

BackBox[©] E5.00 Virtual Installation Guide

Abstract

This Virtual Installation Guide document is for $BackBox^{\odot}$ E5.00

Published: May 2025



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

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

Introduction	. 4
Virtual Machine Requirements	. 5
BackBox Software	. 6
TCP/IP Connection	. 7
PowerShell Execution Policy	. 8
Install Additional Roles and Features	. 9
Server Preparation	12
Virtual Server Naming	12
System Settings	13
Remote Desktop	13
Remote Desktop Session Host Configuration	14
Windows Update	15
Advanced Sharing Settings	15
Firewall Settings	16
VTC Management Concolo	1/
SCEINada	10
Iscal the Virtual Tape Controller Software	10 21
Customize Server Identity	23
License Bequest	24
Start Services	26
Connect Virtual Tape Device to Virtual NonStop System	27
Install BackBox UI Client	28
Atto HBA Target Mode in VMWare ESXi Passthrough Mode	29

This guide documents the preparation of 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.

Virtual Machine Requirements

The following minimum specifications are required to install and use a Virtual BackBox (vBB).



Atto Fiber card in passthrough mode is supported only with VMware ESXi. In this case, vBackBox must remain attached to this ESXi hypervisor host.

2 Cores (or 2 Core per physical Atto port assigned to the VM)
8 Gb of memory (add extra 4 Gb for each Atto port assigned to the VM up to 32 Gb)
250 Gb Hard Drive
2, 10 Gb Ethernet card (one for iSCSI and one to access the storage)

Windows Server Standard 2022, 2019 or 2016.

BackBox Software

Get the latest released software version package and upload it to the newly created virtual machine.



The package for the virtual machine contains the same folders as for the regular BackBox.

Δ
<u> </u>

Upload the binary file (ex: BBE) and the macro text file INSE in a sub-volume different from the current BackBox sub-volume.

Folder Installation Package Latest Released Version	Content
Guardian-E05.00-20241201	Latest BackBox Guardian Software
UI-E05.00.8	Installer for the BackBox UI Client
VTC-E05.00.23	Installer for the VTC application
ServerScripts-20241126	PowerShell installation scripts required for upgrade or new installation
AttoCelerityFC-20241114	Latest (required) AttoCelerity version, if necessary

Fiber Channel (FC) Type	ATTO Driver Version
FC-8	2.130.4001.6000
FC-16 FC-32 FC-64	2.100.4001.6000

TCP/IP Connection

Connect the TCP/IP cable to the appropriate Network adapter and configure TCP/IP according to the following Guidelines:

GUIDELINES

Assign a fixed TCP/IP address (do not use DHCP to obtain the address) according to customer's specification.

Make sure that the IP routing allows communications between the VTC and the NonStop server, between the VTC and the operator/installer workstation.

Make sure the server is registered into the DNS or the Host file, if you plan to use the host name to reach the VTC.

Virtual NonStop must have a second adapter configured on a storage CLIM. This adapter must be able to reach the public LAN on which the vBB is installed.

If ATTO Fiber HBA will be used in passthrough mode, you must configure the ESXi passthrough and assign physical port to the VM. Install the Atto driver prior to running PowerShell VTCServerPreparation.ps1 script. Refer to <u>Atto</u> <u>HBA Target Mode in VMWare ESXi Passthrough Mode</u>section for more details.

PowerShell Execution Policy

While logged as local administrator, start a PowerShell command window and type the following command to allow script execution:

Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope LocalMachine

Answer Yes [Y]

Ensure the policy is in force: Get-ExecutionPolicy -List

Scope	ExecutionPolicy
MachinePolicy	Undefined
UserPolicy	Undefined
Process	Undefined
CurrentUser	Undefined
LocalMachine	RemoteSigned

Keep all default roles and features enabled by the Windows Server Standard edition (Desktop experience or Core installation) used for the operating system installation.

• The BackBox software requires an additional feature called Message Queuing Server (MSMQ-Server), that is automatically installed by the VTCServerPreparation PowerShell script (in case it hasn't been already installed).



Before performing the VTC installation log in with the local Administrator account (Administrator user). Using such an account (with administrator privileges) may require an extra configuration step.



IMPORTANT: If you are using an account with Administrator privileges and not the local Administrator, start PowerShell command line using the Run as Administrator or pre-load macros before running scripts from a PowerShell command line: Import-Module Server Manager.

When using ATTO Fiber Card in Passthrough Mode, ATTO firmware updates will be automatically executed by the VTCServerPreparation script, delivered with the BackBox software package.

In the same folder you unzipped the installation package, locate the VTCServerScripts-yyyymmdd folder, right-click on the file VtcServerPreparation and click on Run with PowerShell (or launch the script from the opened PowerShell command line).

Name		Date modified	Туре		Size
ServerPreparation		3/7/2025 11:21 AM	Text D	ocument	45 KB
VtcServerPreparation		Open		ws PowerSh	47 KB
		Run with PowerShell			
		Edit			
	Ê	Share			
		Open with			
		Give access to	>		
		Restore previous versions			
		Send to	>		
		Cut			
		Сору			
		Create shortcut			
		Delete			
		Rename			
		Properties			
Open File - Security Warning				×	

this file	Name: Type:	\ServerScripts-20241126\VtcServerPreparation.ps1 Windows PowerShell Script
	FIOM.	Open Cancel
8	This file is ir locations yo file if you tr	a a location outside your local network. Files from ou don't recognize can harm your PC. Only open this ust the location. <u>What's the risk?</u>

Administrator: Windows PowerShell	- 🗆
Preparing Microsoft Windows Server 2022 Standard	
verify if Atto HBA installed	
VTC Enable FC-16, FC-32 or FC-64 Target Mode Registery	
VTC Enabling Target Mode Driver Atto Celerity FC-16, FC-32 or FC-64 needs to be installed, downgraded or upgraded to version 2.100	.4001.6000.
Start Installation	
46% For a second	
Foregreenergenergenergenergenergenergener	
VTC Server MS SChannel TLS configuration	
TLS 1.2 has been enabled (Server reboot required) Configure .NET applications to use TLS 1.2 TLS 1.2 has been enabled for .NET applications (Server reboot required) Disabled weak TLS protocols TLS 1.0 has been disabled (Server reboot required) Disable weak ciphers and algorithms Protocol TLS_DHE_RSA_WITH_AES_256_CBC_SHA is currently disabled Protocol TLS_RSA_WITH_AES_256_CGC_SHA384 has been disabled (Server reboot required) Protocol TLS_RSA_WITH_AES_256_CGC_SHA256 has been disabled (Server reboot required) Protocol TLS_RSA_WITH_AES_256_CGC_SHA256 has been disabled (Server reboot required) Protocol TLS_RSA_WITH_AES_226C_SHA256 has been disabled (Server reboot required) Protocol TLS_RSA_WITH_AES_226_CGC_SHA256 has been disabled (Server reboot required) Protocol TLS_RSA_WITH_AES_256_CGC_SHA256 has been disabled (Server reboot required) Protocol TLS_RSA_WITH_AES_256_CGC_SHA256 has been disabled (Server reboot required) Protocol TLS_RSA_WITH_AES_256_CGC_SHA256 has been disabled (Server reboot required) Protocol TLS_RSA_WITH_AES_256_CGC_SHA has been disabled (Server reboot required) Protocol TLS_DHE_DSS_WITH_AES_256_CGC_SHA has been disabled (Server reboot required) Protocol TLS_DHE_DSS_WITH_AES_256_CGC_SHA has been disabled (Server reboot required) Protocol TLS_DHE_DSS_WITH_AES_286_CSHA256 is currently disabled Protocol TLS_DHE_DSS_WITH_AES_286_CSHA is currently disabled Protocol TLS_DHE_DSS_WITH_AES_286_CSHA is currently disabled Protocol TLS_DHE_DSS_WITH_AES_286_CSHA is currently disabled Protocol TLS_RA_WITH_RC4_128_SHA is currently disabled Protocol TLS_RSA_WITH_RC4_128_SHA is currently disabled Protocol TLS_RSA_WITH_RC4_128_SHA is currently disabled Protocol TLS_RSA_WITH_RC4_128_SHA is currently disabled	



Click Y in the PowerShell to restart the server.

Reboot the server.

Some features will require rebooting the server. Re-execute this script until it shows there is no more feature needed to be installed (no red message in the PowerShell).



The server preparation script creates a specific log file in the script folder location: ServerPreparation.log. The transcript of each execution will be automatically logged into this file.

ServerPreparation - Notepad			- 0	×
File Edit Format View Help				
<pre>Windows Powershell transcript start Start time: 20250305141909 Username: KRAKEN\Administrator RunAs User: KRAKEN\Administrator Machine: KRAKEN (Microsoft Windows NT 10.0.14393.0) Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -Command it Process ID: 4180 PSVersion: 5.1.14393.6343 PSEdition: Desktop PSCompatibleVersion: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.14393.6343 BuildVersion: 10.0.14393.6343 CLRVersion: 4.0.30319.42000 WSManStackVersion: 3.0 PSRemotingProtocolVersion: 2.3 SerializationVersion: 1.1.0.1</pre>	F((Get-ExecutionPol:	icy) -ne 'AllSigned	') { Set-E	žxecu.
Transcript started, output file is Microsoft.PowerShell.Core\FileSystem::\\etifps01.eti Server Preparation 5.0.10 Created 2025-01-03	inet.local\DFS\Data	\Projects\BACKBOX\De	livery\CD	H5.0
Preparing Microsoft Windows Server 2016 Datacenter				
Verify if Atto HBA installed				
VTC Enable FC-8 Target Mode Registery				
VTC FC-8 Target Mode was already configured				
٢				>
	Ln 1, Col 1	100% Windows (CRLF)	UTF-8 with	BOM

Update the server with all critical updates recommended by Microsoft. Finalize the server configuration according to corporate standards. This usually includes an anti-virus installation.

As the vBB is a dedicated server, its configuration must be compatible with the BackBox application software and the server access must be restricted to the server manager.

Virtual Server Naming

It is important to name carefully the virtual server, as vBackBox software uses part of that name to generate the virtual tape device serial number. The last three (3) alphanumeric characters of the given name are included in the auto-generated serial number. For example, a vBackBox named vBBOX-1 will show devices with the following serial number: BBOX1100, BBOX1101 and BBOX1102. The serial number always begins with BB followed by the three (3) alphanumeric characters taken from the VBackBox given name, followed by the adapter number (starting at 1), then by a target number.

In a multiple vBackBox environment, it is important to name the server in such a way as to ensure uniqueness in virtual devices serial number.

System Settings

Remote Desktop

Remote Desktop should be enabled to help server management.

To enable Remote Desktop:

Press Start Select Settings Select Remote Desktop

← Settings			-	
ŵ Home	Remote Desktop			
Find a setting	Remote Desktop lets you connect to and control this PC device by using a Remote Desktop client (available for W Android, iOS and macOS). You'll be able to work from an if you were working directly on this PC.	from a remote indows, other device as		
🖵 Display	Enable Remote Desktop			
4)) Sound	On Keep my PC awake for connections when it is plugged in	Show settings		
LJ Notifications & actions				
J Focus assist	 Make my PC discoverable on private networks to enable automatic connection from a remote device 	Show settings		
O Power & sleep	Advanced settings			
□ Storage	How to connect to this PC			
🕢 Tablet	Use this PC name to connect from your remote device:			
H Multitasking	WIN-H8996K5MP9A			
Projecting to this PC	Don't have a Remote Desktop client on your remote devi	ice?		
✓ Remote Desktop	User accounts			
① About	Select users that can remotely access this PC			

Enable Remote Desktop - On



In case of a first-time configuration of the Remote Desktop – or if it needs to be re-enabled - a warning message will pop up. Enable the Firewall exception.

To enable the Firewall exception:

- Press Start
- Select Control Panel
- Select System and Security
- Under Windows Firewall, select Allow a program through Windows Firewall
- Scroll down to Remote Desktop and check the checkbox. Also check desired interface Domain, Private and Public check boxes

Allow apps to communicate through Windows Defender Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Allowed apps and features:				
Name	Pi	rivate	Public	^
■Message Queuing		¥	¥	
⊠Microsoft Edge				
^{II} Microsoft Media Foundation Network Source				
⊠Narrator			×	
□Netlogon Service				
^{III} Network Discovery				
Performance Logs and Alerts				
Remote Desktop			Ø	
Remote Desktop (WebSocket)				
Remote Event Log Management				
Remote Event Monitor				
Remote Scheduled Tasks Management				
BRemote Service Management				v
	Details		Remove	
	Allo	w anot	ther app)

After opening the firewall, the warning message disappears from the Remote tab in the System Properties.

Remote Desktop Session Host Configuration

If two users attempt to perform a remote session using the same user credentials, the second user login session will be force-logged out by the first logged-in user's session. If there are two different users, who need to work on the same VTC using the same user's credentials, this restriction policy must be disabled in order to allow them to be connected in the same time.

To disable one user per session restriction policy:

- Press Start
- Type in the search dialog box gpedit.msc and start the program
- Navigate to: Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections

Change settings

- Locate the Restrict Remote Desktop Services users to a single Remote Desktop Services session setting
- To edit the setting, double click on it and a dialog box will appear
- Check Disabled.
- Apply the change and close the dialog by clicking OK

S Local Group Policy Editor			_	×
File Action View Help				
🗢 🔿 🙍 📷 📓 📓 🐨 🛛 🐨				
NetMeeting OneDrive OneDrive			_	1
Online Assistan OOBE Ordine Assistan OOBE Portable Operat Presentation Se Push To Instell Pus	Setting Automatic reconnection Automatic reconnect remotely by using Remote Desktop S. Configure keep-alive connection interval Unit number of connections Suspend user sign-in to complete app registration Set rules for remote control of Remote Desktop Services use. Select RDP transport protocols Select RDP transport protocols Automate start of unitisted programs Turn off Fair Share CPU Scheduling	State Not configured Not configured Not configured Not configured Not configured Not configured Not configured Not configured Not configured Not configured	Comment No No No No No No No No No	¢
Extended Standard				

🌉 Restrict Remote D	esktop Services us	ers to a single Re	mote Desktop Services session			\times
Restrict Remote D	esktop Services u	sers to a single F	Remote Desktop Services session			
Previous Setting	Next Setting					
O Not Configured	Comment:					^
O Enabled						
Disabled						\sim
	Supported on:	At least Windows Server 2003				^
						~
Options:			Help:			
			This policy setting allows you to n Desktop Services session. If you enable this policy setting, u using Remote Desktop Services w session (either active or disconnect leaves the session in a disconnect reconnects to that session at the n If you disable this policy setting, u unlimited simultaneous remote of Desktop Services. If you do not configure this policy not specified at the Group Policy	estrict users to a sing sers who log on rem ill be restricted to a s ted) on that server. ed state, the user aut text logon. isers are allowed to r onnections by using r setting, this policy level.	le Remot notely by ingle If the user tomatical make Remote setting is	e ~
			OK	Cancel	Appl	у

Windows Update

Windows Update feature should be disabled. To do so, set to download update only or just notify updates availability. Update installation should be managed on a case-by-case basis.

This will avoid unexpected server restart while tape activities are in progress.

To setup Windows Update:

Press Start Select Control Panel Select Settings Select Windows Update and disable automatic updates. Refer to organization group policies to disable Windows Update, if they are managed by your organization.

Advanced Sharing Settings

Advanced sharing settings need to be configured to allow server share creation. BackBox Data store is using network share to access NAS or other BackBox data path.

To configure the Advanced Sharing Settings: Press Start Select Control Panel Select Network and Internet Select Network and Sharing Center Select Change advanced sharing Settings

ATTENTION: If VTC server is part of a Workgroup, the Domain profile will not be shown. A new profile Domain will be added and will require to be set when the server joins the Active Directory.

	Private	Public	Domain	ALL Networks
--	---------	--------	--------	-----------------

Network discovery	Turn off	Turn off	Turn off	n/a
File and printer sharing	Turn on	Turn on	Turn on	n/a
Public folder	n/a	n/a	n/a	Turn off

Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Private (current profile)	
Guest or Public	
All Networks	

Public folder sharing

When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders.

Turn on sharing so anyone with network access can read and write files in the Public folders

 Turn off Public folder sharing (people logged on to this computer can still access these folders)

Media streaming

When media streaming is on, people and devices on the network can access pictures, music, and videos on this computer. This computer can also find media on the network.

Choose media streaming options...

Password protected sharing

When password protected sharing is on, only people who have a user account and password on this computer can access shared files, printers attached to this computer, and the Public folders. To give other people access, you must turn off password protected sharing.

Turn on password protected sharing

○ Turn off password protected sharing

Firewall Settings

We recommend enabling ICMP incoming echo request (ping) for troubleshooting purposes or to allow monitoring tools to work properly. By default, ICMP incoming echo request (ping) firewall rules are defined, but disabled. When the server gets the Files Server role installed with the Advanced sharing settings file and printer sharing turned on, ICMP incoming echo request firewall rules are automatically enabled. The server will answer to the ping request. If the server has been prepared following the guidelines provided in this document, this setting is the recommended one. In other cases, the rules can be manually activated by following these steps:

To manually activate ICMP incoming echo request (ping)

- Press Start
- Search for Firewall and Network Protection
- Go to Advanced Settings
- In the left pane and select the Inbound Rules
- Scroll down to File and Printer Sharing (Echo Request) and enable the rule for Private, Public rules and Domain rules if the VTC is under an Active Directory.

File Action View Help 🗢 🄿 🙍 📅 🔂 🖬 P Windows Defender Firewall with Inbound Rules Inbound Rules Group Name Profile Enabled Action Cutbound Rules Distributed Transaction Coordinator (TCP-In) Distributed Transaction Coo. All No Allow 🌆 Connection Security Rules File and Printer Sharing (Echo Request - ICMPv4-In) File and Printer Sharing (Echo Request - ICMPv4-In) 0 > 🌉 Monitoring 0 Dom Alle File and Printer Sharing 0 Public Allow File and Printer Sharing (Echo Request - ICMPv6-In) 0 File and Printer Sharing Doma Allow Ve File and Printer Sharing (LLMNR-UDP-In) File and Printer Sharing Domai... Allow No Sile and Printer Sharing (LLMNR-UDP-In) File and Printer Sharing Allow Public Yes File and Printer Sharing (NB-Datagram-In) File and Printer Sharing Allow Domai... No 🔮 File and Printer Sharing (NB-Datagram-In) File and Printer Sharing Public Yes Allow Allow File and Printer Sharing (NB-Name-In) File and Printer Sharing Public Yes File and Printer Sharing (NB-Name-In) File and Printer Sharing Domai... No Allow File and Printer Sharing (NB-Session-In) File and Printer Sharing Domai... No Allow 🔮 File and Printer Sharing (NB-Session-In) File and Printer Sharing Public Yes Allow File and Printer Sharing (SMB-In) File and Printer Sharing Domai... No Allow 2 File and Printer Sharing (SMB-In) File and Printer Sharing Public Yes Allow File and Printer Sharing (Spooler Service - RPC) Allow File and Printer Sharing Public Yes File and Printer Sharing (Spooler Service - RPC) File and Printer Sharing Allow Domai... No File and Printer Sharing (Spooler Service - RPC-EPM... File and Printer Sharing Domai... No Allow File and Printer Sharing (Spooler Service - RPC-EPM... File and Printer Sharing Public Yes Allow File and Printer Sharing (SMB-QUIC-In) File and Printer Sharing over... All No Allow File and Printer Sharing over SMBDirect (iWARP-In) File and Printer Sharing over... All No Allow iSCSI Service (TCP-In) iSCSI Service All Allow No Key Management Service (TCP-In) Key Management Service All Allow No mDNS 🔮 mDNS (UDP-In) Public Yes Allow Allow 🔮 mDNS (UDP-In) mDNS Private Yes 🔮 mDNS (UDP-In) mDNS Domain Yes Allow 🥑 Message Queuing TCP Inbound Message Queuing All Yes Allow 🔮 Message Queuing UDP Inbound Message Queuing All Yes Allow Microsoft Edge (mDNS-In) Microsoft Edge All Allow Yes 🔮 Microsoft Media Foundation Network Source IN [TC... Microsoft Media Foundatio... All Yes Allow 🔮 Microsoft Media Foundation Network Source IN [U... Microsoft Media Foundatio... All Yes Allow Netlogon Service (NP-In) Netlogon Service All No Allow >

Domain Node

Add all Domain profile for each NonStop node be connected to the vBackBox.



VTC Management Console

VTC EMULATOR (ISCSI)



These settings must 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.

WIN-H8996K5MP9A	VTC Emulator (ISCSI) Settings Properties	
VTC Admin VTC Emulator (FC) VTC Emulator (ISCSI) VTC Asynclog	Common IP Port Deynostic Device No Write Enable LARGEBLOCKS Mode Trace Level	8767 False True O
License Scripting ✓ VTC Admin ✓ VTC Admin ✓ VTC Emulator (FC) ✓ VTC Emulator (ISCS1) Security Domains ← FC ← ISCSI		
	Device No Write	

A 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 require restarting the services.

iSCSI Node

All VTC iSCSI configurations are grouped under the iSCSI category node. Changing any of the elements described below requires restarting services.

When the iSCSI category node is selected, no information is shown in the right-hand panel.

ISCSI CONFIGURATION

- 1. Configuration of the iSCSI is done through the VTC Management Console.
- 2. Add the NIC address to be used to connect with the Storage CLIM.
- 3. Provision virtual tape devices under the selected NIC address and several NIC addresses can be added. The virtual tape devices will need to be deployed across these NIC addresses.
- 4. Open the VTC Management Console and follow the procedure to add the iSCSI devices:
- 5. Right-click on the iSCSI node in the VTC Management Console and click Add to display the iSCSI device creation box.

VTC Admin			
VTC Script Controller			
E Settings			
🏠 License			
Scripting			
VTC Admin	Add iSCSI Targets	× Add iSCSI Targets	×
VTC Emulator (FC)			
VTC Emulator (ISCSI)	Port	Port	
Security	192.168.31.50 (UP)	✓ 192.168.31.50 (UP) ✓]
Domains	192.168.31.50 (UP)		ʻ (
	192.168.32.51 (UP) 192.168.20.236 (UP)	Number of targets you want to generate	
	V V	3	
Delete All Tarriets			
Eg Delete Air largets	Target Type	Target Type	
	V0505 ~	V0505 ~	
	Ok Canc	Ok Cancel	1
ternses (U)	OS	Microsoft Windows Server 2019 Standard	
😥 System	Compatible with	F4.09 and un	
Users	Compatible Mar	24.05 did dp	
to Event Forwarder			
	FC Ports #	5 ISCSI Devices # 5	
E Settings	Encryption Devices #	5	
	Encryption Devices #	5	
Scripting	QoreStor Enabled	True	
L VIC Admin	Oam Day Susters ID	10007054220545700520200406502000	
VIC Admin	Gore Stor System ID	1000/014328141/38320200406102000	
VTC Emulator (FC)			
VTC Emulator (ISCSI)			
Security			
•	v		

- 6. 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.

WIN-H8996K5MP9A\Administrator (Administrator) Save Cancel Disconnect ISCSI ISCSI <t< th=""><th>User</th><th></th><th>Configuration</th><th></th><th></th><th></th></t<>	User		Configuration			
ISCSI	WIN-H8996K5MP9A\Administrator (Administrator)			Save	Cancel	Disconnect
EBP9A100 BBP9A101 BBP9A102	Image: Win-H8996K5MP9A Image: Services Image: Services Image: Services Image: Win-H8996K5MP9A Image: Services Image: Win-H8996K5MP9A Image: Win-H8996K5MP9A	ISCSI Etheme Microso Status MAC Speed	t 2 ft Hyper-V Network A Up 00155D14EF21 10Gbps	Ndapter #2		

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.

User		Configuration			
WIN-H8996K5MP9A\Administrator (Administrator)			Save	Cancel	Disconnect
WIN-H8996K5MP9A	MP9A000 Ip Address Serial Number	192.168.31.50 BBP9A000			
VTC Script Controller Office Settings Domains C FC A ISCSI		Attention: chang problem with the are not sure.	jing serial numbe host. Please ke	r could cause conn ep the defaut value	ection if you
	Target Type	V0505 Attention: chang problem with the are not sure.	ying target type o host. Please ke	ould cause connected to the defaut value	tion if you
	Lun Initiator IP	0 127.0.0.1	this device will	he available to any	
		initiators that que	ery for devices to	o connect to.	

- 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 be changed, 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.

5. Save the configuration or Cancel it.

User	ETINET\dandrasi (Administrator)	Configuration	Save	Cancel
6.	If you want to delete targets, select the target and righ	nt-click on it. Then Delete	2.	

BBKEN000		
Delete	~	

7. Once you have completed the change, restart VTC Services by right clicking on the Services node and selecting the Restart option.

User TECHWRITER\Administrator (Administrator)



Install the Virtual Tape Controller Software

REQUIREMENTS

Administrator account under Windows on the server acting as the VTC.

Install the VTC application from the BackBox distribution package directory VTC-E.nnn: run setup.exe.

Install the latest UI version from the BackBox distribution package directory UI-E.nnn: run setup.exe.

After the installation it is recommended to:

- Reboot the VTC
 The VTC Windows services will start automatically and will issue messages to EMS.
- Verify that the BackBox Windows Services are started Check that both VTC Admin and VTC Virtual Tape Emulator (FC) services report their state to EMS.

DESCRIPTION

In the folder you uploaded the locate the VTC-E5.00 folder. Double-click on Setup.exe and follow the installer instructions.



You will then be prompted to read and accept the license agreement. Click I Agree to proceed with the installation, a complete copy of the license agreement is available at the end of the present document.

🖟 BackBox Virtual Tape Controller E05	.00 Bu	ild 21			-	-		×
	Lic	ense Agreen	nent					
ETIMET	Plea	ase take a moment to "I Agree", then "Nex) read the lic t". Otherwis	cense agreement no e click "Cancel".	w. If you acce	ept the te	erms b	elow,
	Γ	SOFTWARE	ICENSE /	AND MAINTEN	ANCE AGR	EEME	NT	^
BACK BOX.	BEI CLI TO DO PLE AG	FORE BREAKING CKING ON THE ' THE ELECTRON WNLOADING, C ASE READ TH REEMENT ("AG TIONS INDICATE () IDo	THE SEA "ACCEPT" NIC LICEN OPYING, HIS SOFT REEMEN ACCEPT Not Agree	AL ON THE SOF BUTTON, ENTE ISE ACCEPTANC ACCESSING, OF FWARE LICENS T"). ANY OF ANCE OF. AND	TWARE M RING "YES E INQUIR USING T E AND THE AFO LEGALLY	EDIA I Y IN R Y, INS HE SO MAIN REME BINDS	PACK/ ESPO TALLI FTW/ TENA NTIO	AGE, NSE ING, ARE, NCE NED J TO Y
		Cancel		< Back		Next >		

Installation is now ready to start. Click the Next button to initiate the process.

BackBox Virtual Tape Controller E05.	00 Build 21 -		\times
	Select Installation Folder		
\cap	The installer will install BackBox Virtual Tape Controller E05.00 to the fol	lowing folder.	
ETIMET	To install in this folder, click "Next". To install to a different folder, enter it "Browse".	below or clicl	ĸ
	Application Folder:		
	C:\Program Files\ETINET\VTC\	Brows	е
	⊻TC Data Root Folder:		
BACKBOX ®	C:\ProgramData\etinet\	Brows	е
Disk Cost	Cancel < Back Ne	ext >	
🕼 BackBox Virtual Tape Controller E05.	00 Build 21 –		×
	Confirm Installation		
\square	The installer is ready to install BackBox Virtual Tape Controller E05.00 on	your comput	er.
ETIMET	Click "Next" to start the installation.		
BACKBOX。			
	Cancel < Back Net	d>	

BackBox Virtual Tape Controller E05	.00 Build 21 —	×
	Installing BackBox Virtual Tape Controller E05.00	
ETIMET	BackBox Virtual Tape Controller E05.00 is being installed.	
	Please wait	
BACK BOX		
	Cancel < Back Next >	
BackBox Virtual Tape Controller E05.	00 Build 21 —	×
	Installation Complete	
ETIMET	BackBox Virtual Tape Controller E05.00 has been successfully installed.	
	Click "Close" to exit	
BACK <mark>BOX</mark> 。		
	Please use Windows Update to check for any critical updates to the .NET Framework.	
	Cancel < Back Close	

In case the VTC version comes with a patch, the patch is being installed along with the controller and is being mentioned between brackets.

Once the installation process is over, click the Close button. BackBox VTC software is installed, ready to be used.

Customize Server Identity

HOST FILE

Edit the HOSTS file and map the server host name with all alias name to his loopback address. By doing so, you avoid bad DNS hostname resolution to local network resources, when one Ethernet adapter failed or it had network traffic down. This is a configuration requirement for cross-connected VTC pairs. The host file is located in the system folder Windows\System32\drivers\etc\. For example, for a VTC with a server name BBOX1:

localhost name resolution for BBOX1handled within DNS to itself.

127.1.1.1 localhost

127.1.1.1 BBOX1.etinetlab BBOX1.backboxlocal BBOX1

License Request

Iser ASTERIX\Administrator (Administrator)	Configurat	Save	Reload	Disconnect		
ASTEFUX ∧ → Q ⁰ Services ✓ → Q ⁰ VTC Emulator (FC) ✓ → Q ⁰ VTC Endustor (FC) ✓ → Q ⁰ VTC Script Controller ✓ → Q ⁰ Estructures ✓ → Q ⁰ Estructures ✓ → Q Core Stor ✓ → Beplication → → © Loanses (0) → → © System → → © Licenses (0) → → © Settings → → License → → VTC Emulator (FC) ✓ → VTC Emulator (FC) ✓ → VTC Emulator (FC) ✓ → Secutly ✓	Server Information Computer Name AS Domain etin Operating System Mic Server Model IP Server Serial Number MX VTC Software Version E02	TERIX et local rosoft Windows Server 20 ProLiant DL360p Gen8 Q42904X8 5.00.22	019 Standard	Copy To File		

For the license request, go to VTC MC > Server Information > Copy To File...

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.

Request a vBackBox license through the License Desk, using the license information in the file.

ASTERIX.txt - Notepad

File Edit Format View Help Computer Name: ASTERIX Domain: etinet.local Operating System: Microsoft Windows Server 2019 Standard Server Model: HP ProLiant DL360p Gen8 Server Serial Number: MXQ42904XB VTC Software Version: E05.00.22 UUID: 30353837-3139-584D-5134-323930345842

License Number: xxxx0019 License Expiration : 2025-02-25T18:58:43.2290239Z License Creation : 2025-02-11T19:00:42.5473836Z License To: E5056900 Serial Number: MXQ42904XB Hpe Number: Unknown License Type: Emergency Host Name: ASTERIX Release Version: E Software Version: 4.09 Product: Unknown Os Version: Microsoft Windows Server 2019 Standard Number Of FC Ports : 5 Number Of Encryption Devices: 5 Number Of Iscsi Devices: 5 Number Of Devices Per Port : 64 OoreStor Enable: True QoreStor ID: 10007CF4328F4F79852020C4D6FC2CCD

Once you receive the license file (XML format), upload it on the vBackBox and import it. Go to VTC MC, right-click on the License node under Setting and Import.

User WIN-H8996K5MP9A\Administrator (Administrator)	Configu	ration Save	Reload	Disconnect
WIN-H8956K5MP9A	License Information License Number Creation Date License Type Host Name VTC Serial Number HPE Number Server Model OS	Unknown Unknown Unknown Unknown Unknown Unknown Unknown	License To Expiration Date	Unknown Unknown
L ♥ Security - ② Domains - ❖ FC - ❖ ISCSI	Compatible with FC Ports # Encryption Devices # QoreStor Enabled QoreStor System ID	Unknown 0 0 False Unknown	ISCSI Devices #	0

In the pop-up window, browse for the folder the license file has been copied to and click the OK button. In this example the license file has been copied on the Desktop in the folder License.

r TECHWRITER\Administrator (Administrator)	Configuration Save Cancel	Disconnect
TECHWRITER Services VTC Admin VTC Emulator (FC) VTC Annolog VTC Annolog VTC Scipt Controller Scipting VTC Emulator (SCSI) Security Domains FC Scipting VTC Emulator (SCSI) Security Demains FC Scipting VTC Emulator (SCSI) BBTER000 BBTER001 BBTER002 BBTER003 BBTER004 BBTER005	License Information License Number x00011 License To Creation Date 2024-07-04 Expiration Date License Type Emergency Browse For Folder >> Host VTC HPE Serv Serv Com Guardian-E04.13-20240601 ServerScripts-20240614 Com Guardian-E04.13-20240601 ServerScripts-20240614 Com Core Make New Folder OK Cancel	E5056900 2024-07-18

In the License Selection dialog select the license XML file. Click Select and then Save the configuration.

🔜 License Selection	×
Licensexxx0011For2386-9494-0583-5505-3404-5981-83.XML Licensexxx0001For2386-9494-0583-5505-3404-5981-83.XML Licensexxx0010For2386-9494-0583-5505-3404-5981-83.XML Licensexxx0009For2386-9494-0583-5505-3404-5981-83.XML Licensexxx0008For2386-9494-0583-5505-3404-5981-83.XML Licensexxx0007For2386-9494-0583-5505-3404-5981-83.XML Licensexxx0006For2386-9494-0583-5505-3404-5981-83.XML Licensexxx0005For2386-9494-0583-5505-3404-5981-83.XML	
	Cancel Select

ASTERIX\Administrator (Administr	ator)	Contigu	Save	e Cancel	Disconnect	
■ ASTERIX ● -	Licensexxxx0006FG	License Information License Number Creation Date License Type Host Name VTC Serial Number LIDE Mumber	xxxx0019 2025-02-11 Emergency ASTERIX MXQ42904XB Lintercom	License To Expiration Date	E5056900 2025-02-25	
		PC Ports # Encryption Devices # QoreStor Enabled QoreStor System ID	ок 5 True 10007CF4328F4	5CSI Devices #	5	

Start Services

Starting the services finishes the installation of the vBackBox VTC and it makes the system ready for configuration. Validate that all services listed under the Services node are started – marked with a green checkmark. An X icon will be shown in front of the service name, if the service has been stopped.

Virtual tape devices are connected to a virtual NonStop system through the storage CLIM. The CLIMs provisions the network adapter accessible on the corporate LAN (different from the vNonStop maintenance LAN).

The following new commands are available to add and remove iSCSI tape target devices on a CLIM:

-t Or addiscsitape	<iscsi address="" ip="" target=""> Initiates a discovery request to an iSCSI target at the input IP address. Then it logs in to all new targets. The addiscsitape command is only applicable to virtual CLIMs.</iscsi>
deliscsitape	<iscsi name="" target=""> Initiates a logoff request to an iSCSI target at the input iSCSI target name and deletes the target from the database. The deleteiscsitape command is only applicable to virtual CLIMs.</iscsi>

Adding and deleting iSCSi tape devices can be done using the lunmgr utility of a climcmd. A basic add command would look like this: climcmd SCLIM000 lunmgr -t 192.168.30.20

This command would be adding all virtual iSCSI tape devices on the vBackBox located at the IP address **192.168.30.20**.

To install the BackBoxUI Client:

- 1. Open the BackBox distribution set and navigate to the UI-v.vv.vvvv directory.
- 2. Run Setup.exe.
- 3. Launch the UI Client Setup Wizard and follow the steps required to install the application. Click Next.
- 4. Select the installation folder. Use the default folder or browse to install the UI Client to a different folder. If the access to the UI Client must be restricted to the current user, select **Just me**.



It is highly recommended to use no restriction. Choose Everyone to install the UI Client for anyone who may use this computer, especially when installing on a VTC.

- 5. Follow the Wizard installation steps.
- 6. Once the installation is complete, close the Wizard and use BackBox User Interface to connect to each Domain configured.

ENVIRONMENT PREPARATION FOR VM WARE

- Install the physical Atto HBA into the ESXi hypervisor server.
- In the ESXi client, find Atto HBA port and activate the Passthrough mode

vm ESXi Host Cli	ent				root@192.168.2	10.187 • Help • Q Search
Avigator	~	localhost.etinet.local - Manage				
V 🖬 Host		System Hardware Licensing	Packages Services 5	Security & users		
Manage						
Monitor		PCI Devices	Toggle passthrough	h 🖋 Configure SR-IOV 🖋 Hardware label 🖓 🔂 Reboot host 🤇	Refresh	Q Search
~엽 Virtual Machines	1	Power Management	Address 🗸	Description v	SR-IOV 🗸	Passthrough 🗸 Hardware Label 🗸
VBackBox			0000:0b:00.0	ASPEED Technology, Inc. ASPEED Graphics Family	Not capable	Disabled 🔺
Monitor			0000:00:1d.0	Intel Corporation C610/X99 series chipset USB Enhanced Host Controller #1	Not capable	Disabled
More VMs			✓ 0000:81:00.1	ATTO Technology, Inc. Celerity FC-162P	Disabled	Active
Storage Networking	3		✓ 0000:81:00.0	ATTO Technology, Inc. Celerity FC-162P	Disabled	Active
2			0000:82:00.1	QLogic Corp 2600 Series 16Gb Fibre Channel to PCI Express HBA	Not capable	Disabled
			0000-82-00.0	OLINNIC CORN 2600 Series 16Gh Eibre Channel to PCI Evoress HR&	Not canable	Dieablad
			Passthrough capable	×		14 items

• Assign Atto port in the vBackBox VM setting. The VM needs to be shut down. In the setting editor add a new PCI device.

3 ~	~		× × × ×
3 ×	~		× × ×
	~ ~		×××××
	~		×
	~		×
			×
	N 17 Co	annost	
	• •	Jineci	~
	~ 🗆 Co	onnect	×
	~		
		~	×
		~	×
		- 0000:81:00.0 - 0000:81:00.1	- 0000.8100.0 V

• Start the VM. The new ATTO devices are displayed in Device Manager. Install the drivers from the distribution package provided (AttoCelerityFC-yyyymmdd) and resume the server preparation script (VTCServerPreparation.ps1).