HPE NonStop Volume Level Encryption

Benefits

- Supports HPE NonStop and HPE Virtualized NonStop systems
- Integrates with ESKM for secure access to encryption keys
- Supports storage solutions—disks, XP arrays, BackBox, and LTO tapes supported on HPE NonStop systems
- Supports industry-standard encryption algorithms

More than 20,000 security standards have emerged worldwide and nearly all include requirements to protect data-at-rest from exposure by theft or media losses. You may find that you need to simultaneously comply with industry-related standards as well as local and country-specific laws controlling how to protect your sensitive customer data. Failure to comply can result in negative publicity and possibly cost millions of dollars in fines and remediation to correct the problem. Encryption of data-at-rest on storage devices protects sensitive data from exposure. It also helps you comply with data-at-rest regulations described by the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR) and others.

HPE NonStop Volume Level Encryption (VLE) product provides a fully integrated encryption solution for storage devices connected to HPE NonStop systems that use HPE NonStop Storage Cluster I/O Module (CLIM). All data on selected disks and tape devices are encrypted using industry-standard algorithms. Utimaco Enterprise Secure Key Manager (ESKM) generates, manages, and serves encryption keys as needed, giving you a single trusted supplier for key management as well as encryption.

You can implement HPE NonStop VLE without changes to your applications. HPE NonStop VLE features exceptional data availability and fault tolerance; it allows you to perform initial volume encryption and rotate encryption keys online without taking any data offline.

HPE GreenLake

Key features and benefits

Integrated with HPE NonStop fundamentals and utilities

When enabled, the HPE NonStop VLE product is seamlessly integrated into your system. It uses existing manageability tools such as Open System Management (OSM), Subsystem Control Facility (SCF), and HPE NonStop I/O Essentials to configure, manage, and monitor encryption activities on the system. Data being written to or read from encrypted disk or tape is transparently encrypted and decrypted as it passes through the HPE NonStop Storage CLIM. Your applications continue to see the data in clear text.

A registration tool is included to make it easy for you to configure your HPE NonStop Storage CLIMs as clients of ESKM. This tool is a guided procedure in the OSM Service Connection and provides a GUI wizard for simplified CLIM registration.

HPE NonStop VLE and ESKM environment is designed to support your security policies, with separation of duties for managing encryption, including configuration of disks and tape devices as encrypted devices and key rotation. All encryption configuration activities are audited.

HPE NonStop fundamentals for fault tolerance are fully extended to HPE NonStop VLE. You can encrypt existing disk data online and perform periodic key rotations for disks with concurrent access to the data, including write operations. Encryption, including key rotation, can be performed online using one of the two methods. The CLIM-based method directly encrypts and rewrites the data on the disk online by sequentially reading and rewriting from beginning to the last used block while still permitting application read/write operations. For key rotation, the CLIM decrypts the data using the old key and re-encrypts it using the new key.

An alternate method revives one member of a mirrored disk pair from the other member, writing the data using a new key. Either method allows you to perform encryption or key rotation without incurring a service outage on your system.

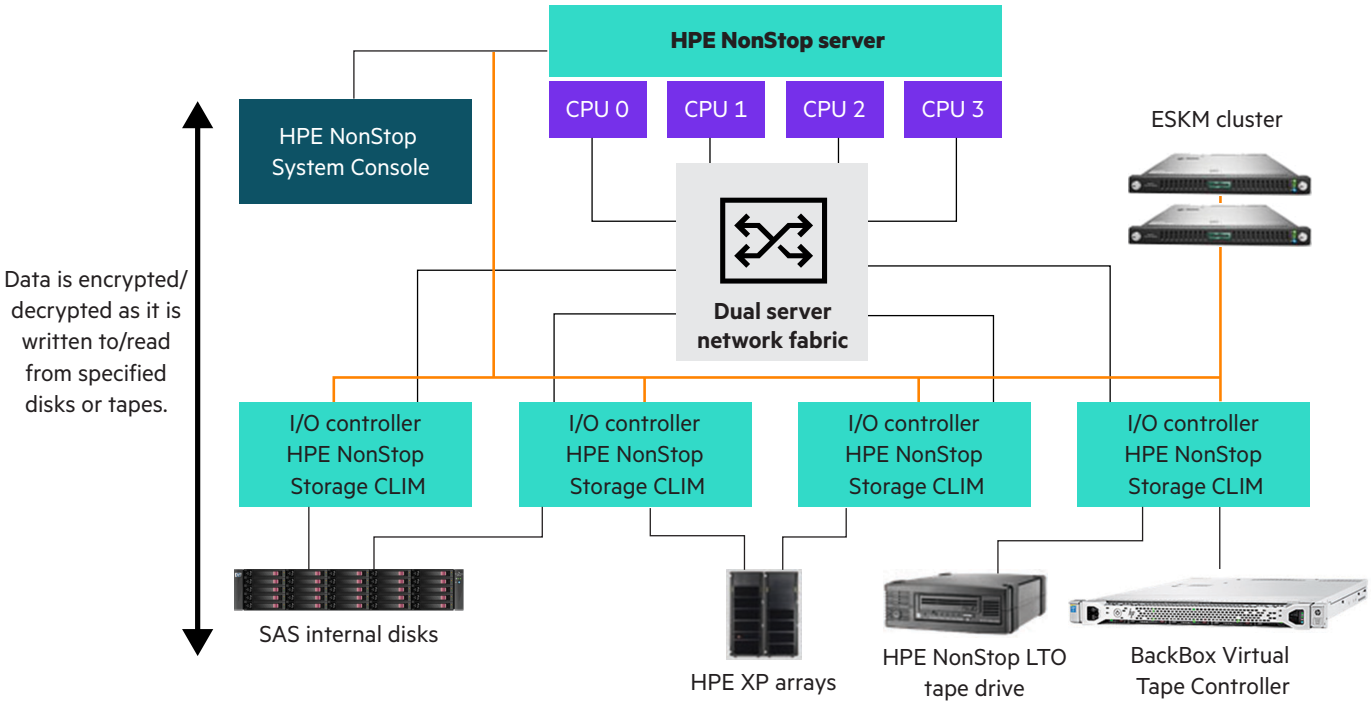

Figure 1. Architecture of an HPE NonStop system using VLE

Strong encryption

HPE NonStop VLE uses the following algorithms. You can select the disk encryption algorithm to use for each encrypted drive.

Disk encryption algorithms

- XTS-AES (key size 256) NIST SP 800-38E compliant
- CBC-AES (key size 256), NIST SP 800-38A compliant

Tape encryption algorithm

- GCM-AES (key size 256)

Note: HPE NonStop VLE does not encrypt data while it is in transit or in use within the system, or in transit over external networks between systems and workstations. You must continue to configure your environment using Secure Shell (SSH) or Transport Layer Security (TLS) for data in motion. To control insider access to information, you must apply appropriate access control lists (ACLs) to sensitive data.

Supports multiple devices

HPE NonStop VLE is supported on HPE NonStop X systems, HPE NonStop i systems, as well as on HPE Virtualized NonStop systems.

Supported systems are capable of using the HPE NonStop Storage CLIM. Storage devices supported are

Table 1. Supported device types for VLE encryption

Device type	Support level
HPE NonStop SAS disk drives	Fully supported at the disk level
HPE XP—XP disk arrays	Fully supported, encryption selectable at the logical unit number (LUN) level
HPE NonStop LTO tape drives	Fully supported at both the device and tape level
HPE NonStop BackBox VTC	Fully supported at both device and tape level

Exclusions: This solution does not encrypt Fibre Channel disk module (FCDM) disk because they are connected through Fibre Channel ServerNet Adapters (FCSAs) not through HPE NonStop Storage CLIM. Tape devices older than LTO-4 are not supported.

HPE NonStop VLE uses the supported LTO drives and HPE NonStop BackBox virtual drives' built-in bulk encryption capabilities to perform encryption and decryption. HPE NonStop CLIM acts as the key management client for the drive, interacting with ESKM to generate encryption keys as needed, and retrieves them to the tape drive on demand.

Integrates with ESKM

Utimaco ESKM provides a centralized key management solution for unifying and automating an organization's encryption key controls by creating, protecting, serving, and auditing access to encryption keys for secure and reliable administration. HPE NonStop supports both Utimaco ESKM hardware and Virtual ESKM. ESKM manages access to millions of encryption keys for your data center across multiple HPE NonStop systems and other encryption solutions and devices. Keys are as valuable an asset as the data they protect and must be protected and preserved for the life of the data. ESKM supports these assets by automating key generation, protection, and management based on your business security policies.

You can deploy ESKM in multinode, high-availability, geographically extended clusters. They can also support enterprise-scale infrastructure across a diverse set of products and applications. For HPE NonStop servers, ESKM should be installed in pairs or larger clusters for high availability. You can install ESKM cluster nodes in the same or other data centers, as long as they remain network accessible to HPE NonStop Storage CLIMs on the **HPE NonStop** platform. HPE NonStop VLE takes advantage of these capabilities to bring you an enterprise-class key management capability fully integrated with HPE NonStop VLE to generate, store, and serve keys to HPE NonStop Storage CLIMs in your HPE NonStop environment. **HPE NonStop** Storage CLIMs are registered as clients of ESKM.

Hewlett Packard Enterprise and Utimaco have partnered together to support ESKM by the HPE NonStop VLE solution. In order to implement VLE in their HPE NonStop environment, customers should purchase ESKM directly from Utimaco.

Ordering information

Refer to the following table for the list of HPE NonStop VLE and ESKM Product Identifiers (PIDs) for ordering purposes.

PID	Product short description	Supported HPE NonStop platform
BE376AL(E)	HPE NonStop VLE LTU	L-Series
QVLE	HPE NonStop Volume Level Encryption LTU	J-Series

ESKM automatically replicates keys across clusters of up to eight nodes and performs backups and restores of the key database. It also provides a built-in local certificate authority to help create client certificates for strong TLS authentication of HPE NonStop Storage CLIMs to the key manager. Also, the ESKM offers identity-based administrator access, dual-control administration, and event logging. It is deployed in high-availability clusters with built-in client load balancing and failover to make sure that it is as highly available as the HPE NonStop environment that it supports. An ESKM cluster can service HPE NonStop and other systems across multiple data centers and supports multiple HPE NonStop servers.

HPE NonStop VLE performance

As with any solution where encryption becomes part of the transaction path length, performance is a priority. Because HPE NonStop Storage CLIM or LTO tape performs data encryption for HPE NonStop VLE, the performance of HPE NonStop CPUs is unaffected. Actual performance can vary from system to system depending on configuration and application workload characteristics.

Licensing

On supported HPE NonStop platforms, HPE NonStop VLE capabilities are included in the system software and may be enabled by purchasing an encryption license from HPE. HPE NonStop system needs to be running L15.02, or J06.08, or H06.19 or a later Release Version Update (RVU). No system load or other service interruption is required to enable HPE NonStop VLE after the license file is in place. You can add more encrypted disks and configure additional HPE NonStop Storage CLIMs for encryption online when needed. Note that each HPE NonStop Storage CLIM enabled for encryption must be separately licensed as a client of ESKM cluster.

Learn more at

HPE.com/info/NonStop

Visit **HPE GreenLake**

Chat now (sales)

Hewlett Packard Enterprise

a00029745ENW, Rev. 3