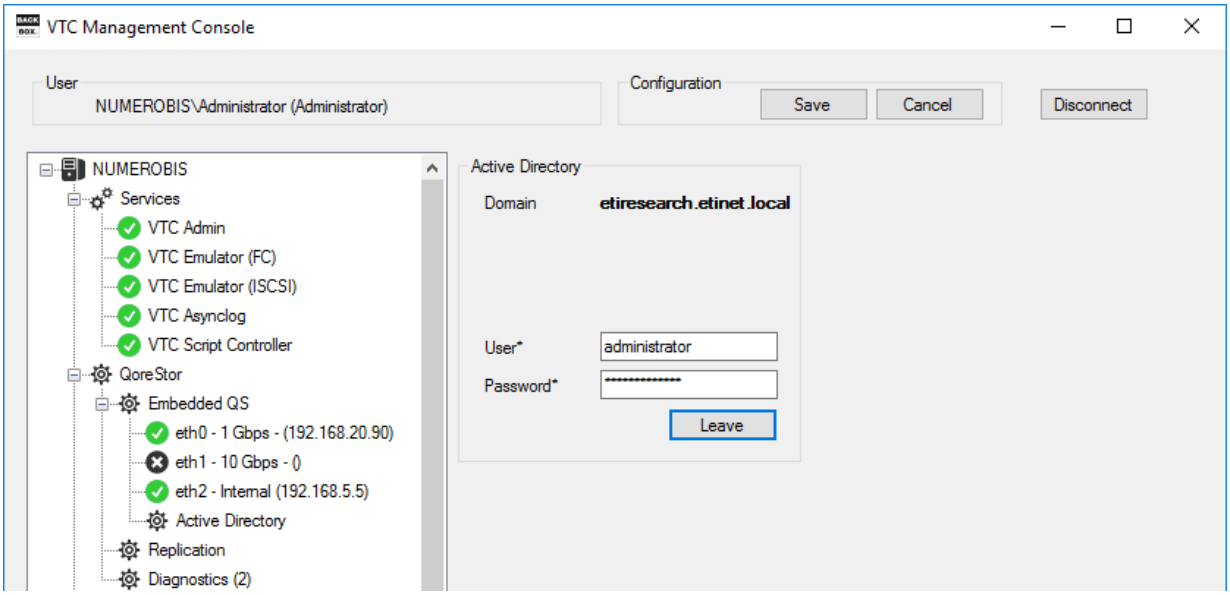


3. Set up the domain*, user* and password* (mandatory).
4. Click the **Join** button.

⚠	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.

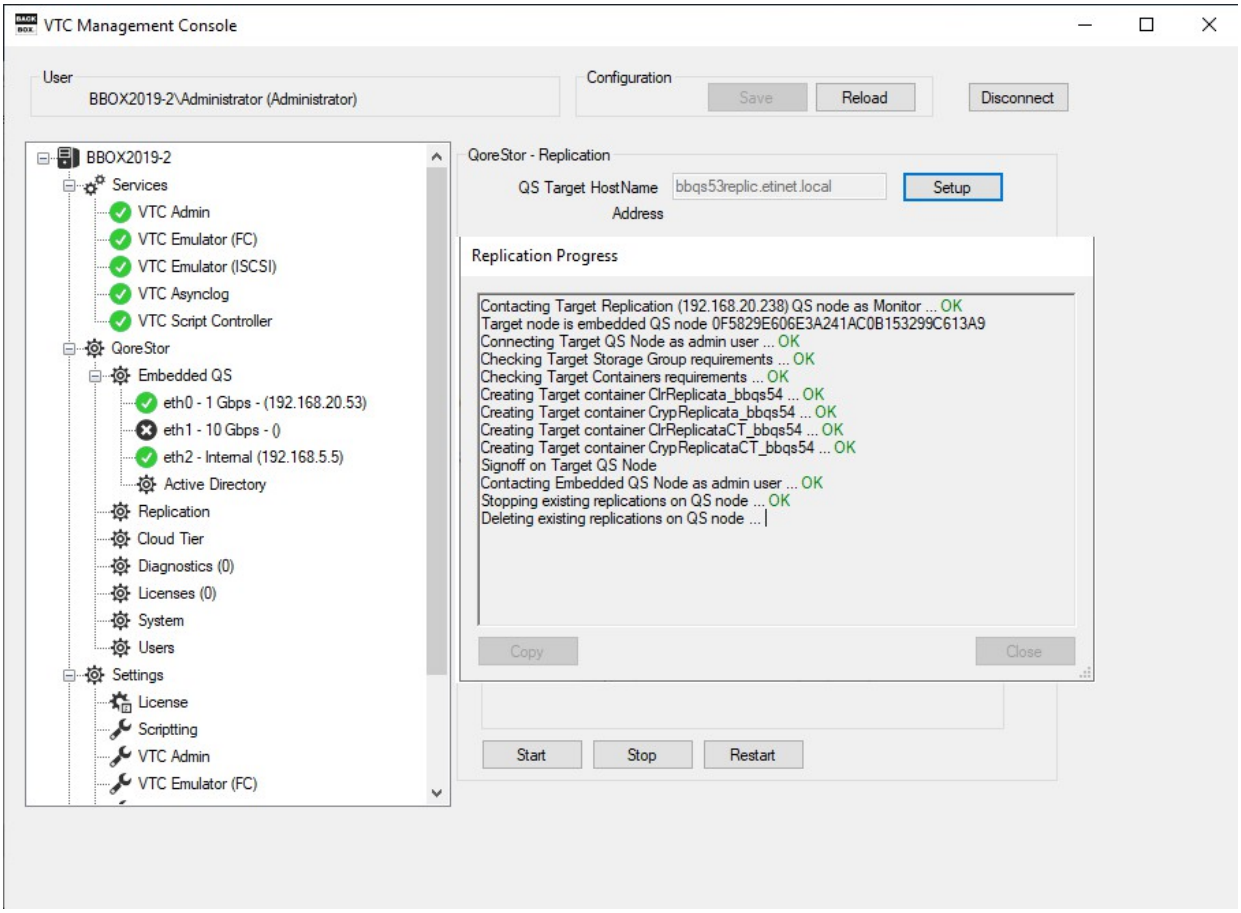


⚠	If any account seems to have lost ownership of the files and folders generated after joining the Windows Domain, log into VTC server with Domain Administration account and change the ownership. Follow the procedure described in Appendix F - Procedure for Files/Folders Ownership Recovery

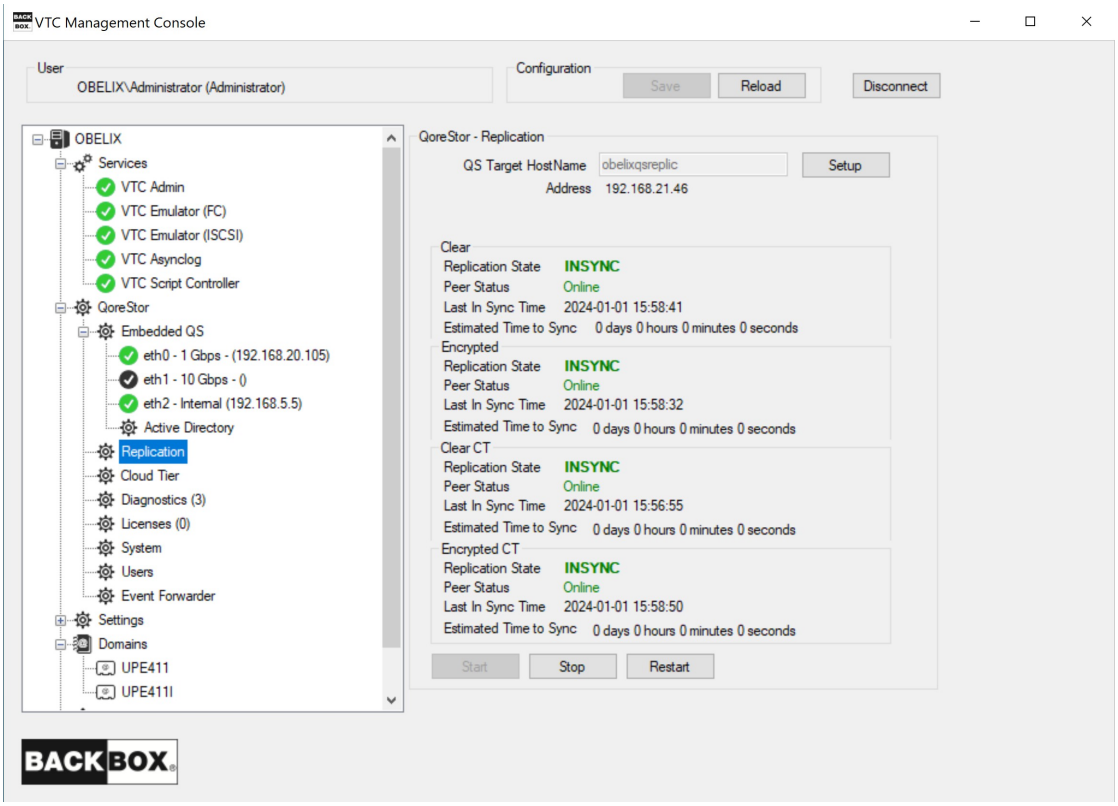
Replication

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 input the Target Hostname that points to the IP address (the status of the target and source containers for the replication process). If the QS Target HostName is not correct, the Setup button is grayed-out and an error message will be displayed.



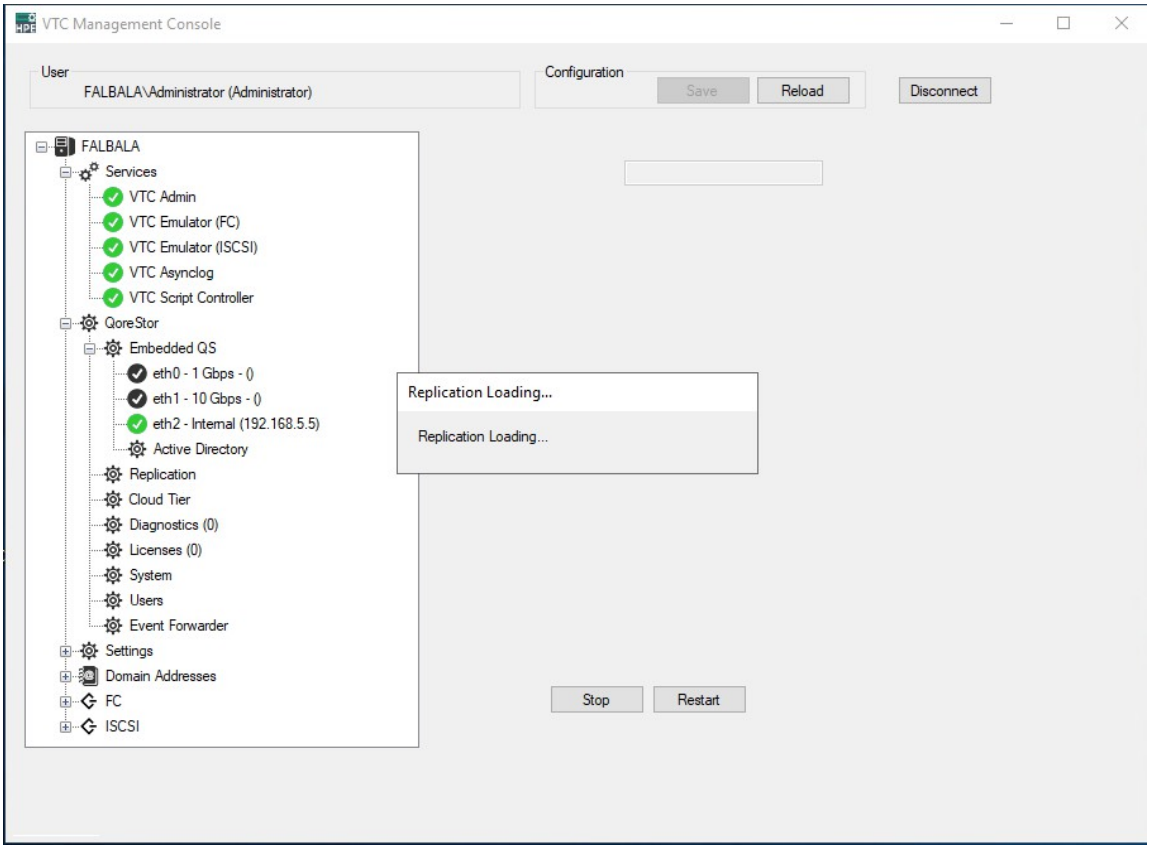
Once the replication setup progress has been finished and the state is marked INSYNC, the initial replication setup is complete.



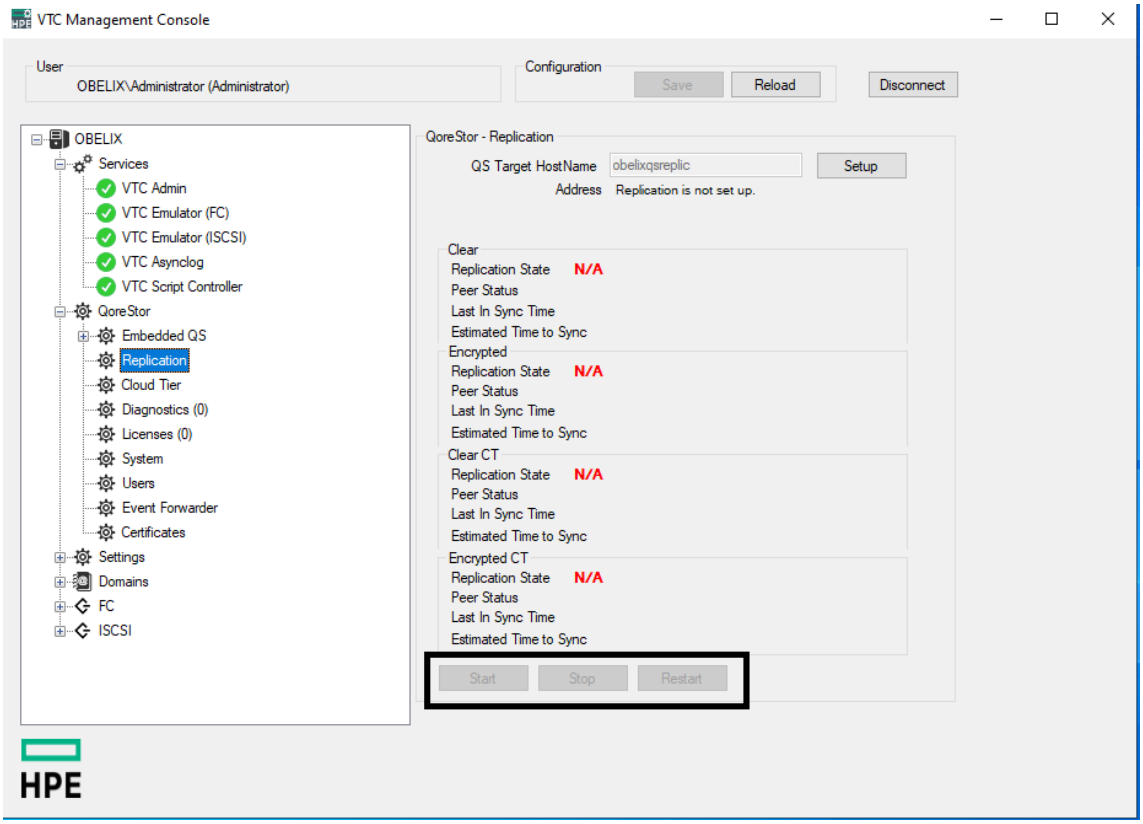
To view replication status:

- 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.



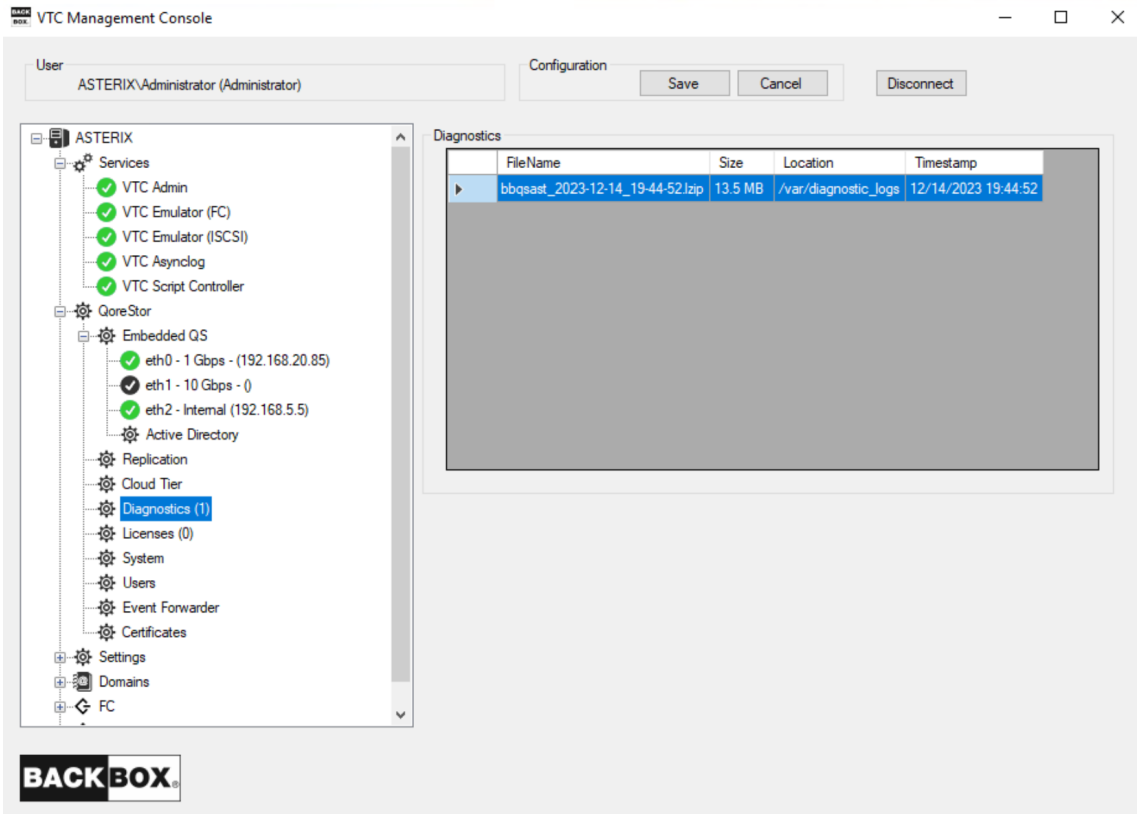
In the example above, the process running in the background and real-time tracked is the Replication. The pop-up displays info on the ongoing **Replication** Loading... process.



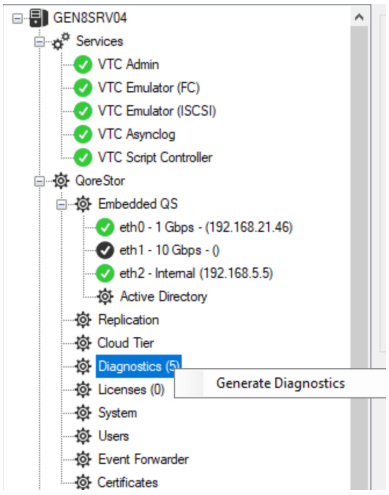
⚠	If the replication is not set up on both replication points, an error message will be displayed stating that the host is unknown. Therefore, the replication cannot be started. The Start, Stop and Restart buttons are grayed out.

DIAGNOSTICS

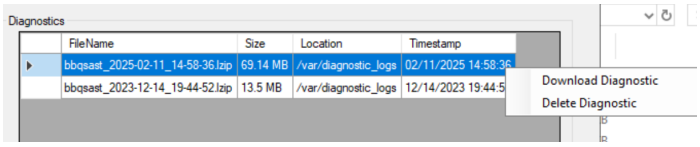
Remotely generate, delete and/or download diagnostics log (s) using the diagnostics feature.



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.

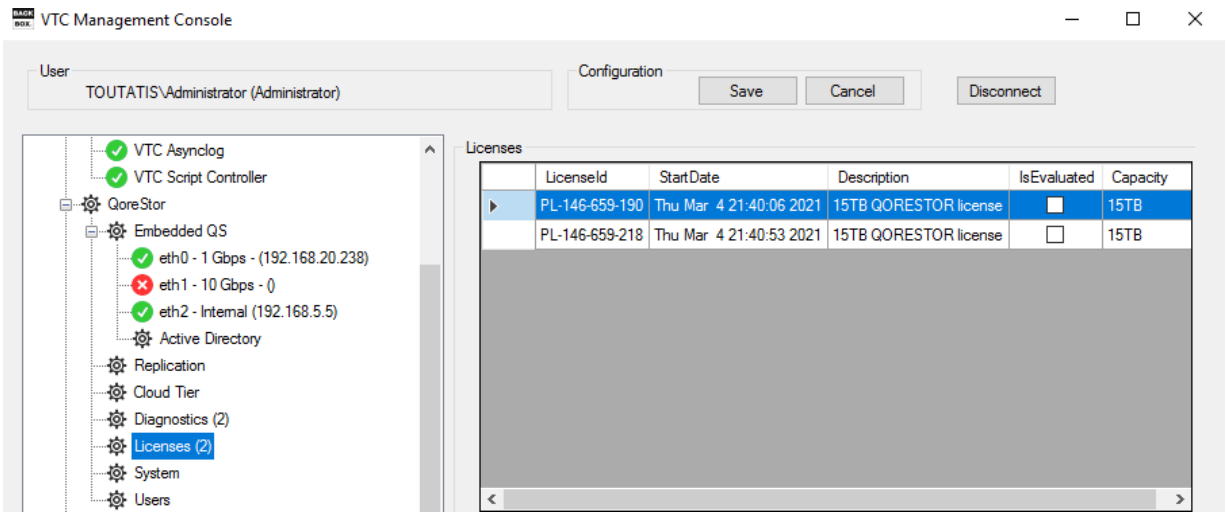


The files are in sync with the QoreStor log files and they contain the name of the embedded QoreStor and the timestamp of the log file.Once the file is generated it can be either downloaded or deleted. Select the file and right-click on it to choose **Download Diagnostic** or **Delete Diagnostic**.



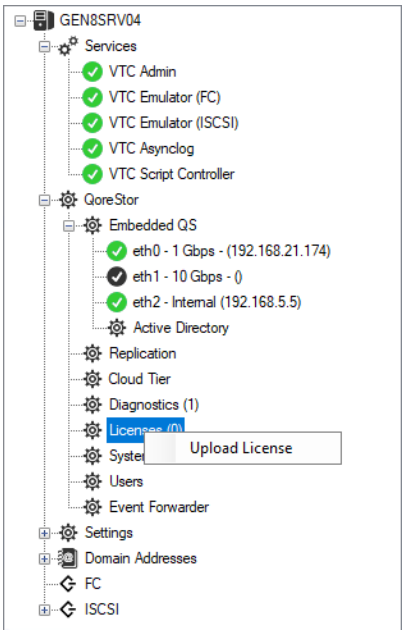
The diagnostic log file is by default saved in an automatically created folder on the local machine with the path name: `C:\ProgramData\ETINET\VTC\Diagnostics`. You can change the location of the diagnostic file after it has been generated, but any deleted or newly generated diagnostic files will not be automatically updated in this folder `C:\ProgramData\ETINET\VTC\Diagnostics`.

Licenses

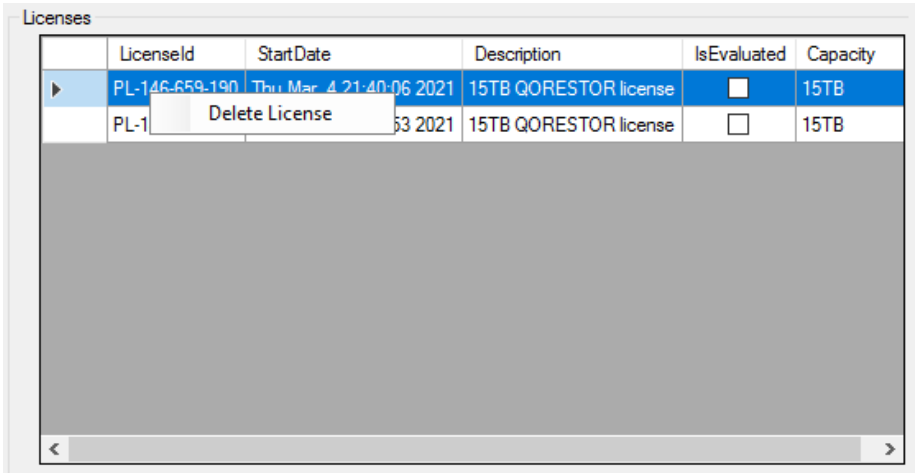


The node lists all active QoreStor licenses.

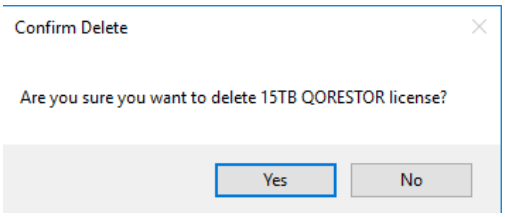
To upload a new license right-click on the license node.



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.



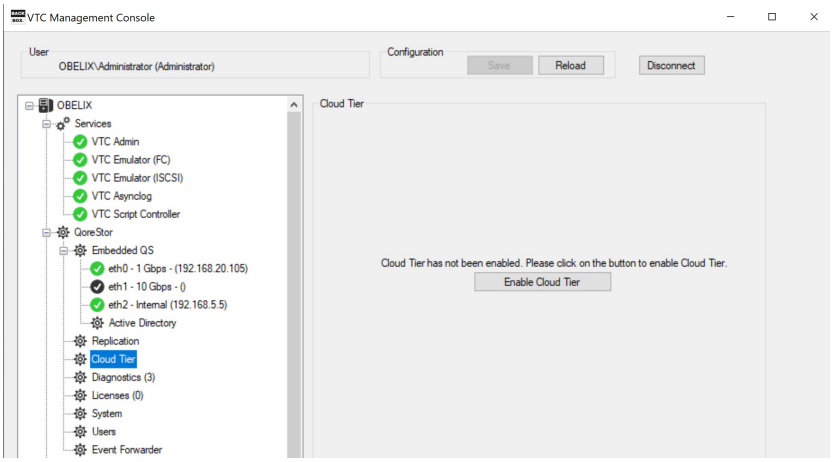
Confirm the deletion in the pop-up window by clicking **YES**. Click **NO**, if you don't want to delete the license.



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:

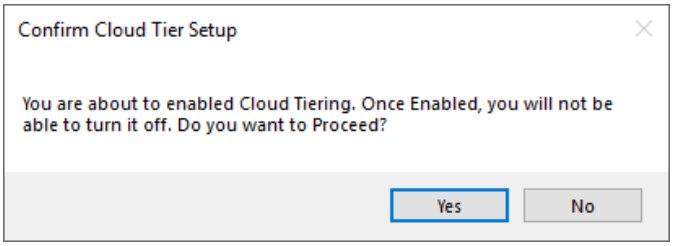
1. Select **Cloud Tier** node under QoreStor.



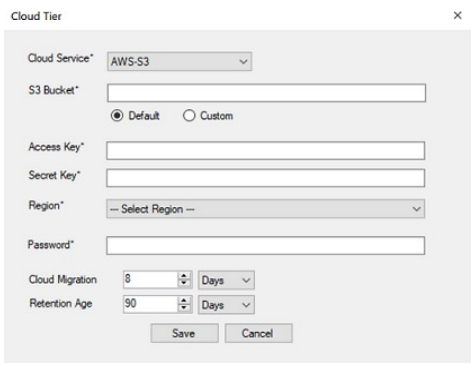
2. When pressing the button **Enable Cloud Tier**, a warning will pop up to inform the user that the enabling option is not reversible.

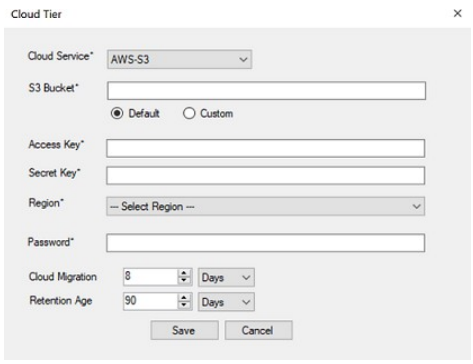
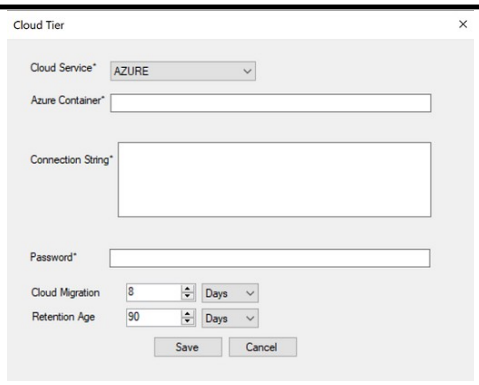
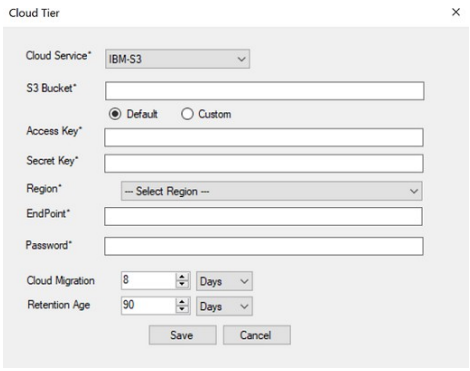
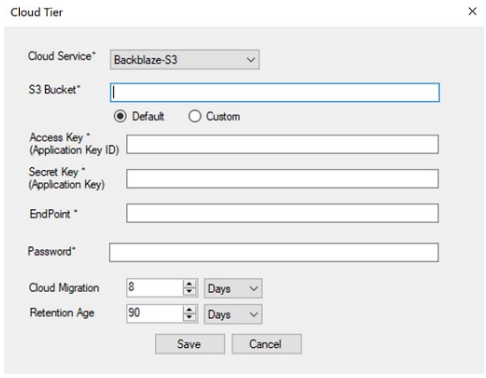
⚠	Once the Cloud Tiering is enabled and set up, it can no longer be disabled.

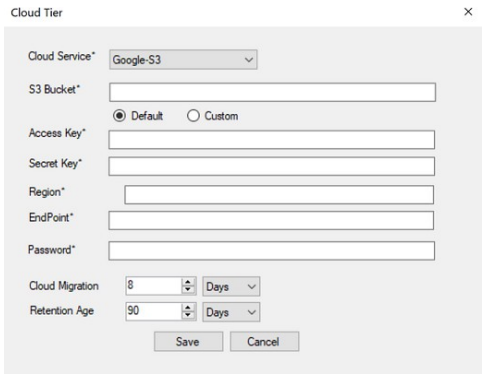
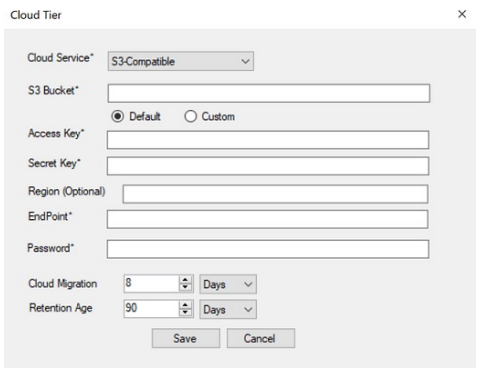
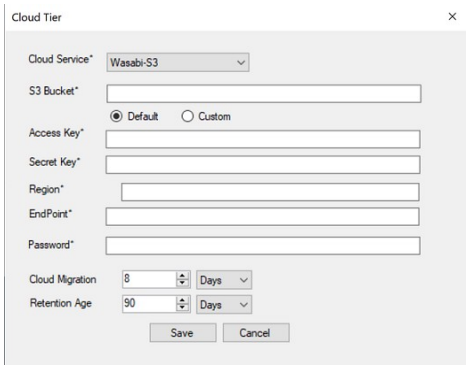
The pop-up will offer the choice to continue with the current operation or to keep the cloud tier disabled.



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 Cloud Service (AWS-S3, Azure, IBM-S3, Google -S3, Backblaze-S3, Wasabi-S3 and S3-Compatible), Container, Connection String, associated Password, Cloud Migration (in days) and Retention Age (in days). The default parameters are provider-specific.

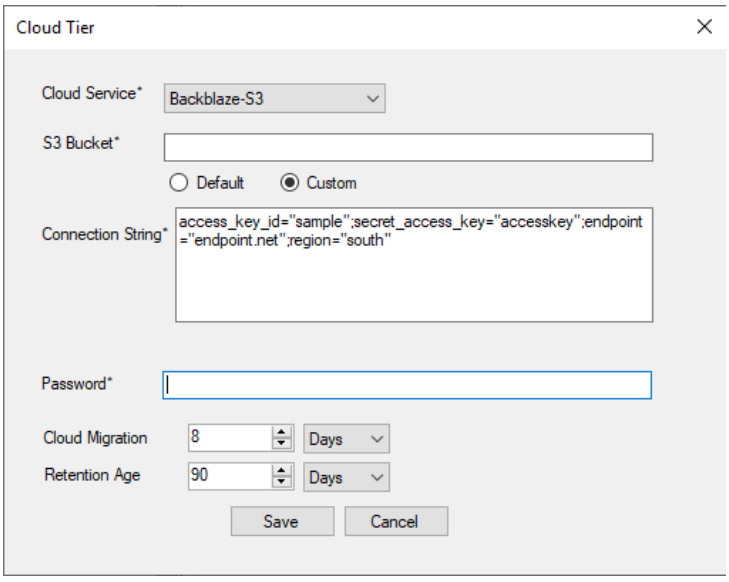
Cloud Service Provider	Cloud Service Settings
AWS-S3	
Azure	

AWS-S3	
	
IBM-S3	
Backblaze-S3	

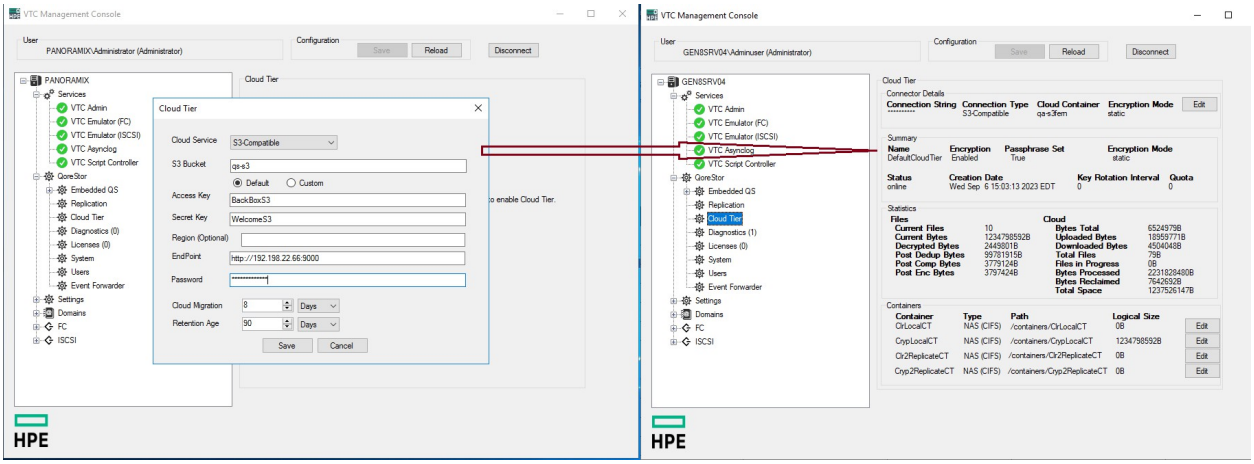
Google-S3	
Compatible-S3	
Wasabi-S3	

Depending on the Cloud Service chosen, the cloud tier setup parameters are different: AWS-S3, S3-Compatible, Wasabi-S3, Google-S3, Backblaze-S3 and IBM-S3 have mandatory extra fields, such as S3 Bucket, Access Key, Secret Key and EndPoint (Region is not mandatory for all cloud tier providers).

For **Custom** setup, all the parameters need to be added as a string to the **Connection String** field. See the example below.



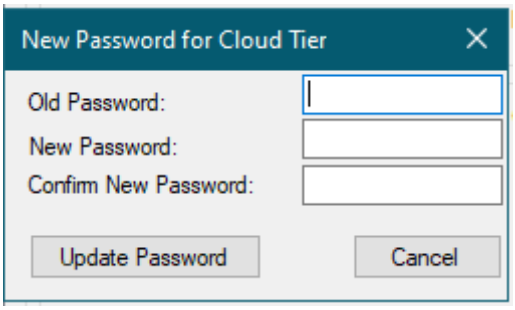
Once the Cloud Tier configuration is set up, details and editing options are displayed in the right-hand panel.



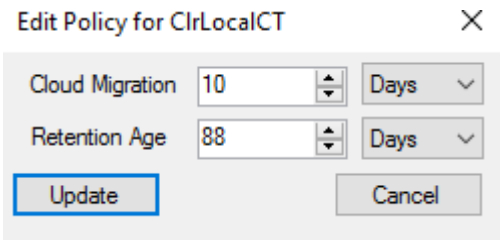
The Cloud Tier panel has four sections with details on **Cloud** Tier connection (String, Type, Container and Encryption Mode), Summary (Name of the cloud tier, encryption status and mode, passphrase set- ting, creation date, etc.), various Statistics and the cloud tier **Containers**.

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 password and confirm it. Click Update Password to have the new password updated.



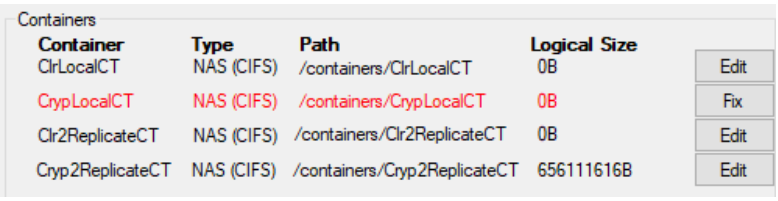
To modify containers' policies, click Edit for the specific container you want to change the policy to.



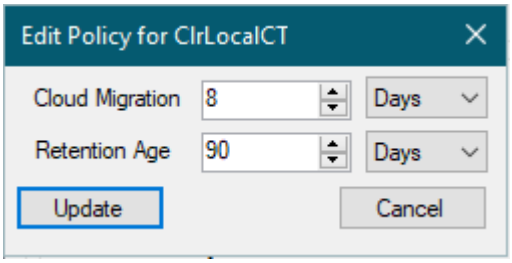
Edit the policies according to your specific requirements: cloud migration (in days and hours) and retention age (in days).Click Update to save the new policies or **Cancel**.

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.

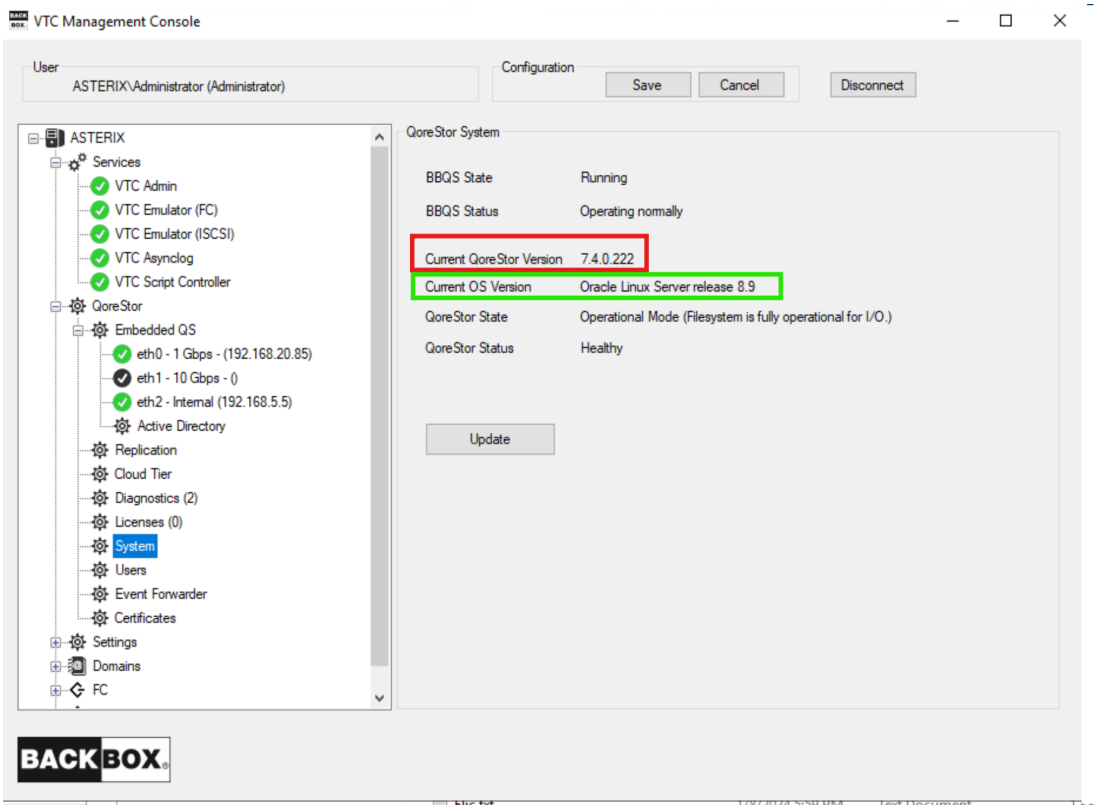


System

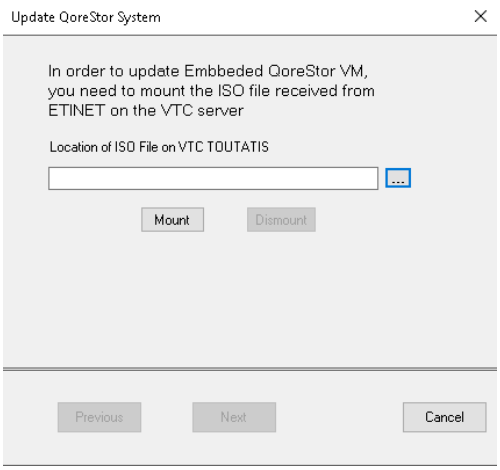
The System tab displays both QoreStor and OS current versions. The tab allows automatic updates of the embedded QoreStor and/or OS for Oracle Linux Server.

The update will automatically run both QoreStor and OS updates.

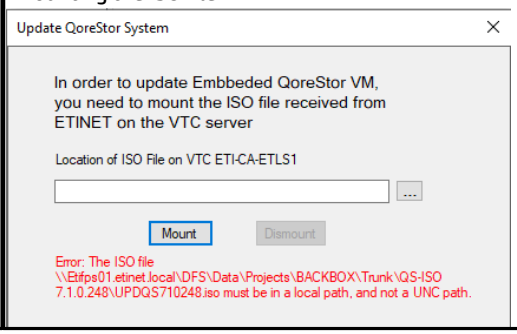
- If the QoreStor server is joined to an active directory, the QoreStor Server will need to leave the Active Directory prior to the OS upgrade. Once upgrade done, the QoreStor server can rejoin the AD. This will need to be done using an account with AD Administrator privilege.
- Temporarily stop the replication either on the source and the target QoreStor servers during the system upgrade.



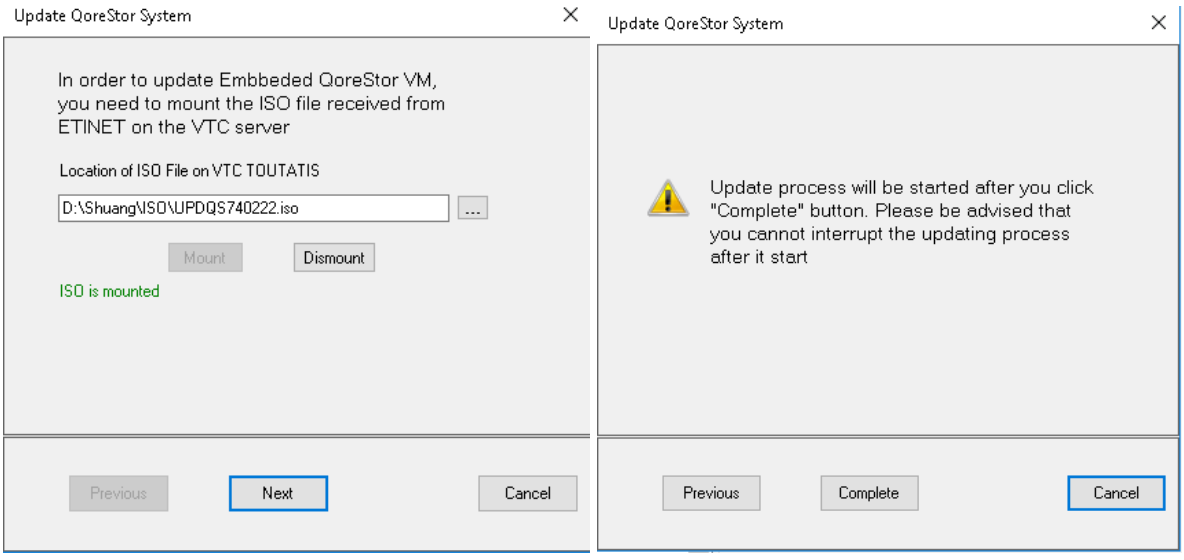
Before proceeding with the automated update, locate the ISO file necessary for theprocedure. The ISO file is delivered with the BabckBox version package and contains the update scripts for both QoreStor and OS. Click Update.



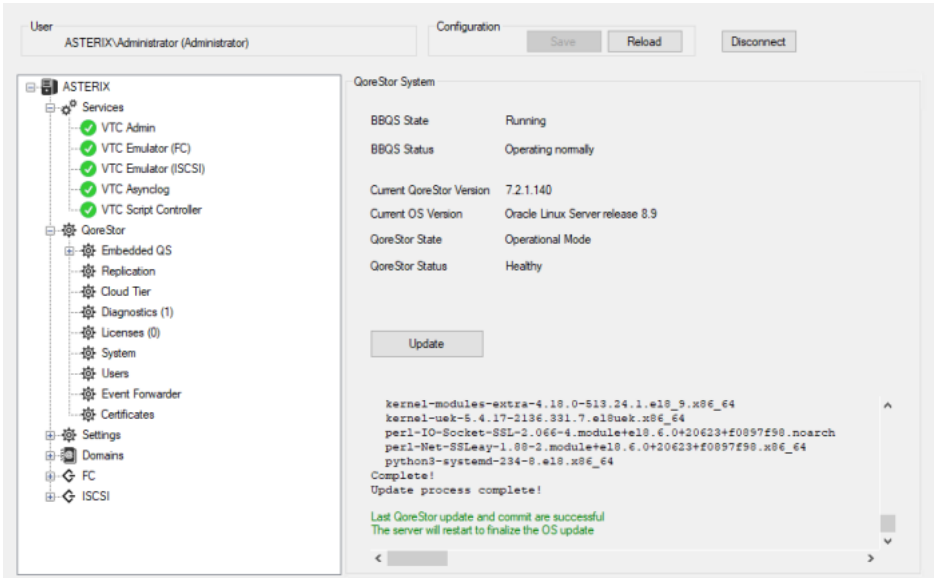
Click **Mount** to mount the ISO file. In case of a file error location, **Dismount** and choose the right ISO file.

⚠	Follow the procedure delivered in the ReadMe file along with the ISO zipped package.
⚠	Make sure the ISO file location is not remote. Copy the file on the local machine to avoid getting an error message when mounting the ISO file. 

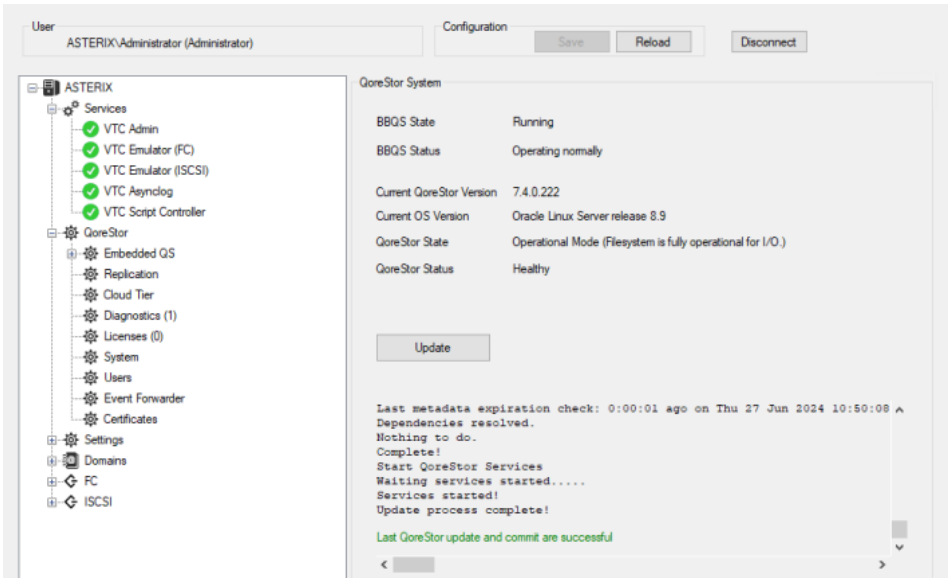
Once the ISO is mounted, click **Next** and **Complete** to start the update process.



While the update process is running, all the processing actions are displayed at the bottom of the VTC MC update window.

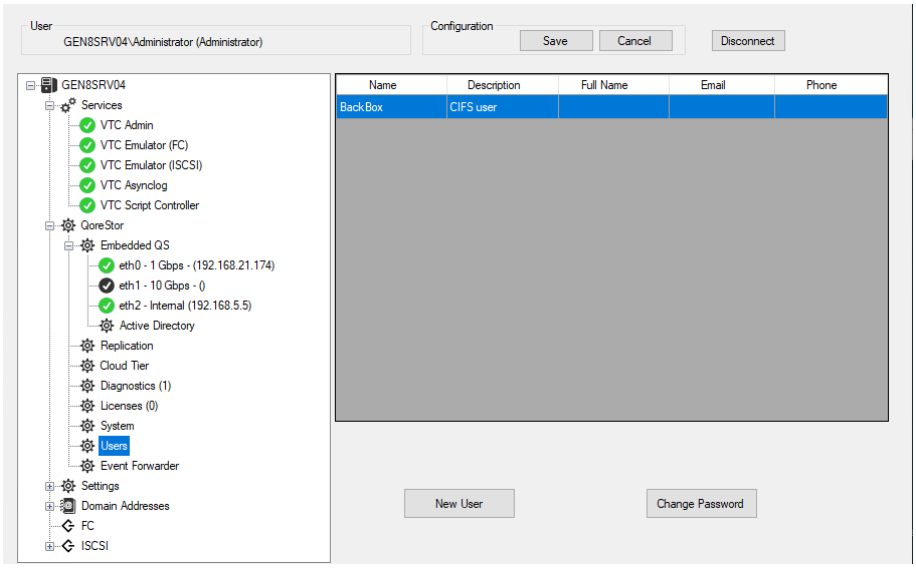


At the end of the updating process, the System tab will display the QoreStor version updated to.

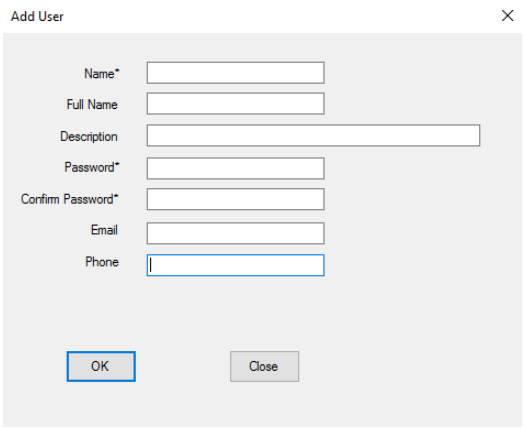


Users

QoreStor users are listed on the right-hand panel when the Users node is selected.



To add a new user, click New User.



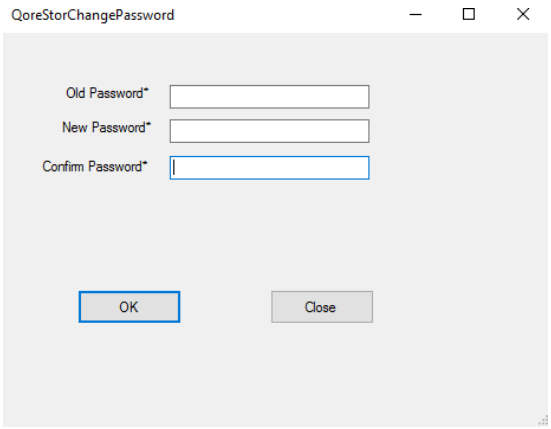
Specify the values for the mandatory fields* (Name, Password, Confirm Password) and click OK to save the entries.

⚠	Administrator, admin or monitor as user Name* values are not accepted. Only alphanumeric (letter and/or digit) values are allowed as names for users.

⚠	Only letter and space (no number) values are accepted in the Full Name field.

⚠	Description field does not accept special characters, but only numbers, letters and spaces.

To change the password for an existing user, select the user from the users list and click Change Password.

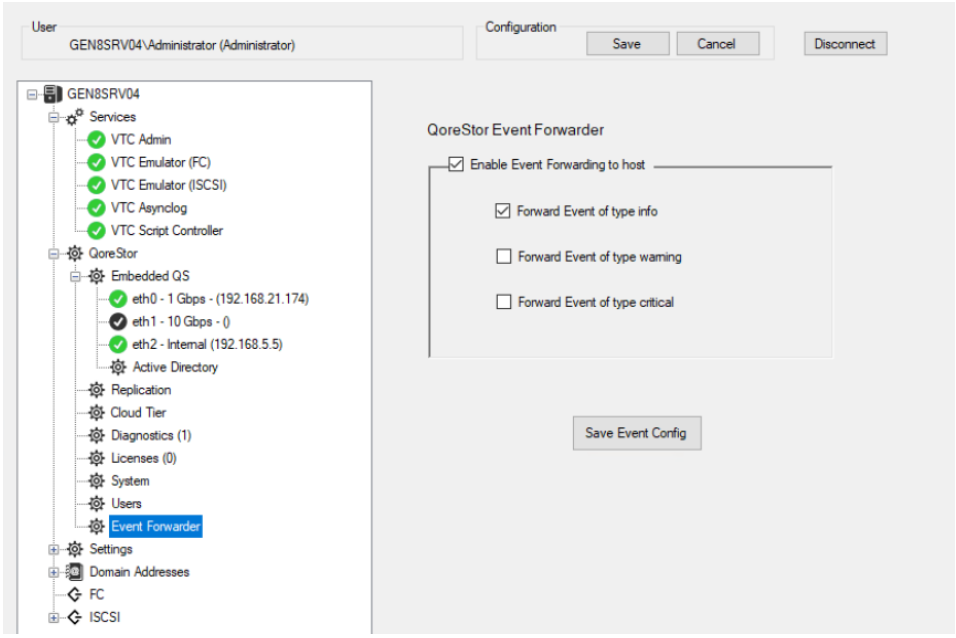


The pop-up window allows changing the password for the selected user. All fields are mandatory.Click OK to save the password change.

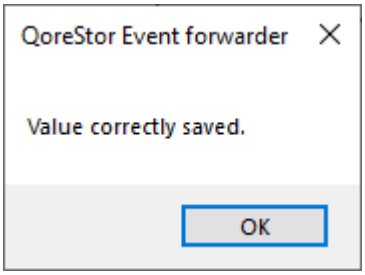
⚠	For QoreStor users, when deleting a user from Windows server, the user will not be automatically deleted in the VTC MC, therefore generating a display inconsistency in the user list. Do NOT delete QoreStor users in the Windows server list to avoid such inconsistencies.

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.

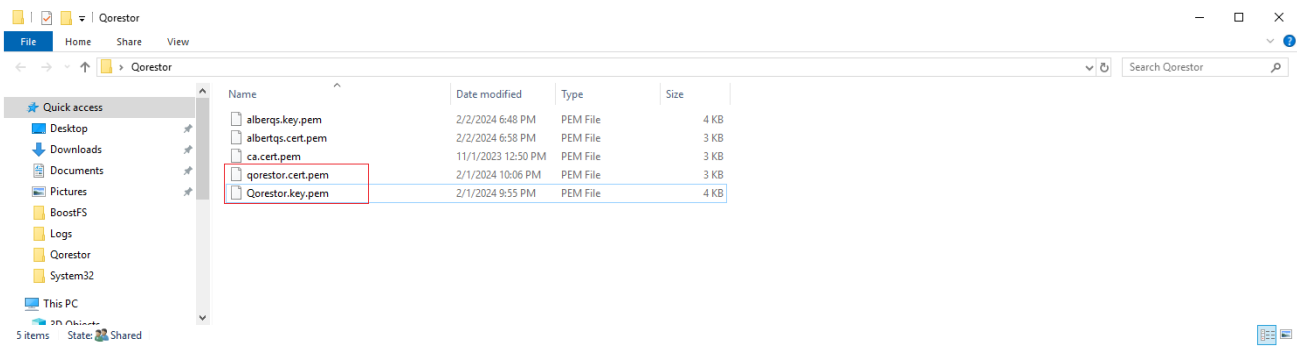


Certificates

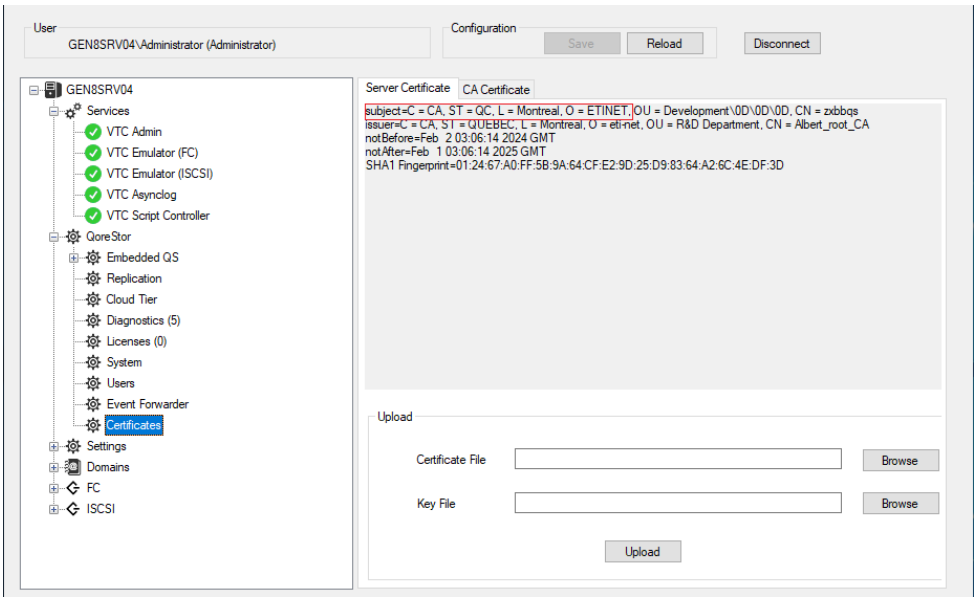
For an extra security layer, use the **Certificates** feature to upload your organization certificates:Server Certificate and CA(Certified Authority) Certificate.

1. Under QoreStor node, go to **Certificates** > Server Certificate and browse to upload the two server certificate files.

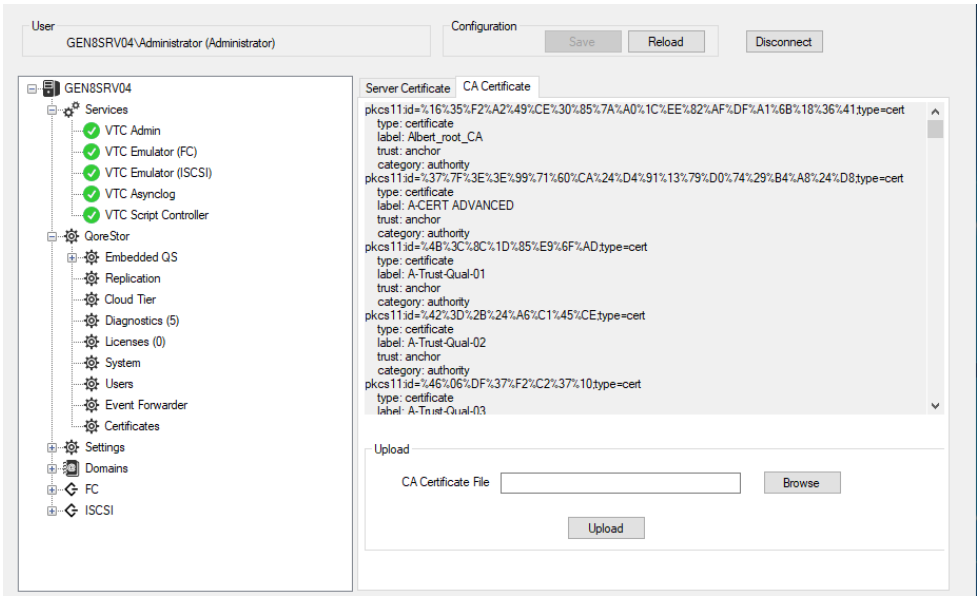
The files should be with a .pem extension, tagged as cert and key in the file name.



2. Once uploaded, the certificate panel will display details related to the certificate, showing - next to the subject line - the organization name the certificate belongs to.



3. Browse to the same certificate folder and upload the CA Certificate. Once uploaded, the tab will display details related to the CA Certificate.



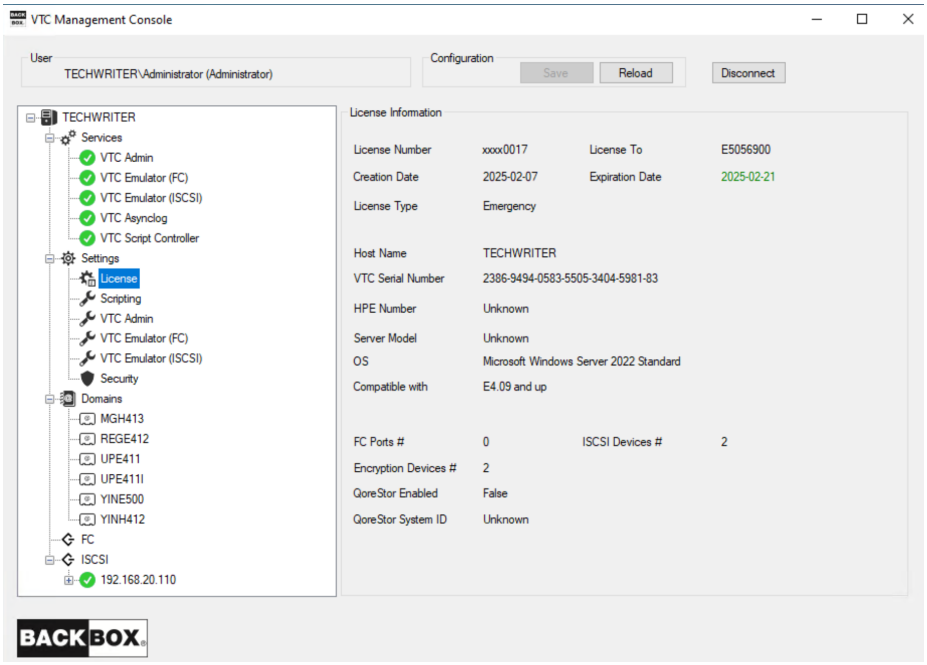
4. Save the configuration by clicking on the **Save** button on top of the panel.

Settings

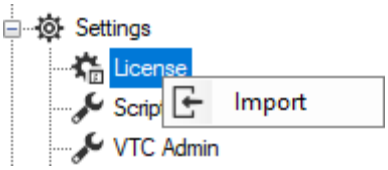
The following settings are available:

LICENSE

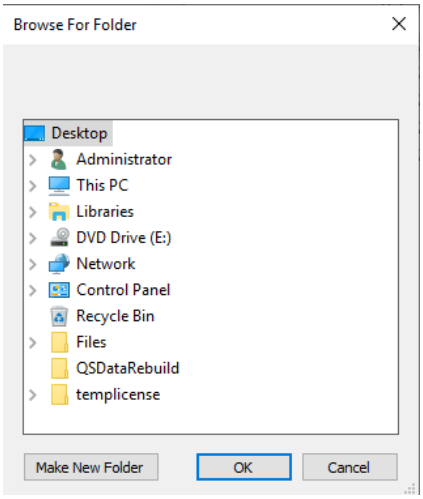
All details (including, expiration date, license number and type, host name details, FC ports, iSCSI devices connected and system ID) related to the active license are listed under the **License** node.



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.

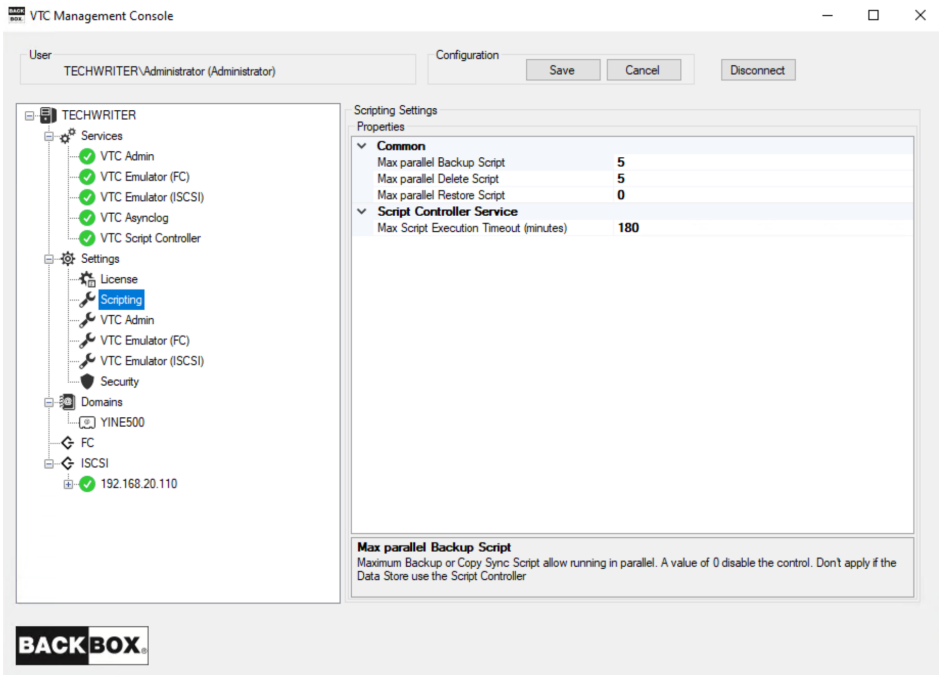
To install a new license: Import the license .xml file provided (via email along with the report .txt file) by your ETI-NET representative.The License is sent via email containing two files: license & license report.

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 license.

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.

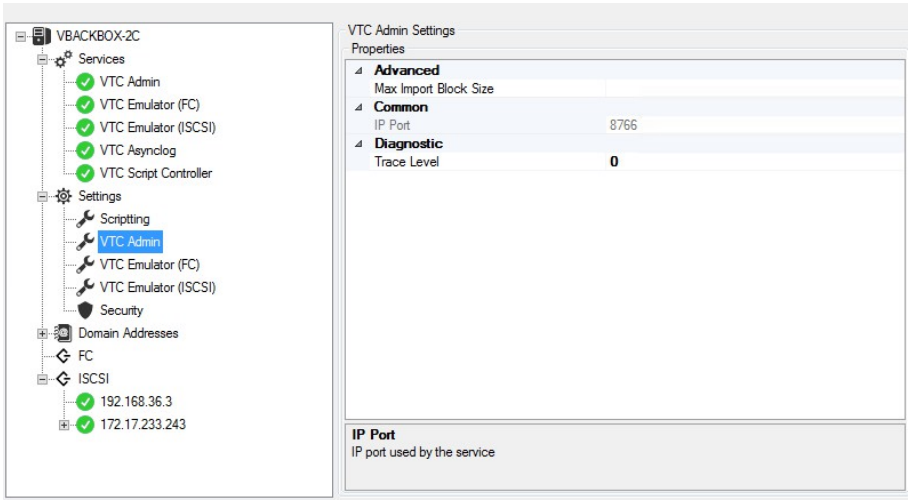


A gray-scaled panel indicates the read-only properties associated with the specified setting. When selected, any of the listed properties is shortly explained at the bottom of the window. Any change made to this setting requires restarting all the services listed under Services: right-click Services > 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.

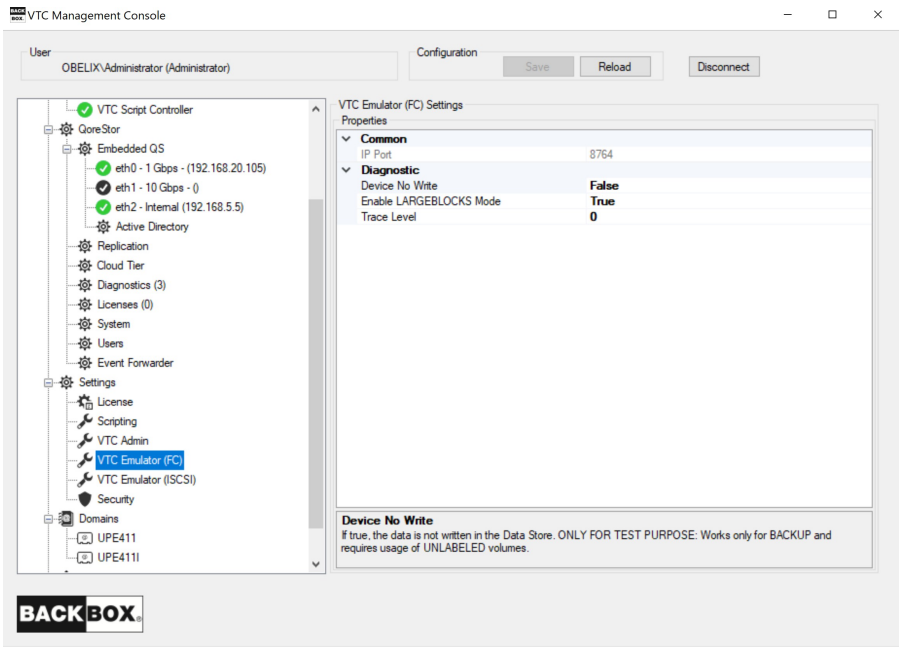


A gray-scaled window indicates read-only properties associated with the specified setting. When selected, any of the listed properties is shortly explained at the bottom of the window. Any change made to the setting requires restarting the server services.

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.

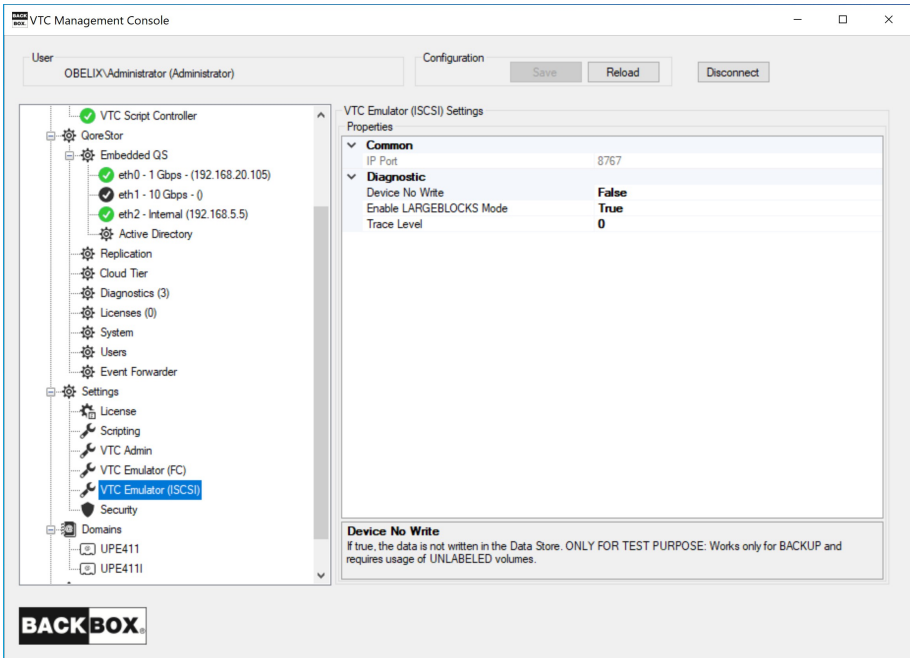


A gray-scaled window indicates read-only properties associated with the specified setting. When selected, any of the listed properties is shortly explained at the bottom of the window. Any changes made to this page requires restarting Services for the change to take effect.

VTC EMULATOR (ISCSI)

⚠	These settings should not be changed before communicating with technical support.

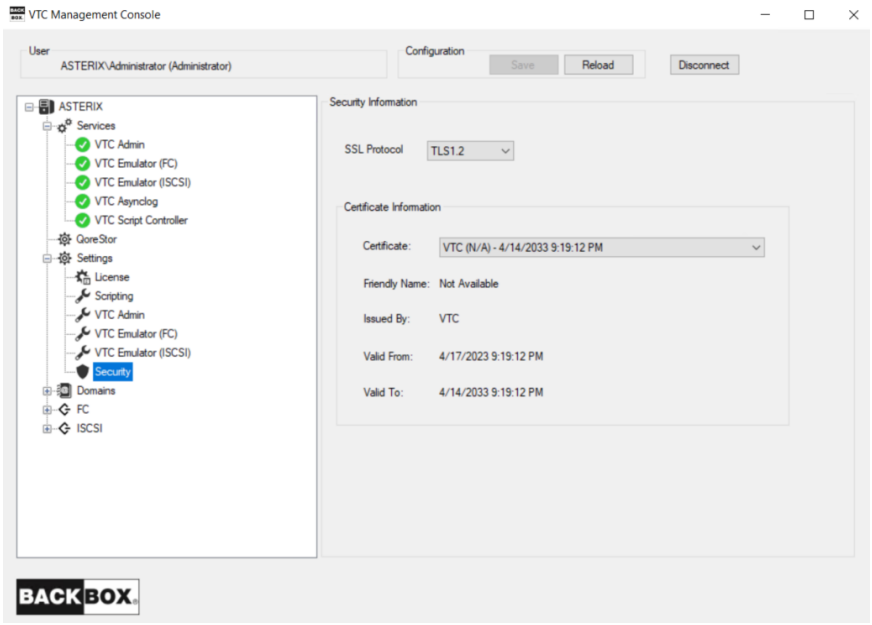
When VTC Emulator (ISCSI) is selected, the available properties for the service are displayed on the screen in the right-hand side panel. There are no actions available when right-clicking on the VTC Emulator (ISCSI) setting node.



A gray-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

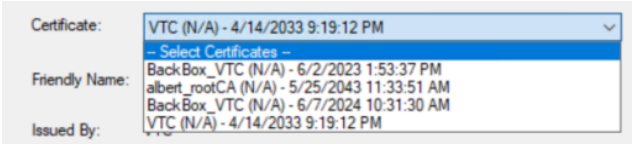
When selected, information related to the support of TLS/SSL from the VTC server is displayed in the right-hand side panel. LARGEBLOCK mode is set to ON at installation for both FC and iSCSI. It is recommended to leave it ON as it has no impact on the system when not using this option. On the contrary, 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 Information: VTC certificate details, listed by type, validity period and

Certificate: Certificate summary including type (VTC), friendly name, expiration date and time. The drop-down list displays the available certificates to choose from.



Friendly Name: Name set up in the license generator

Issued By: Server type that issued the certificate

Valid From: the starting date and time of the certificate validity

Valid To: the end date and time of the certificate validity

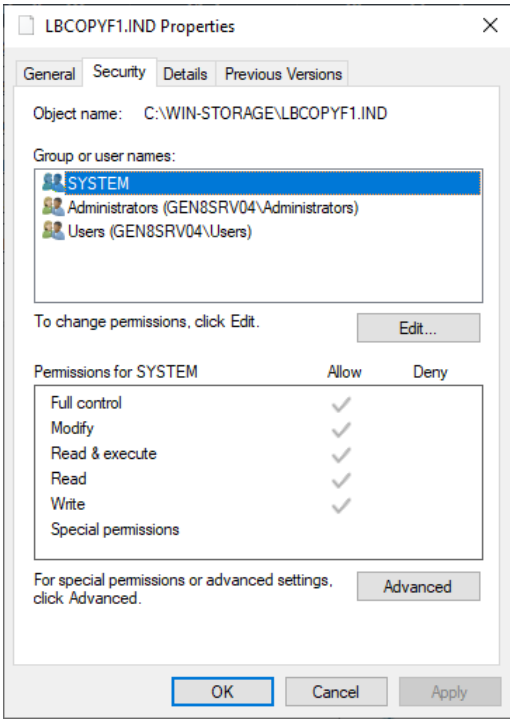
⚠	If you don't use any SSL Security protocol select NONE from the drop-down list.
⚠	If the UI is separately installed - on another instance - than the VTC MC, go to UI > Preferences and set up the SSL protocol manually to match the VTC MC settings. For more details, see section User Interface.
⚠	Go to the NonStop to set up the SSL parameters in such a way that the SSL settings are accordingly applied to correctly communicate with the VTC MC. Moreover, if you need to encrypt the server key pass code, you have to run an encryption program: BBpsCode. For more details, see section Sign In/Out in the User Guide for more information on enabling/disabling SSL.

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 or a pre-defined pass phrase sent to the client along with the other certificates.The Pass Phrase- if generated along with the certificate - will be validated by VTC MC.Click **Save** to validate certificates and pass phrase.**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.

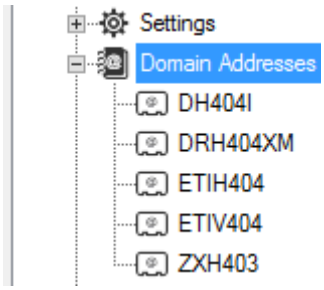
⚠	Customers using their own security certificates have to store these certificates in a special local folder after they have been issued by a certification authority. In order to copy certificate trust lists and certificate revocation lists they need to be saved in a certificate store, along with identity confirmation used to protect data and establish secure network connections.

For additional information see Certificate Store section in APPENDIX - SSL SETUP.

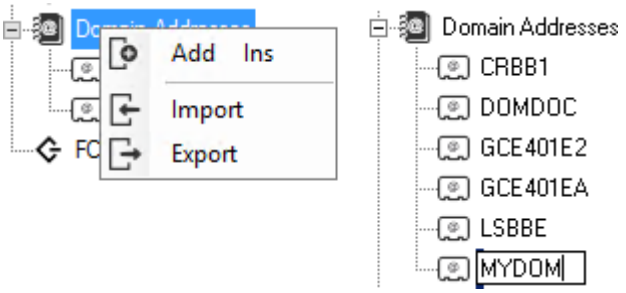
Domain Addresses

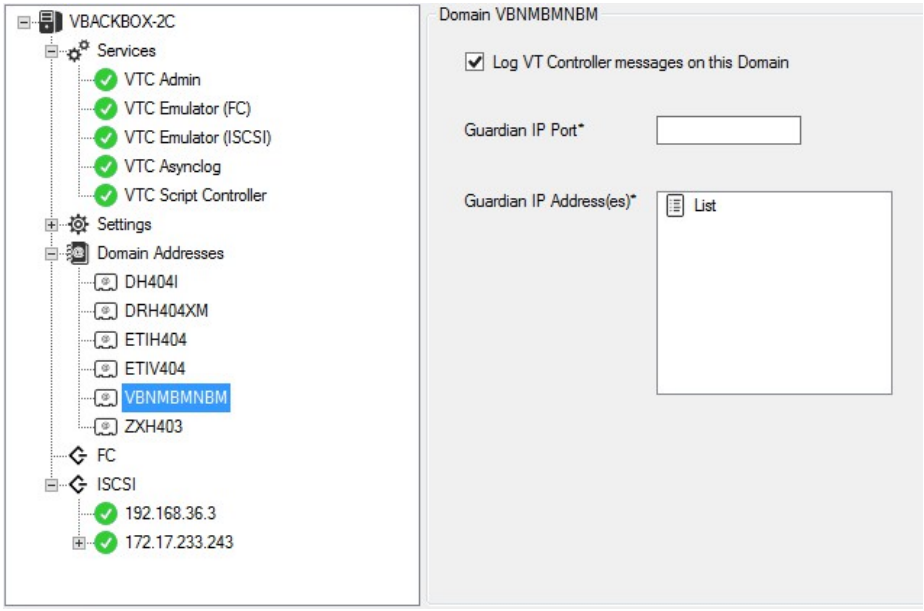
When expanded, the **Domain Addresses** node displays all domains currently configured on the VTC server.

⚠	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.



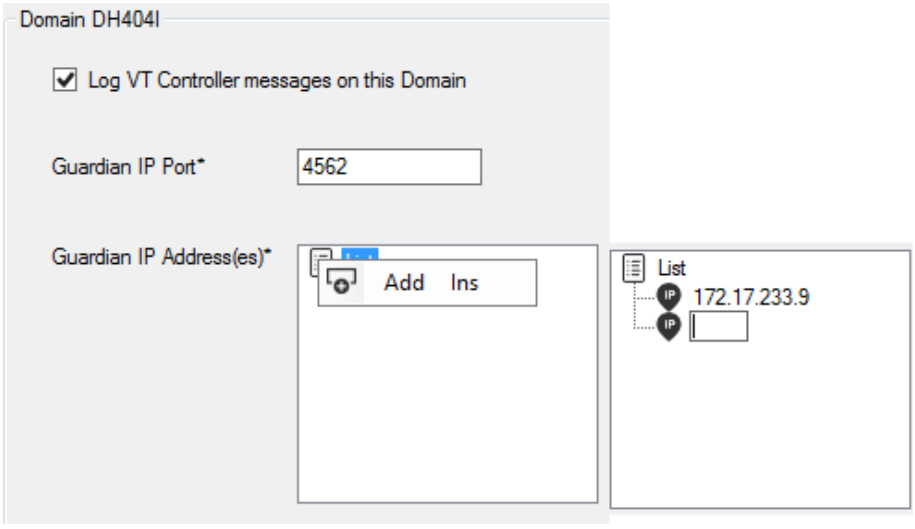
A new domain can be added to the list by right-clicking on the **Domain Addresses** category node and selecting Add or by pressing the Insert key while the Domain Addresses category node is selected. Type the name of the domain and press Enter to complete the node insertion.





Complete the domain registration by entering the appropriate information in the fields on the right-hand side panel.

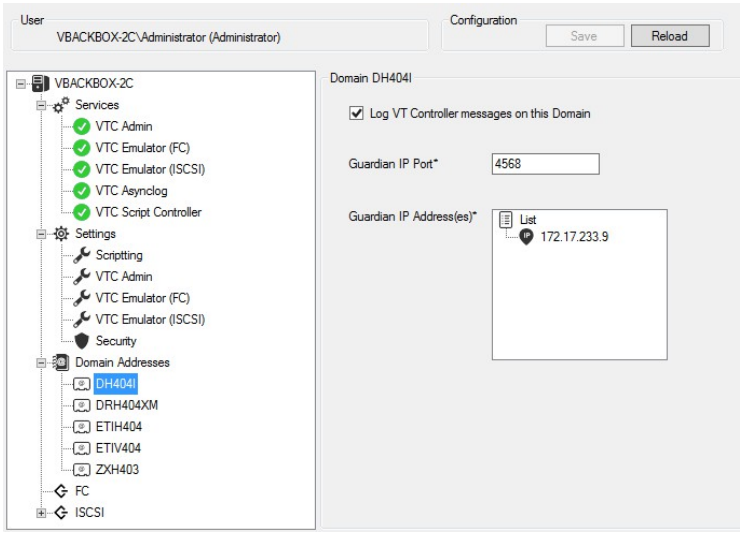
To add a Guardian IP Address, right-click on the List node and select Add or press the Insert key while the List node is selected. A new IP node will be added in the list. Enter the network address in either numeric or DNS form. Check the option Log VT Controller messages on this Domain that allows the VTC to send information (as an .xml file) to the domain .



If missing or invalid information is entered, an error marker will appear to the right side of the field.

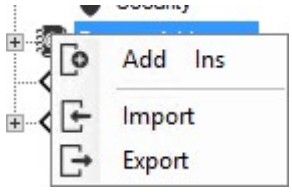
Hover the pointer on the error marker to get the error description.When the registration process has been completed, Add a new domain name or Save the modification(s).

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).

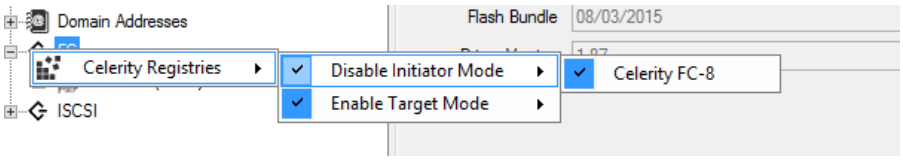
To Export/Import a Domain Addresses List right-click on the Domain Addresses node and select either Export or Import. The Export feature allows using the Domain Addresses list on another VTC server of the same domain by extracting the (Domain Addresses) list and placing it in a local file as backup.



- 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 exportedfile, press theOpen 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.

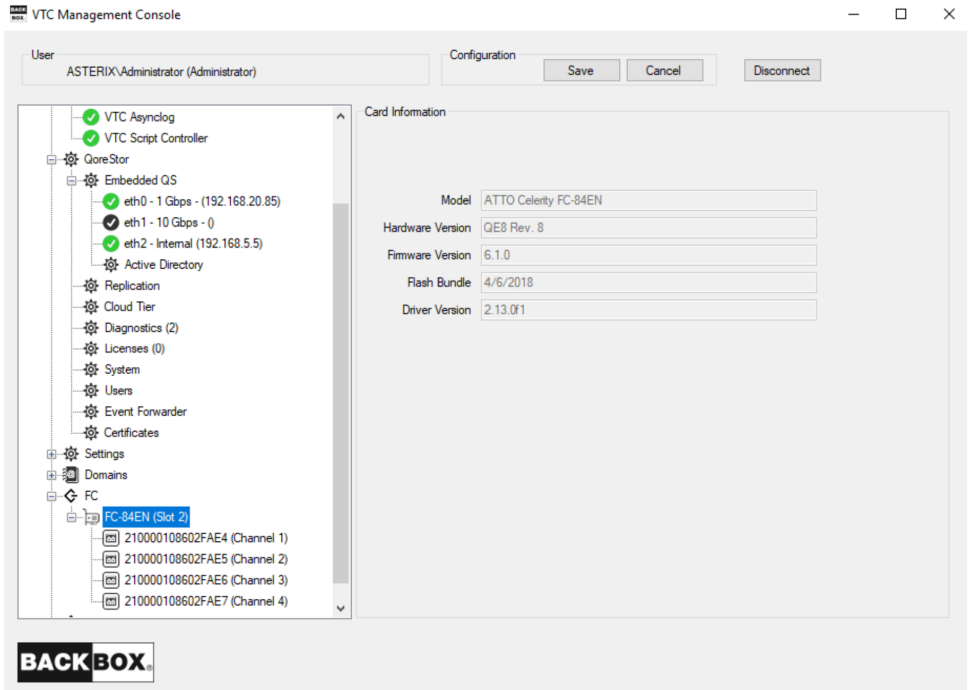


When enabled, the feature will be checked .A diamond indicates that the feature is enabled only for part of the HBAs on the server.

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.

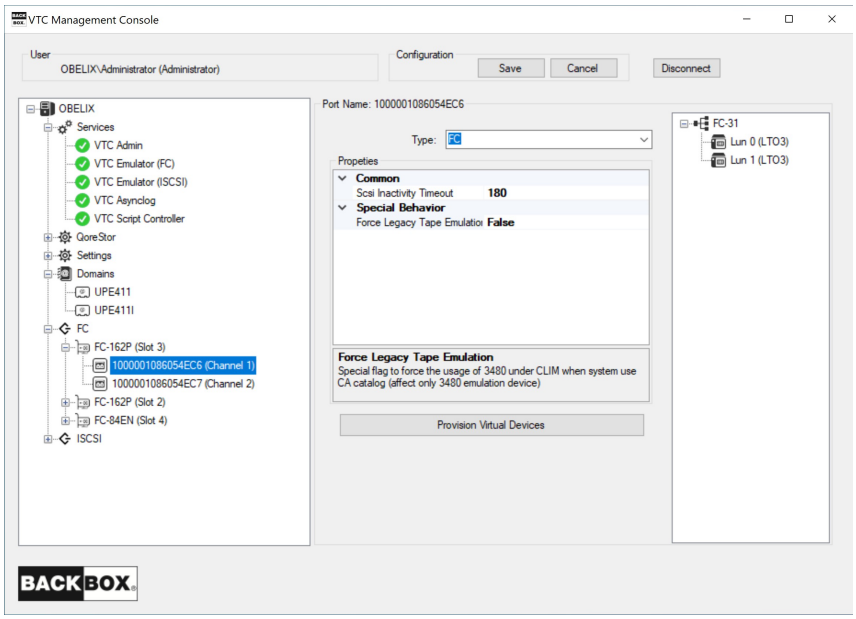
TARGET MODE CARDS LIST

When the FC category node is expanded a list of all target mode cards available on the server is dis- played. 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.

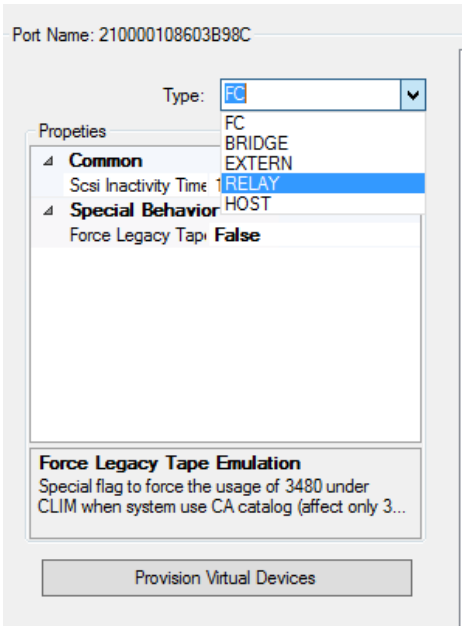


PORT CONFIGURATION ELEMENTS

- Port Type

To change the port type, open the Type selection box and choose one of the types.

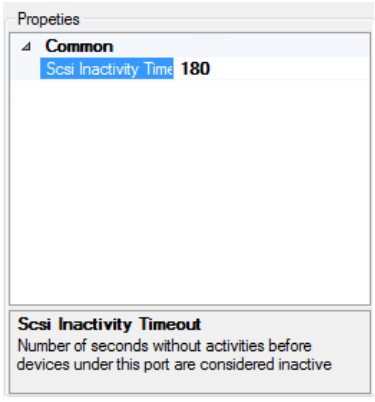
⚠	Changing a port type automatically resets the port configuration elements to the default values as per the newly selected type. (ex: The number of the LUN is reset, as is the device emulation).



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 aVirtual Tape System for LTS media migration.
RELAY and HOST type are reserved for BackLib usage.

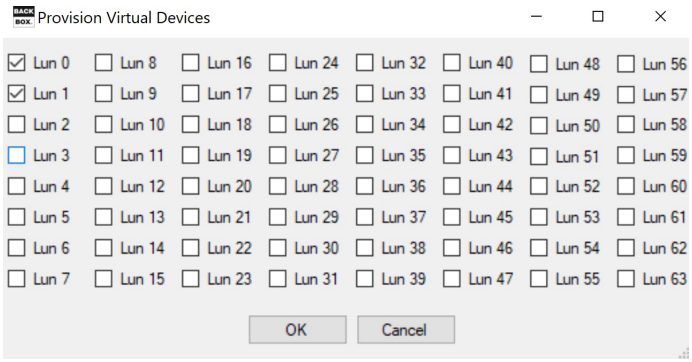
- Port Properties

Port properties are related to the port type. A grayed-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

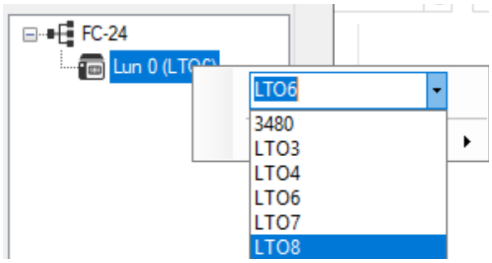
To add or remove LUN in the port available device list use the **Provision** Virtual Devices button.This button launches a dialog box that allows adding or removing LUN by checking or unchecking the LUN number.



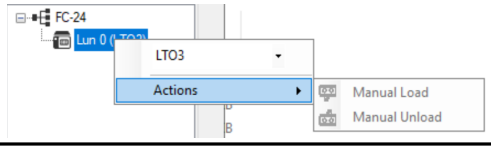
PORT LUN LIST

The port Alias used in the BackBox 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 grayed-out. 

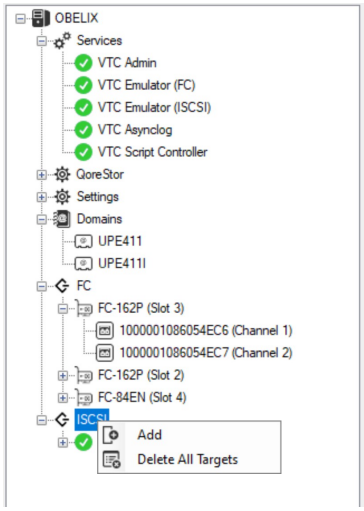
iSCSI Node

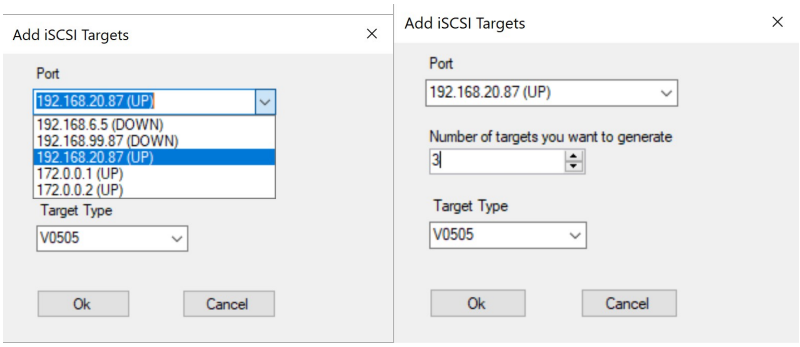
All VTC iSCSI configurations are grouped under the iSCSI category node. Changing of any of the elements described below requires restarting Services for the change to take effect.
When expanded, the iSCSI category node lists all target IP addresses installed on the VTC Server. When the iSCSI category node is selected, no information is shown in the right-hand panel.

Installing iSCSI

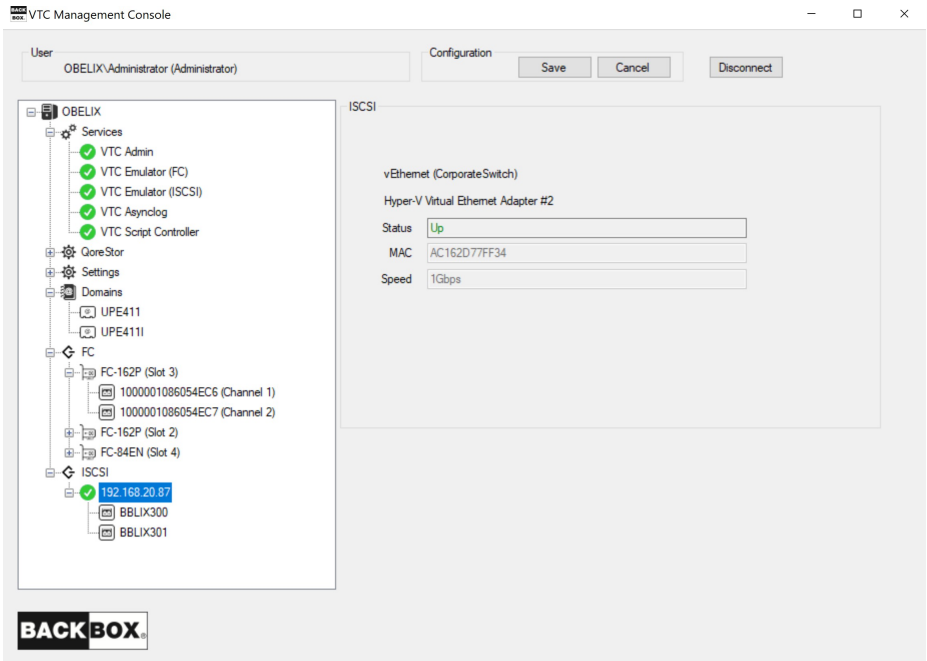
Configuration of the iSCSI is done through the VTC Management Console. The VTCMC displays the avail- able NIC cards as nodes (node name is IP address of the NIC). Under each node you can add up to 12 iSCSI devices. These devices must be added to the interface that reaches the virtual NonStop public LAN 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. Right-click on the iSCSI node in the VTC Management Console and click Add to display the iSCSI device creation box.

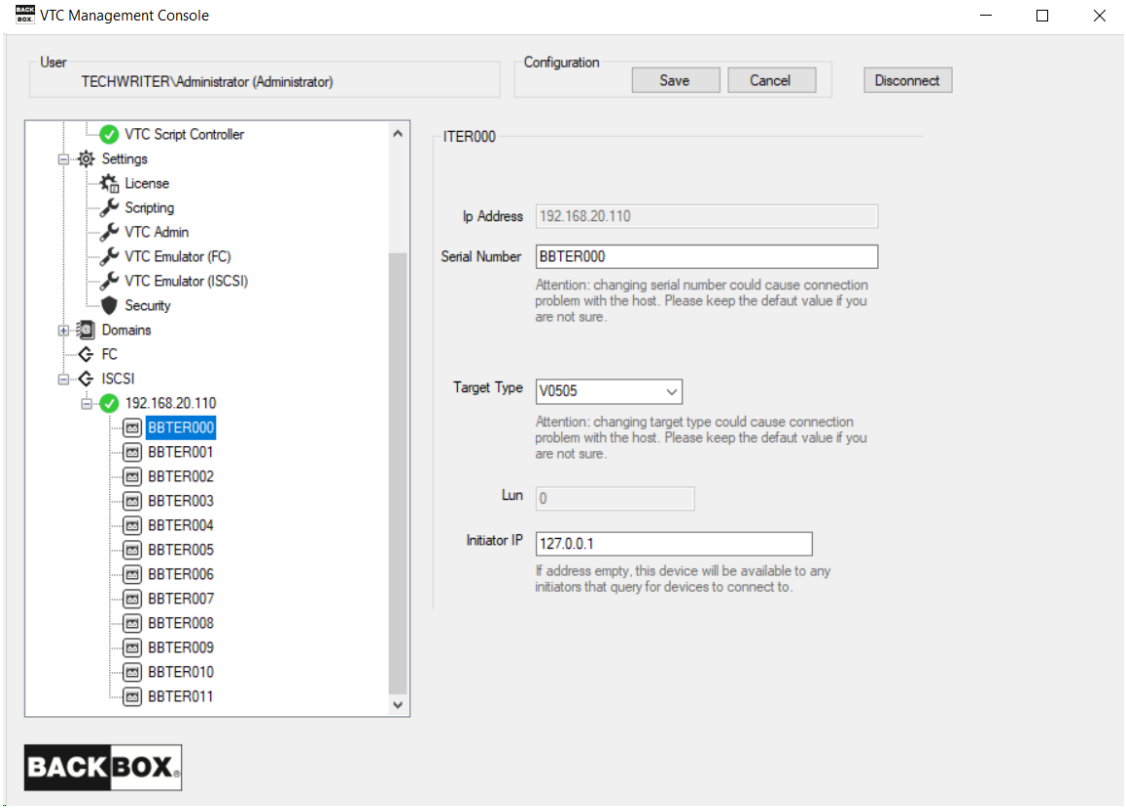




2. In the pop-up window, first select a NIC address to be used for the Storage CLIM connection and choose the number of targets (up to maximum 12 devices per port) to be added with tape emulation type. If you have a limited number of targets licensed, you can either add them to the same storage CLIM or spread them across all ports. Click ok.
3. If you have multiple ports dedicated to different CLIM connection, the Add iSCSI Targets procedure needs to be redone for each port.
4. Once the targets are added, they will be shown under each IP address.



5. Select, one by one the targets and define its connection parameters. Changing the Serial Number and/or the target Type could cause connection errors.



a. Serial Number is the target identifier and shouldn't be modified, as the connection is securely established with the host based on the serial number.

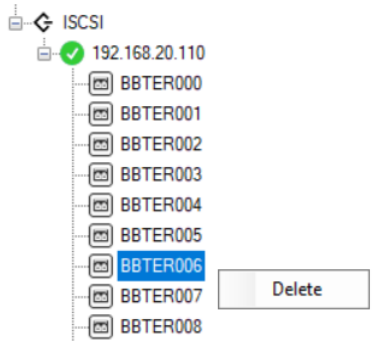
b. Target Type is the emulation tape type to be used for the target (V0505, LT04, LT06 to LT08).

c. Lun is assigned by default and cannot bechanged, as it's used to provision virtual devices.

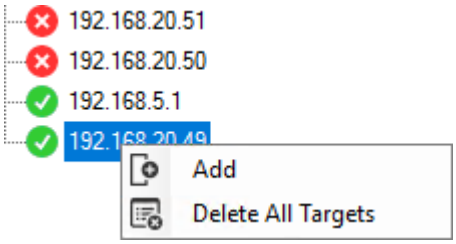
d. Initiator IP links the selected target to a specific CLIM. Once linked, the iSCSI device will only answer to the discovery command from that specific storage CLIM. By default, new added device is assigned with a dummy value of 127.0.0.1 that must be changed with the CLIM storage IP address of the target device to be to connected to. The new added device IP address can be left blank to answer to any CLIM storage.

⚠	If not updated and left with the default value (127.0.0.1), the target device will not answer to any CLIM storage when attempting to adding iSCSI tape target devices by using the CLIMCMD `--addiscsitape`. If updated to blank, the target device will answer to any CLIM storage when attempting to adding iSCSI tape target devices by using the CLIMCMD `--addiscsitape`. If updated to a specific CLIM address IP, the target device will only answer to that specific CLIM storage when attempting to adding iSCSI tape target devices by using the CLIMCMD `--addiscsitape`.

6. To delete an existing target, right-click on the selected target and Delete.

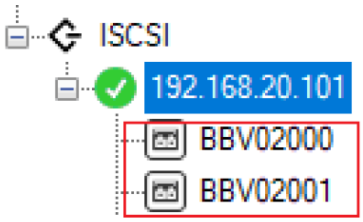


⚠	If all targets under a port are deleted, the port itself will be deleted along with the associated targets.



7. Once the targets are added, they will be shown under the IP address with their respective IDs/- names.

⚠	Devices are identified in the target list by the prefix identifier BB followed by the target specific ID.

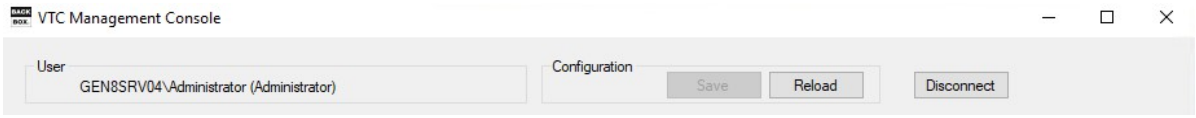


⚠	If the device has been manually added in the BackBox UI on the VT Controller page, refresh the UI page to make sure the device is properly displayed in the Virtual Devices list.

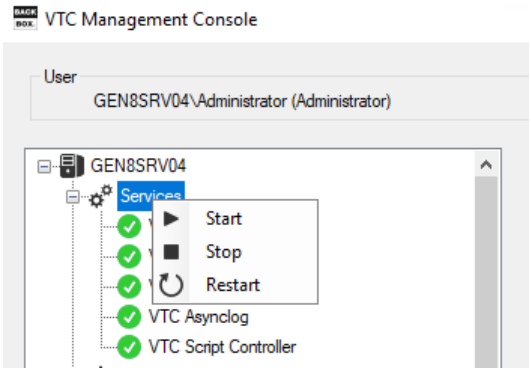
When the NonStop scans and adds the devices, each device ID is displayed with the IQN identifier.

```
$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
```

8. 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 - SSL SETUP

TRUST ROOT CERTIFICATION

The way to add certificates into the Trust Root Certification Authorities Store is as follow:

1. Run MMC in command line.
2. On the menu, click file **Add/Remove snap-in** > select "certificates" in "Available snap-in" list > Add > choose "Computer Account" > Next and finish. You will then see certificates console.
3. In certificates console, click **Trust Root Certification Authorities** and add CA certificates (or the server certificate if self-signed)

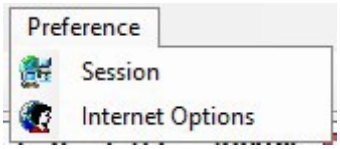
Note that CA and Certificate file must be PEM format.

For more details on how to add CA or Certificate File to the Trust Root Certification Authorities Store refer to documentation of the OS you are using.

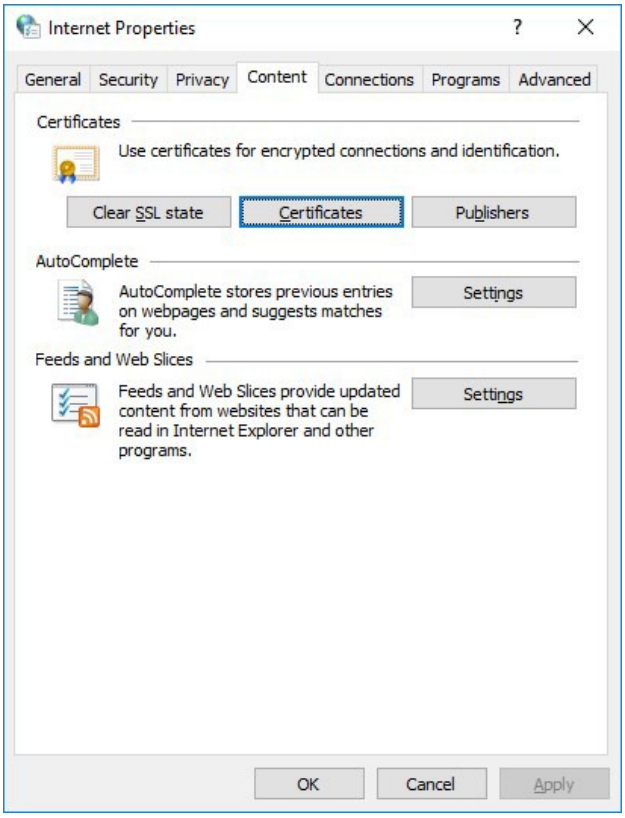
⚠	Perform the following steps only if the User Interface is installed on a workstation.

To install the CA Certificate in the operating system, follow the steps described below:

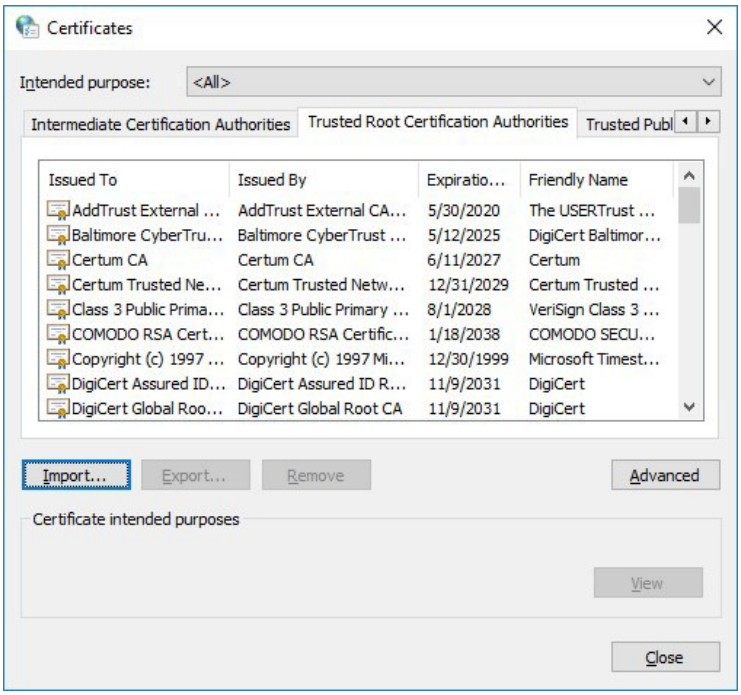
1. On the BackBox UI menu > **Preference** > **Internet Options**.

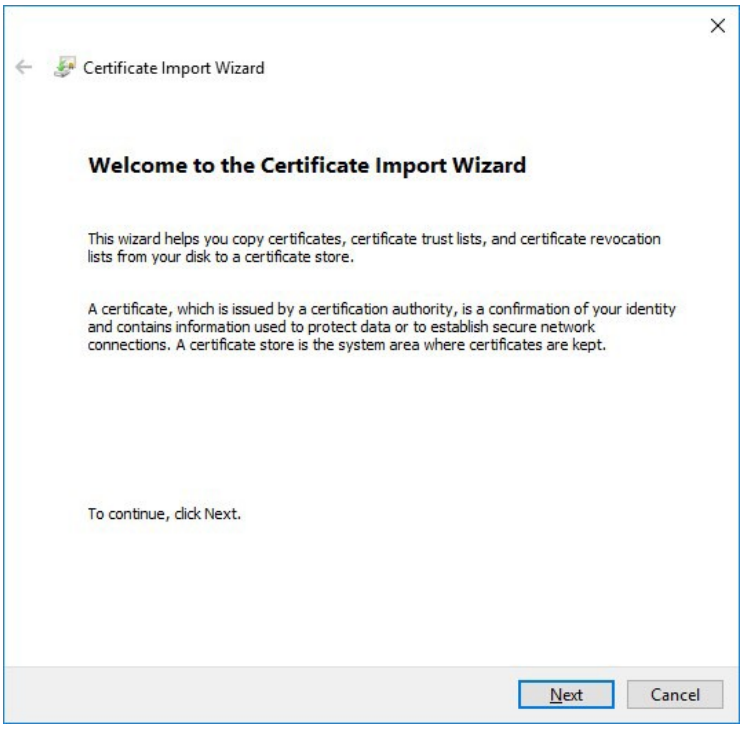


2. In the pop-up window click on the **Content** tab and then choose **Certificates** in the appropriate section.

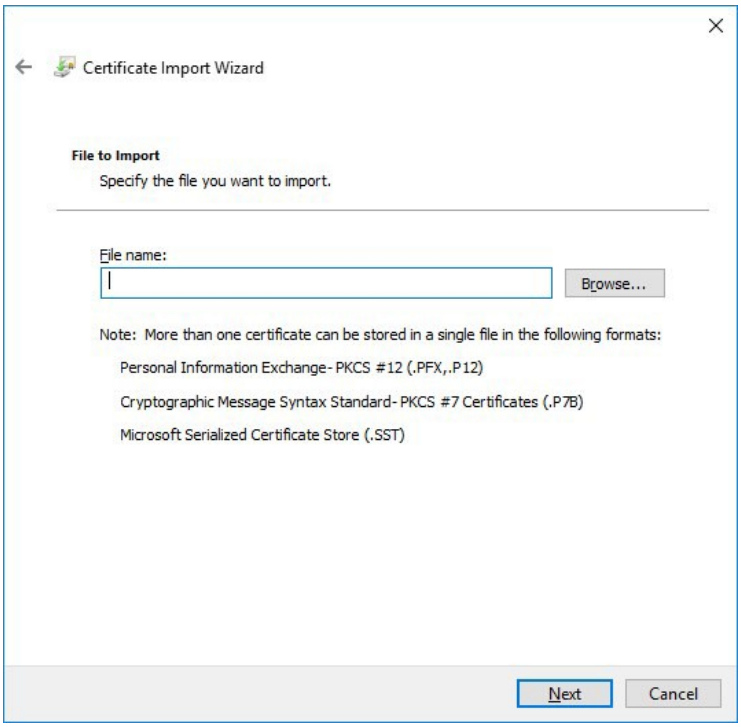


3. In the Certificates window select Trusted Root Certification Authority and **Import**.



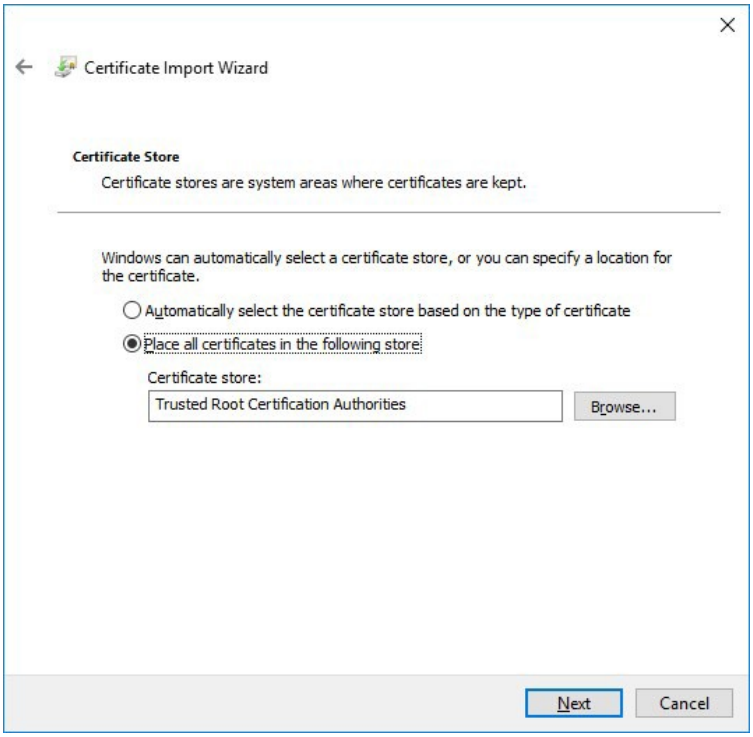


4. Specify the file to be imported. Browse it or simply pasted in the File name field. Click Next.

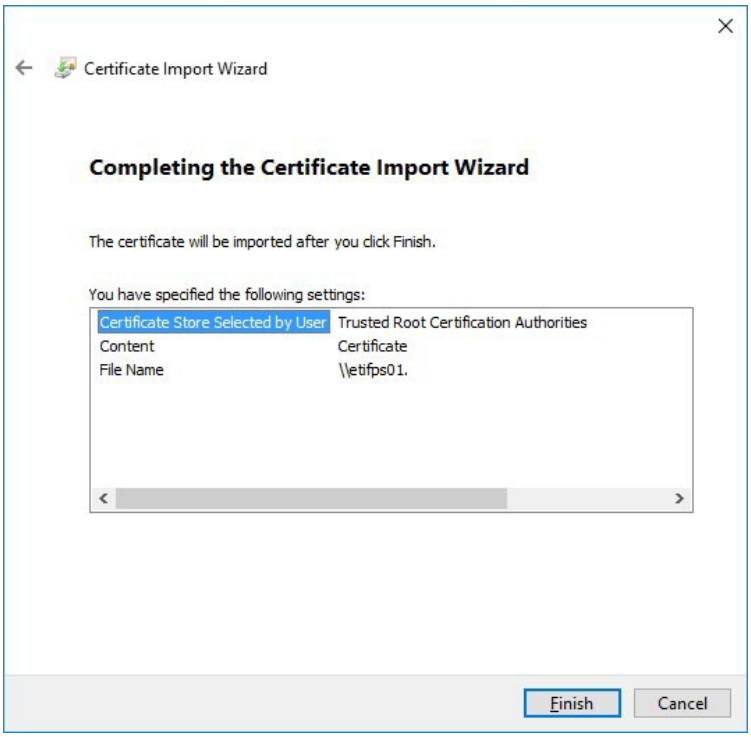


	The certificates and the key files provided by ETI- NET can be found in C:\Pro-gramData\ETINET\VTC\Cert.

5. Select a certificate store. Keep the default settings. Click Next.



6. To complete the importing process, click Finish. Verify if you selected the right path, certificate type, and content before exiting the Wizard.



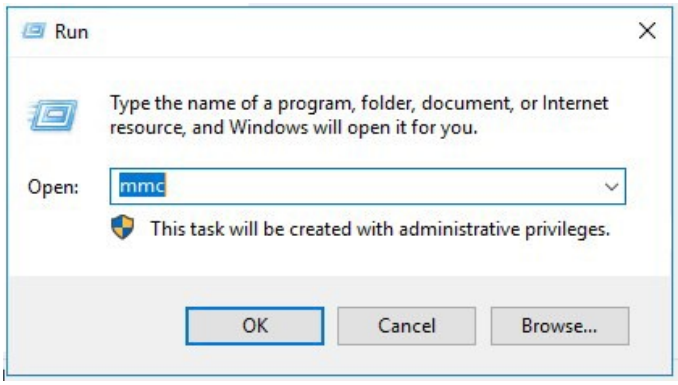
CERTIFICATE STORE

Customers using their own security certificates have to store these certificates in a special local folder after they have been issued by a certification authority. In order to copy certificate trust lists and certificate revocation lists they need to be saved in a certificate store, along with identity confirmation used to protect data and establish secure network connections.

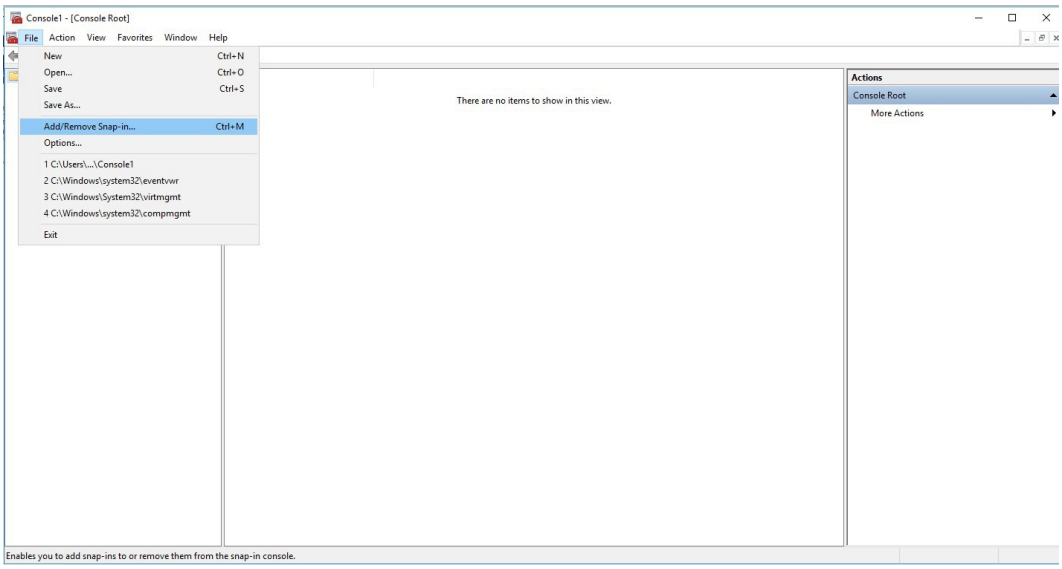
⚠	Self-signed certificates distributed with the BackBox application are for test purposes only. For details, see VTC Management Console section in the User Guide.

To import your own certificates use the Microsoft Management Console (mmc)

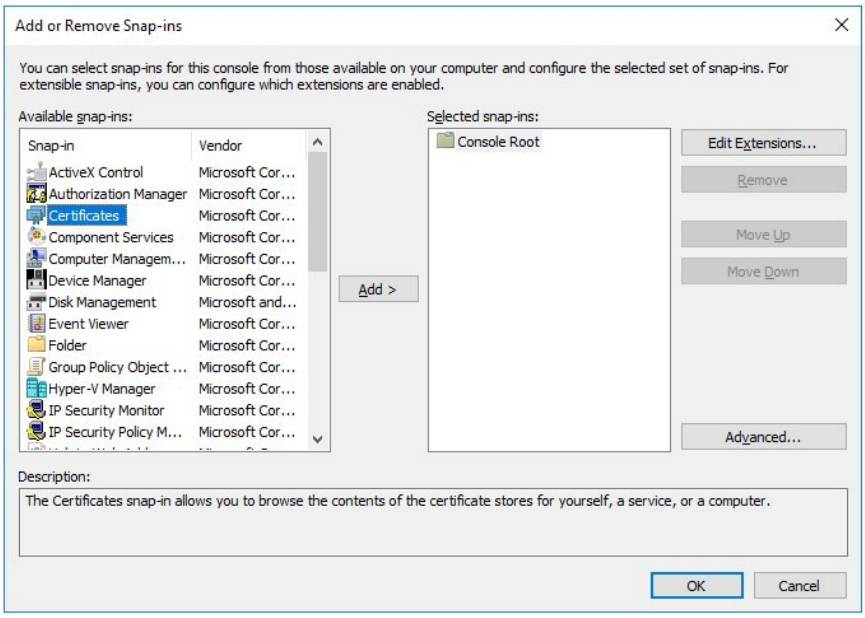
1. Right click on Windowsicon, click on Run item, input mmc in the Open field and click OK.



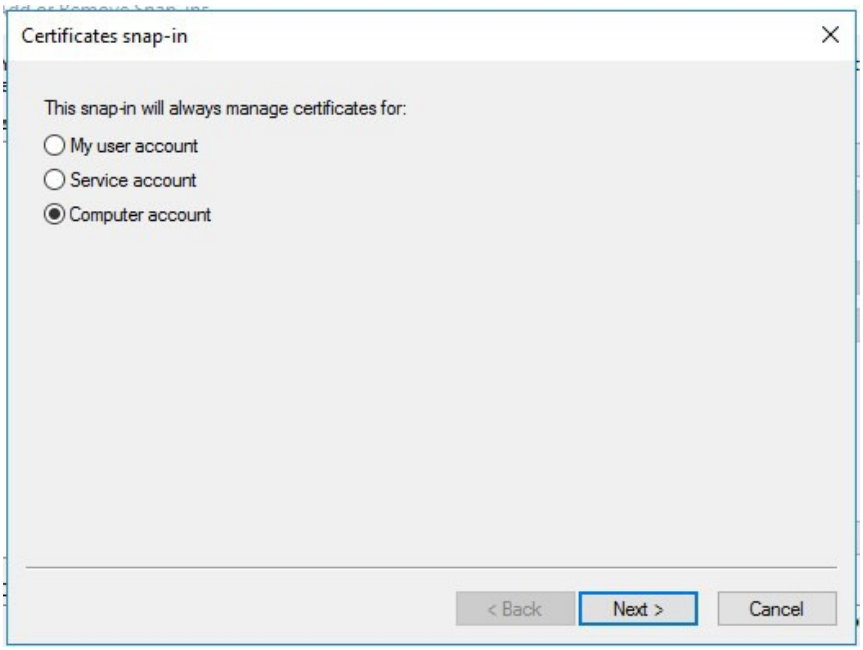
2. After the new Management Console pops up, click on File menu and click Add/Remove Snap-in item.



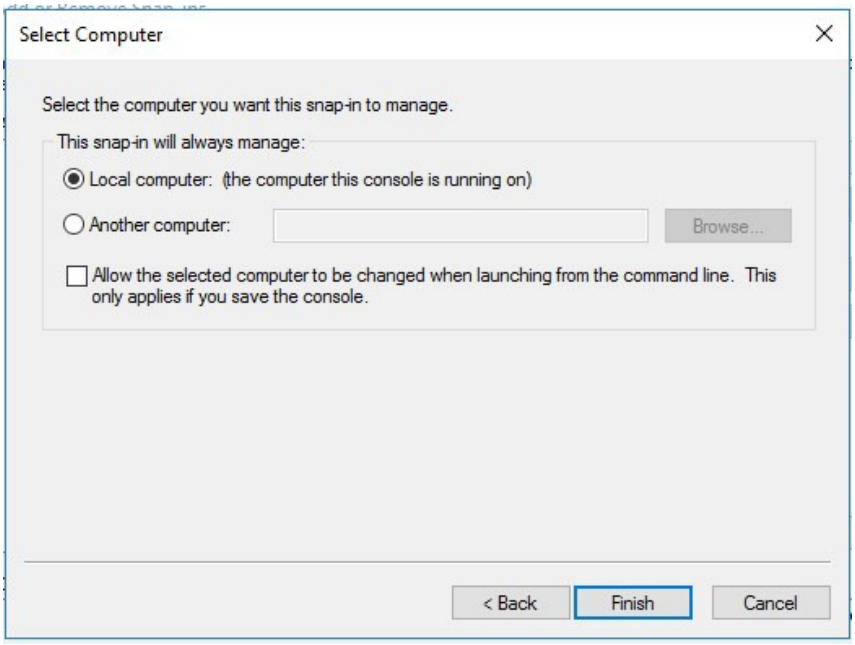
3. Choose **Certificates** item and click the **Add** button.



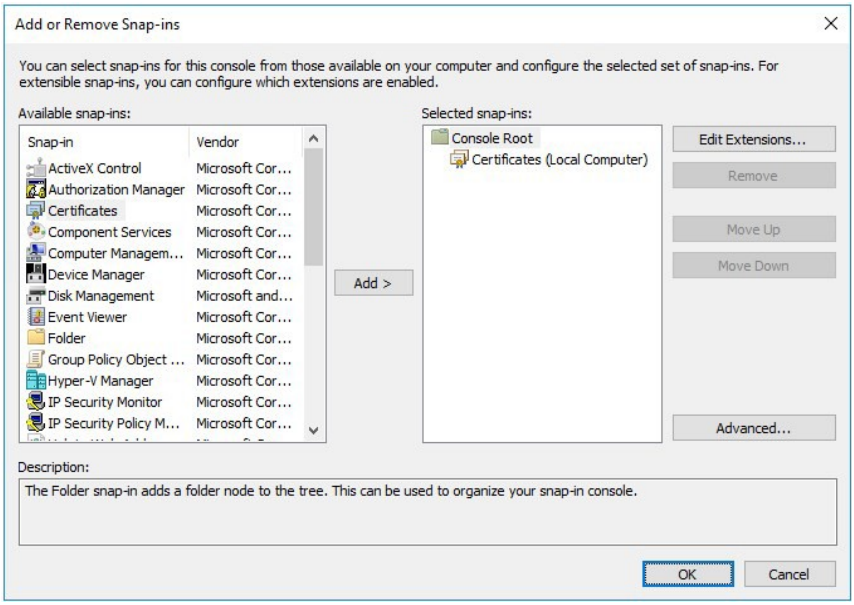
4. Choose **Computer account** and click **Next**.



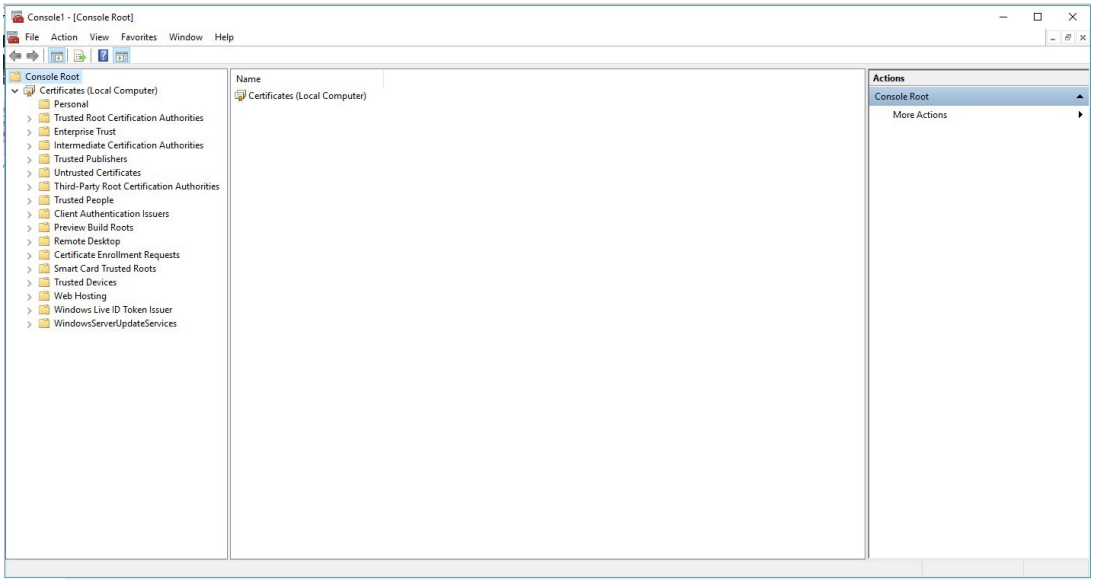
5. Keep **Local computer** radio box selected and click the **Finish** button.



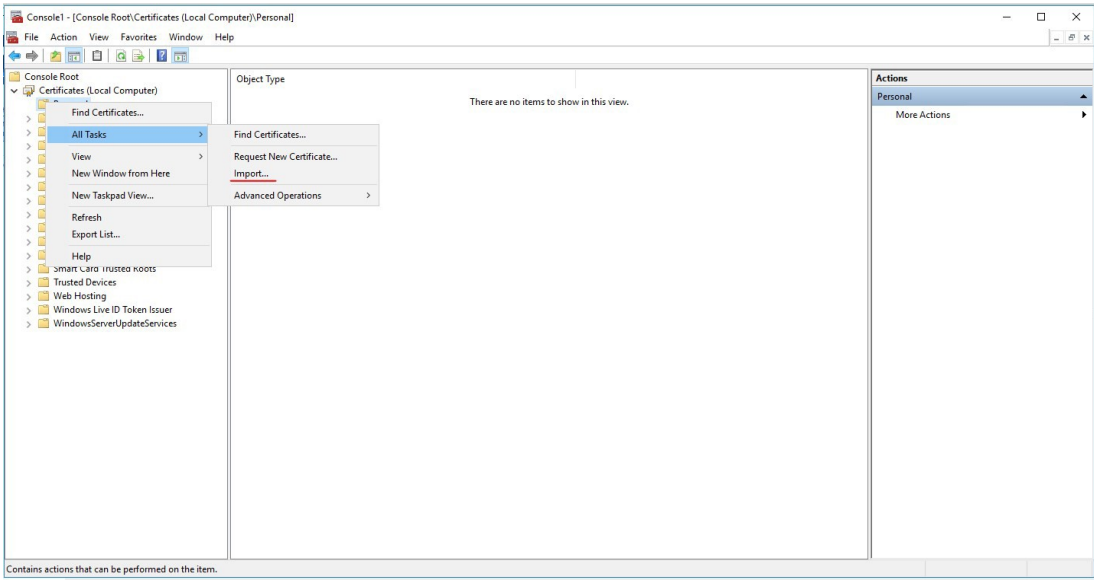
6. Click **OK** in the Add or Remove Snap-ins dialog.



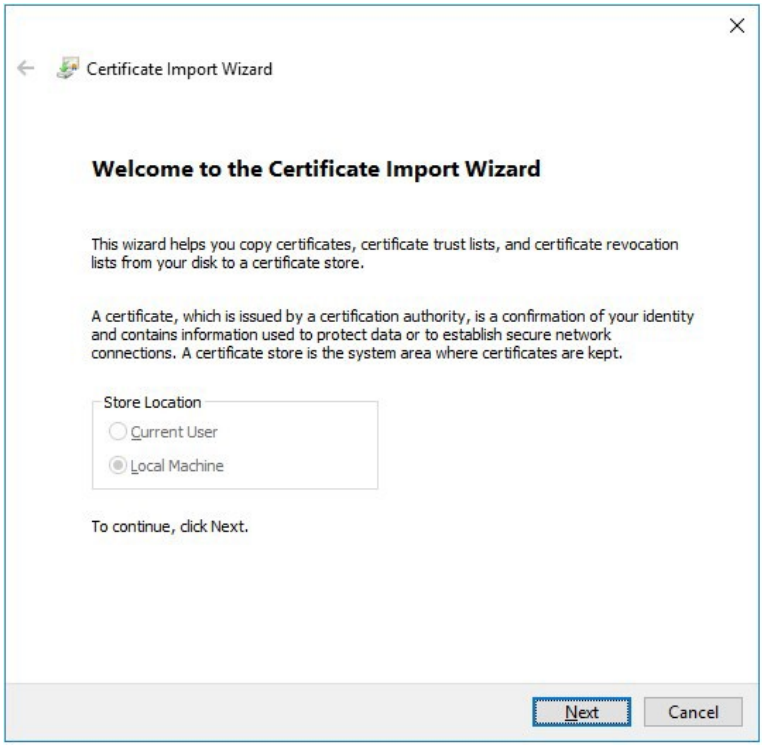
7. Expand **Certificates** (Local Computer) tree node.



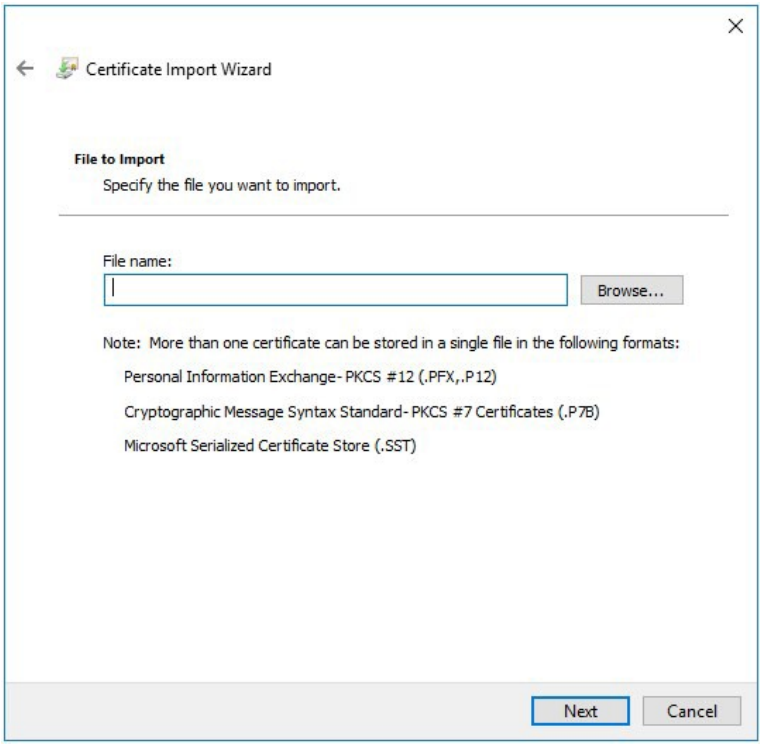
8. Right click on Personal item, chose All tasks and click Import item.



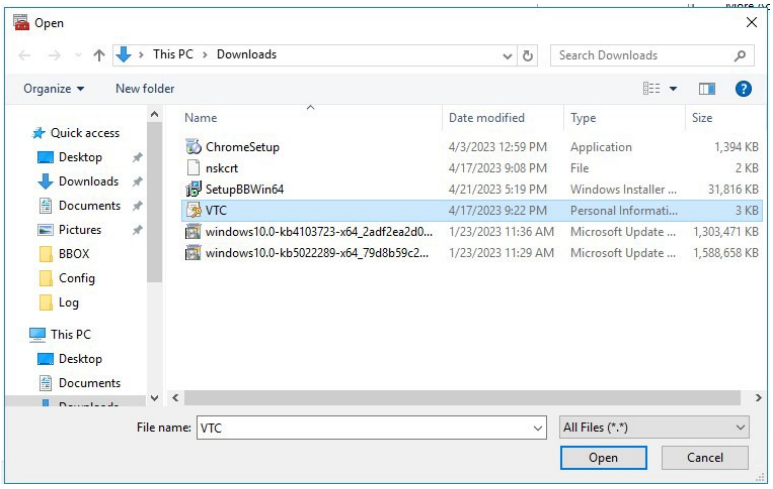
9. Click Next to start the import.



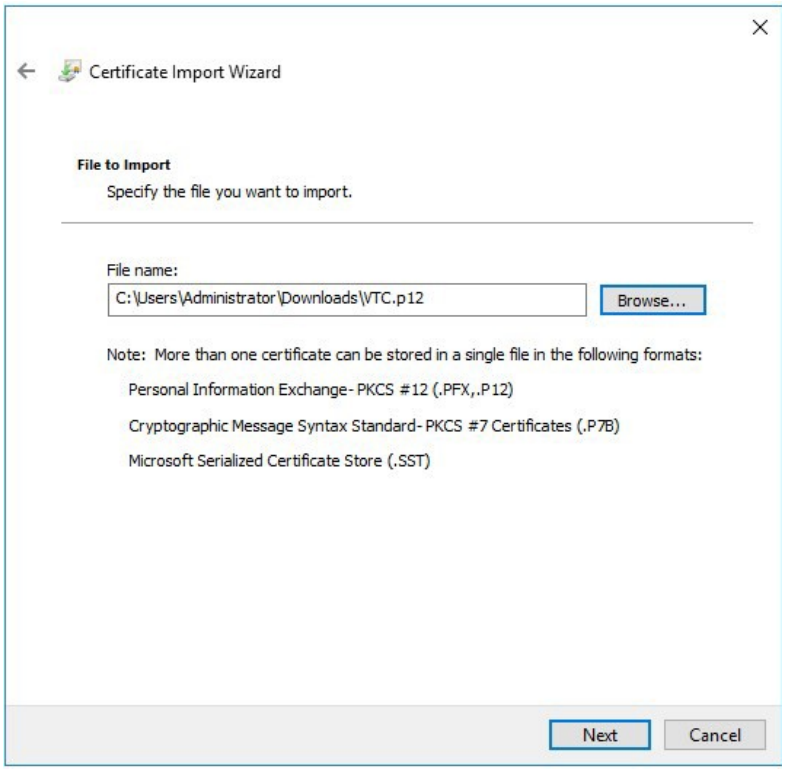
10. Click Browse to look for the file to import.



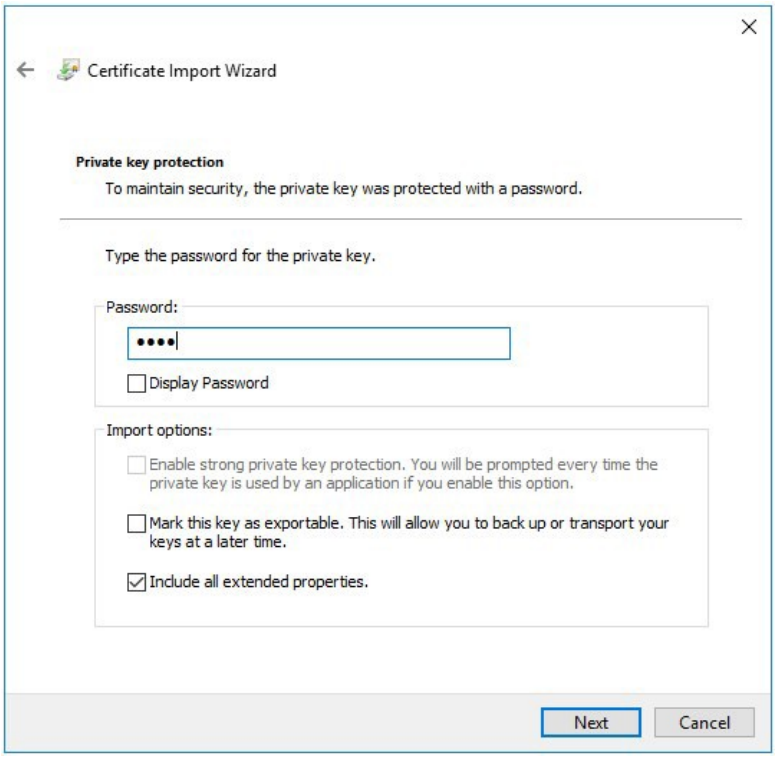
11. Select **All Files(*.*)** in file type drop down list, then select **VTC**.



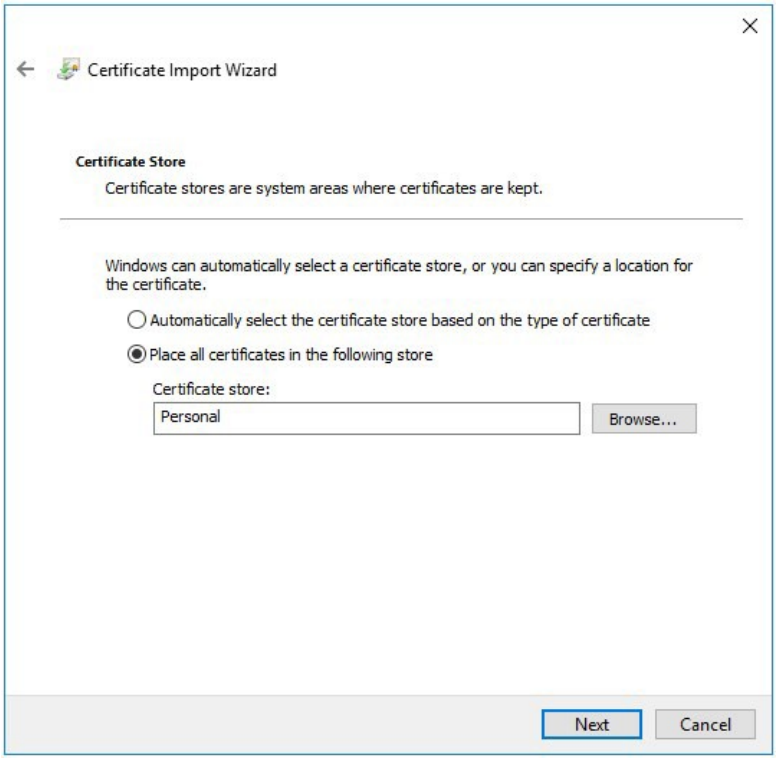
12. Click **Next**.



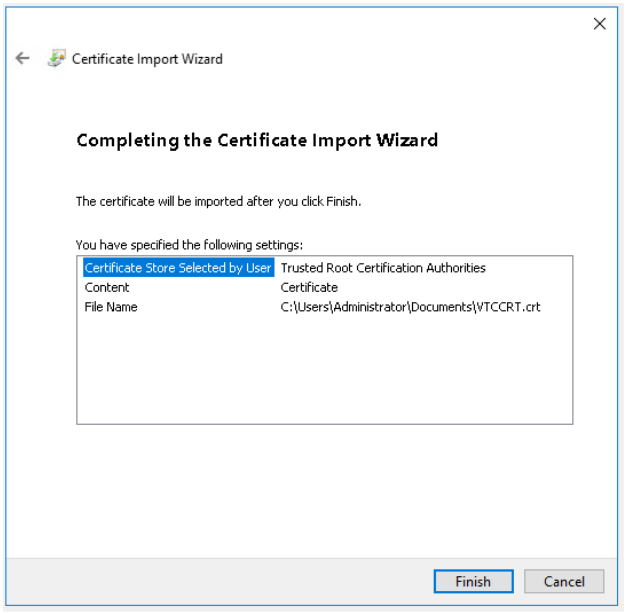
13. Input the password of private key and click **Next**.

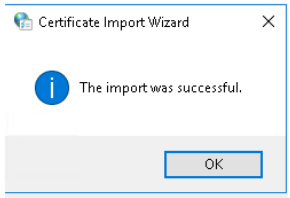


14. Choose Place all certificates in the following store and click Next.

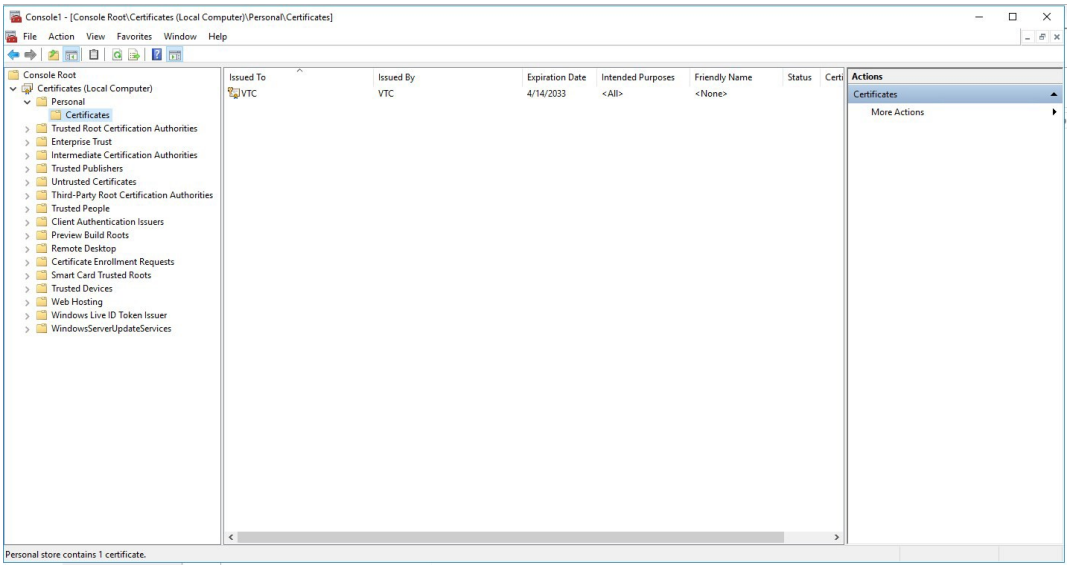


15. Once you complete the import, the Import wizard will prompt the The import was successful message.

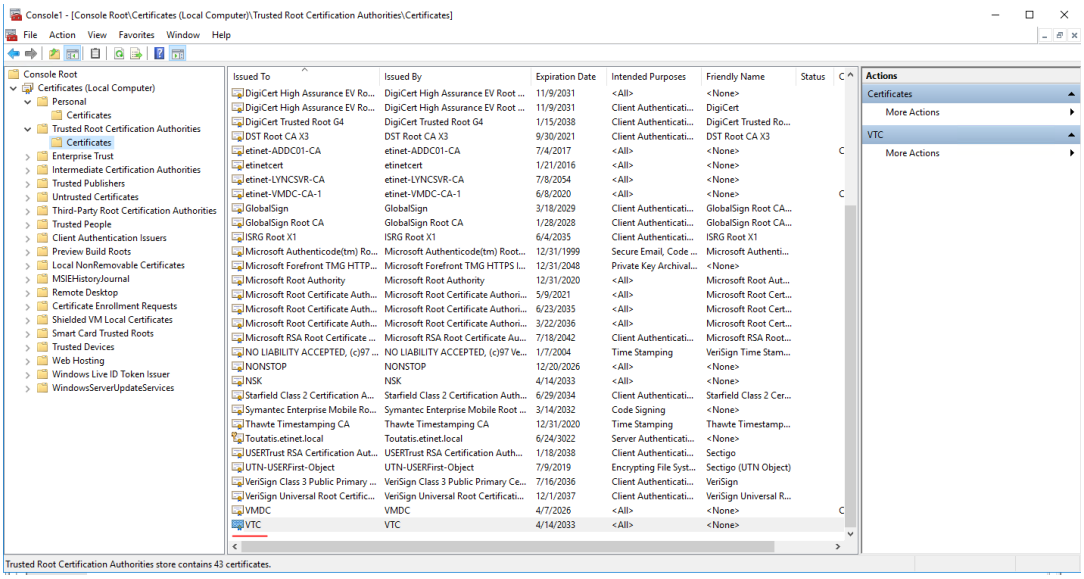




16. The VTC certificate can be located under **Certificates (Local Computer)** > **Personal** > **Certificates** folder.

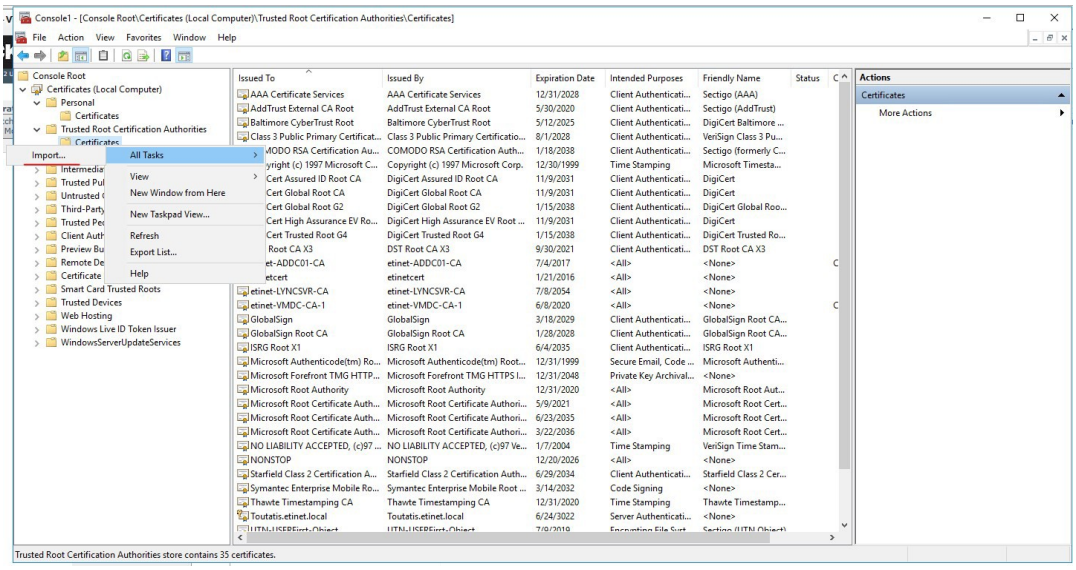


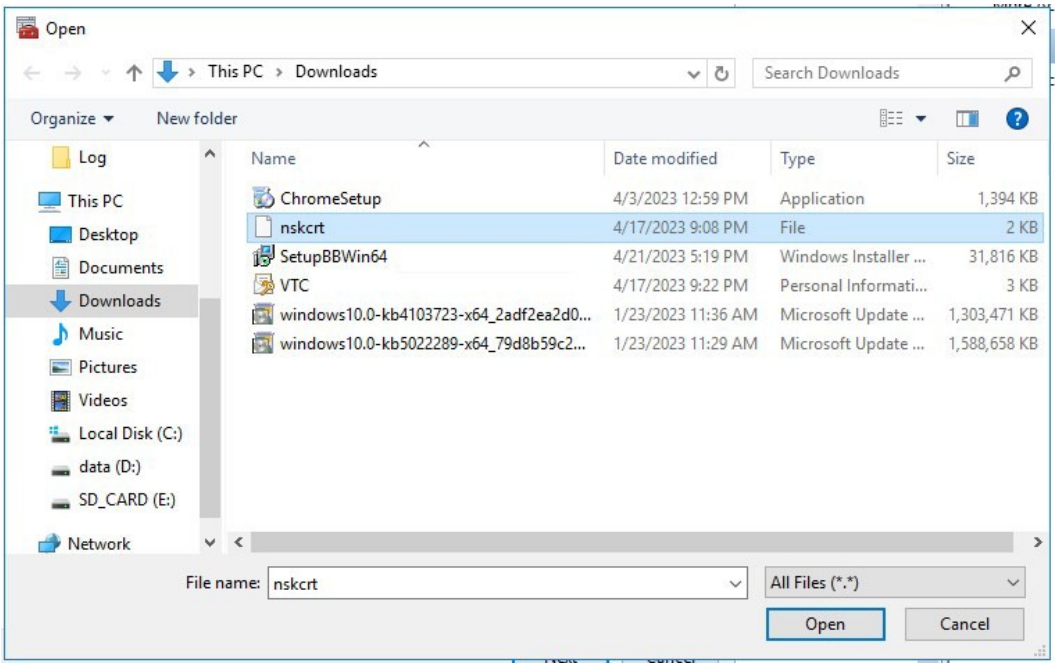
17. Repeat steps 8 to 16 to import VTC certificate to **Trusted Root Certification Authorities** > **Certificates** folder. Make sure **Stand Alone Load** works properly. Skip this step if the certificate is not self-signed.

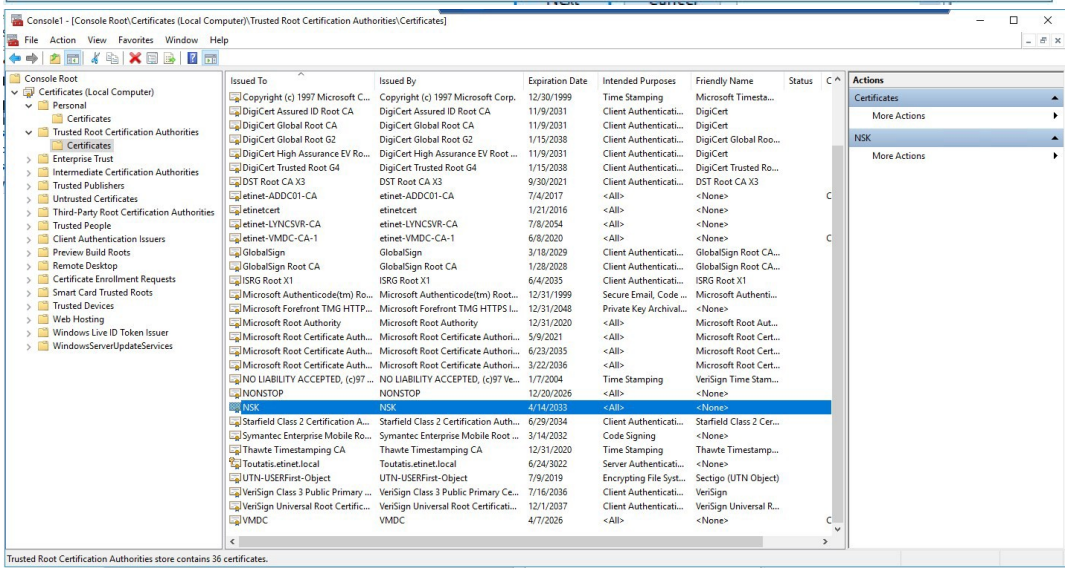


18. Repeat steps 8 to 16 to import NSK certificate to **Trusted Root Certification Authorities** > **Certificates**

folder. Select nskcrt in step 11. The NSK certificate can be found under Certificates (Local Computer) > **Trusted Root Certification** Authorities > Certificates folder.



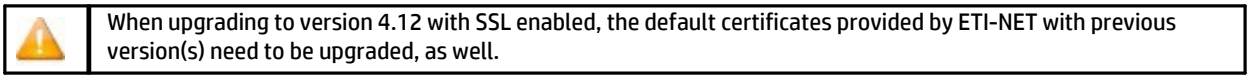




19. Certificate Information has been correctly added to the VTC MC and selected accordingly under **Settings** > **Security**.

CERTIFICATES UPGRADE ON NONSTOP

Certificates are part of the upgrade procedure, therefore they need to be up to date.



In order to have the certificates updated to be at the latest version, retrieve the new certificates from the BBE412 package using the following TACL command:

```
UNPAK BBE , ($*.*.NSKDER,$*.*.VTCCRT,$*.*.NSKCRT), VOL <DOMAIN SUBVOLUME>, LISTALL,
MYID,OPEN,AUDITED
```

EXAMPLE:

```
$DATA15 NGE412 18> UNPAK BPAKTMPH.BBE
$*.*.NSKDER,$*.*.VTCCRT,$*.*.NSKCRT),
VOL $DATA15.NGE412, LISTALL,MYID,OPEN,AUDITED
UNPAK - File decompression program - T1255H01 - (2024-02-15)
```

Archive version: 1

```
File Mode RESTORE Program - T9074H01 (19OCT2022) (AGX)
(C)Copyright 2015 Hewlett Packard Enterprise Development LP Drives: (\ETINIUM.$Y43P)
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.
Restore time: 6Nov2023 10:17 Backup time: 30Oct2023 11:13 Page: 1 Tape: 1 Code EOF Last
modif Owner RWEP Type Rec Bl
$DATA15.NGE412
NSKCRT 1316 17Apr2024 21:25 255,100 NCNC
NSKDER 1773 18Apr2024 13:05 255,100 NCNC
VTCCRT 1316 17Apr2024 21:24 255,100 NCNC

Summary Information

Files restored = 3 Files not restored = 0
$DATA15 NGE412 19>
```

APPENDIX A - GUARDIAN TOOL 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 BackBox Catalog Record

```
$DATA15 SHE409 11> run bb010 RT3* report
BB010 - Extraction of the BackBox 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 BackBox : 16
Number of volumes in DSM/TC of \INSIDX : 741 Number
of volumes in TMF of \INSIDX : 10 BB044-1 Labels in
BackBox domain RTE409 Labels Number of Label Media
Catalogue
from to volumes type type type Volume Group

VNCP01-VNCP08 8 BACKUP LTO3 BackBox VG_NC_SN VWCP01-
VWCP08 8 BACKUP LTO3 BackBox 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 BackBox domain RTE409 and in catalogs seen from
\INSIDX
Labels Number of Label BackBox TMF node, or
from to volumes type Volume group Catalog DSM/TC pool,volcat

BBA000-BBA739 740 BACKUP (unknown in BackBox) BBOXPOOL, INSIDCAT DAVE -DAVE
1 BACKUP (unknown in BackBox) DAVE, DAVETEST
INSID0-INSID9 10 TMF (unknown in BackBox) 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 BackBox 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 BackBox 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
BackBox 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 BackBox 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 BackBox 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 BackBox 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


$DATA15 QCE409 22> run obb038 *
BB010 - Extraction of the BackBox 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 OBB038
```

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 =BackBox_BBSETUP
ADD DEFINE =BackBox_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) successful. 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 NGH412 11> o obb017A
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 * PARAM VOLUME-SYNC-ONLY  1 (TO BYPASS CLEANING volumes in DataStore)
COMMENT *    DEFAULT 0
COMMENT ************************************************************************

LOAD /KEEP 1/ $DATA15.NGH412.BBSETUP  $DATA15.NGH412.MACROS

Loaded from $DATA15.NGH412.BBSETUP:

BBSV_ADDR       BBSV_PORT       BBSV_TCPIP      VTC_OBJECT      EZX_MAXRETRY
EZX_RETRYDELAY  EZX_TIMEOUT

Loaded from $DATA15.NGH412.MACROS:

BB_BBOX_PGM_VERSION           BB_041_TIMEOUT
BB_041_DEVICE                 BB_041_LABELS
BB_041_PROCESS                BB_VALID_HHMMSS
BB_QUALIFY_SUBVOL             BB_GET_EXISTING_FILE
BB_CHECK_EXIST_FILE           BB_FILENAME_SYNTAX
BB_VALID_TIMESTAMP            BB_TCPIP
BB_GET_TMP_FILE               IS_NUMERIC
LOG_TEXT                      BB_GET_DEFAULT_VOL
BB_GET_IN_SUBVOL              BB000_COLLECT
BB001_TIME_EDIT               BB002_VERSION
BB003_UPGRADE                 BB003_GET_OPTION
BB003_VALID_TARGET            BB003_VALID_BKUP
BB003_UPGRADE_EXEC            BB017_FREE_EXPIRED
BB018_DEFAULTS                BB030_EXTRACT_STATS
BB020_RESERVE                 BB022_CHECK_SPACE
BB004_DATASTORE_UPDATEPW      BB004_DATASTORE_VALIDATE_ACC
BB005_DATASTORE_MIGRATION     BB023_DEL_BACKEDUP
BB024_LIB_SYNC                BB026_EXPORT_CATALOG
BB027_IMPORT_CATALOG          BB036_BACKUP_STORE
BB038_FREE_LIB_MEDIA          BB040_VIRTUALIZE_PREP
BB041_VIRTUALIZE_START        BB042_VIRTUALIZE
LISTT                         VIEWT
TMFC2                         BB054_SHUTDOWN

CLEAR ALL
PARAM   BB017IGNORECHECKHDR1      0
PARAM    VOLUME-SYNC-ONLY         0

BB017_FREE_EXPIRED

NGH412XX-BB017    Free BackBox expired storage      2023-11-07 13:15
```

```
$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 catalog
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
following 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

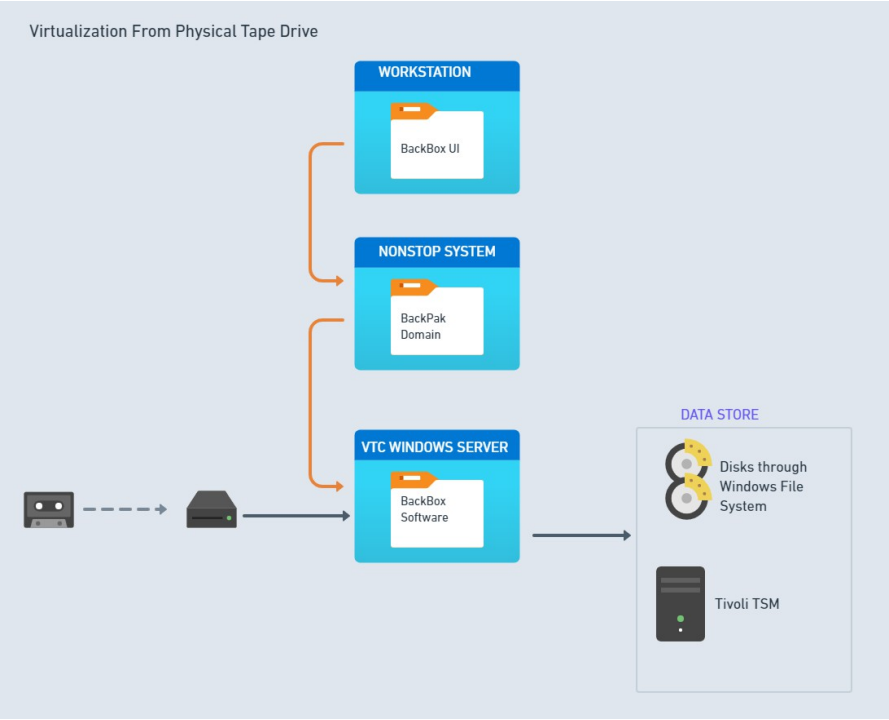
⚠	This section does NOT apply to the Virtualized BackBox

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 a 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 BackBox 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



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.

VTC Configuration

⚠	NonStop devices attached to the VTC should be stopped before the service is restarted.

CONFIGURATION IN THE BACKBOX DOMAIN

For physical devices , two items must be configured in the Domain configuration through the BackBox UI:

- In VT Controller Advanced Properties, the physical 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 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 BackBox 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 BackBox, 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 catalogs. 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 uncataloged 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 BackBox'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, BackBox tries to process it even if the volume is unknown in BackBox.
If the requested volume belongs to one of the tape catalogs associated with BackBox Volume Groups configured for "Migration to BackBox" IN-PROGRESS:

- The volume will be automatically registered in BackBox.
- 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 BackBox 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 BackBox and processed by BackBox.
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 BackBox domain all volumes that are currently SCRATCH.

On the BackBox 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 BackBox 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 BackBox 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

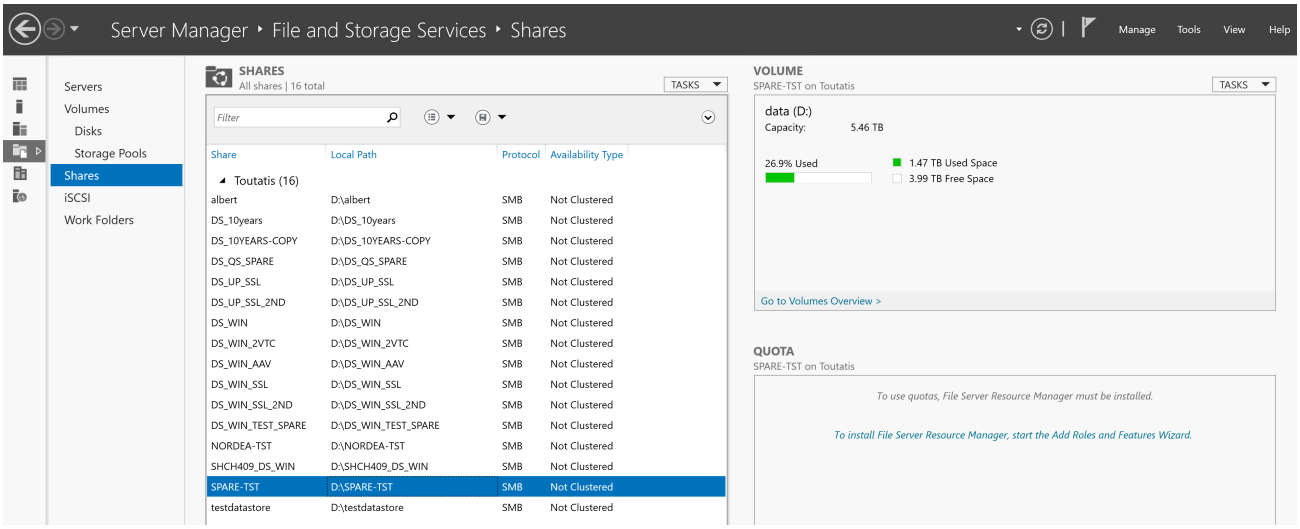
- Register the latest legacy volumes that have expired in the BackBox domain.
  On BackBox UI > Volume > choose Import from Tape Catalog > select the Volume group and ask for registering only SCRATCH Volumes
- Verify all the legacy volumes are now in the BackBox system.

Volume summary page can be compared to the number reported by DSM/TC: MEDIACOM INFO TAPEVOLUME *, POOL xyz

- Update the BackBox configuration to disable the Auto-import in all Volume groups.

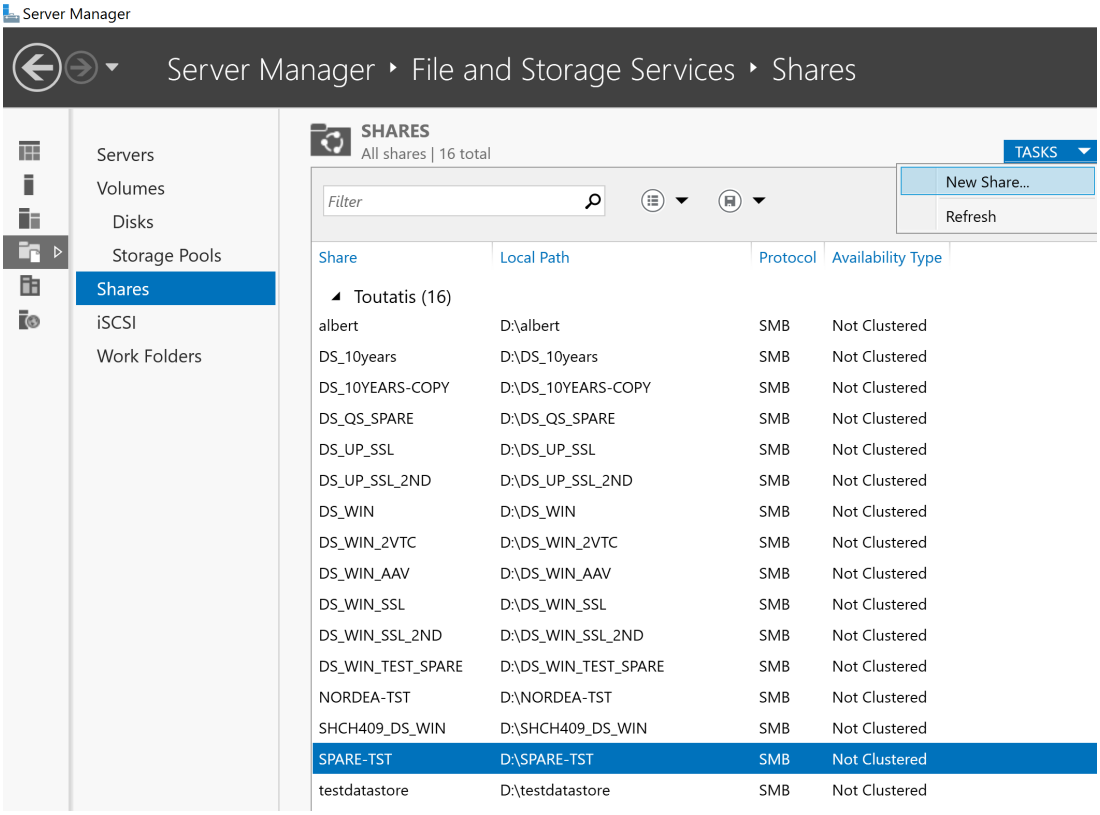
APPENDIX D - SHARED FILES PERMISSIONS

To set the permissions go to Server Manager > File and Storage Services > Shares and select the store you want to change the permissions for.

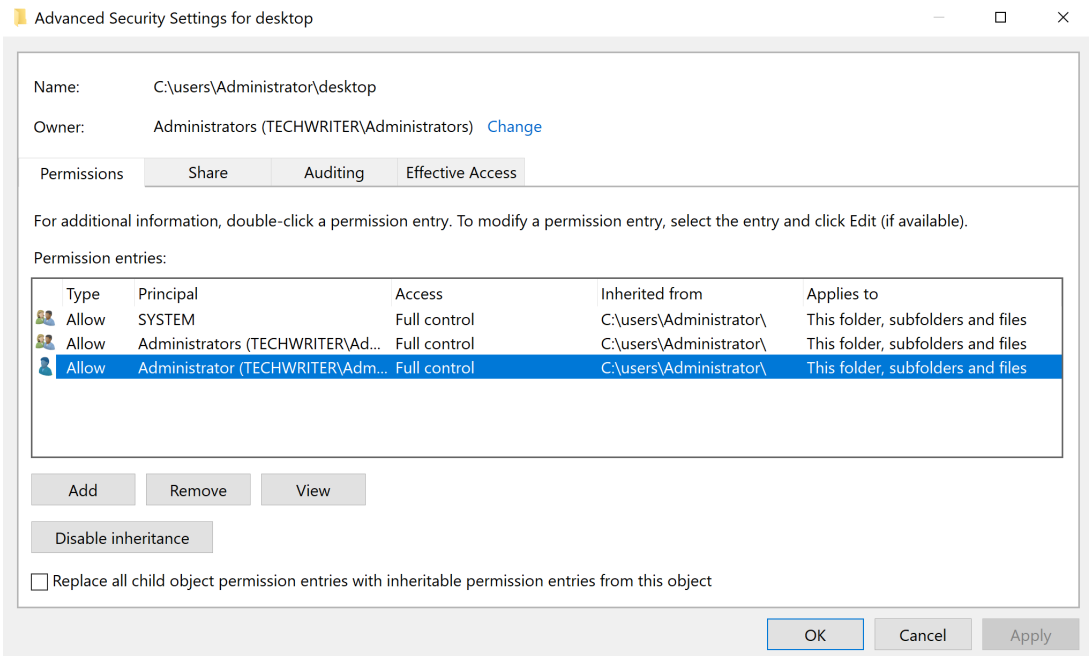


Right-click on the selected store and **Properties**.

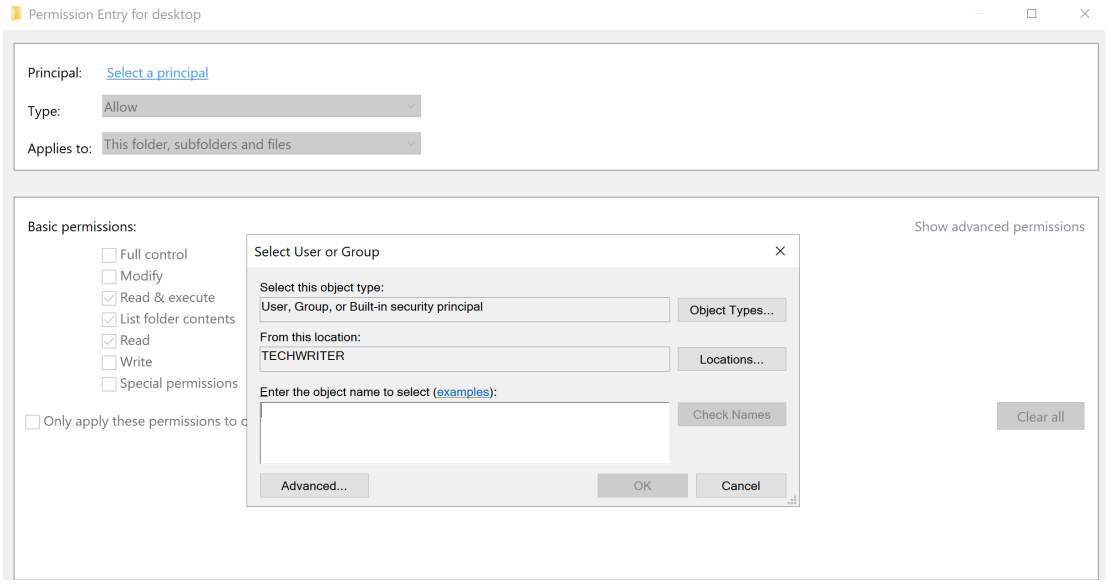
If the specified location does not exist and you want to create it, go to TASKS tab and select New Share. Follow the wizard's steps to create a new share.



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 levels can be configured 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.

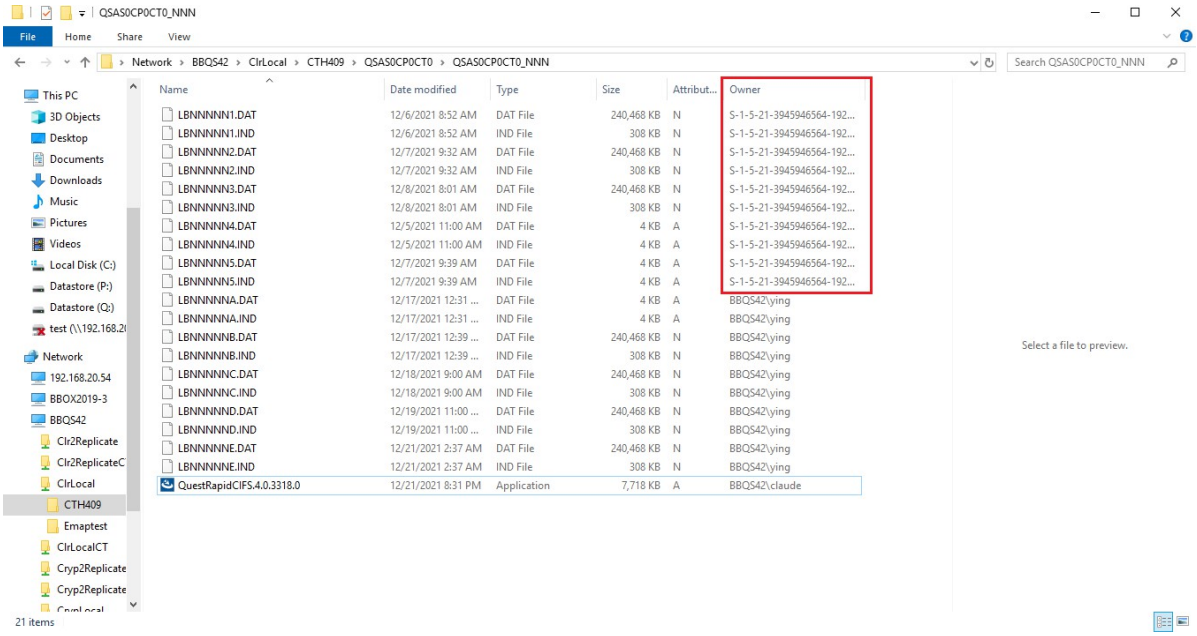
Set up the interface on the eth2 connection; specify the ip address, netmask and gateway. To add the network interface use the commands below:

```
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.



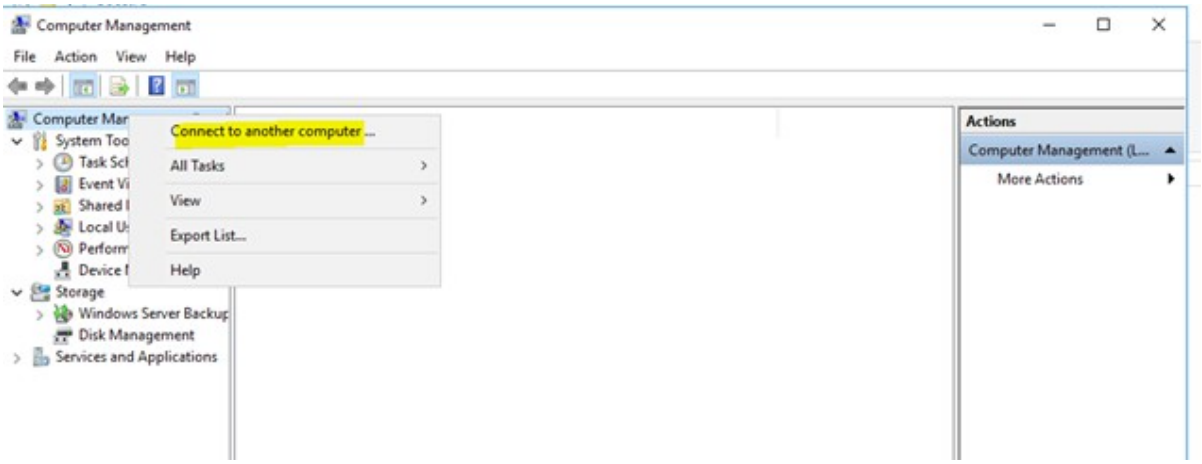
In order to avoid being locked out of the accounts, users need to log into VTC server with Domain Administration accounts (accounts in Domain Admin group).

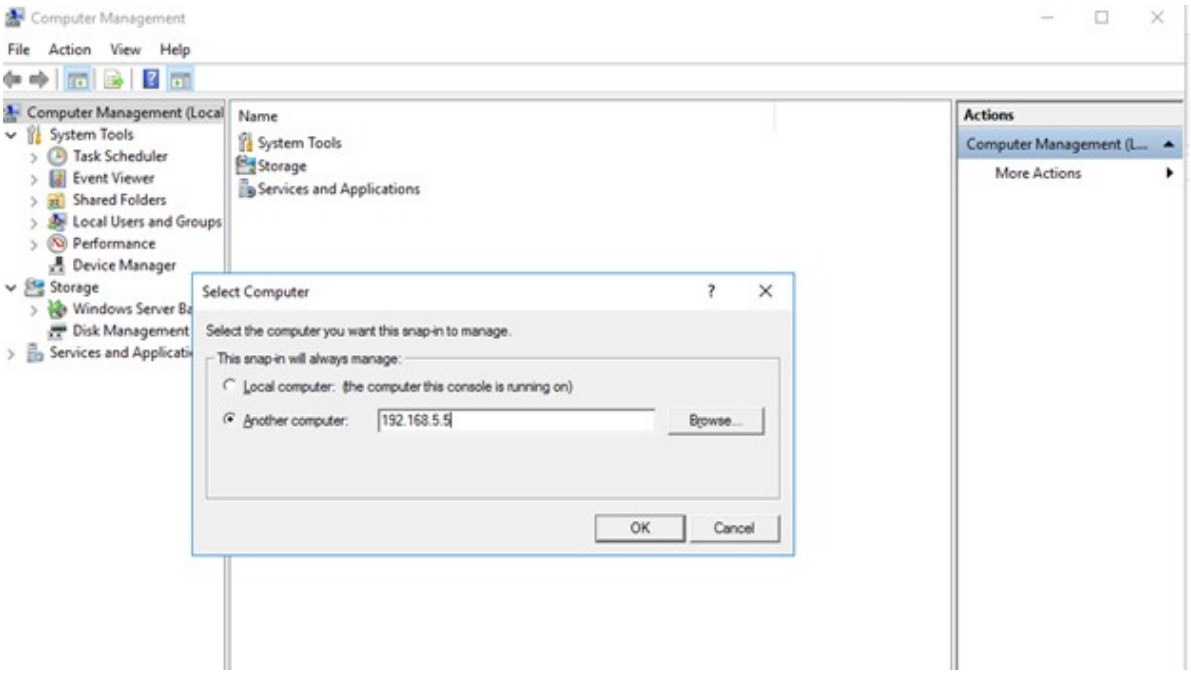
Once logged into the domain with Administration account, users can change the ownership of the files and folders into valid accounts.

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.

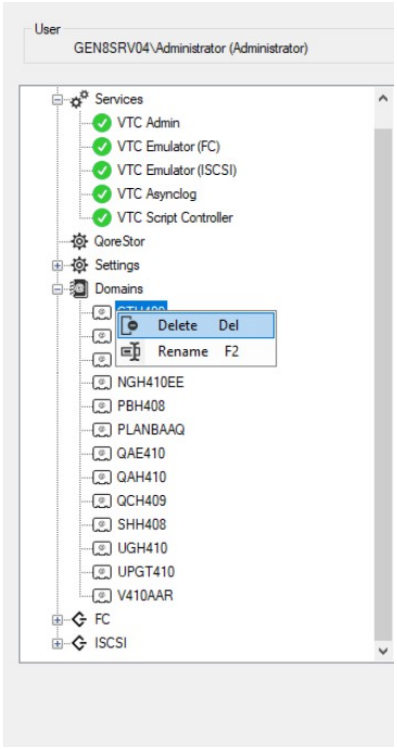
APPENDIX G - REMOVING NONSTOP NODES

Use this procedure to decommission NonStop systemsand 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.



APPENDIX H - BARE-METAL BACKUP AND RESTORE

Prepare BackBox Domain System

BackBox H4.11 AAV or newer version:

- Bare-Metal Backup procedure (that creates System Image Tape-SIT) requires manual load done by the Domain Manager.
- Bare-Metal Restore procedure doesn't need access to any BackBox domain.

Use an existing domain or create a new one, dedicated to system recovery. No extra license is required. On the selected domain:

1. On the dedicated domain (if any) define the VTC with iSCSI or FC Tape Drives.
2. Define a Data Store used to store the System Image Tape (SIT).
3. Define a volume group to create virtual drives with a maximum volume size, big enough to sup- port the System Image Tape (SIT).
4. Create some virtual media in that volume group.

⚠	Virtual Media needs to be in a volume group under a Data Store type Windows or QoreStor.

Encryption		Supported with Bare-Metal Backup & Restore	Storage Type
Tape Encryption	VLE/ESKM, KMIP or Com-forte SecureTape	✗	
Encryption at Rest	DataDomain , StoreOnce , QoreStor	✓	Windows (DAS and SAN) bitlocker

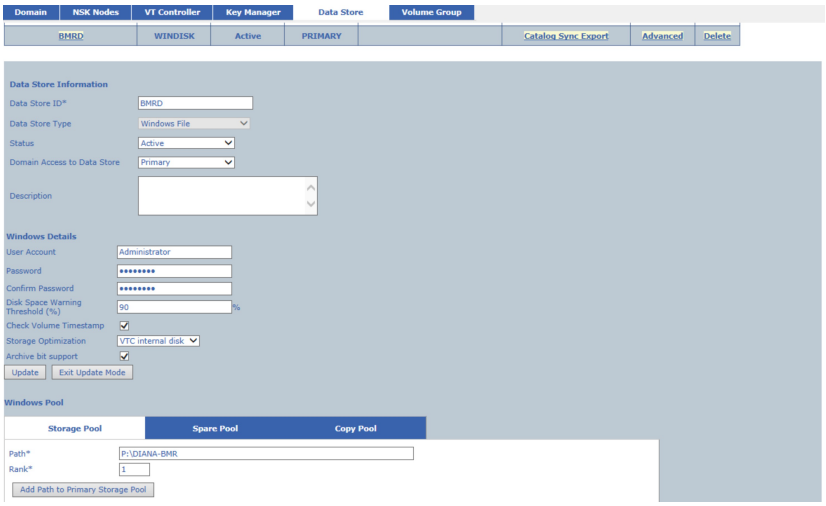
Media Creation

Create Volumes with No Label. Created Media must be UNLABELED type and with a max volume size big enough to contain $system disk image.

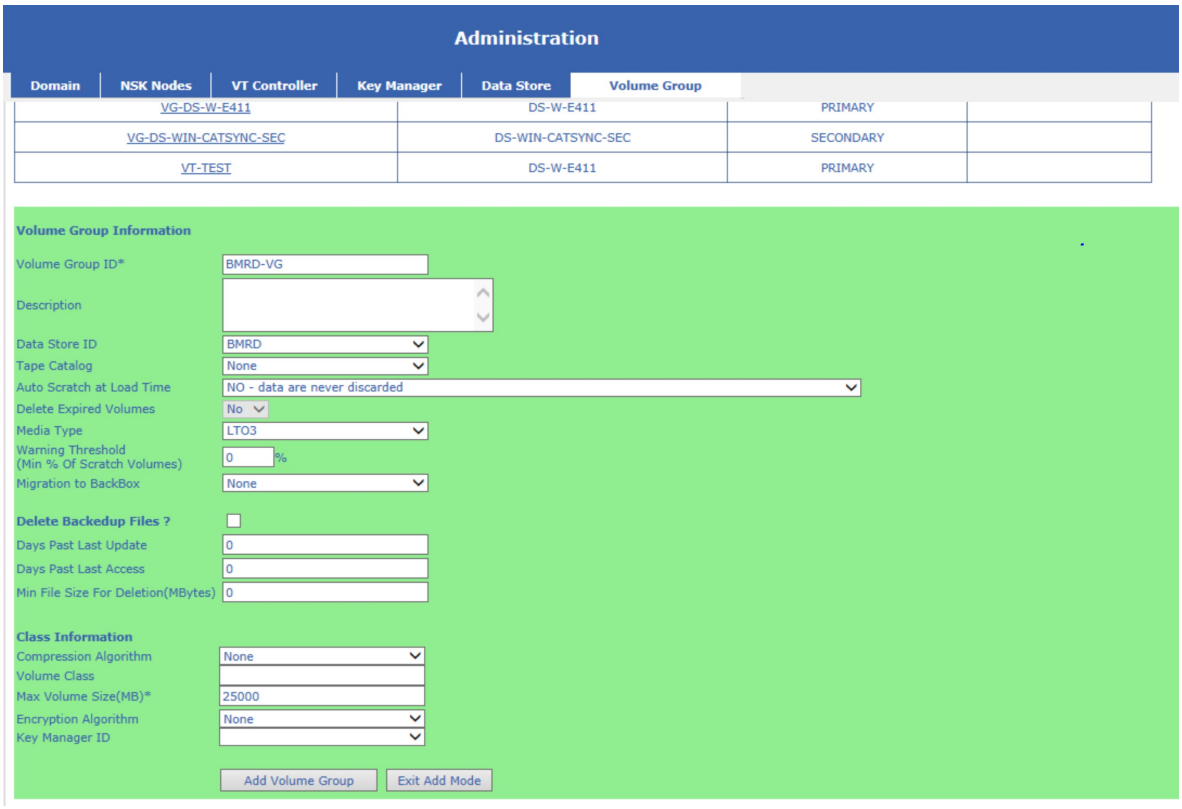
⚠	Best Practice: always use a dedicated Data Store with a dedicated Storage path in order to avoid mixing up unlabeled volumes with standard volumes. This practice will also simplify the retrieving volume process when restore is needed.

To crate unlabeled media:

1. On the BackBox UI configure Data Store by creating Windows type Data Store.

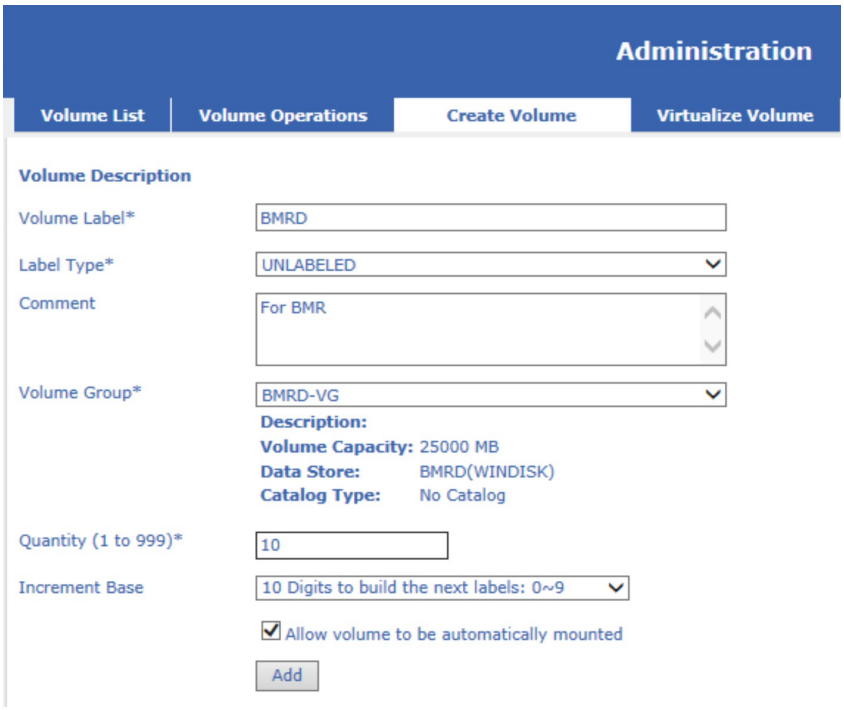


2. Create a Volume Group.

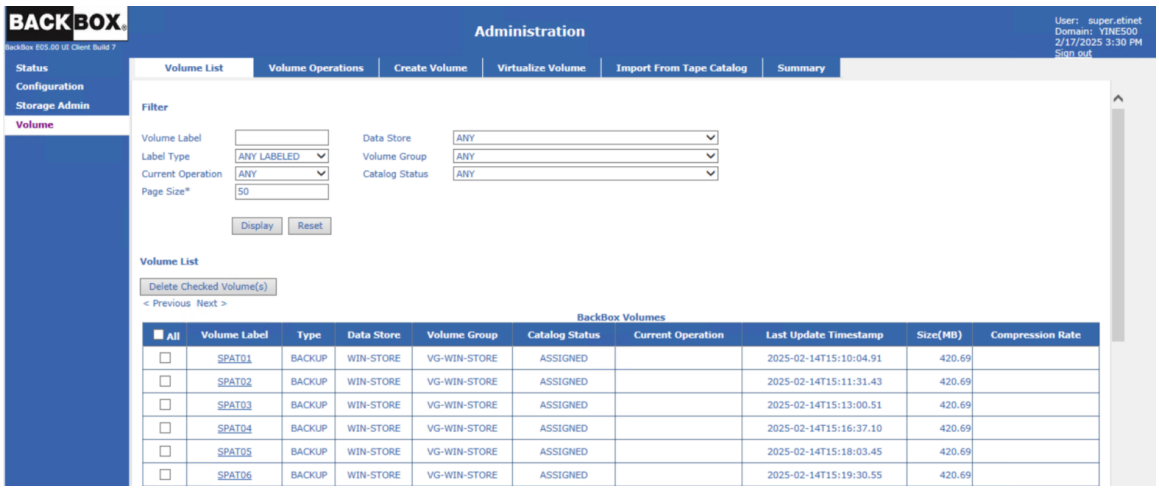


3. Go to the Volume page and create UNLABELED volumes in the Volume Group.

⚠	Always add a comment, such as For BRM, in the Comment filed to set apart empty volumes from actual System Image Tape (SIT) backup.

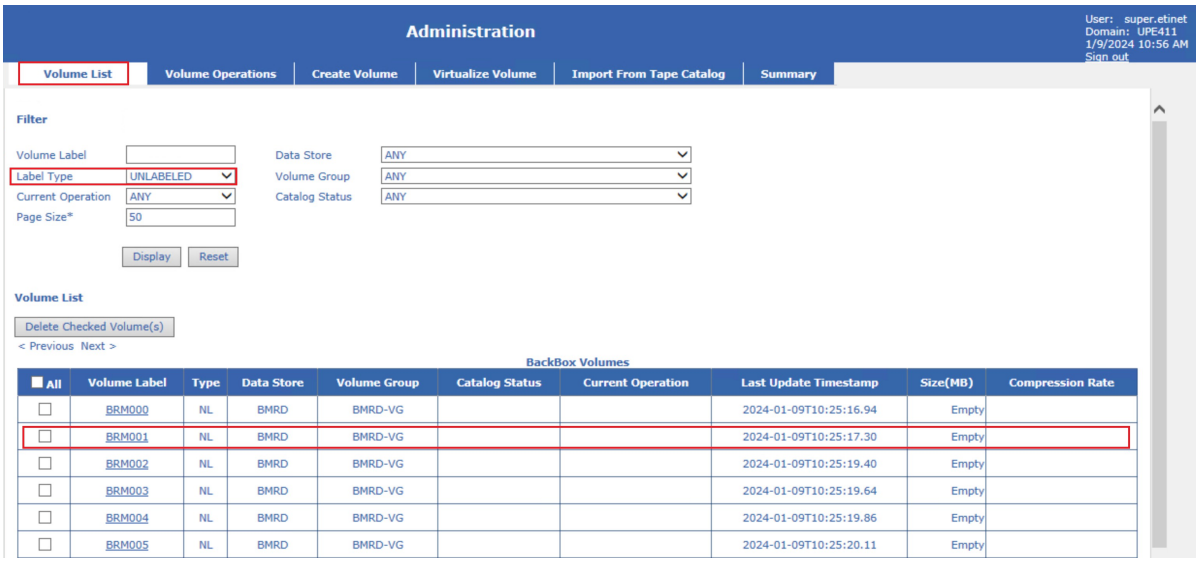


4. In the Volume List select label type UNLABELED to see the created volumes.

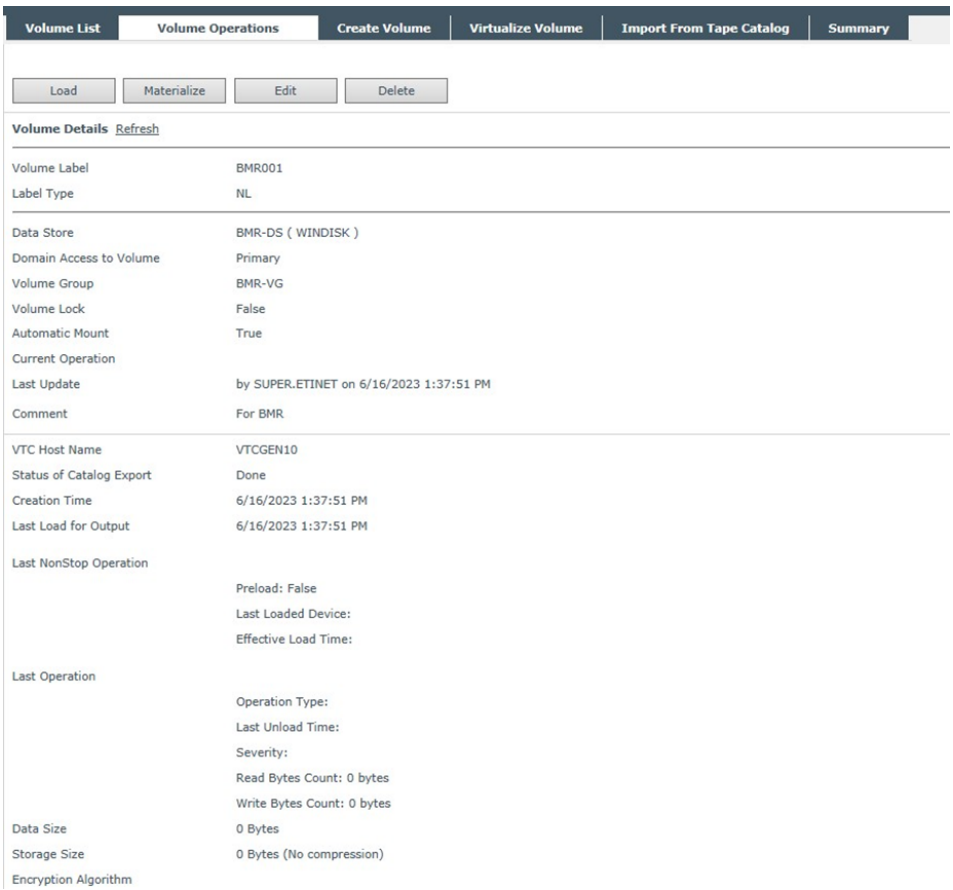


Bare-Metal Backup

1. To load an unlabeled tape volume for System Image Tape (SIT) creation go to **Volume**>Volume List and select Label Type UNLABELED to display unlabeled volumes (or filter your volume by DataStore or Volume Group).
2. Check and click on the Volume Label name.

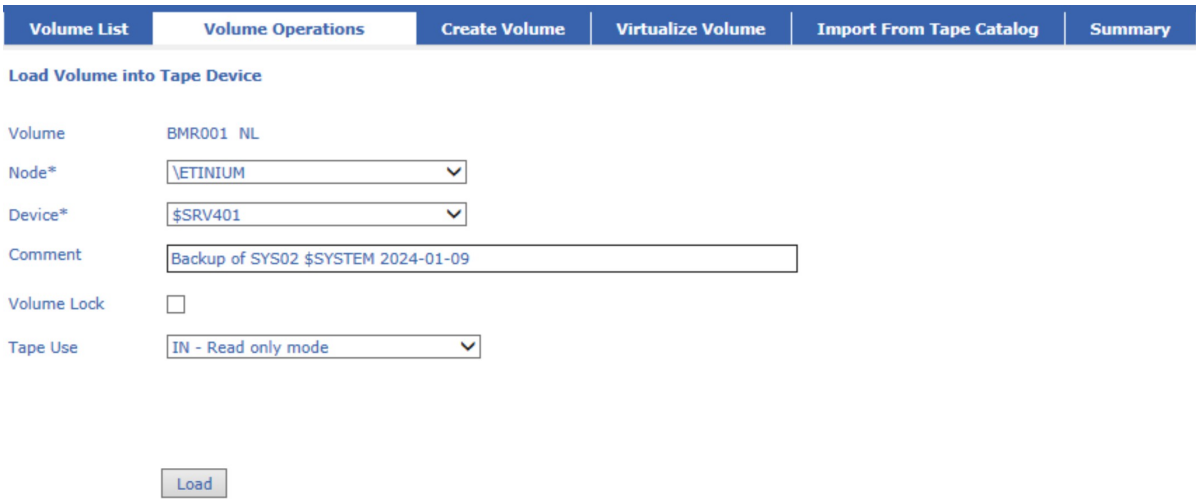


3. Display selected volume details and click the Load button.



4. Select the system (Node*) and the Device* you want to load the selected media to. Select Tape Use as OUT – Read/Write mode and click Load.

⚠	Always add a comment, such as Backup of SYS02 $SYSTEM 2024-01-09, in the Comment field to ease retrieving the System Image Tape (SIT) backup at restore time.



The media is now ready to be used by the Bare Metal Backup.

Bare-Metal Restore

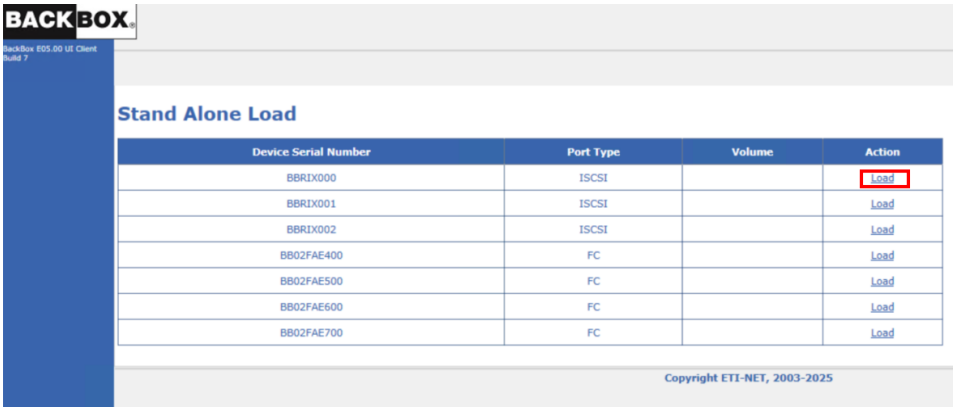
For NonStop System recovery, use Stand Alone Load to mount the media, as the BackBox domain and the NonStop node will be down.

⚠	Make sure the SSL is properly set (if enabled) and the CA Trusted Root Certificate is correctly installed. Otherwise, you might get an exception error at load.

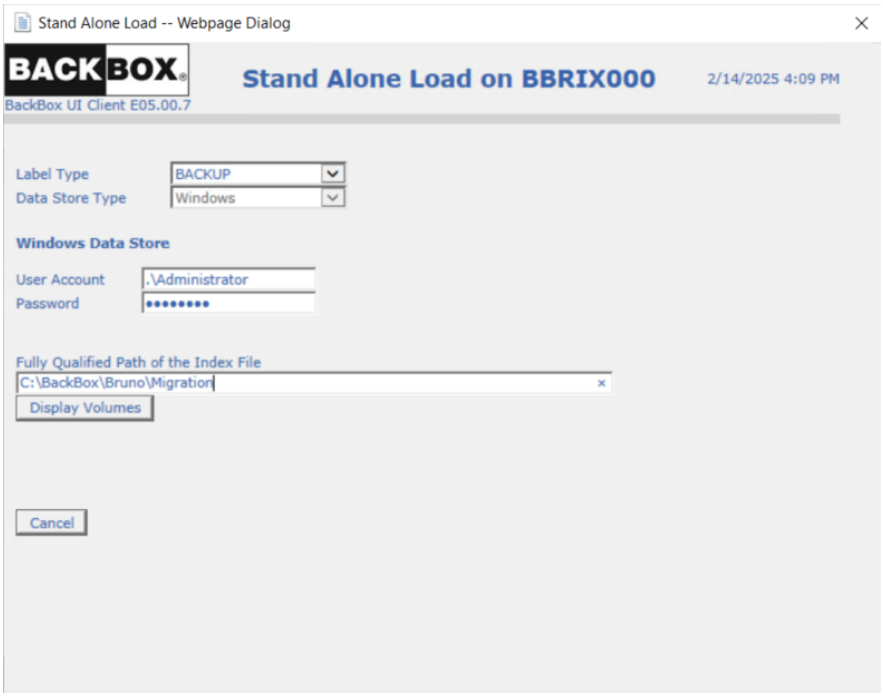
To run the Bare-Metal restore:

1. Go to Stand Alone Load tab. The page allows stand alone volume loads. The table displayed on the page shows all connected devices listed by serial number.
2. Load or unload a volume by following the instructions below:

To load:



a. Choose the device from the table and click on the Load button associated with the device to be loaded. In the pop-up window select the appropriate value for each field:



Label Type: Volume label type (values are ANSI, Backup, TMF, IBM or UNLABEL).

Data Storage Type: Windows Data Store is the default value and cannot be changed. TSM volumes are not available at this time.

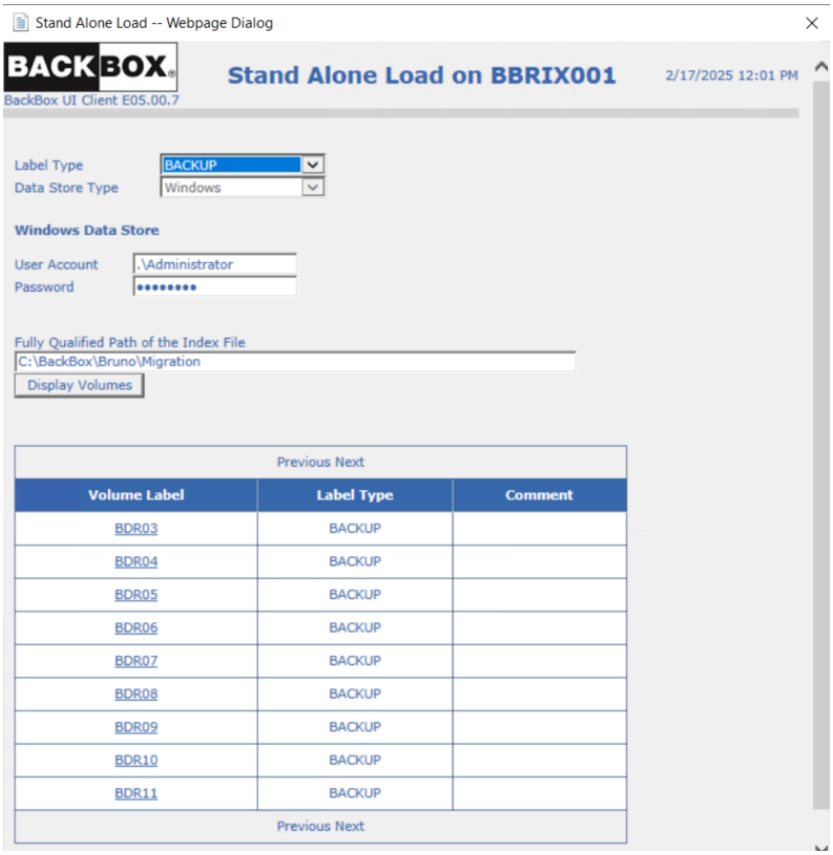
Input the user account details for the selected Data Store: User Account and Password (credentials used to access the Windows disk pool). Use the assigned credentials for the Data Store to avoid getting access errors.

Specify the Fully Qualified Path of the Index File: name of the path containing the virtual media index file (*.IND file).

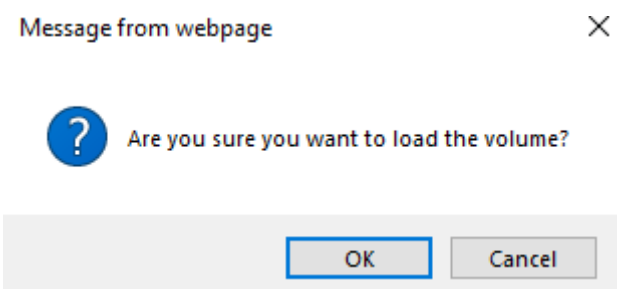
⚠	If the path is not correct, an error message will be generated to let you know that the system cannot find the path specified.

b. Click the **Display Volumes** button to open up the table with all volumes associated with the specified index file.

Based on their label, all volumes are listed in the table, along with all comments, if any.



C. Click on any displayed volume to load it. In the confirmation pop-up window click OK to load the volume or Cancel to cancel the load.



The tape is ready to be used for a Bare-Metal Restore.

APPENDIX I - VTC SCRIPTING OPTIONS

Scripts in VTC

Scripts are available for the Data Store type WINDISK for which the VTC Tape Emulator stores two MS- Windows disk files per virtual volume:

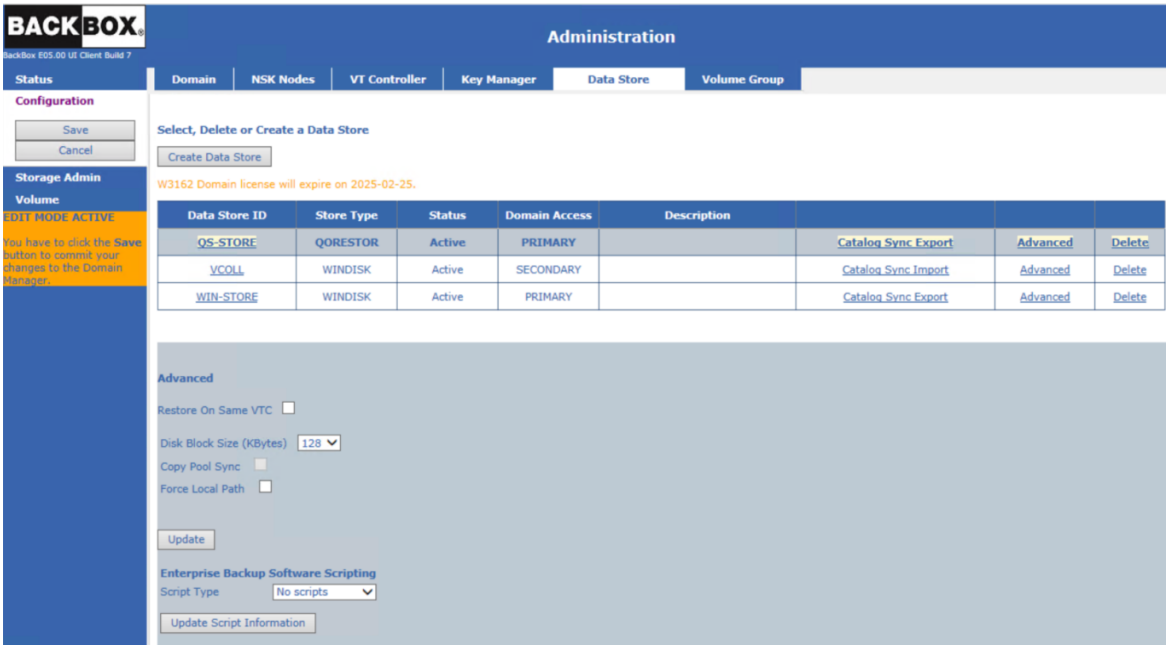
- index file containing metadata (file name *.IND).
- data file, size based on the current content of the volume (file name *.DAT). Scripts send virtual volumes to a back-end Enterprise backup infrastructure in order to:

- Retain additional copies of virtual volumes for safety.
- Free-up the online storage, moving the virtual volumes to a cheaper storage for long term archiving

Scripts move back and forth between the above-mentioned two files, from the MS-Windows file system to the back-end storage by any means implemented by MS-Windows command scripts.

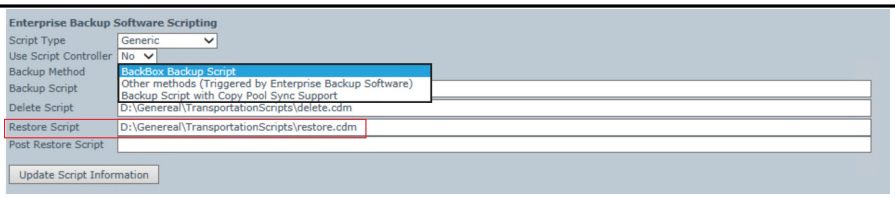
A script could move disk files to a remote NAS server by a simple Windows command copy source-file, target-file, but in most production environments, the MS-Windows files are saved by the Windows command line client of an Enterprise backup infrastructure.
Scripts are configured in the BackBox UI in the Data Store Advanced Configuration. Depending on the type of the script, you can choose no scripts or up to four scripts, with optional user parameters. The available options for scripting are:

- No script
- Generic
- TSM
- Manual Restore



When selecting Generic scripting type, you will have the choice to select the script you want to execute for a specific event.

For Generic script type with backup method Triggered by Enterprise Backup Software all the scripts are provided by the customer as path to the script location, depending on the script type (backup, delete and/or restore).



Scripting Type	Event Type
Backup script	Executed to copy the two disk files of a virtual volume to a back-end Backup infrastructure. If the Copy Pool Sync option is enabled, this script is not available.
Restore script	Executed to restore the disk files of a virtual volume
Delete script	Executed to delete the copies of a virtual volume in the back-end Backup infrastructure
Post-Restore script	This script is obsolete, but still available for compatibility. It is replaced by the macro BB023_DEL_BACKEDUP and the Volume group configuration of Delete Backed-up Files.

If the TSM scripting type is selected, the options are: BackBox Backup Script or Other Methods (Triggered by Enterprise Backup software).

If BackBox Backup Script is selected, the available options are Archive with the delete files option, which allows a selection between two TSM scripts: Archive and immediate delete or Archive with reset of the Archive Bit (if this option is selected for the current data store).

	If the Copy Pool Sync option is enabled, selection of the Backup Method is not possible.

Last scripting type available - Manual Restore - does not allow configuration of any script.

	If an Enterprise Backup infrastructure has no available command line to write a restore script, a pseudo restore script is required to coordinate the operations, to reply to a mount request.

Script Execution Case Scenarios

Event	Action	VTC Script Execution
A NonStop backup completes	The volume in two Windows disk files must be backed-up.	Backup script. Triggered at volume unload. Unavailable if Copy Pool Sync option is enabled.

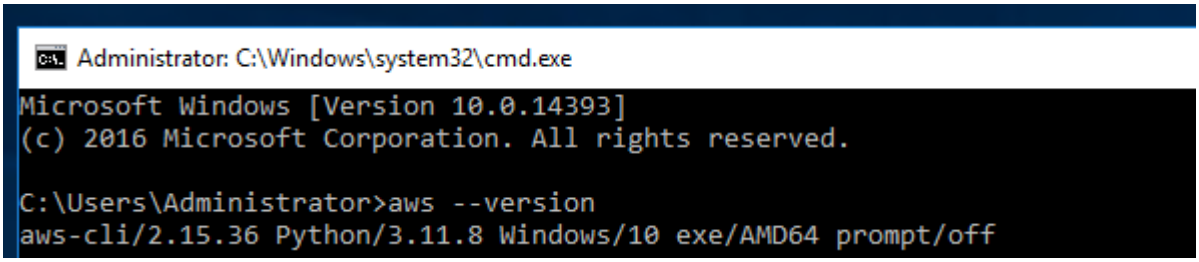
In the BackBox UI: - Storage Admin page, (backup all non-backed-up files), - or Volume page for a single volume (Run script).	The volume in two Windows disk files must be backed-up. (if a previous backup failed)	 Backup script. Unavailable if Copy Pool Sync option is enabled
The daily batch OBB017 executes the macro BB023_ DEL_BACKEDUP.	Delete backed-up disk files after the time configured in the Volume group.	Usually no script. Restore script only for StoreOnce.
The volume mount is requested for a NonStop restore, and the two Windows files are not found.	Restore the Windows disk files.	Restore script.
The daily batch OBB017 executes the macro BB017_ FREE_EXPIRED.	Delete the backups of the disk files for the volumes that became SCRATCH in DSM/TC or TMF.	Delete script. The VTC runs the Delete script after deleting the disk files.
In the BackBox GUI: delete a virtual volume.	Delete the backups of the disk files.	Delete script. The VTC runs the Delete script after deleting the disk files.
A NonStop backup completes.	Synchronization of the Storage pool with a copy pool.	A command is generated to the CopySync program to carry out the syncing of a volume.
In the BackBox GUI: - Storage Admin page, (Copied all non-copied files), - or Volume page for a single volume (Copy to Copy pool).	Synchronization of a volume or multiple volume is not done.	A command is generated to the CopySync program to carry out the syncing of a volume.

 If an Enterprise Backup infrastructure has no available command line to write a restore script, a pseudo restore script is required to coordinate the operations, to reply to a mount request.

Offline CopySync with S3 Cloud as Target

This case scenario allows creating a secure offline copysync file on the cloud (S3). Proceed with the script preparation and execution by following the steps.

1. Install aws client (AWSCLIV2.msi).
2. Run command aws–version to confirm the installation.

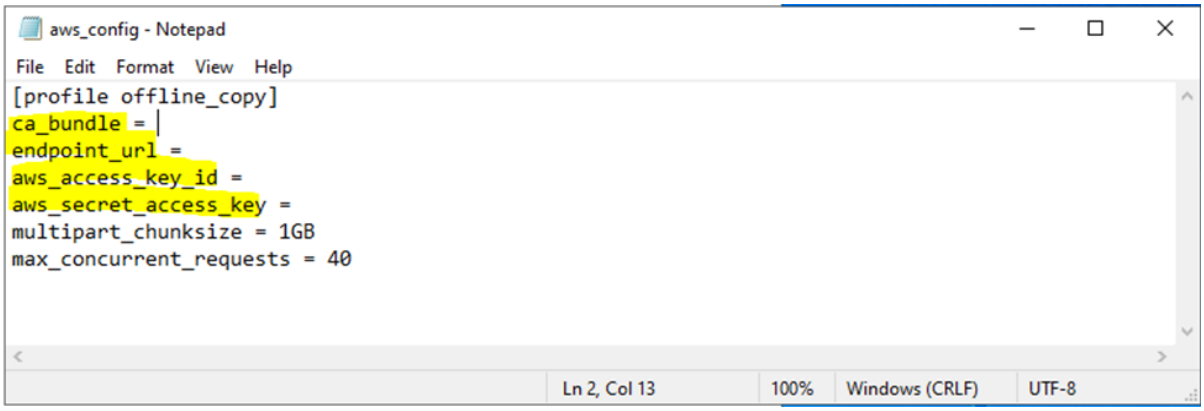


3. Copy from ProgramData\ETINET\VTC\Samples\Script\OfflineCopy thefiles CopySyncWithS3OfflineCopy.cmd and aws_config to the location the Windows user account (defined for BackBox DataStore) has access to. For example, C:\ScriptS3

or any other folder created for the S3 script purpose.

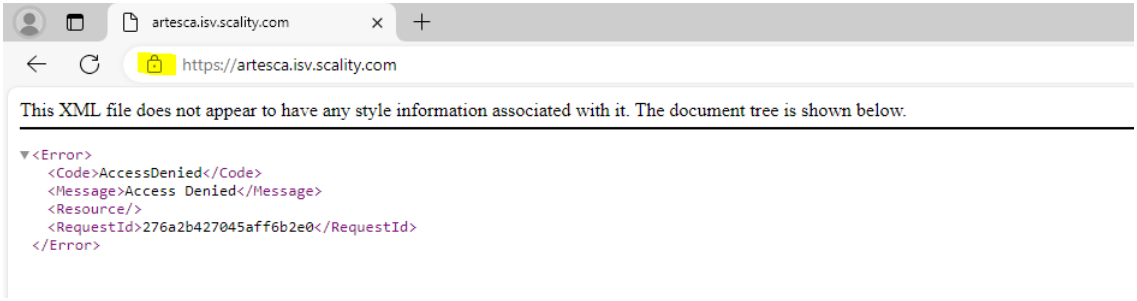
4. Customize aws_config with any text editor, such as notepad, by modifying the variable values according to the user's S3 environment.

a.

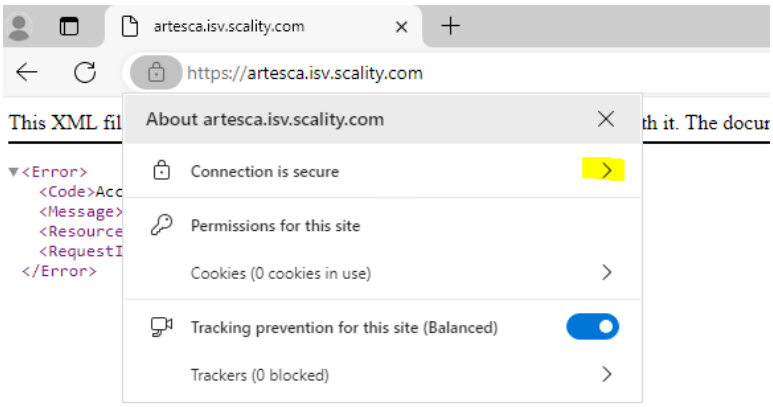


b. Update the scalitycabundle.pem file with appropriate private cloud CA.

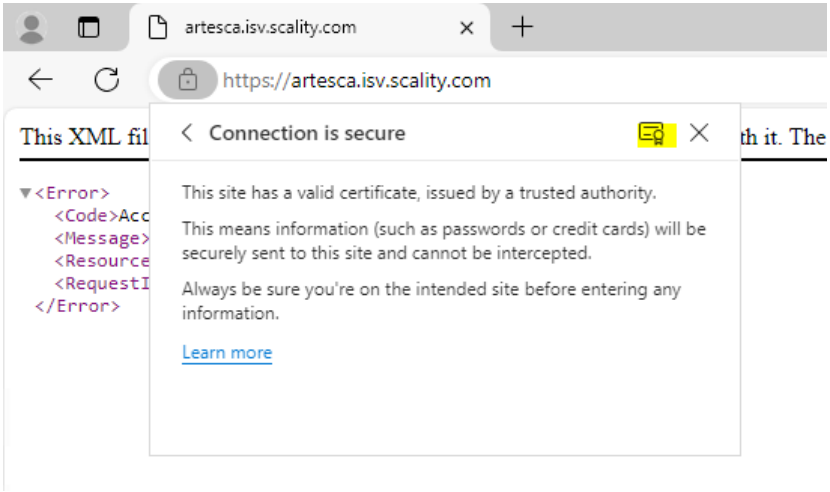
From Edge browser, access the end point URL of the private cloud (value set in the config file)



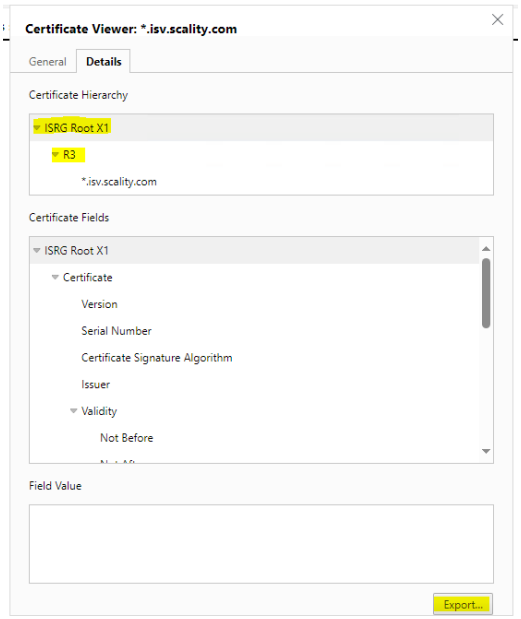
Right-click on the lock icon and expand Connection is secure



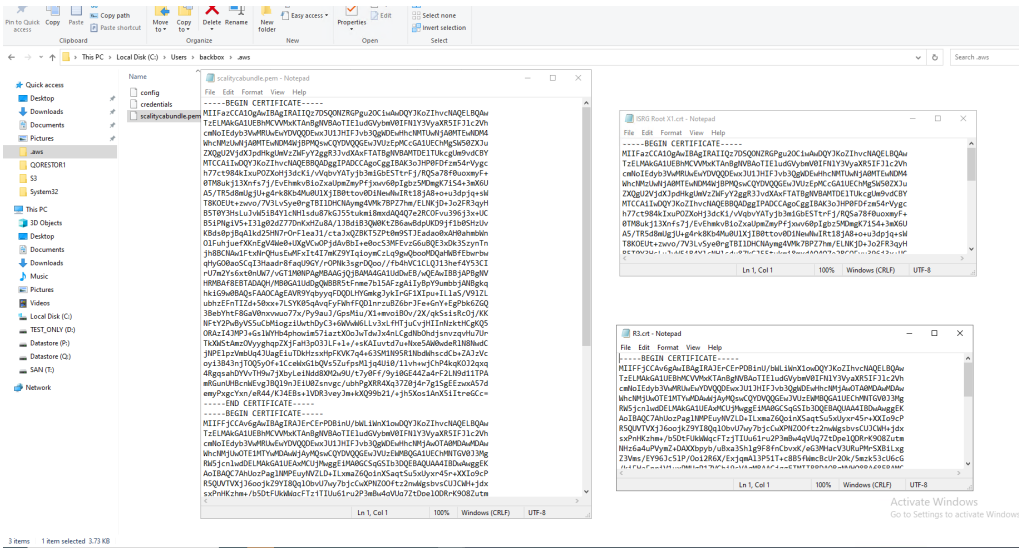
Click on the certificate icon and select the "Details" tab



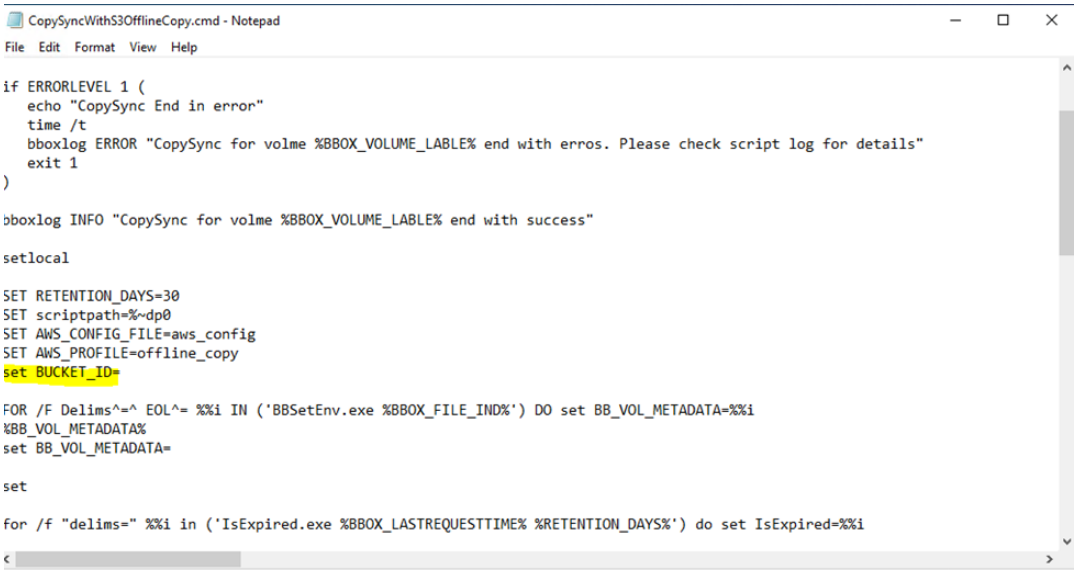
Select the ISRG Root and click export into a file. Repeat with R3 and export in another file.



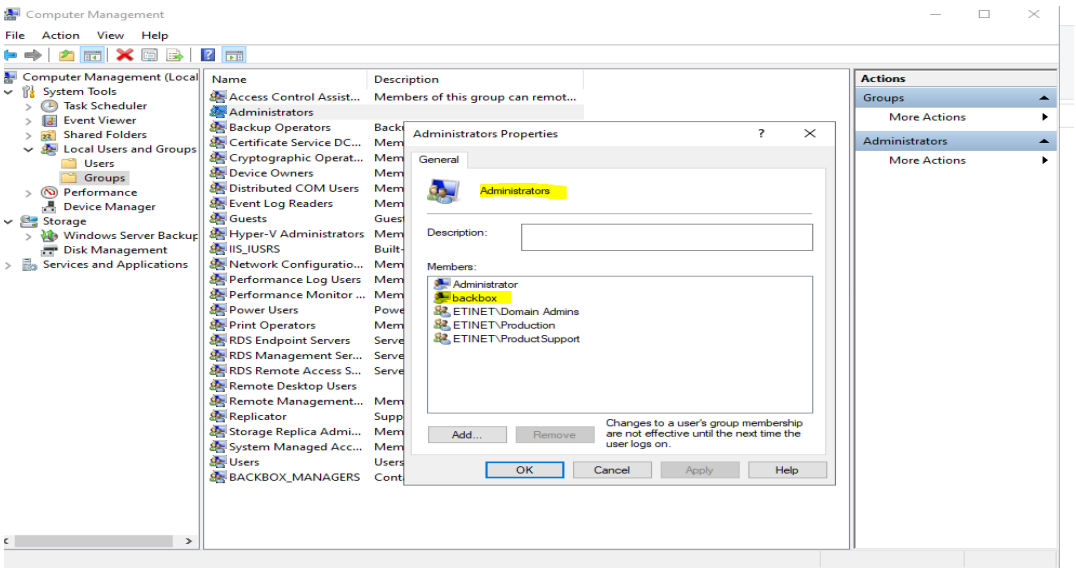
c. Open with notepad the two exported files (ISRG Root X1 and R3) and copy both where the scalitycabundle.pem file is. Overwrite the actual file certificate with the exported RISRG Root X1 and S3 certificate.



5. Change the value of variables BUCKET_ID in the script file CopySyncWithS3OfflineCopy.cmd, accordingly, based on the user's environment..



6. In Computer management, add BackBox user in the local Administrators group to make sure the user has access to the script files.



Enabling / Not Enabling the Script Controller

There are two processing modes for the scripts:

1. The first mode corresponds to a simpler setup, where there is one execution of the script for each virtual volume.
2. The second set is used when scripts are managed by the Script Controller. In this case, the first level of scripts just forward backup or restore requests to the VTC Script Controller. These requests are thenqueued and managed by the Script Controller. When a batch is submitted by the Script Controller, a distinct sub-script is executed to process a variable number of volumes, whose file names are received in a file list.

In both cases, the first level of scripts looks identical, and they are identified in the Data Store advanced configuration page. User parameters can also be defined and their value set in the same page.

The Script Controller is described in the last chapter of this manual. It is a batch sub-system used for two reasons:

- Retries : When the user wants another layer of error recovery on top of whatever retries the Enterprise Backup clients implement. By default, the Script controller will retry for 24 hours, with a delay of 5 minutes before a 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 accesses directly a sequential media, such as a physical tape library, and the number of drives in the tape library is very limited. The Script Controller queues the backup or restore requests, consolidates similar requests together, and submits them in a configured number of queues and threads per queue.

Script Implementation

Scripts are implemented by:

- Planning the storage management
- Installing the Enterprise Backup client
- Location and security of the script files
- Writing scripts or revising the Distributed Samples, possibly using the Distributed Utilities
- Testing them manually, outside the BackBox automation
- Configuring the scripts in the Data store

Backup of Windows Files

The Windows disk files containing virtual tape volumes can be backed-up in two ways:

1. The Enterprise Backup controls the whole processing and initiates a regular backup, typically according a daily schedule. It is recommended to make an incremental backup. In the BackBox configuration, no backup script is specified (but restore script and delete script are specified). This backup is called "pull backup".
2. To save a tape virtual volume each time it is re-written, a backup script is configured in BackBox and is executed by the VTC immediately after the tape volume is unloaded by the host. This backup called "push backup".

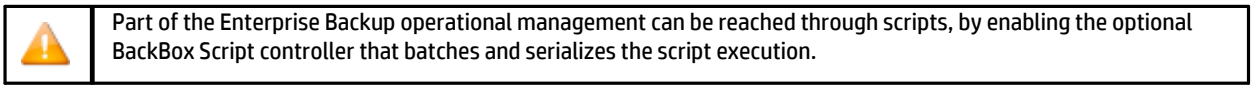
Backups executed at each unload work better if:

- the archive has a logical name that is independent of the actual Windows path: for example, the archive might be named by the concatenation of Data Store name and the volume label.
- the path name is removed from the identification of backup objects to restore; easier to manage, for example, if the BackBox virtual volume catalog has been lost and no backup is available.

The enterprise backup server allows stacking archives from several sessions on the same physical media.

Global "pull backups" can be used to:

- Set up familiar Enterprise Backups and operate the backups.
- Stack several virtual volumes on the same sequential media.
- Control the Enterprise Backup resources (physical tape drives) by the team managing the Enterprise Backup.



Single "push backups" by scripts can be used to:

- Save a volume immediately after it has been written.
- Differentiate between the storage services, by different backup parameters set in the different BackBox Data stores and Volume groups.

Deletion of Files in the Online Storage

When the Volume group is linked to DSM/TC or TMF, the image of virtual tape is not materialized in Windows files; an empty volume will be created "on the fly" when the volume is requested for a new backup.

Windows files can be deleted:

- To remove the files corresponding to SCRATCH tape volumes.
- To free-up the disk space from files that have been archived.

The deletion of SCRATCH volumes is executed by the macro BB017_FREE_EXPIRED. The deletion of backed up files can be done:

- Just after the backup of a virtual volume, in the backup script or by the global daily backup. Some backup software allows safe archive/delete combined operations.
- A few days after the virtual volumes were written, or accessed for a restore, to allow for fast retrieval of recent volumes or for volumes mounted repeatedly for multiple restore attempts.

This last deletion after a delay is enabled on the Volume Group configuration page. The delete is triggered by the macro BB023_DEL_BACKEDUP and must be scheduled in NetBatch.

The Archive Bit of the backed-up Windows files must be reset by the Enterprise Backup to allow deletion.

Deletion of Back-End Archives and Reuse of Physical Media

The Enterprise Backup should be configured for infinite retention of the archives - or backups. A Back- Box delete script is used to delete the expired stored virtual volume saved in the Enterprise Backup. This way, the expiration of a NonStop tape volume in DSM/TC or TMF or QTOS is automatically propagated not only to the online storage in the data Store, but also to the archives in the Enterprise Backup.

This automation requires an Enterprise Backup command that deletes the archives of only two Windows files, passed by BackBox to the Delete script.

Some Enterprise Backup allow to attach a free identifier to a backup session.

For example, the backup script saves the two .DAT and .IND files of a volume label VOL123 and associates them with a "session name" VOL123; then the delete script can remove the two file backups by deleting or expiring all archives associated with the "session name" VOL123.

When it is not possible to automatically forward the actual expiration of each virtual volume in a DSM/TC or TMF, two other means could be used to set a predefined expiration to the archives.

1. Some predefined expired tapes are configured in the Enterprise Backup; they are associated with specific Windows directory names themselves and are configured in different Data stores and different Volume groups. Thus the DSM/TC pool will contain specific Windows directories and be indirectly retained in the Enterprise Backup.
2. A parameter to the Enterprise Backup executed in the backup script specifies the retention or a storage management class. This retention must be set in the backup script according to the available Windows parameters provided to the script, such as the Volume group name or the Volume class.

Windows Files Restore

When the NonStop requires a virtual volume and the disk files have been archived and deleted, the missing Windows disk files are then automatically restored by executing the restore script.

In case of an extremely high volume restore running several concurrent NonStop restores reading in the Enterprise Backup from sequential media, the restore and backup the process must be carefully planned.

The restore script, as well as the other scripts, must be implemented in such a way that any VTC con- figured as a route to the Data Store, can execute it.

INSTALLING THE ENTERPRISE BACKUP CLIENT

Any Enterprise Backup Client uses normally a backup software client to install in all VTCs that are routed to the Data Store to configure with Scripts.

The software must:

- Be able to save and restore files named by UNC (\\svr\share\dir...\file.ext).
- Provide a command line interface to use in Windows scripts. It is highly preferable that the software is also able to:

- Reset the Archive Bit in the file system when the file has been saved.
- Restore in a different VTC from the VTC that held the original file and that is different from the VTC that executed the Backup script - if any.

LOCATION AND SECURITY OF THE SCRIPT FILES

The script files must be present on the same local disk location, in all VTCs that are routed to the Data Store to configure with scripts.

The distributed sample scripts are installed in: C:\ProgramData\ETINET\VTC\Script.

These can be used as a starting point and copied to the location where they will be updated and executed.

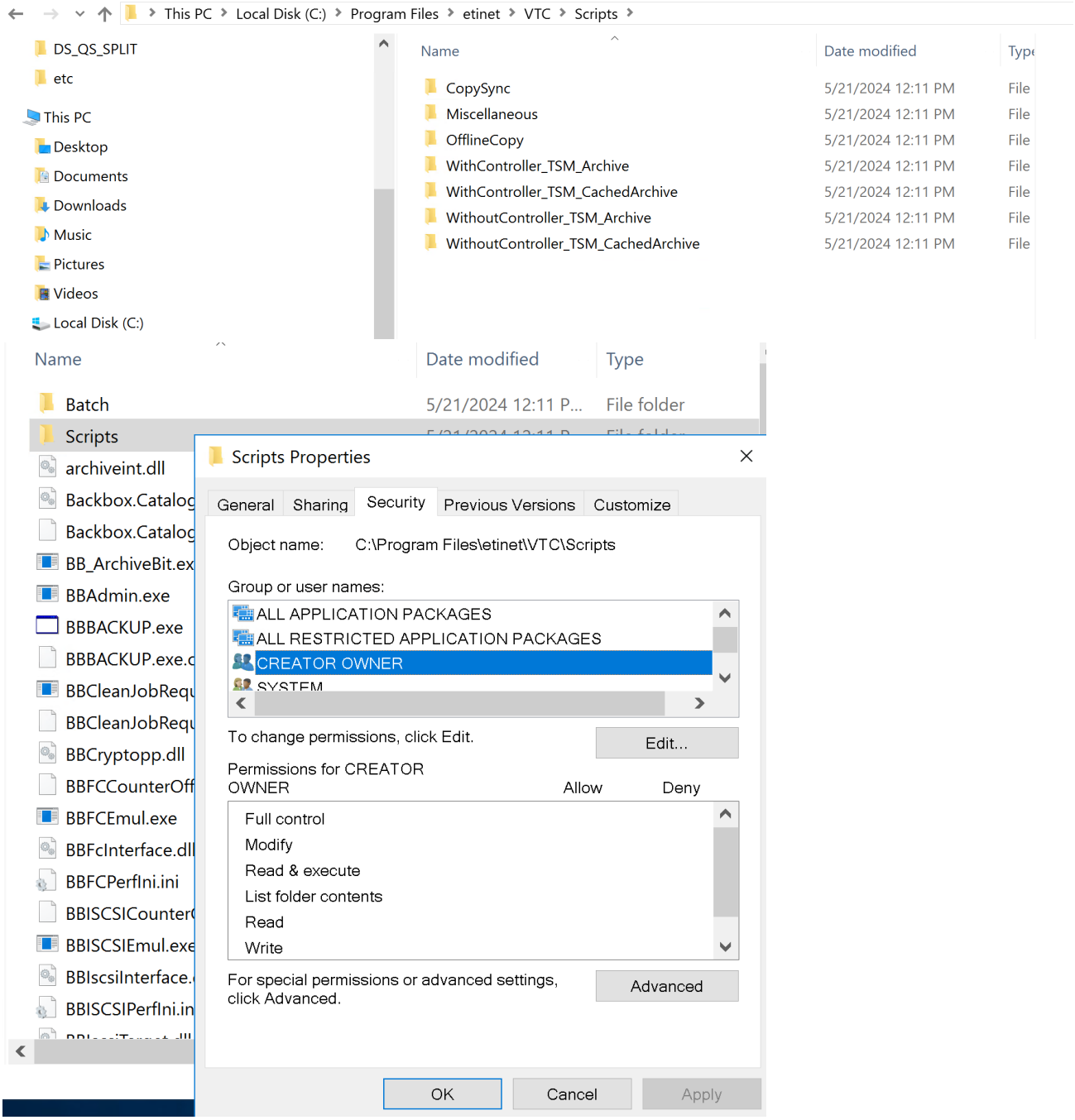
For TSM or for WinFile (simple COPY file command) the sample can be used without any modification. In this case, the Data Store can be configured to directly run the samples in:

C:\ProgramData\ETINET\VTC\Script

The directory containing the scripts must be authorized in full to access all Windows accounts that will execute the scripts. This includes the account configured to access the storage in the Data Store UI page. The VTC executes a Windows login with this account to run the script.

Users with access to Data Store UI page have default read/write permissions to the VTC Script folder: C:\ProgramData\ETINET\VTC\Script.

⚠	For local administrator (group) users, the script is customized in such a way that allows running the script under the folder c:\program files\etinet\vtc\script with default per-missions READ, LIST and EXECUTE. To make sure the local admin users have access to the script, check the Windows-based script folder permissions.



Description	For local administrator (group) users - different from the ones defined for BackBox/VTC - , the script is customized in such a way that allows running the script under the folder c:\Program Files\etinet\vtc\script with default permissions READ, LIST and EXECUTE.
Script Location	C:\Program Files\etinet\vtc\script

Script Reports	C:\ProgramData\ETINET\VTC\Script Need READ and WRITE permissions
Permissions to the custom user	The custom script running under c:\Program Files\etinet\vtc\script has default permissions Read, List&Execute
Grant permissions to the regular user	1. Locate the Scripts folder on C: under VTC folder. 2. Right-click on the folder. Go to Properties>Security 3. Select the user (local admin user) group. 4. Check Read&Execute (or the permissions you want to grant to the user) checkbox in the Permissions panel to assign the respective per- mission to the user/group. For version prior to 4.09, add the Write permission.

Specifications

Usage	For local administrator created Users/Groups.
Behavior	The custom script script under folder c:\Program Files\etinet\vtc\script with default permissions READ, LIST and EXECUTE
Variations (regular user)	For BackBox/VTC created users - via BackBox UI - refer to the regular procedure described in the VTC Scripting Option guide, section Location and Security of the Script Files.
Variations - Versions prior to 4.09	Warning: For version prior to 4.09, add the Write permission to the procedure on granting permissions to the user(s).

Script Samples

Sample scripts are provided in the BackBox installation directory **C:\Program** Files\ETINET\Virtual Tape **Controller\Script**

Simple examples are provided for common enterprise backup software.

The following example illustrates a very primitive backup script using the VERITAS NetBackup's command line.

The VERITAS server name is specified by a user configuration parameter NETB_SERVER set in the VTC domain configuration.

The policy name is built with the Volume Group name of the volume being processed (BBOX_ VOLGROUP).

The two file names to backup are specified by %1 and %2.

```
cd \scripting
bpbackup - p BBOX%BBOX_VOLGROUP%
-s INCR
-S %NETB_SERVER%
-w 01:00:00
-k "BACKBOX archive"
%1 %2
```

TSM Scripts

For Tivoli Storage Manager (IBM TSM), the scripts are more elaborate. Four script sets are presented in distinct directories combining two options:

- With or without the BackBox Script Controller.
- Archive with immediate deletion of the Windows files with cache of archived files on disk with the resetting of the Archive Bit by the BackBox tool.

```
Script\TSM\WithController_TSM_Archive\*.*

Script\TSM\WithController_TSM_CachedArchive\*.*

Script\TSM\WithoutController_TSM_Archive\*.*

Script\TSM\WithoutController_TSM_CachedArchive \*.*
```

The file: Script\TSM\dsm.opt is a sample TSM client configuration file.

Manual_Restore.cmd

A special script - Manual_Retsore.cmd - is also distributed for cases where the Enterprise Backup has no command line. The backup is completely operated by the backup server, according its own schedule.

The special script Manual_Restore.cmd is distributed for the following purposes:

- Notify the operator of the original name of the files to manually restore, and in which server and directory the VTC expects the files be restored.
- Wait for the files to be actually restored, before the VTC reads them to present the tape volume to the host.

Utilities

BBOXLOG, BB_ArchiveBit and WAITFILE are distributed Windows programs that can be used in user - written BackBox scripts. When a script is started, the MS-Windows PATH variable is increased with the VTC program directory to make these utilities available.

BBOXLOG

BBOXLOG sends a message to the EMS subsystem of a NonStop node.

BBOXLOG can be run in scripts triggered by the BackBox software used in a stand-alone Windows script. BBOXLOG must run in a Windows server hosting a BackBox, as it communicates with a BackBox Domain Manager.

Syntax:

```
SET BBOX_NSK_NODE=<\node-name> SET

BBOX_DOMAIN=<domain-name>

BBOXLOG event-number message text [param-1 [param-2] ]
```

BBOX_NSK_NODE and BBOX_DOMAIN set the message destination.

These environment variables are already set with appropriate values when run in scripts triggered by BackBox.

- Event-number is the generated EMS event number. It must be in the range 8000 to 8999.
- Message text is the generated EMS event message text. Text with a syntax similar to the format in the C function sprintf().
- [Param-1 [Param-2].] are the parameters for sprintf(). Parameter values being strings in the command line, the parameter conversion type must be only %s in the Message text - ultimately it must be %%s.

- The target EMS collector name is specified in the BackBox Domain configuration.

- When sprintf() parameters are specified in the Message text, the % character must be doubled.
- Example:bboxlog 8001 "Restoring files for tape volume %%s" %BBOX_VOLUME%
- When BBOXLOG is executed outside the BackBox environment, the Windows PATH must be updated to include the BackBox installation directory. SET PATH
- %PATH%; C:\Program Files\ETINET\BackBox Virtual Tape Emulation

BB_ARCHIVEBIT

This program is used at the end of backup scripts archiving Windows files to a IBM Spectrum Protect Tivoli Storage Manager - TSM).

It queries the TSM server to verify the files that have been archived by a previous dsmc archive command, that are actually known by the TSM server.

If the archives are known by the TSM server, the Archive Bit isreset in the Windowsfile system, allowing later "Delete Backed-up files" functionality enabled in the Volume groups.

Prerequisites:

- The regular TSM environment variables DSM_DIR, DSM_CONFIG and DSM_LOG must be available in the process context.
- The TSM login is assumed to be automated by the DSM.OPT option PASSWORDACCESS GENERATE.

Syntax:

```
BB_ArchiveBit file-pattern1 [file-pattern2]
```

or

```
BB_ArchiveBit - l filelist-file1 [file-file2]
```

- BB_ArchiveBit is included in these two sets of distributed scripts:

  Script\TSM\WithController_TSM_CachedArchive*.*

  Script\TSM\WithoutController_TSM_CachedArchive *.*
- File-pattern1 file-pattern2 etc. are the patterns of the files to process. Supported wildcards: * and ?
- Filelist-file1 filelist-file2 etc. are the names of files containing the list of files to process.
- BB_ArchiveBit does not query TSM for backup objects, only archive objects.

WAITFILE

WAITFILE waits for the creation of a Windows file and its availability. It does so by looping while trying to open the file with exclusive access, and sets the Windows Error level when ending, possible values are:

- Errorlevel 0: the file is available.
- Errorlevel 14: there is an error in parameters.
- Errorlevel 40: timeout, the file does not exist or is not available within the allocated time. Other values may be set by the Windows command line interpreter for severe errors.

Syntax:

```
WAITFILE file-name [maximum-number-of-seconds]
```

File-name is the name of the Windows file to wait for.

Maximum-number-of-seconds is the maximum number of seconds WAITFILE will wait. Default value is 0 seconds, preventing WAITFILE from waiting if the file does not exist or is not available.

Testing the Scripts Manually

It is recommended to manually test the scripts on a VTC in a Remote Desktop session at the Windows command prompt, without using BackBox software.

The parameters passed by the VTC can be manually set in a test script, using the detailed description of script parameters in this manual.

Sample:

```
SET BBOX_VOLUME=LBVOL123

SET BBOX_SCRIPT_DIR=c:\script\

SET BBOX_FILE_IND=\\MTLBBLAB1\BPAK\WIN1\LBVOL123.ind SET BBOX_FILE_ DAT=\
\MTLBBLAB1\BPAK\WIN1\LBVOL123.dat

   /

BACKUP.CMD  \\MTLBBLAB1\BPAK\WIN1\LBVOL123.ind

\\MTLBBLAB1\BPAK\WIN1\LBVOL123.dat
```

Configuring the Scripts in the BackBox Domain

The scripts are configured by the BackBox UI, Configuration, Data Store, Advanced.

When a scripting option is present in the license key, the Advanced Data Store configuration makes it possible to:

- Identify the back-end Enterprise Backup software.
- Specify the location of the scripts in the VTCs, where all scripts are optional. It is possible to specify only a restore script.
- Specify user MS-Windows environmental parameters for the scripts

APPENDIX J - SCRIPT TYPES

Backup Script

After a virtual volume mounted for output is unloaded, the backup script is executed. This script typically archives the two disk files representing a virtual volume.

Preliminary Cleanup

Before archiving a new virtual volume, the script must first delete previous archives of the same volume, providing the enterprise backup software allows the deletion of archives at the file level. Multiple archives of the same volume consume storage, but depending on the backup software used, may also be the cause of various issues at restore time, which may include, for example:

Script interrupted for unexpected prompt to choose the archive versions. Repeated restore of all avail- able archives of the same volume image.

If no operational problem has occurred during the previous execution of a specific volume, there should be a single previous archive of the .DAT and .IND. If the enterprise backup software does not automatically overwrite an archive with a newer version, then it should be deleted using the environment variables %BBOX_PREV_PATH%%BBOX_VOLUME%.*.

In very rare cases where the files .DAT and .IND were not written in the same path, an additional cleanup should be done for % BBOX_PREV_DATA_PATH%%BBOX_VOLUME%.* archives. This additional cleanup is useful if the Volume Group is configured for Auto- Scratch, and when cleaning up all files, even if there was a severe operational problem during the previous backup of the volume.

It is recommended to also delete existing archives from the same path as the new volume %1 and %2 positional parameters.

Positional Parameters

The Backup script receives two positional parameters with the name of the disk files to backup or archive:

- %1 contains the fully qualified file name of the index (file type .IND). %BBOX_FILE_IND%
- %2 contains the fully qualified file name of the data (file type .DAT). %BBOX_FILE_DAT%

Restore Script

When a virtual volume is loaded and either one or both of the two disk files representing the volume are missing, the restore script is executed. When the two files are missing, a single script execution can restore both files. The emulator waits for the script completion to complete the volume load.

Positional Parameters

In addition to the named parameters set in the Windows process context the Restore script receives either two or five positional parameters to pass on the original file name(s) and the new name(s) to the restored volumes.

If a single file - either the index file or the data file - must be restored, the script receives two parameters:

- %1 contains the fully qualified original file name that is missing.
- %2 contains the fully qualified target file name (might be equal to %1).

If both index file (file type .IND) and data file (file type .DAT) are to be restored, the script receives the 5 following parameters:

- %1 contains the fully qualified original index file name (type .IND).
- %2 contains the fully qualified target index file name (type .IND).
- %3 contains the fully qualified original data file name (type .DAT).
- %4 contains the fully qualified target data file name (type .DAT).
- %5 contains a fully qualified file name pattern for both files.

If the script receives 5 parameters but processes only the parameters %1 and %2, the script will be retrieved with 2 parameters to restore the 2nd file.

The content of the positional parameters is also available in the following named parameters:

%1 value is in %BBOX_ORIG_FILE_IND%

%2 value is in %BBOX_DEST_FILE_IND%

%3 value is in %BBOX_ORIG_FILE_DAT%

%4 value is in %BBOX_DEST_FILE_DAT%

%5 value is in %BBOX_ORIG_FILE_PATTERN%

Note: The Archive Bit of files restored by the restore script for a NonStop restore operation, is reset by the VTC emulator.

Execution Control

The emulator uses the restored files only if the return code of the restore script is 0.

Post-Restore Script

The main purpose of this script, deleting backed-up files, is obsolete. This functionality is better handled by the macro BB023_DEL_BACKEDUP (see OBB017 OBEY file), controlled by the "Delete backed-up files" parameters in the Volume groups.

This script is still kept for compatibility purposes.

This script is called up at unload time, only when the Restore script has been executed to satisfy the load request for a NonStop application requesting a tape volume for input.

The user might choose to enable this script to systematically delete restored files at unload time.

In addition to the named parameters set in the Windows process context, the Restore script receives these two named parameters, which can contain the restored Windows disk files:

%BBOX_RESTORED_IND%

%BBOX_RESTORED_DAT%

If the variable is not null, the file named in the variable is restored at load time, is not modified, and can be deleted.

Delete Script

The delete script is executed when a virtual volume is deleted using the BackBox User Interface.

The two Windows disk files, if they exist, are deleted by the VTC and the script should be written to free up resources in the Enterprise backup software used to archive the Windows files.

Positional Parameters

In addition to the named parameters set in the Windows process context, the Delete script receives two positional parameters set with the name of the disk files of the virtual volume to be deleted.

- %1 contains the fully qualified file name of the index (file type .IND).
- %2 contains the fully qualified file name of the data (file type .DAT). The content of the positional parameters is also available in the parameters named:

%BBOX_FILE_IND%

%BBOX_FILE_DAT%

The recommended cleanup of the Data Store configuration is achieved by deleting all of the potential archives saved from any path.

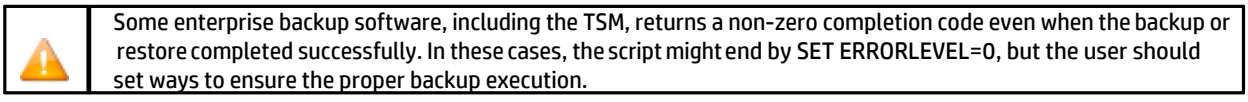
For this purpose, the name of all paths configured in the Data Store is passed in two Windows variables:

%BBOX_CONF_PATH_NUMBER% and %BBOX_CONF_PATH<n>%. This maximum cleanup might take several minutes depending on the startup time of the backup software and the number of paths to clean.

Script Variables and Controls

The BackBox software does not monitor the outcome of the script execution, except in reporting the return code of each script execution to the Guardian EMS sub-system.

However, when running the restore script, the restored files are used only if the script completes with a zero return-code.



The Guardian tape application will consider the execution successful if the virtual volume was written to the Data Store. If a backup script fails to archive a virtual volume it is critical that the script reports the error. The EMS message #3171 is issued in addition to

other messages reporting an error in a script execution.

The output of the script execution is located in the Windows ProgramData directory, in a distinct sub- directory per Data Store. The name of the output file is built with:

- The name of the initiator script (Windows service):

  VTC - Emulator Service

  ADMIN - Administrative Service

  SCRIPTCTLR - Script Controller

  Service

- The file name of the script.
- A sequence number assigned up to 1000 in a round-robin fashion.
- The .log suffix.

The round-robin assignment of the sequence number provides an automatic purge in each script Log directory.

File Name Syntax in Script Parameters

The fully qualified names of files to process are passed to the scripts.

In positional parameters (%1, %2 etc..), the file name is enclosed by double-quotes when it contains a space; no double-quotes when no space.

In named parameters (%BBOX_DEST_FILE_DAT%...), the file name isnever enclosed by double-quotes.

Pre-defined Named Parameters

In addition to the positional parameters, the following variables are passed to the executing scripts:

Parameter Name	Backup Script	Restore Script	Post-Restore Script	Delete Script	Content
%BBOX_ BACKUP_ HOST %	✓	✓	✓	✓	Host name of the VTC that executed the last volume write, or the last backup script. For volumes written or backed up previously, a default value is extracted from % BBOX_FILE_IND% Available to : All scripts.
%BBOX_CONF_ PATH_ NUMBER%	✓	✓	✓	✓	Number of configured paths in the Data Store. Available to : All scripts.
%BBOX_CONF_ PATH<n>%	✓	✓	✓	✓	Configured paths, <n> varying from 1 to %BBOX_CONF_PATH_ NUMBER% Available to : All scripts.
%BBOX_ COMPRESSION%					Compression algorithm used Possible values: NONE ZLIB MINILZO
%BBOX_DATA_ SIZE%					Number of bytes received from the NSK (uncompressed). Currently displayed in the BackBox UI as "Size", "Write byte count", or "User Data Size". The size includes the tape headers and trailers (less than 1 K). Variable is always set with zero value. When the original value is not available (in a restore from a RESTRICTED Data Store), the value used is the maximum volume size configured in the

					Volume Group converted to bytes.
%BBOX_DEST_ FILE_DAT %		✓			Fully qualified target data file name (type .DAT). Restore script.
%BBOX_DEST_ FILE_IND %		✓			Fully qualified target index file name (type .IND). Restore script.
%BBOX_ DOMAIN%	✓	✓	✓	✓	Domain name. Available to : All scripts.
%BBOX_FILE_ DAT%	✓			✓	Fully qualified file name of the data (file type .DAT). Backup and Delete scripts.
%BBOX_FILE_ IND%	✓			✓	Fully qualified file name of the index (file type .IND). Backup and Delete scripts.
%BBOX_LABEL_ TYPE%	✓	✓	✓	✓	Label type. ANSI, BACKUP, TMF, or NL Available to : All scripts.
%BBOX_NEW_ DIR%		✓			Contains the fully qualified directory name of the file to restore. Same value as at the beginning of %2 parameter of the restore script. Restore script.
%BBOX_NSK_ NODE%	✓	✓	✓		Contains the name of the NonStop node where the current tape device is attached. Backup, Restore and Post-restore scripts only.
%BBOX_ORIG_ FILE_DAT%		✓			Contains the fully qualified data file name to restore, used when it was backed up. Same value as the %2 parameter of the restore script. Restore script.
%BBOX_ORIG_ FILE_IND%		✓			Contains the fully qualified index file name to restore, used when it was backed up. Redundant with the %3 parameter of the restore script. Restore script.
%BBOX_ORIG_ FILE_SVR<n>%		✓			Name of the server in the path of the file named in the <n> positional parameter. If the file name of the 1st positional parameter is \\BBOX2\SHARE1\LB123456.IND, the %BBOX_ORIG_FILE_SRV1% parameter will contain BBOX2. If the file name of the 3rd positional parameter is C: \DATASTORE1\LB123456.DAT, the %BBOX_ORIG_FILE_SRV3% parameter will contain the name of the local system. Restore script.
%BBOX_PREV_ PATH %	✓				Path of the virtual volume files before the current operation for IND and DAT files, or only for the IND file. Backup script.

%BBOX_PREV_ DATA_PATH%	✓				Path of the virtual volume files before the current operation for the DAT written by BackBox V3.10 and above. Backup script.
%BBOX_PREV_ UNLOAD%					Unload time of last time the volume was written; format: yyy- mm-ddTh-h:mn:ss.0000000Shh:mn . GMT time up to S position T is always the letter "T" sub-second value is always "0000000" "S:hh:mm" gives the signed difference with GMT, ex: US Eastern time will have -05:00. Example: 2017-11- 12T14:31:35.0000000-05:00 . Available if the volume was written by BackBox V2.03 and above. Used by Script controller to sort restore script requests by backup time.
%BBOX_ STORAGE_ SIZE%					Number of bytes written to the storage (possibly compressed). Currently displayed in the Web UI as "Storage Size". The size includes the BackBox packaging (block headers etc.) with the data possibly compressed. Variable is always set with a zero value. When the original value is not available, the value used is equal to BBOX_DATA_SIZE.
%BBOX_TMF_ TYPE %	✓	✓	✓	✓	ONLINE DUMP or AUDIT DUMP. Available to : All scripts.
%BBOX_ VOLUME%	✓	✓	✓	✓	Label prefix and volume label. Label prefix is LB for labeled volumes, NL for unlabeled volumes. Example: A backup volume 123456 is labeled LB123456. Available to : All scripts.
%BBOX_ VOLUME_CLASS%	✓	✓	✓	✓	Current volume class for the volume. Available to : All scripts.
%BBOX_ VOLGROUP%	✓	✓	✓	✓	Name of the current VTC Volume Group. Available to : All scripts.

In addition, the Data Store configuration allows the specification of up to 10 user-defined parameters. The name and value are entered for each parameter. For a user-defined parameter SERVER with value SRV1, the keyword %SERVER% will contain SRV1 at the script execution time.

APPENDIX K - SCRIPT GUIDELINES

Cross System Restores

The restore script, as well as the other scripts, must be implemented in such a way that any VTC con- figured as a route to the Data Store can execute it.

Extremely Large Jobs through Concurrent NonStop Drives

If there is the possibility of processing an extremely large job running several concurrent NonStop backups or restores and accessing sequential media in the Enterprise Backup, the process must be planned carefully.

In the Enterprise Backup, there might be both limited concurrent availability of tape drives and contention on the non-shareable sequential media.

Before efficiently migrating to tape, the backup process is usually solved by a Backup Enterprise firstly writing on disk.

•••

For backups, it is possible to write in parallel on several back-end media. Restoring is more difficult, as the reading of a NonStop volume requires a very specific Backup Enterprise media. All other NonStop restores needing the same back-end non-shareable media, will have to wait for the restore script of the first NonStop restore to complete, before their own script receives the required media and begins executing.

The above noted issues can become more complex because the number of NonStop virtual drives are usually more numerous than the number of tape drives in the Enterprise Backup.

In both cases, the BackBox Script Controller can help by serializing the execution of scripts. The backup problem is generally solved by firstly staging on disk inside the Enterprise Backup.

The restore is more difficult to solve, one solution would be to massively restore the images of "all needed volumes" requiring a very large disk space. This does not take into consideration the difficulty to identify "all volumes".

Tight control and organization of the Enterprise Backup storage pool is required. The content of back- end media must be planned - including the expiration process.

Specific extensions have been developed for the TSM in the Script Controller. Essentially, they query the TSM server to know the back-end media needed for a NonStop volume, then sort the execution of restore scripts by back-end media.

Archive Bit

Among other disk file properties, the Windows file system maintains an Archive Bit, and BackBox expects that this Archive Bit is reset by the backup script or by the Enterprise backup software.

When the Archive Bit is not reset:

- In the BackBox UI, the Storage Admin page cannot display the number of files that are not backed up yet, and the "Backup all non-backed up files" will back up all Windows files.
- The "Delete backed-up files" (disk staging) cannot be used efficiently.

As a workaround to current special conditions of HPE StoreOnce, the successful file archiving is not notified by an Archive Bit reset or by a file deletion; the Script Controller cannot be used.

Archive-Bit with a TSM Enterprise Backup

In the TSM for which Archive is recommended over Backup, the BackBox utility BB_ArchiveBit verifies the successful Archive in the server and then resets the Archive Bit at the end of the backup script.

No Archive-Bit in StoreOnce NAS

To free up the online storage and only keep the offline copy, the "Delete backed-up files" processing is based on the Archive Bit reset by the backup software.

Special conditions make it such that the Archive Bit is not currently supported by the HPE StoreOnce. For this storage type, the current method to verify a file that has been backed-up, is to restore it.

When a VTC executes BB023_DEL_BACKEDUP ("Delete backed-up files") for a Data store configured as StoreOnce NAS, it will restore the file with the regular restore script, to a temporary storage, when a file becomes a candidate for removal from the online storage. If the restored file looks identical to its original, both are deleted.

Directing to Different Storage Services

If there is a need for directing different NonStop backups to different kinds of storage services inside the Enterprise Backup software, it can be done several different ways.

The natural parameter in NonStop OBEY files is using different DSM/TC pools, with each pool being associated with a different BackBox Volume Group.

Two Windows named parameters, depending on the Volume group, are available in the scripts:

%BBOX_VOLGROUP%

%BBOX_VOLUME_CLASS%

This contains the Volume Group ID, which can never be modified.

This contains the Volume Class parameter configured in the Volume Groups, with several Volume groups capable of specifying the same Volume Class. The Volume Class can be updated at any time in order to provide a different value for the next execution of scripts.

Recommendations for the Enterprise Backup Software

Exclude the Virtual Volumes from the Regular Server Backup

The regular backup of the VTC Windows server, such as the backup of Windows programs, must exclude the BackBox virtual volumes:

- The need for backup retention and replication are different.
- The scheduling and automation are different.
- The size of Windows files is different.

These two kinds of backups, regular Windows backup and virtual volumes backups, are configured and operated totally independently.

Client Name in the Enterprise Backup Software

It is recommended to define dedicated, specific client name(s) in the Backup software. A client name per NonStop system, or small group of NonStop systems, usually allows the Enterprise Backup software to manage data differently.

Dedicated client name(s) will isolate the BackBox virtual volumes from the other general Windows files in the VTC servers.

In most Enterprise Backup software, this is a simple way to allow several VTC servers accessing the backup of the same volumes.

TSM specific recommendations below, can be browsed to derive specific recommendations and con- figuration procedure for other Enterprise Backup software.

TSM-Specific Recommendations and Configuration Procedure

For the TSM, be sure to install the TSM Backup command line client dsmc which will be retrieved by the scripts.

The TSM Administrative client command line dsmadmc, along with an Administrative client name authorized for queries only, has two potential usages:

- For massive concurrent restores directly accessing TSM sequential media, the TSM Administrative client can be used based on various programs by the BackBox Script Controller to optimize the restores scripts, thereby grouping scripts accessing the same TSM physical media.
- The NonStop operator who manages the NonStop backups gets some autonomy, for example, to query the available TSM storage space and the state of specific virtual volumes.

•••

One of these for distributed sets of scripts is suggested.

```
Script\TSM\WithController_TSM_CachedArchive\*.*
```

```
Script\TSM\WithoutController_TSM_CachedArchive \*.*

Script\TSM\WithController_TSM_Archive\*.* Script\TSM\WithoutController_TSM_Archive \*.*
```

In the "cached" versions with, the archived file versions are kept on disk for a limited period, configured by the "Deleted Backed Up files" parameters in the Volume groups.

In the versions without "cached" the TSM immediately deletes a file that has been successfully archived.

In the "WithController" versions, the BackBox Script controller is enabled for retries and batching. This is recommended for setups where a sequential media is directly accessed by backups or restores, such as LAN- FREE setups, and especially when extremely large volumes, concurrent backups or restore, are executed.

In the version "WithoutController", simple scripts are executed. This is recommended for simplicity in setups that access only TSM disk pools, or marginally run concurrent backups or restores.

•••

The scripts save the files in "Archives" objects, rather than "Backups" objects. Archives are more appropriate as the backup multiple versions of an object do not make sense with virtual volumes.

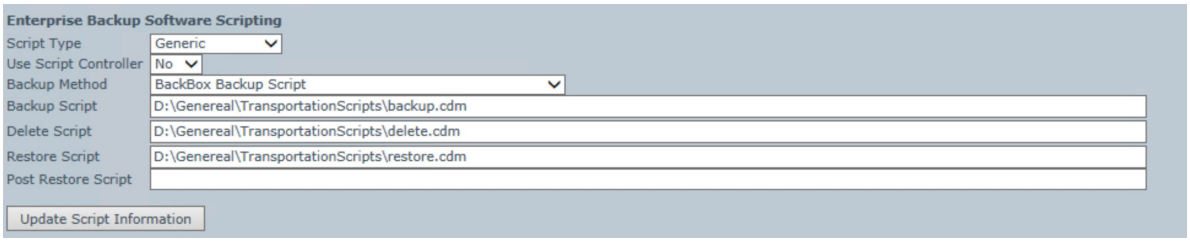
The TSM Management Class must be configured for the Archive Copy Group, and the retention should be infinite - as the BackBox "delete script" will delete the Archive when the corresponding virtual volume has expired in DSM/TC, or in other NonStop catalogs supported for the Auto-Scratch which are enabled in the Volume Group.

For non- cataloged volumes or unsupported tape catalogs, the infinite retention will not keep more than the last version of each virtual volume.

Not using an infinite retention in the TSM, brings up the possibility of potentially mismatched retentions between the TSM and the NonStop. For example, a NonStop operator might not be aware of a maximum retention in the TSM, and expect that the retention specified in a backup OBEY file, will be considered in the TSM.

•••

To avoid unnecessary script modification, and to have more accurate configurations, enter the value of the three Windows variables required by the TSM (DSM_DIR, DSM_CONFIG, DSM_LOG) Script Parameters in the BackBox UI, Data Store Advanced properties page, where the script names are also entered.



The distributed DSM.OPT should be taken as a sample and should be copied in all VTC to the same location as the scripts; then it must be customized VTC by VTC.

```
commmethod tcpip tcpport 1500 TCPServeraddress

tsmdev

PASSWORDACCESS GENERATE NODE VTC85 ASNODENAME NSK_BACKBOX DOMAIN C:

LANGUAGE AMENG

Resetarchiveattribute yes Errorlogretention 90

TXNBYTELIMIT 2097152

TCPBUFFSIZE 32

TCPWINDOWSIZE 63
```

In this DSM.OPT, three options must be updated or added:

- ASNODENAME: This is the common client name owning the backups in TSM, it is a proxy node (also named "target node"), and there must be a unique value given for all VTC routes to the Data Store.
- NODENAME: Is the "login node" that must be distinct for each VTC server, but which must also be allowed to access

the data of the proxy node.

- DOMAIN: Tells the scope of the backup of the whole server - where BackBox virtual volumes must be excluded.

A proxy node NSK_BACKBOX can be configured through a TSM administrator client by commands similar to:

```
register node VTC85 password85 register

node VTC86 password86 register node

NSK_BACKBOX passwordnsk

grant proxynode target=NSK_BACKBOX agent=VTC85,VTC86
```

To complete the isolation between the regular server backups and the non-BackBox backups, include the DOMAIN keyword in the DSM.OPT of these regular backups to explicitly list the local disks for the regular server backups. It excludes both the disks used by BackBox to store virtual volumes and also the BackBox files from the scope of an INCREMENTAL command applied to the whole server.

DOMAIN should be set in all DSM.OPT files in the server, which is the one installed by TSM in C:\Program Files\Tivoli\TSM\baclient, and the DSM.OPT file(s) for BackBox scripts.

•••

Directing to different TSM Management Classes and different storage services:

If there is a need to send to various TSM Management Classes depending on the DSM/TC POOL specified in NonStop backup OBEY files, the setup must be completed.

The distributed backup scripts contain the syntax to set up an explicit TSM Management Class if the Windows variable % BBOX_TSM_MC% is set. Set it by one of the three following ways:

1. Update the backup.cmd script to insert at the beginning: SET BBOX_TSM_MC=%BBOX_VOLUME_ CLASS% (suggested and preferred course of action).
2. Update the backup.cmd script to insert at the beginning: SET BBOX_ TSM_ MC=%BBOX_ VOLGROUP% .
3. Add this BBOX_TSM_MC in the Script Parameters of the Data Store configuration - Advanced propertiespage.

•••

Customize and run the distributed setup_for_test.cmd to test and finalize the TSM client installation:

1. Enter in "setup_for_test.cmd" the values for three TSM Windows environment variables (DSM_ CONFIG. DSM_DIR and DSM_LOG.) that were added as Script Parameters in the BackBox Data Store Advanced configuration.

setup_for_test.cmd content:

```
set DSM_DIR=C:\Program Files\Tivoli\TSM\baclient set

DSM_CONFIG=C:\BPAK\script\dsm.opt

set DSM_LOG=c:\BPAK\script set

PATH=%PATH%;%DSM_DIR%

dsmc
```

2. Run "setup_for_test.cmd" once to:

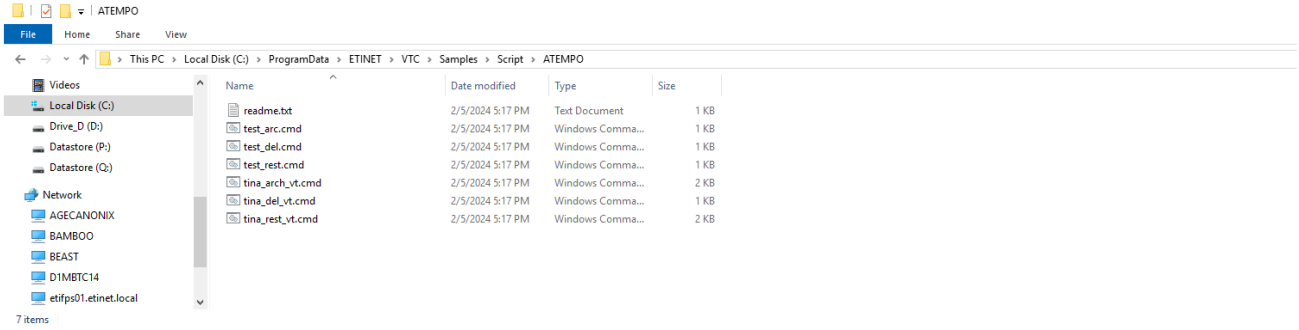
- Enter the node password when prompted. The password will then be encrypted and stored in the Windows registry and automatically managed by the TSM (because of PASSWORDACCESS GENERATE in DSM.OPT)
- Archive a small Windows file to ensure the TSM storage is available.

Sample run:

```
C:\BPAK\script>setup_for_test

C:\BPAK\script>set DSM_DIR=C:\Program Files\Tivoli\TSM\baclient C:\BPAK\script>set

DSM_CONFIG=C:\BPAK\script\dsm.opt
```

```
C:\BPAK\script>set DSM_LOG=c:\BPAK\script C:\BPAK\script>dsmc

IBM Tivoli Storage Manager

Command Line Backup-Archive Client Interface Client

 Version 6, Release 1, Level 5.2 Client

date/time: 11/22/2020 11:17:17

Node Name: VTC85

Please enter your user id <VTC85>:

Please enter password for user id "VTC85": ******

Session established with server TSMDEV_SERVER1: Windows Server Version 5, Release
3, Level 5.2

Server date/time: 11/22/2020 11:18:14 Last access: 11/22/2020 11:18:14

Accessing as node: NSK_BACKBOX

tsm> archive delete.cmd Archive

function invoked.

Directory--> 0 \\nsk_backbox\c$\BPAK [Sent] Directory--> 0

\\nsk_backbox\c$\BPAK\script [Sent]

Normal File--> 1,004 \\nsk_backbox\c$\BPAK\script\delete.cmd [Sent]

Archive processing of '\\nsk_backbox\c$\BPAK\script\delete.cmd' finished without
failure.

Total number of objects inspected: 3 Total

number of objects archived: 3

              Total number of objects updated:                          0
              Total number of objects rebound:                          0
              Total number of objects deleted:                          0
              Total number of objects expired:                          0
              Total number of objects failed:                           0


Total number of bytes transferred: 1.75 KB Data

transfer time: 0.00 sec


Network data transfer rate: 0.00 KB/sec Aggregate

data transfer rate: 1.65 KB/sec Objects compressed

by: 0%

Elapsed processing time: 00:00:01 tsm>

quit

C:\BPAK\script>
```

Verify the Script folder location to make sure you run the right script. In the example below, the location of the script folder is not the same as the one in the sample.



Tips for TSM Scripts

"A required NT privilege is not held".

This message is issued by the TSM Windows client executed in backup or restore scripts, when:

- A path on a remote file server is configured in the disk pool of a Windows File Data Store.
- And the account configured to access the remote file server doesn't have the permission to "Manage auditing and security log".

The account running the TSM client must have the rights as noted below. For exact reference, refer to the IBM Tivoli Storage Manager documentation.

- Backup files and directories.
- Restore files and directories.
- Manage auditing and security logs.

The right "Manage auditing and security logs" is often missing. To add it:

- Log into the Windows box acting as a file server for BackBox.
- Administrative Tools.
- Local Security Policy.
- Security Settings.
- Local Policies.
- User Rights assignment.

Find the policy "Manage auditing and security log", and add the account under this policy. Then restart the file server once all tasks have been completed.

Testing the Completion of the Command Line Client (dsmc)

The client command line DSMC can set the Windows error level to a non-zero value as soon as an error occurs, and even internal retries allow for a successful completion of the command. Network failures are sample of errors that are solved by retries and which set a non-zero error level.

The BackBox VTC tests the script return code, and does not use any script if the result of the error level is not zero.

The line SET ERRORLEVEL 0 as a last script line disables the verification of the return-code.

The actual success of a script is evaluated by its result on the file system: a file to restore is present, a file to archive has been deleted by the TSM - delete files option, or the Archive Bit has been reset by the program BB_ArchiveBit.

APPENDIX L - SCRIPT CONTROLLER

The Script Controller is an optional tool used to manage Windows backup and restore scripts initiated by the VTC.

The Script Controller is a mini-batch subsystem that manages a queue of script requests inside a VTC to:

- Group the backup or restore of several files in the same script execution.
- Control the maximum number of scripts running concurrently.
- Provide retries at the file level when a script is not successful.

The purpose of grouping the restore scripts execution is to reduce the chances of tapes being rearranged when backed-up files are restored on sequential physical media.

⚠	Target environments are environments where numerous scripts are submitted and where the back-end Enterprise Backup server saves BackBox Windows files on physical sequential media.

The retry mechanism does not rely on return codes to detect errors, but checks the actual result of a restore or backup by accessing the Windows file after the script execution:

- A file was successfully restored if the file is available.
- A file was successfully saved if the file's Archive Bit (the Windows file system attribute) was reset, or if

the file is no longer present. The file is assumed to have been archived in the latter case.

The VTC emulator is not aware of the usage of the script controller, but does communicate requests to the usual script using Windows parameters.

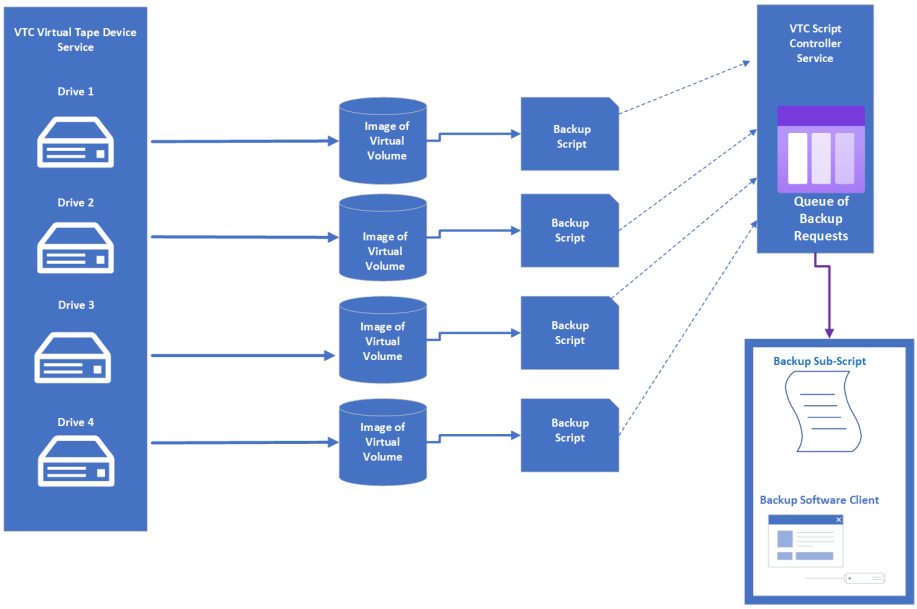
To enable the script controller, the user must either update the regular scripts or create a backup and restore script.

Update the regular scripts:

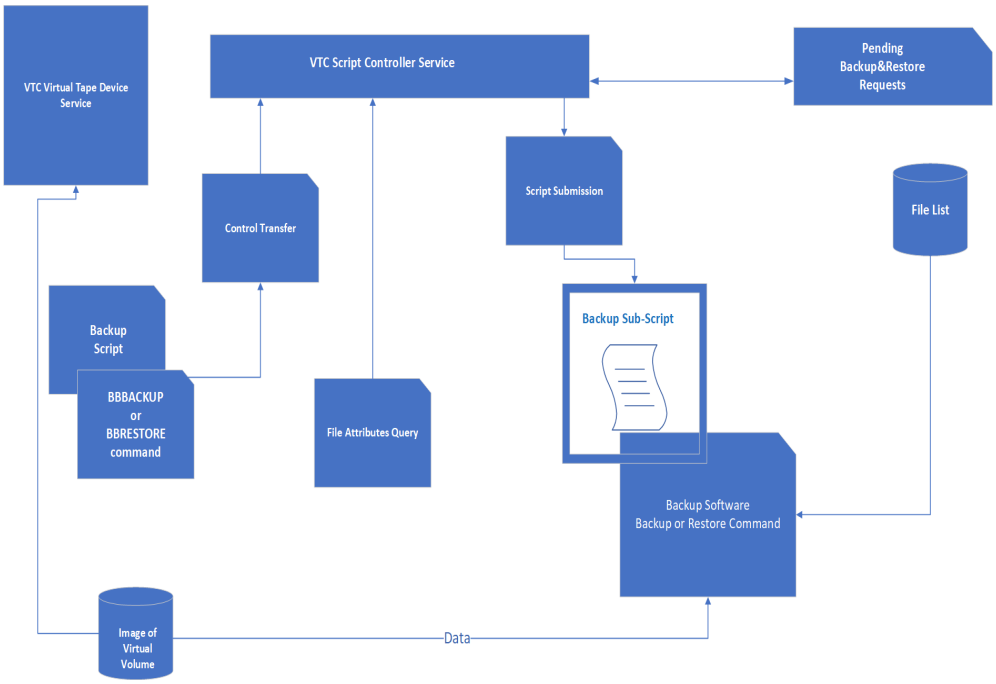
- Update the backup script, replacing the Enterprise Backup client command by a BBBACKUP command.
- Update the restore script, replacing the Enterprise Backup client command by a BBRESTORE command.

Create a backup and a restore sub-script:

- The subscript will be started by the script manager.
- The subscript runs the Enterprise Backup client; it uses a temporary file (%BBOX_FILELIST%) that contains the name of files to be processed.
- Requirement: The execution of backup sub-script must either delete the archived file or reset the Archive Bit of the file in the Windows file-system. Most Enterprise Backup software is able to reset the Archive Bit, but sometimes it requires a special configuration in the files to achieve a successful back-up.



Processing Summary



BBBACKUP/BBRESTORE forwards the backup/restore request, one request per file, and usually two requests per virtual volume: one for the *.DAT file, another for the *.IND file.

The script controller queues the list of backup/restore requests in memory, and processes them according to the parameters passed along by the commands BBBACKUP or BBRESTORE.

Requests made in different queue names are processed concurrently. Several concurrent threads can be processed in the same queue name by setting the parameter BBOX_SCRIPT_MAX_THREADS.

When the script controller initiates a specific job and submits a subscript, it gathers requests for files with the same script context.

It builds a temporary file that contains a line per file to process. The name of this temporary file is given to the subscript by the variable %BBOX_FILELIST%.

The temporary file can be used as file list and referred to by an Enterprise Backup command in the sub- script.

When the parameter BBOX_GENERATED_LINE is present, the temporary file contains an Enterprise Backup command per file to process. This file is to be used as the standard input of the Enterprise Backup client in the subscript.

When the subscript ends, the script manager accesses all the files processed in the subscript. The file existence and Archive Bit setting indicate whether or not the file was processed correctly. Files not processed correctly are kept in queue on a file-per-file basis for subsequent retry.

The script controller sends messages to the NonStop EMS to report execution of subscripts, statistics and retry status.

•••

The script controller runs automatically as a Windows service that is started by either the BBBACKUP or BBRESTORE programs, unless the service is disabled in the Windows Services.

All parameters specific to the Script Controller are provided as parameters of the BBBACKUP or BBRESTORE command. The value of global parameters is set by the last startup of BBBACKUP/BBESTORE.

- Sample of Backup script (File-list version):

```
SET BBOX_SCRIPT_RETRY_DELAY=5
SET BBOX_ SCRIPT_ TEMP_ DIR= C:\Bbox\script\temp BBBACKUP QUEUE_ 1 C:\Bbox\script\tsm_archive.cmd
```

Corresponding subscript C:\Bbox\script\tsm_archive.cmd:

```
DSMC ARCHIVE - DELETEFILES -FILELIST=%BBOX_FILELIST%
```

- Sample of Backup script (standard-input-file version):

```
SET BBOX_SCRIPT_RETRY_DELAY=5
SET BBOX_SCRIPT_TEMP_DIR= C:\Bbox\script\temp
SET BBOX_GENERATED_LINE=retrieve-replace=all #file# %BBOX_NEW_DIR%
BBRESTORE QUEUE_2 C:\Bbox\script\tsm_restore.cmd
```

Corresponding subscript "C:\Bbox\script\tsm_restore.cmd":

```
DSMC MACRO %BBOX_FILELIST% <%BBOX_SCRIPT_DIR%\abort_reply.txt
```

BBBACKUP

BBBACKUP sends the backup request to the controller and waits for the BBOX_SCRIPT_TIMEOUT para- meter, for completion of the backup subscript.

When the timeout is reached, BBBACKUP issues an EMS message, even though the backup request is still being processed by the Script Controller.

The Script Controller will process the backup requests on a FIFO basis for each queue.

Syntax:

```
SET  BBOX_SCRIPT_TIMEOUT=<number-of-seconds>

SET BBOX_SUBSCRIPT_TIMEOUT=<number-of-seconds>

SET BBOX_SCRIPT_RETRY_DELAY=<number-of-minutes>

SET  BBOX_SCRIPT_TEMP_DIR=<directory-for-temporary-files>

SET BBOX_SCRIPT_MAX_THREADS=<number-of-concurrent-executors>

SET BBOX_BACKUP_SIZE=<number-of-MB>

SET BBOX_GENERATED_LINE=<Enterprise Backup command> BBBACKUP  <queue-name>  <sub-script-
file-name>
```

Example:

```
SET  BBOX_SCRIPT_RETRY_DELAY=5

SET BBOX_SCRIPT_TEMP_DIR=C:\BBOX_B2PHASE2\script\temp

SET BBOX_SCRIPT_MAX_THREADS=1
BBBACKUP.exe MyQueue C:\BBOX\script\sub_backup.cmd
```

Parameters:

BBOX_SCRIPT_TIMEOUT

Number of seconds.

After this interval, BBBACKUP stops waiting for the completion of the backup and returns the control to the VTC Emulator. All values here are express in seconds.

Default value is 86400 (24 hours)

BBOX_SUBSCRIPT_TIMEOUT

Number of seconds.

The Script Controller will cancel a sub-script that lasts more than this time. Default value is 86400 (24 hours).

BBOX_SCRIPT_RETRY_DELAY

Number of minutes.

Artificial time delay between a failure and a retry. Default value is 10.

BBOX_SCRIPT_TEMP_DIR

Windows directory used to create temporary files. Default value is current directory.

BBOX_SCRIPT_MAX_THREADS

Number of concurrent threads per queue. Default value is 1.

BBOX_BACKUP_SIZE

Number of MBs.

Maximum total size of Windows files to process in a single subscript execution. The goal is only to avoid extraordinarily long script executions.

Default value is 102400 (28 hours).

BBOX_GENERATED_LINE

Pattern for the Enterprise Backup command line to back up a file.

Use #file# as a placeholder in the command pattern for the name of the file to backup.

Windows variables set by the VTC for the regular backup script are available, e.g. %BBOX_DOMAIN%. Windows parameters that vary for each virtual volume must be not used, e.g. %BBOX_VOLUME%. Default value is #file#, to produces a file-list.

<queue-name>

User defined queue name. No default value.

<sub-script-file-name>

Subscript name to be started by the Script Controller.

No default value.

BBRESTORE

BBRESTORE sends the restore request to the controller and waits for to the timeout. The restore sub- script completes after the timeout is over.

In a given queue, the Script Controller will process the requests in FIFO sequence, until the parameter BBOX_SCRIPT_SORT_MAX_DELAY number-of-minutes are specified. This parameter ensures that the files are restored in the same sequence that they were backed up in, in order to minimize repositioning on the physical media.

Restoring the files in the sequence they were backed-up in can be very inefficient for unrelated and con- current restore requests. For this reason, the request sort order is limited by the BBOX_SCRIPT_SORT_ MAX_DELAY number-of-minutes. Only recent requests initiated during the specified value of this para- meter, will be sorted by backup time.

If the variables % BBOX_SCRIPT_BK_SOFTWARE% are set, the controller will query the Enterprise Backup server to know the label of the physical media containing the backup of files.

The controller will then adjust the sequence of restores to minimize the media unload/reloads. If several threads are configured, each thread will be specially configured so that it is possible to achieve restore from a specific media label.

To check the success of a restore, the Script Controller does not test the return code of the sub-script; it rather checks that the Windows files have been created.

Syntax:

```
SET  BBOX_SCRIPT_TIMEOUT=<number-of-seconds>

SET BBOX_SUBSCRIPT_TIMEOUT=<number-of-seconds> SET BBOX_SCRIPT_BK_SOFTWARE=TSM

SET BBOX_SCRIPT_BK_SOFTWARE_USER=<user-id> SET BBOX_SCRIPT_BK_SOFTWARE_PSWD=<password>

SET  BBOX_SCRIPT_RETRY_DELAY=<number-of-minutes>

SET BBOX_SCRIPT_TEMP_DIR=<directory-for-temporary-files> SET BBOX_TSM_CURLY_BRACKETS {ON|

OFF}

SET BBOX_SCRIPT_MAX_THREADS=<number-of-concurrent-executors> SET
```

```
BBOX_SCRIPT_SORT_MAX_DELAY number-of-minutes

SET BBOX_GENERATED_LINE=<Enterprise Backup command> BBRESTORE <queue-name> <sub-script-
file-name>
```

Example:

```
SET BBOX_SCRIPT_TIMEOUT=36000 SET BBOX_SCRIPT_RETRY_DELAY=5

SET BBOX_SCRIPT_TEMP_DIR=C:\BBOX\script\temp SET BBOX_SCRIPT_MAX_THREADS=1

BBRESTORE MyQueue C:\BBOX\script\sub_restore.cmd
```

Parameters:

BBOX_SCRIPT_BK_SOFTWARE

Software identifier.

Type of Enterprise backup software run by the sub-script. Used for querying the backup server and optimizing the restore.

No default value. Should be set to TSM or omitted.

BBOX_SCRIPT_BK_SOFTWARE_USER

Client user-id used to login to the Enterprise Backup server. No default value.

BBOX_SCRIPT_BK_SOFTWARE_ PSWD

Password used to login to the Enterprise Backup server. No default value.

BBOX_SCRIPT_TIMEOUT

Number of seconds.

After this time interval, BBBACKUP stops waiting for the completion of the backup and returns the control to the VTC Emulator.

Default value is 86400 (=24 hours).

BBOX_SUBSCRIPT_TIMEOUT

Number of seconds.

The Script Controller will cancel a sub-script that lasts more than this amount time. Default value is 86400 seconds (= 24 hours)

BBOX_SCRIPT_RETRY_DELAY

Number of minutes

Artificial delay waited between a failure and a retry. Default value is 10 seconds.

BBOX_SCRIPT_TEMP_DIR

Windows directory used to create temporary files. Default value is current directory.

BBOX_SCRIPT_MAX_THREADS

Number of concurrent threads per queue Default value is 1 second.

BBOX_BACKUP_SIZE

Number of MBs.

Maximum total size of Windows files to process in a single sub-script execution. The goal is only to avoid extraordinary long script executions.

Default value is 102400 seconds.

BBOX_SCRIPT_SORT_MAX_DELAY

Number of minutes.

The controller will alter the execution sequence of requests still waiting in queue and initiated recently, i.e. initiated in the last specified number of minutes.

Default value is 0 minutes.

BBOX_TSM_CURLY_BRACKETS ON | OFF

This is for special cases where the TSM needs clues to interpret the original backed up or archived file name, in order to identify the original node and file space. Without curly brackets, the TSM symptom is "archive / backup not found". The presence of curly brackets is not an inconvenience, even if they are not needed.

This parameter should be used as a second choice solution when several archives / backups are present in the TSM server, but not retrieved by the regular TSM dsmc command. Contacting IBM support is recommended, in order to avoid using this parameter as much as possible.

Sample TSM command without BBOX_TSM_CURLY_BRACKETS:

```
retrieve -PRESERVEPATH=none -replace=all

\\192.168.15.85\SHARE1\WITH BLANK\LBVTW001.IND

\\192.168.15.79\SHARE2\WITH BLANK\\
```

TSM command modified by BBOX_TSM_CURLY_BRACKETS ON:

```
retrieve -PRESERVEPATH=none -replace=all

{\\192.168.15.85\SHARE1}\WITH BLANK\LBVTW001.IND

\\192.168.15.79\SHARE2\WITH BLANK\\
```

Default value is OFF.

BBOX_GENERATED_LINE

Command pattern for the Enterprise Backup command line client to restore a file.

Use #file# as a placeholder in the command pattern, for the name of the file to restore. Windows variables set by the VTC for the regular restore script are available (%BBOX_DOMAIN%,

%BBOX_NEW_DIR%).

Windows parameters that vary for each virtual volume, must be not used (%BBOX_VOLUME%). Default value is #file#, to produce a file-list.

<queue-name>

User defined queue name.

No default value.

<sub-script-file-name>

Subscript name to be started by the Script Controller. No default value.

APPENDIX M - DISASTER RECOVERY SCENARIO FOR DATASTORE QORESTOR

Use the information in this Appendix to set up the environment for NonStop recovery purposes, in case the main system (local NonStop node) crashes and data needs to be recovered right away from a secondary system (DR NonStop node).

NonStop Systems:

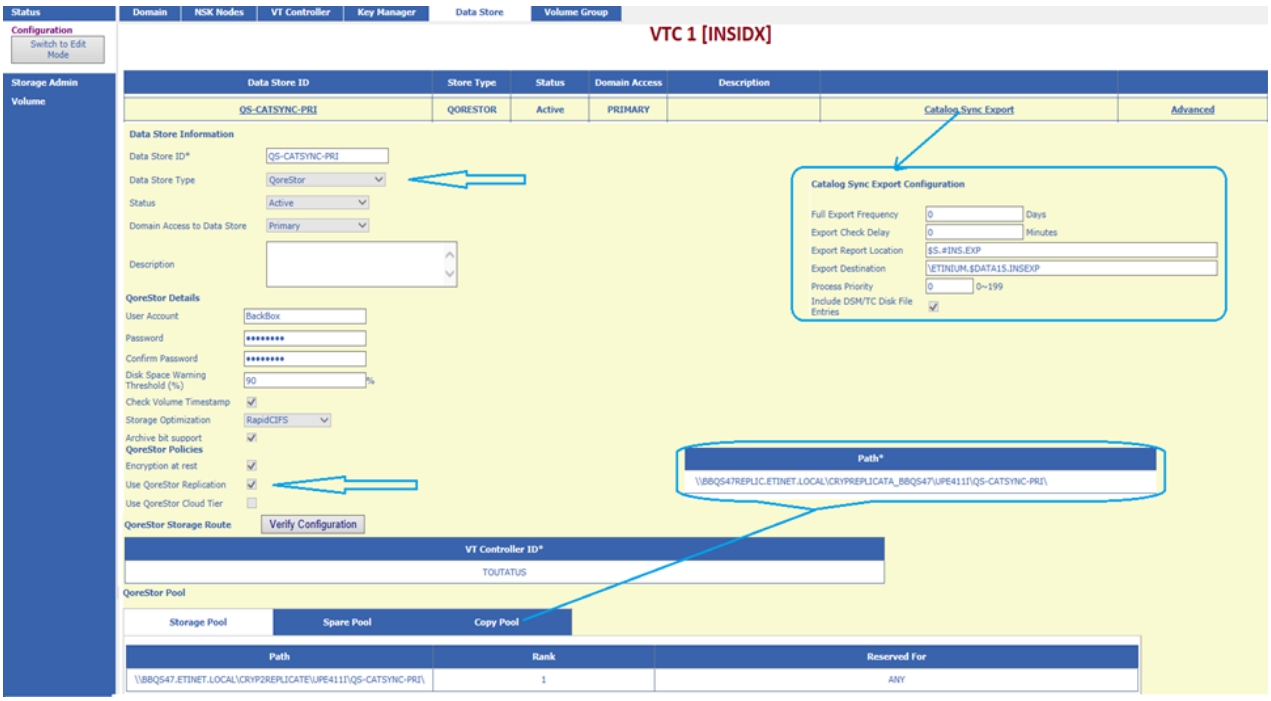
- Primary [local NonStop node]
- Secondary [DR NonStop node]

SETUP

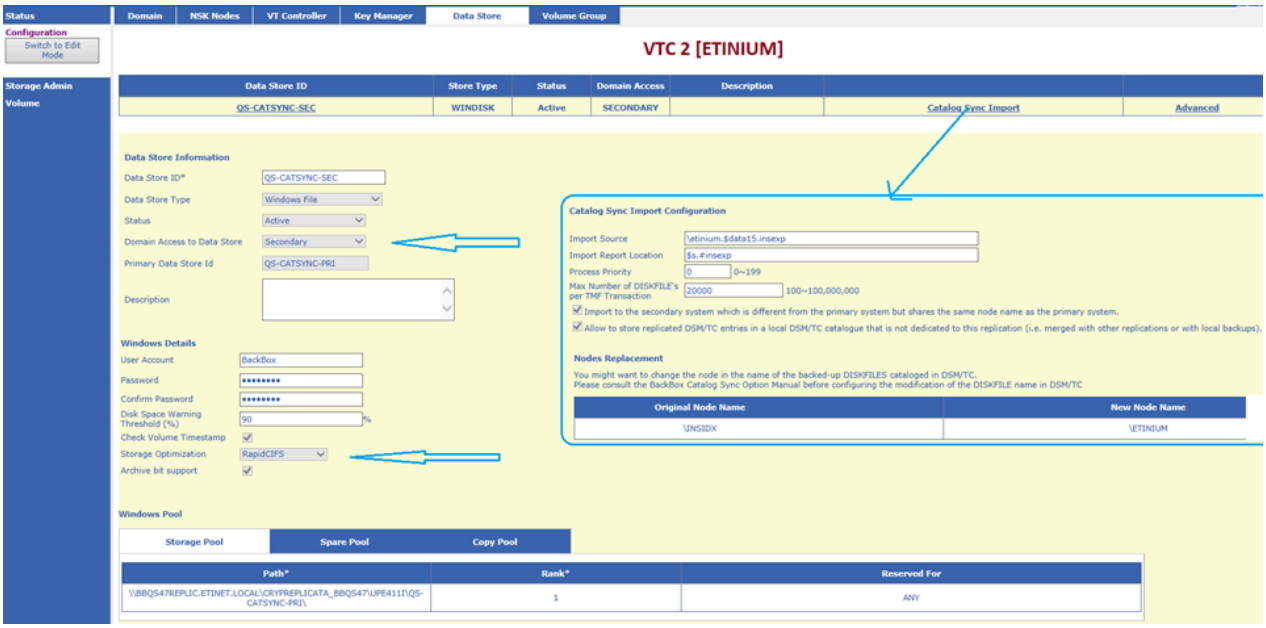
1. Setup two systems:

- VTC1 Primary [local NonStop node] with QoreStor Replication
- VTC2 Secondary [DR NonStop node] with Win-Store

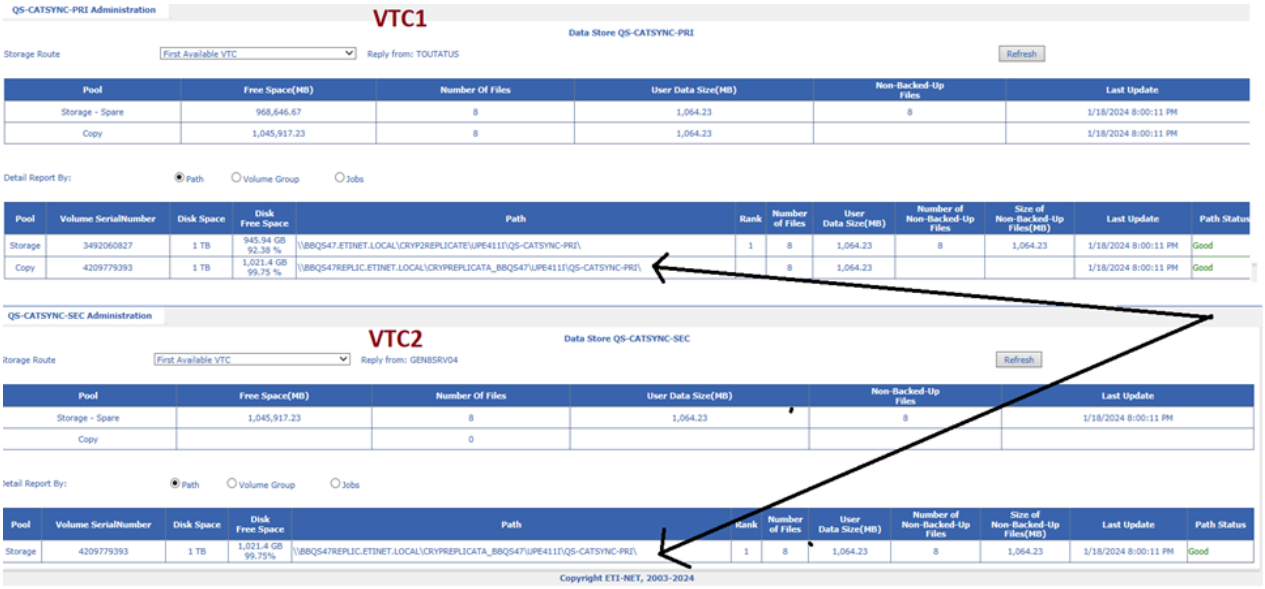
2. Configure Data Store[QoreStor] with QoreStor Replication in system VTC1 Primary [local NonStop node]



3. Set up Data Store [Windows File] in VTC2 Secondary [DR NonStop node].



⚠	The Storage Optimization = RapidCIFS Storage Pool path for [SECONDARY] = Copy Pool path of QoreStor for [PRIMARY]



4. Check the export/import results.

```
UPE411I-BB051 -  CatSync Export/Import process \INSIDX.$S5V3   2024-01-23 21:39

UPE411I-W3162 Domain license will expire on 2024-01-30.
Data store   : QS-CATSYNC-PRI -
Process type          : EXPORT FULL catalogs
DSM/TC disk files     : included
Export id             : 2024-01-23_21:39:01
Export destination    : \ETINIUM.$DATA15.INSEXP

Volume   Group                    Catalog status
------   ------                   ---------------

CATPR1   VG-QS-CATSYNC-PRI        ASSIGNED   QSCATA, gen=4
CATPR2   VG-QS-CATSYNC-PRI        ASSIGNED   QSCATA, gen=5
CATPR3   VG-QS-CATSYNC-PRI        ASSIGNED   QSCATA, gen=6
CATPR4   VG-QS-CATSYNC-PRI        ASSIGNED   QSCATA, gen=7
CATPR5   VG-QS-CATSYNC-PRI        ASSIGNED   QSCATA, gen=0
CATPR6   VG-QS-CATSYNC-PRI        ASSIGNED   QSCATA, gen=9
CATPR7   VG-QS-CATSYNC-PRI        ASSIGNED   QSCATA, gen=1
CATPR8   VG-QS-CATSYNC-PRI        ASSIGNED   QSCATA, gen=2
CATPR9   VG-QS-CATSYNC-PRI        ASSIGNED   QSCATA, gen=3


Volume group          NSK primary catalog (pool name)          Number of   Nbr DSM/TC
                      Most recently written volume               volumes   disk files
------------          ------------------------------           --------   ----------

VG-QS-CATSYNC-PRI     DSM/TC volcat \INSIDX.YINGTEST_VOLCAT, pool QS_CATSYNC_PRI
                      CATPR6 unloaded on 2024-01-23 21:37:34           9           0

UPE411I-I3279 \INSIDX.$S5V3 exported FULL catalogs for data store
QS-CATSYNC-PRI (9 volumes processed). Report in $S.#INS.EXP

UPE411I-BB051 Process \INSIDX.$S5V3 ended on  2024-01-23 21:39
$ETINET YINGQC 18>
```

5. For full or Update Export/Import and manual preparation of BBDBM, follow the procedure in the BackBox Catalog Sync Option document.

For more details regarding Catalog Sync customized environments and settings, contact ETI-NET Support.