

Advanced Security and Encryption with External Key Exchange

Table of Contents

Introduction	3
Building on a secure foundation: Operating System (OS)	4
Hardening the OS	4
FIPS Capable Crypto	5
Crypto Linkage	6
At Rest Encryption with External Key Management	6
Key Management within the Platform	6
Data Encryption Process	7
Phase 1	8
Phase 2	8
Crypto Erase	8
Conclusion	8

Introduction

In today's interconnected digital landscape, the importance of robust security mechanisms cannot be overstated. As cyber threats grow in sophistication, ensuring the protection of data becomes paramount, especially for platforms tasked with large-scale data storage and management. This paper elucidates how VAST meets these ever-evolving security challenges, presenting a deep dive into a multi-faceted security approach that spans from the foundational operating system to sophisticated encryption methods.

This white paper details VAST's implementation of data encryption utilizing external key exchange. In this current iteration, VAST has certified Thales CipherTrust and requires requires the 5.0 version of the platform.

Building on a secure foundation: Operating System (OS)

VAST selected CIQ to provide and maintain a secure operating system due to its commitment to rigorous security methodology and ability to provide rapid response for CVE remediation. VAST leverages CIQ's Mountain Platform, a cloud-native, secure, authoritative, highly scalable image, package, and container delivery solution available on both public cloud and on-premises. 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 that are 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 <https://errata.rockylinux.org/> 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, which contribute to securing the 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 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 at <https://public.cyber.mil/announcement/stig-update-disa-has-released-the-red-hat-enterprise-linux-8-stig/>.

FIPS Capable Crypto

CIQ provides VAST access to five NIST 140-3 capable libraries that are in the testing phase with National Institute of Standards and Technology's Cryptographic Module Validation Program. (<https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process/IUT-List>)

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

VAST is currently undergoing FIPS 140-3 Level 1 encryption accreditation with NIST. It already boasts a FIPS 140-2 Level 1 validation, with Certificate #4107 to its credit. We leverage the Kernel Crypto API Cryptographic Module and the OpenSSL Cryptographic Module 1.1.1 within the platform for our FIPS 140-3 capabilities.

Entropy

VAST's CNodes leverage Intel's Digital Random Number Generator (DRNG) instruction, an onboard hardware-based random number generator, present in modern Intel CPUs. This instruction set provides cryptographically secure random numbers directly from the hardware, ensuring a high-quality source of entropy. Secondly, the system supplements this with the jitter entropy source, which derives randomness from the minute variances in system timing events. These timing variances, though small, are unpredictable and provide a valuable additional source of entropy. By leveraging both 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 (Federal Information Processing Standard) 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. Activating FIPS mode is essential for VAST customers who handle sensitive data, especially when the system is used by governmental agencies or entities that work with the U.S. government. 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 cryptographic operations to OpenSSL 1.1.1 (a FIPS-140-3 capable cipher), which provides several benefits. The OpenSSL 1.1.1 version has passed rigorous testing by an accredited laboratory the testing Phase for FIPS 140-3 level validation.

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. This enables VAST to utilize TLS 1.3 in the platform which is more performant and secure for in-flight encryption for management traffic (SSH & HTTPS), S3 (Object), NFSv4 over TLS (File), KMIP, and Replication between VAST deployments.

At Rest Encryption with External Key Management

VAST Data Platform supports external key exchange with Thales Ciphertrust's Enterprise Key Manager (EKM) via the RestAPI, and KMIP API (1.4).

Always operating in FIPS mode, the Linux kernel guarantees all platform encryption meets FIPS standards. VAST is currently undergoing FIPS 140-3 Level 1 encryption accreditation with NIST. It already boasts a FIPS 140-2 Level 1 validation, with Certificate #4107 to its credit.

The platform utilizes XTS-AES Mode when encrypting data, relying on the OpenSSL 1.1.1 library in user space for all at rest encryption.

In Memory Key Management

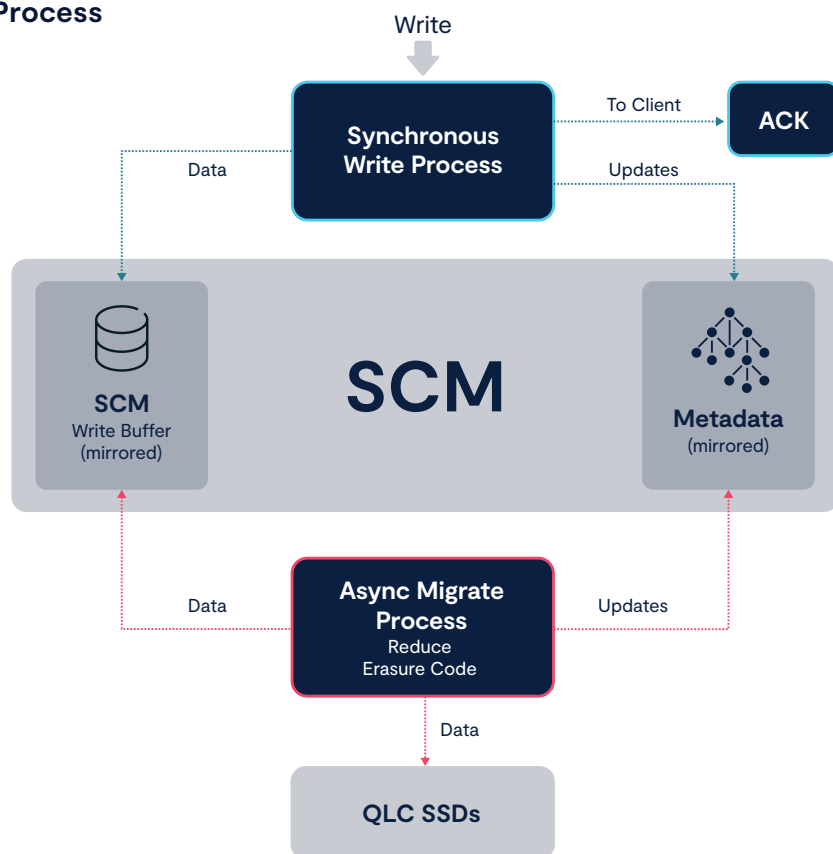
When a Leader Node is elected it retrieves the Master Key (MK), Key Encryption Key (KEK), and Data Encryption Key (DEK) From the Enterprise Key Manager (EKM). The platform has the following controls implemented to secure access to the keys in memory.

- 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 Revocation of a KEK and DEK
- Key Renewal (Rekey) of the DEK
- All communications with the EKM are over TLS 1.3 leveraging AES-256-GCM encryption
- The Platform allows for every tenant to have a unique KEK and DEK per tenant or share a DEK
- The Platform supports key renewal (rekey) by the EKM for the KEK and DEK

Data Encryption Process



Phase 1: Synchronous Write with KMIP Encryption

- Data is received from Buffer and encrypted in 512-byte chunks and a header is added with the encryption key ID
- Updates metadata
- Sends ACK

Phase 2: 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
- 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

Phase 1

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 and persisted on two storage class memory devices. Following this, system metadata gets updated, and an acknowledgment is sent to the client.

Phase 2

The migration function, while writing data to QLC NAND, segments it into 256 Kilobyte shards, casting them broadly across the drives. Data retrieval from QLC necessitates chunk location details, the key ID, a reference block from storage class memory, 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 that was written with the revoked DEK and KEK.

Conclusion

In this age of digital transformation, 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 the 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 Universal Storage and how it can help you solve your application problems, reach out to us at hello@vastdata.com.