FALCONSTOR

FalconStor StorSafe VTL

Security Specifications

Introduction

FalconStor® StorSafe® VTL is a software solution that can run in the cloud, on physical servers, and virtual machines. The virtual tape library (VTL) solution works with any leading backup software, emulating physical tape drives and libraries while shrinking backup images with advanced compression and patented deduplication. StorSafe VTL includes StorSight®, a central management tool, that allows easy management of any number of StorSafe VTL instances running across on-premises, cloud, and hybrid cloud environments.

This document describes the security features of StorSafe VTL, including:

- General security guidelines
- Operating system (OS) security
- Software product security, covering authentication, communication, and network traffic encryption
- Password management
- Data security, covering data encryption, data structure, Write-Once-Read-Many (WORM) tapes, immutable Cloud Object Storage (COS), tape shredding, and data isolation for multi-tenancy
- Event logging

General Security Guidelines

FalconStor recommends the following general guidelines to ensure security for StorSafe VTL:

- Apply only OS patches certified by FalconStor.
- Do not open any unnecessary communication ports.
- Do not install any unauthorized software.

OS Security

OS Packaging

The FalconStor software image contains a scaled down version of the Linux OS, which contains only required packages. Only a subset of Linux support modules is included to keep unneeded services from being available for malicious entry points.

The hardening of OS packaging is a controlled process and does not use an automated update program, such as yum, in order to avoid adding or updating unnecessary files.

OS Security Options

The following security options are available during installation:

1. The OS GRUB (Grand Unified Bootloader) security feature allows setting a password so users cannot edit any grub entries or pass arguments to the kernel from the grub command line without entering the password.

2. The Linux Audit framework can log system calls, such as opening a file, killing a process, or creating a network connection. These audit logs can be used to monitor systems for suspicious activity.

3. The Linux Advanced Intrusion Detection Environment (AIDE) can be configured with predefined rules to check the integrity of files and directories in the Linux OS.

4. The OpenSCAP scanner packages are included for the Security Content Automation Protocol (SCAP). SCAP content is based on Security Technical Implementation Guide (STIG) published by the Department of Defense Cyber Exchange (DoD), which is sponsored by the Defense Information Systems Agency (DISA). It contains guidance on how to configure systems to defend against potential threats. The OpenSCAP scanner can be regularly run in order to apply required fixes and bring the system to a compliant state.

Software Product Security

The following measures are taken in order to maintain a high level of security at the product software usage level:

Authentication

- Linux secure login with shadow passwords is used to access the server terminal console.
- Remote SSH access is disabled for the *root* user account on the StorSight management server and StorSafe VTL in the cloud.
- A shared secret mechanism based on the Diffie-Hellman algorithm is used for authentication between:
    - source and replica servers
    - management console and server
    - host clients and server

  Diffie-Hellman key exchange sets a shared secret of 48 bytes between primary and target components. When a communication session starts, the primary authenticates itself with the target and generates two symmetric keys following the TLS 1.2 standard, one for sending and one for receiving data.
- StorSafe VTL network-attached storage (NAS) feature provides two security modes to authenticate users/groups trying to access NAS shares:

    1. Domain mode where authentication is controlled by a Windows Active Directory Domain Controller; POSIX Access Control Lists (ACLs) can be set on files and folders
    2. User mode where authentication is controlled by passwords that are set for each Windows user
- StorSight uses the Spring framework where the security module is a flexible and powerful authentication and access control framework to secure Spring-based Java web application.
- StorSight offers the option to use an Active Directory or LDAP server for authenticating and authorizing users.
- StorSight offers the Multi-Factor Authentication (MFA) option. MFA is a multi-step account login process that requires users to enter more information than just a password. Along with the password, users will be asked to enter a verification code sent to their email to validate their identity.

Communication

- Most of the standard communication ports are disabled and only those required for FalconStor software are left open. Although you may temporarily open some ports during initial setup, such as the telnet port (23) and FTP ports (20 and 21), you should shut them down after your work is complete.
- Non-standard dedicated communication ports are used by the software modules for internal communication. The list of used ports is available in an appendix in the user guide.
- The management console and host clients use a secured RPC link to communicate with FalconStor servers.
- The web-based StorSight GUI can use an SSL certificate for secure https communication with the StorSight management module.

Traffic Encryption

Replication Traffic

Encryption provides an additional layer of security during replication by securing data transmission over open, public networks. Initial key distribution is accomplished using the authenticated Diffie-Hellman exchange protocol. Subsequent session keys are derived from the master shared secret, making it very secure. The available replication encryption methods are ARC4 (128-bit), AES (128-bit), and AES (256-bit).

128-bit ARC4 stream cipher usage is fully licensed by the U.S. government for export to countries outside of North America, other than specifically restricted areas.

AES encryption is compliant with Federal Information Processing Standard (FIPS) 140; all cryptographic code/algorithms are located in a single FIPS 140 compliant software module.

iSCSI Traffic

The Mutual CHAP level of security allows the target and the initiator to authenticate to each other. A separate secret is set for each target and for each initiator in the storage area network.

SNMP Traffic

SNMP user authentication uses the MD5 or SHA algorithm.
SNMP data traffic uses AES or DES for encryption of data sent over the network. A passphrase (8-127 characters) is used.

Strong Password Management

The system checks whether the password meets the following complexity requirements in the default configuration:

1. The password contains at least 14 characters
2. The password meets at least two of the following conditions:
   1. Contains at least one lower-case letter
   2. Contains at least one upper-case letter
   3. Contains at least one digit
   4. Contains at least one space or one of the following special characters:
      ~!@#$%^&*()-_=+\|[{}];:'",<.>/?
3. The password is not the same as the account or its reverse order.
4. At least 5 different characters between the old and new password.

The system provides either of the following mechanisms for locking user accounts:

1. The system locks the account if the user enters a wrong password for a number of times more than the threshold specified during product configuration; the default value is three times.
2. The system allows setting the account locking duration for user accounts locked due to more than *n* login attempts with wrong passwords. The recommended locking duration is five minutes.
3. When the account locking duration elapses, the account is unlocked automatically. The security administrator can also unlock the user accounts manually.
4. When an account is locked, only the security administrator can unlock the account manually.

Password encryption rules are as follows:

1. Passwords are encrypted with AES 256.
2. The password must be entered in encrypted text. That is, the entered password is presented by asterisks * on the user interface. The password cannot be displayed in plain text in terminals or logs.
3. A password without encryption in memory (for example, at login) must be overwritten right after being used.
4. The password cannot be saved in log files, configuration files, cookies, or buffers without encryption.
5. Access control is implemented for password files and common users cannot read or copy the encrypted content.
6. A password in a text box cannot be copied.
7. The old password is required for a password change.
8. Users (except for administrators) cannot change the passwords of other user accounts.
9. GUI console login authentication uses SHA 512.

Data Security

StorSafe VTL moves data, thus data security is vital. The following advanced security features are included with the software:

Data Encryption

Encryption can be enabled for:

- Virtual libraries to encrypt virtual tape data using an encryption key defined by the user
- Exporting data to a physical tape using an encryption key defined by the user
- Migrating tape data to an object storage account in-flight and at-rest (end-to-end) using an encryption key obtained for each tape from the Network Security Service (NSS) internal key management system
- SIR Deduplication Repository using an internal encryption key

Data Structure

All data are stored as disaggregated without a file system construct; data layout is not discoverable outside the FalconStor server or across user accounts to provide the first “air-gap” security layer.

WORM Tapes

On a VTL or drive, the WORM property can be enabled for tapes that support ULTRIUM5 media type and above. WORM tapes cannot be overwritten. WORM allows non-rewriteable and non-erasable data to be written and provides extra data security by prohibiting accidental data erasure. Since tapes are written once, they cannot be altered or overwritten by some virus/ransomware/other malicious software.

Immutable COS

The immutable option can be enabled for tape migration to the IBM® Cloud Object Storage (COS). Immutable COS locks data to provide a safe backup and to maintain data integrity. Users can enable an object lock at the bucket level to get secure backups and long-term data retention. Retention policies ensure that data is stored in a non-erasable and non-rewritable manner for a specified time frame. Data cannot be changed until the retention period has expired. Once the retention period is over, data can be unlocked for further actions, according to your company policies.

From the IBM COS management GUI, users can configure the retention policy of their bucket and set the minimum and default values to zero, and the maximum retention period to the number of days they want to lock the bucket data.

From the FalconStor portal, users can set a tape migration policy for a VTL or drive. At the end of each backup job, the tape is ejected to the

vault, where the tape data gets packaged and migrated to the object storage of a cloud provider.

This copy of data remains intact during the retention period and is protected from malicious activity or accidental deletion.

Tape Shredding

Just as deleting a file from a hard drive does not completely destroy the file, deleting a virtual tape does not completely destroy the data on the tape. If users want to ensure that the data is unrecoverable, they must shred the tape. Shredding a virtual tape destroys all data on the tape, making it impossible to recover the data. Tape shredding uses a military standard to destroy data on virtual tapes by overwriting it with a random pattern of bits, rendering the data unreadable.

Data Isolation for Multi-tenancy

StorSight provides a secure multi-tenant architecture that allows Managed Service Providers (MSPs) and large enterprises to offer data protection-as-a-service to their customers, called tenants. Each tenant (a business or organization) has its own secure computing environment, called a domain (i.e., *companyA.com*). While all storage and network resources are shared among domains, StorSight logically isolates data by restricting visibility of storage resources to specific customers. Therefore, customers only see their own data and are not aware of other tenants.

The landlord in a multi-tenant environment is a Super Administrator, the master role that does not belong to any domain. By default, there is one Super Administrator account per StorSight server; however, the Super Administrator can create additional Super Administrator accounts.

The Super Administrator creates an administrator account for each company or organization, associating each tenant's domain with the account.

The Administrator for each domain then creates user accounts within their organization. Typically, the Administrator will create Administrator accounts for departments within their organization, possibly creating one Administrator for each department. Each Administrator will then create other user accounts as needed for their department.

For privacy, access to downstream storage can be isolated via storage pools, access to Fibre Channel targets via separate Fibre Channel zones, and access to networks via separate private subnets.

StorSafe VTL servers can be assigned to a customer domain in exclusive or shared mode:

- In exclusive mode, the server is only available to the users in that customer domain.
- In shared mode, the server is available to users of multiple customers. Data isolation among those customers is by assigning dif-

ferent storage pools to each single customer so they can only see resources created from storage pools assigned to them.

A hierarchy of user account types is used to control access to the system:

- Superadmin: A master role that does not belong to any domain with full access to StorSight who can create customer domains, add and assign StorSafe VTL servers, virtualize physical resources, reserve resources for specific usages (Configuration, Tapes, Deduplication, NAS), create storage pools of virtualized storage, perform global configuration and maintenance of servers, set up failover, and create deduplication repository SIR.
- Admin: The administrator for a customer domain who can create User or Viewer accounts and assign these accounts to specific storage pools, virtual resources, and clients. An Administrator can also create and manage virtual resources for their domain.
  An Administrator of a server in exclusive mode has the same rights as the superadmin (root) user on the server.
- User: A tenant user with read-write access to resources that have been created by that user or assigned to that user by the domain admin.
- Viewer: A tenant user with read-only access to resources within a domain who can view configuration and reports as well as receive alerts but cannot make any configuration changes.

Accounts with a higher or equal role can change the properties of other accounts. For example, Superadmin can change the password of other Superadmin, Admin, User, or Viewer accounts. Admin can change the password of other Admin, User, and Viewer accounts. Users and Viewers can only change their own passwords.

Event Logging

StorSight includes event logging for added security. Any operation done through both the Management Console and CLI that changes the current state/configuration is recorded in the event log. Likewise, any user login and logout are recorded in the event log.

Additionally, the StorSight audit log tracks and logs system activities for all servers by all administrators and users.

Conclusion

FalconStor has a long history of providing advanced security in its products. FalconStor will continue to enhance the security provided in the OS, product software, and product features of StorSafe VTL and StorSight as new standards and processes become available.

Contact FalconStor for more information.