

CipherTrust Manager for VMware VMs on Google GCVE



Overview:

Securing virtual machines (VMs) as enterprises achieve digital transformation

VMs are at the heart of growing digital transformation initiatives. The critical applications and sensitive data running on these must be protected to ensure that the technology can be used effectively and with confidence. Compromise can result in severe fines, costly remediation efforts, and damage reputations.

The Challenge:

Encrypting VM input/output and data at rest with minimum management overhead and impact to operational flexibility

Encrypting the input/output of VMs is the new norm and a fundamental part of the IT infrastructure as it expands to fulfill enterprises' need for achieving digital transformation. Another fundamental requirement is to protect data at rest. As encryption is typically considered to be demanding on operations, particularly as it relates to the management of increasing number of cryptographic keys, innovative technologies and standards-based protocols are making encryption more transparent to the operation and its users.

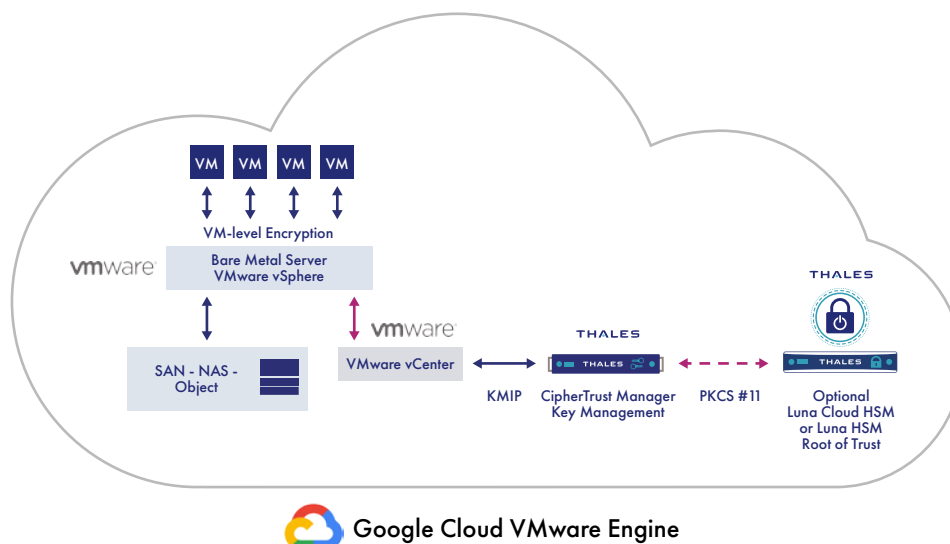
The Solution:

VMware vSphere® Virtual Machine Encryption and Thales CipherTrust Manager

VMware vSphere®, is an industry-leading virtualization platform that empowers users to scale-up and scale-out applications with confidence. vSphere helps you get the best performance, availability, and efficiency from your infrastructure and applications. It's the ideal foundation for any cloud environment.

VMware vSphere VM Encryption is a feature introduced in vSphere 6.5 to enable the encryption of virtual machines. VM Encryption protects virtual machine files, virtual disk files, and core dump files by encrypting the input/output from the virtual machine before it gets stored in disk. The solution leverages the Key Management Interoperability Protocol (KMIP) for encryption key management and key vaulting.

vSphere enables a flexible key management root of trust to match the customer risk profile – from a software virtual appliance to a FIPS 140-2 Level 3 physical protected boundary. vSphere can be used with the CipherTrust Manager from Thales to provide the full range of protection for key management and role separation. The combined solution delivers non-disruptive encryption, ensuring the security of VMs, the applications they run, and the sensitive data they process. The combination provides a cost-effective and comprehensive solution that meets the most stringent security requirements. Leveraging hardware-based data encryption ensures no adverse impact to system performance.



In addition, Google now supports running the VMware stack in Google Cloud using the Google Cloud VMware Engine (GCVE). Now apps and workloads designed to run within VMware can be seamlessly migrated to the cloud.

The combination of Google GCVE, VMware and Thales CipherTrust Manager ensures a secure path to the cloud. This joint solution simplifies migration, while adding all the benefits of the cloud, including scale, agility, lower cost, best in class security of dedicated infrastructure, and streamlined management of private encryption keys.

Typical use cases involve data center consolidation, enhanced application performance and availability, and intelligent operations management and prioritization. Use of VMware vSphere VM Encryption with Thales CipherTrust Manager can also facilitate regulatory compliance.

Why use Thales CipherTrust Manager?

Security keys can be instantly reprogrammed to meet site-specific security policies. Security mechanisms enable compliance with data-at-rest encryption requirements set forth in HIPAA, PCI DSS and SOX standards among others. The appliance provides:

- Centralized key management of encryption keys.
- Centralized and simplified key management for your entire VMware vSphere VM infrastructure while improving compliance and auditability.
- Enable multi-tenant data isolation and leverage shared resources while securing data by business policy to segregate data for multiple departments, business units, or customers.
- Achieve high-availability to support cloud-scale deployments.
- Ability to cluster multiple Thales CipherTrust Manager appliances to maintain encrypted data availability even in geographically dispersed data centers.
- Enable auditing, logging, and alerting.
- Improve regulatory compliance for your entire VMware environment with a non-repudiative audit trail.

In addition, Google now supports running the VMware stack in Google Cloud using the Google Cloud VMware Engine (GCVE). Now apps and workloads designed to run within VMware can be seamlessly migrated to the cloud.

The combination of Google GCVE, VMware and Thales CipherTrust Manager ensures a secure path to the cloud. This joint solution simplifies migration, while adding all the benefits of the cloud,

including scale, agility, lower cost, best in class security of dedicated infrastructure, and streamlined management of private encryption keys.

The CipherTrust Manager is a high-availability appliance that centralizes encryption key management for Thales Data Security Products and third-party encryption solutions. The appliance manages key lifecycle tasks including generation, rotation, destruction, import and export.

The CipherTrust Manager additionally enhances key management by providing convenient back-up services and delivering strong separation of duties for increased security. The CipherTrust Manager can be separated into logical entities, or domains, dedicated to unique key management environments, providing additional security and ultimate separation of duties, where no single administrator has access to all domains.

The CipherTrust Manager is available as either a hardware or a virtual appliance. The k470 CM hardware appliance is FIPS 140-2 Level 2 compliant and the k570 CM hardware appliance is equipped with a hardware security module (HSM), is FIPS 140-2 Level 3 compliant. The virtual appliance, K170V is FIPS 140-2 Level 1 compliant.

The consolidation of enterprise encryption key management delivers consistent policy implementation between systems and reduces training and maintenance costs.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

VMware

VMware, a global leader in cloud infrastructure and business mobility, helps customers accelerate their digital transformation. VMware enables enterprises to master a software-defined approach to business and IT with VMware Cross-Cloud Architecture™ and solutions for the data center, mobility, and security.

For more detailed technical specifications, please visit cpl.thalesgroup.com or www.vmware.com

> cpl.thalesgroup.com < [in](#) [twitter](#) [facebook](#) [youtube](#)

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us