BackBox© Security Implementation Best Practices

Abstract

This Security Implementation Best Practices document is for BackBox

Published: June 2024

Legal Notice

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.

Table of Contents

OVERVIEW

This guide provides guidelines and recommendations to implement and deploy various BackBox security features to protect data, backups and migrations. The intended audiences for this document are system security administrators with NonStop background knowledge looking for guidance on secured data best practices at both the system and subsystem level. Guidelines and best practices are provided in order to protect NonStop and storage platforms against malware, viruses and data breaches. For detailed explanations, processes and practices refer to BackBox documentation on HPE Integrity NonStop L-Series | Product Support

DOCUMENTATION AND SECURITY PRODUCTS

The following documents are of particular interest, along with HPE NonStop security overview support references.

BackBox® Tape Encryption Option
BackBox® SSL Setup
BackBox® Messages Manual and Troubleshooting
BackBox® Catalog Sync Option
BackBox® Third Party Components
BackBox® User Guide

SECURITY GUIDELINES

Any document on how to harden a specific platform can only give some general guidelines. To establish your specific NonStop security strategy, work with your internal security groups and auditors to determine your system security requirements and map them against your current configuration and practices to identify gaps. Also factor in recommendations on best practices and security settings from your software providers. When that investigation is reasonably complete, develop a phased remediation plan for tightening controls as identified. You should consult with both your auditors and your internal security group on acceptable phasing. You should regard security hardening as an ongoing project that will require continuing attention and updating.

Regardless of the project and/or organization security practices and general guidelines, all working environments should be up to date (Windows updates, anti-virus platforms and secure connections) in order to ensure systems' performance and to avoid data breaches.

SOFTWARE SECURITY UPDATES

Contact ETI-NET Support or visit ETI-NET Product & Security Updates page for details on the latest software version and/or patch available.

ETI-NET recommends to have all the systems up-to-date. Download and install all Windows updates, especially the Windows security updates.

All BackBox software on NSK nodes of a single domain must be of the same version. To have an operational BackBox application, the following components are required:

- BackBox NSK component (latest available version)
- User Interface (UI) current version
- VTC current version

⚠	Different versions of the NSK software can be installed on the same NSK node, but for different domains and for different VTCs.

For more details on the package components, see Upgrade Procedure > BackBox Upgrade Package.

To keep data and environments protected across all storage systems (including the cloud tier), keep the NSK component, UI and VTC updated at the latest version.

ETI-NET clients are notified when a new version is available and advised to install the most recent released package.

INITIAL SECURITY IMPLEMENTATION

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.

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 User Guide > NonStop Access Authorizations.

Data Store Encryption

Data encryption refers to security methods that encode information and data at different levels. The encrypted data can be decoded only by users having access privileges and/or the right encryption/decryption keys. Encryption keys are usually generated either at the time of encoding or beforehand.

For data stores protection BackBox uses different encryption methods based on encryption algorithms to generate encryption keys and IDs.

All BackBox data stores are automatically encrypted (unless the administrative data store configuration specifies it differently) when set up, along with all the data copies used for replication, backup, restore, etc.

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, the BackBox VTC creates and retrieves the same encryption keys as would a CLIM with VLE.

⚠	For storage subsystems that implement data deduplication, BackBox data encryption SHOULD 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.

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.

For more details, refer to User Guide > Tools > Guardian Tools > OBB038 – LIST OF ENCRYPTED VOLUMES and Tape Encryption Option manual.

3rd Party NonStop Encryption Integration

BackBox supports any 3rd party NonStop encryption component.

For third party NonStop tape encryption solutions, such as TapeSecure, BackBox data encryption should be disabled. Additionally, for storage subsystems that implement data deduplication and encryption, third party tape encryption is NOT RECOMMENDED (since these systems will deliver encryption and users can benefit from data deduplication).

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, the last image of the tape volume is presented to the NonStop host.

Auto-scratch is incompatible with POOL set to APPEND ON.
The auto-scratch mechanism is active for automatic mounts and for manual loads initiated through the Pending Mounts section of the User Interface.

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.

SECURITY CONFIGURATION

Compliance

Various regulatory guidelines require organizations to implement compliance in different ways. For instance, some requirements enforce the separation of duty between the NonStop operator and storage administrator. ETI-NET recommends checking with the assigned compliance officer in order to properly implement user IDs, passwords, and associated system access permissions in line with the organization's compliance requirements.
At the NonStop level, the QoreStor cloud tiering storage and backup-restore-replication actions comply with the 3-2-1 rule: the 3rd copy of data is securely placed to an S3 (cloud) storage location, using different encryption modes.
Data tiering provides the ability to migrate data to the S3 storage location by reducing local QoreStor physical data size and maintaining data pointer reference. Tiered data is thus highly protected by an extra security layer. Moreover, by object locking mechanism, data becomes immutable and unchangeable. When object lock is enabled, data cannot be tempered with, encrypted/decrypted or deleted.

Policies

A security policy is frequently used in conjunction with other types of security operating procedures. The policy defines the main strategy and security stance involved in access protection to certain tools, data, actions.

BackBox integrates different policies that apply to user access, permissions and data manipulation actions.

Data stores are managed by policies that can be defined when configuring the setting-up rules.

Backup, replication, cloud tiering, data containers, configuration options and certificates are all controlled by policies.

For more details, see User Guide>QoreStor Data Store> Replication, User Guide>QoreStor Data Store>Cloud Tiering, and User Guide>Configuration>Domain Network>Network Configuration,

A Data Store can be defined 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 the cloud policies are enabled, 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.
For more details, see User Guide>QoreStor Data Store> DataStore Managed by Policies and User Guide > VTC Management Console > Cloud Tier

User Management

There are 2 main types of BabckBox users, administrator and operator, both with different security levels definition. For more details refer to User Guide> User Interface> User Management and User Guide>VTC Management Console> Users.

To add and/or edit users security permissions and capabilities see details in the User Guide> User Interface> User Management>Settings>Security.

Users/ Owner Identity

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

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 writ- ten for a new backup.

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.

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.

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.

For more details, see User Guide>VTC Management Console

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.

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

Secured Files - VTC-based

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.

For details, refer to User Guide> Configuration>Data Store>File Access Authorizations and User Guide> Configuration>Data Store>Data on the NonStop Servers

Secured Data Stores

Data Stores are password-protected to ensure secure access to data. The password gives the user log-in access to the server.

For details, refer to User Guide> User Interface > Data Store.

License Files - VTC/NonStop Linceses

License files are provided by the ETI-NET representative. The license is in a .dlv format (DLV File).

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.

On the User Interface, the license details (license key, expiration, type of license, etc.) are displayed on the Configuration page under Domain tab. For details, refer to User Guide> User Interface > Configuration>Domain.

On the VTC Management Console, the right-hand panel displays the license ID, licensing starting date, description, license number and type, host name details, FC ports, iSCSI devices connected and system
ID and the storage capacity associated with the license. For details, refer to User Guide>VTC Management Console > Licenses.

For new licenses, see User Guide>VTC Management Console >Settings > License.

The license file received has to be uploaded on the NonStop in binary mode. peripheral node is controlled and managed by its own peripheral node license. Licenses are available upon request. Contact HPE License Desk for peripheral node license request.

ACCESS RESTRICTIONS AND PRIVILEGIES

Restricted Data Stores

A Restricted Data Store is a view of a Data Store owned by another domain. Restricted Data Store provides read access to virtual volumes owned by another 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.

To set up a restricted Data Store in a domain, refer to User Guide> Additional Functionalities > Device Reservation > Restricted Data Stores

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

A data store can be configured for simultaneous access by: a single PRIMARY domain and/or one or several RESTRICTED domains.

Restricted Users

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.

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.

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

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.

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.

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.

For more details, see User Guide > NonStop Access Authorizations and VTC Server Installation > Server Preparation > Install Additional Roles and Features.

SECURE TRANSPORT CONIGURATION

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.

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

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.

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 about SSL configuration and setup, see SSL Setup manual.