

Security and Encryption with External Key Exchange

Table of Contents

Introduction	3
Building on a Secure Foundation	4
Operating System (OS)	4
Hardening the OS	4
FIPS Capable Crypto	5
Crypto Linkage	6
External Key Management	6
In Memory Key Management	6
At-Rest Data Encryption	7
Data Encryption Process	8
1st Event	9
2nd Event	9
Crypto Erase	9
Conclusion	9

Introduction

The importance of robust security mechanisms cannot be overstated in today's interconnected digital landscape. Data protection becomes paramount as cyber threats grow in sophistication, especially for platforms tasked with large-scale data storage and management. This paper details how VAST Data meets these ever-evolving security challenges and presents a deep dive into VAST's multi-faceted security approach that spans its foundational operating system to its sophisticated encryption methods, and specifically, the implementation of data encryption utilizing external key exchange.

Building on a Secure Foundation

Operating System (OS)

VAST selected CIQ to provide and maintain a secure operating system due to CIQ's commitment to rigorous security methodology and ability to provide rapid response for CVE remediation. VAST leverages CIQ's Mountain Platform, a cloud-native, secure, and highly-scalable image, package, and container delivery solution. VAST utilizes the Global Repository-as-a-Service to deliver an Enterprise Rocky 8.x, a RHEL binary compatible operating system image and verified packages leveraged in the platform. CIQ also maintains the operating system and packages as part of this solution. All CVE remediation is handled by CIQ for the operating system and the packages included. CIQ's provides a detailed [CVE and Patch Management Dashboard](#) to keep customers up to date.

Hardening the OS

VAST applies the DISA STIG for Redhat 8 Ver 1, Rel11 with the MAC 1 – Mission Critical Classified profile to the VAST Data Platform's operating system, which meets a comprehensive set of security guidelines. These guidelines address various aspects, such as configuration settings, patch management, and access control that contribute to securing the VAST platform.

The DISA STIG guidelines align with several NIST SP 800-53 Revision 5 Configuration Management (CM) controls, including CM-2, CM-3, CM-6, CM-7, CM-8, and CM-9. These controls focus on baseline configurations, change control, and security impact analysis, and are designed to ensure systems are securely and reliably configured and maintained.

Additionally, the DISA STIG guidelines align with numerous NIST SP 800-53 Revision 5 Access Control (AC) controls, such as AC-2, AC-3, AC-4, AC-5, AC-6, AC-7, AC-8, AC-9, AC-10, and AC-11. These controls address user access, network access, remote access, and separation of duties, and are intended to ensure that only authorized users have access to system resources and that access is granted based on a need-to-know basis.

By adhering to the DISA STIG guidelines the VAST Data Platform establishes a more robust security posture that meets or exceeds regulatory compliance requirements such as PCI DSS, HIPAA, and SOX. For more details consult the [DISA STIG download and document library](#).

FIPS Capable Crypto

CIQ provides VAST access to five NIST 140-3 capable libraries in the testing phase with [National Institute of Standards and Technology's Cryptographic Module Validation Program](#).

- GnuTLS Cryptographic Module
- Kernel Crypto API Cryptographic Module
- Libgcrypt Cryptographic Module
- NSS Cryptographic Module
- OpenSSL Cryptographic Module

VAST is currently undergoing FIPS (Federal Information Processing Standard) 140-3 Level 1 encryption accreditation with NIST. VAST has achieved a FIPS 140-2 Level 1 validation with Certificate #4107 to its credit. VAST leverages the Kernel Crypto API Cryptographic Module and the OpenSSL Cryptographic Module 1.1.1 within the platform for its FIPS 140-3 capabilities.

Entropy

VAST's CNodes (stateless, containerized servers) leverage Intel's Digital Random Number Generator (DRNG) instruction, Jitter RNG random number generator, and CSPRNG, the kernel random number generator. These instruction sets provide cryptographically secure random numbers directly from the CNodes, ensuring a high-quality source of entropy for the cluster. By leveraging three sources, your system ensures a robust and diversified pool of entropy essential for cryptographic operations and security processes.

FIPS Mode

VAST CNodes operate with the kernel in FIPS mode and that signifies that the system is adhering to specific cryptographic standards set by the U.S. federal government. FIPS mode ensures that the cryptographic operations performed by the system rely only on algorithms that have been certified and validated against the FIPS 140 standard. It offers an assurance of the cryptographic integrity and security of the processed information, ensuring that data encryption, decryption, and communication adhere to recognized and trusted standards.

Crypto Linkage

VAST links all in-flight and at-rest cryptographic operations to OpenSSL 1.1.1 (a FIPS-140-3 capable cipher), which enables the use of TLS 1.3 in the platform for in-flight encryption for management traffic (SSH & HTTPS), S3 (Object), NFSv4 over TLS (File), KMIP, and Replication between VAST deployments.

Linking all cryptographic operations to a FIPS-capable module ensures consistency in security measures. It reduces the possibility of some parts of a system being less secure due to reliance on non-validated algorithms or modules. Linkage and enforcement enables VAST to ensure that all crypto operations are done with FIPS-capable ciphers.

External Key Management

VAST Data Platform supports external key exchange with multiple providers to include:

- Thales Ciphertrust Enterprise Key Manager (EKM)
- Fornetix Vaultcore Enterprise Key Manager (EKM)

The platform KMIP 1.4 and the vendor's Rest API perform all key management operations.

In Memory Key Management

When a Leader Node is elected it retrieves the Master Key (MK), Key Encryption Key (KEK), and Data Encryption Key (DEK) from the Enterprise Key Manager (EKM). The platform has the following controls implemented to secure access to the keys in memory.

- VAST does not allow any RPC, API, or CLI method to produce the keys in any way
- Full Linux process core dumps are disabled via kernel
- Kernel kdump is disabled via one-way kexec
- Memory locations with keys are locked and never paged to non-volatile storage with mlock
- The platform secure purges keys from memory utilizing OPENSSL_cleanse() when a key is revoked, a container is shutdown, pause command, and an system shutdown
- The kernel has disabled gdb, strace, and ptrace attachment to running processes that access keys
- The ability to load un-approved kernel modules is disabled during the boot process

VAST creates all keys within the EKM and leverages the EKM to store keys persistently. We have support for the following Key exchange capabilities:

- Master key rotation (14 Days)
- Key rotation of the KEK
- Key evocation of a KEK and DEK
- Key renewal (Rekey) of the DEK
- All communications with the EKM are over TLS 1.3, leveraging ES-256-GCM encryption
- Every tenant has a unique KEK and DEK per tenant or shares a DEK
- Key renewal (rekey) by the EKM for the KEK and DEK

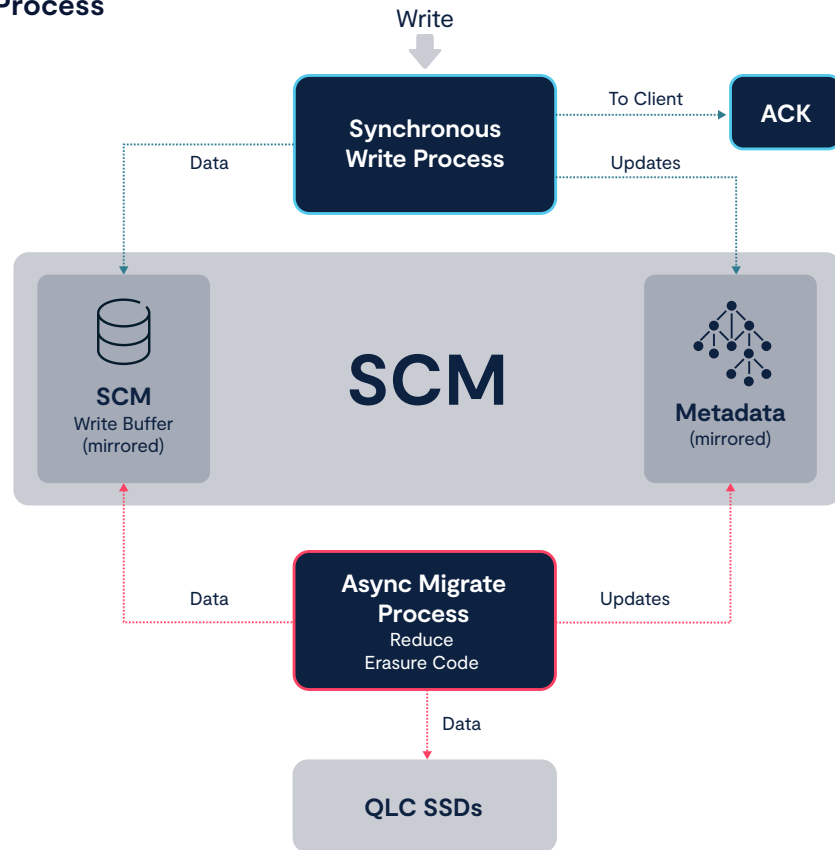
At-Rest Data Encryption

VAST utilizes AES-XTS-256 encryption, which is a specific implementation of the Advanced Encryption Standard (AES) algorithm in XTS mode with a 256-bit key size. This encryption method is commonly employed to safeguard data at rest, particularly on storage devices such as solid-state drives (SSD). Below, you'll find an overview of AES-XTS-256 encryption for securing data within the VAST Data Platform.

- **AES Encryption:** AES is a symmetric encryption algorithm renowned for its robust security and operational efficiency. AES functions on fixed-size data blocks.
- **256-Bit Key Size:** AES-256 employs a 256-bit encryption key that yields an astronomical number of possible keys (approximately 2^{256}). This immense key space renders brute-force attacks exceedingly impractical, as it would require an unfeasible amount of computational power to decipher the encrypted data without the correct key.
- **XTS Mode:** XTS (XEX-based Tweakable Codebook mode with ciphertext Stealing) represents a specialized mode of operation tailored for block level encryption. It amalgamates the XEX mode, responsible for data confidentiality, with the XTS mode, ensuring data integrity. XTS guarantees that identical plaintext blocks do not result in identical ciphertext blocks, even when identical data is written to distinct locations on the storage medium.

The VAST platform has two encryption events for all data written or inserted into the platform via NFS, S3, SMB, and SQL. The encryption process is outlined below:

Data Encryption Process



1st event:

Synchronous Write

- Data is received from Buffer and encrypted in 512-byte chunks and a header is added with the encryption key ID
- Mirrored or RAIDed the encrypted chunk to storage class memory
- Updates metadata
- Sends ACK

2nd event:

Asynchronous Migrate

- System reads encryption ID from header then locates the specified key from DRAM
- Decrypts and Reads SCM buffer
- Calls Similarity pipeline and reduces block size
- Encrypt reduced block with same key use for the initial write
- Erasure codes
- Writes to QLC
- Updates metadata
- Pointers from SCM to QLC
- Releases write buffers

1st Event

Initially, prior to platform acknowledgment of an I/O, data is segmented into 512-byte units, each garnished with a header. The respective tenant's DEK key ID is written into the chunk's header then mirrored or raided on multiple storage class memory (SCM) devices. Following this, the system metadata is updated and an acknowledgment is sent to the client.

2nd Event

The migration function, while writing data to QLC NAND, segments it into 256 Kilobyte shards and casts them broadly across the drives. Data retrieval from QLC necessitates chunk location details, the key ID, a reference block from SCM, and decryption for client requests.

Crypto Erase

The platform supports crypto erase at the tenant level. An administrator can choose to revoke tenant(s) keys and erase all the data written with the revoked DEK and KEK.

Conclusion

In the digital transformation era the safety of data is at the forefront of concerns for organizations worldwide. The multifaceted security approach adopted by VAST, as discussed in this paper, ensures the platform's resilience against a plethora of cyber threats. From the robust foundation of the operating system to the intricate processes of encryption and key management, each layer of protection fortifies data against breaches, unauthorized access, and potential vulnerabilities. As cyber threats continue to evolve, platforms like VAST serve as a beacon, showcasing the importance of comprehensive, multi-layered security in safeguarding valuable data assets.



For more information on the VAST Data Platform and how it can help you solve your application problems, reach out to us at hello@vastdata.com.