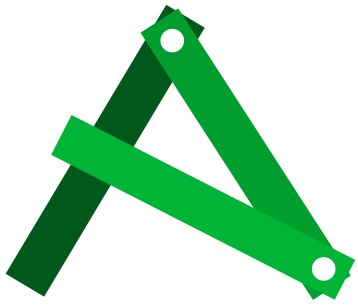


FROM THE ARCHITECTS | Whitepaper

Veeam in a vSphere environment with Multiple KMS services

Use Veeam Backup and Replication in highly secured VMware vSphere environments with multiple KMS.

Luca Dell'Oca

April 2026 — Version 1.0

Whitepapers by "From the architects" are technical L300 whitepapers created by the EMEA Solution Architect Team. They are not validated by Veeam QA and should as such be considered as individual contributions to the community.

THE WHITEPAPER IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Contents

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

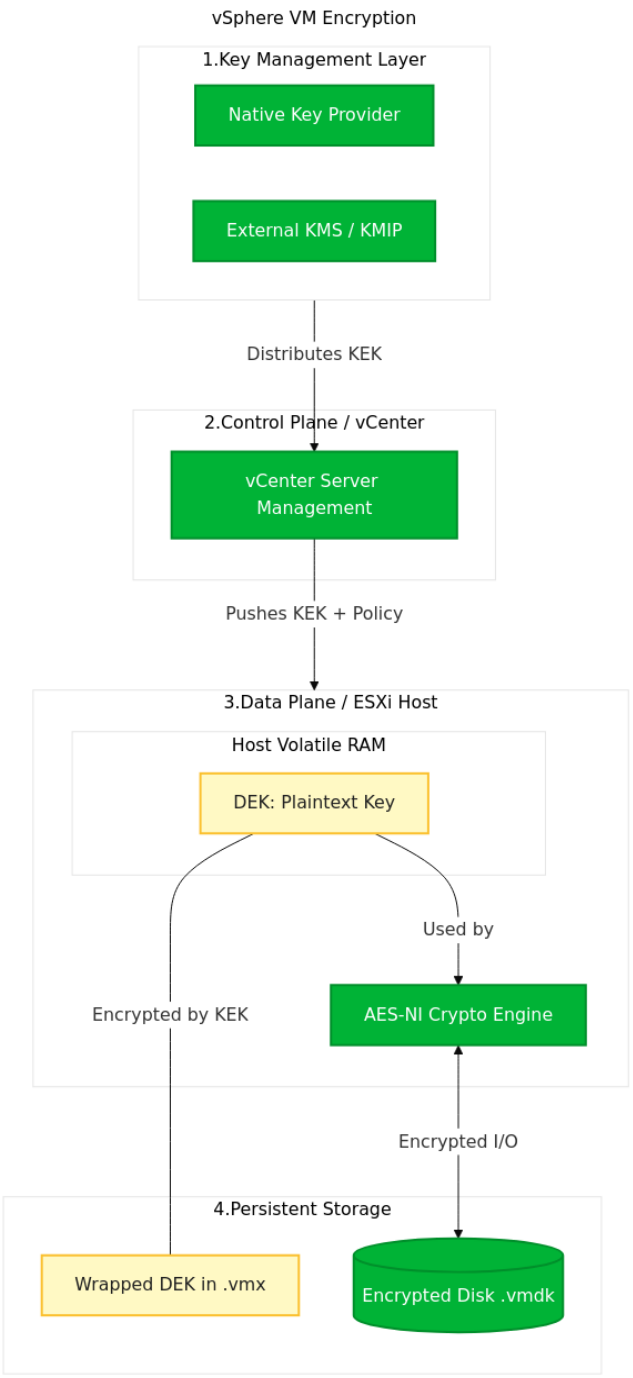
In an IaaS environment designed for the highest level of security, a service provider may decide to deploy VMware vSphere, with or without Cloud Director, and leverage the VMware capability of registering multiple Key Management Servers (KMS). Each tenant then receives a dedicated KMS service, either directly offered by the service provider or provided by the tenant (Bring Your Own Key - BYOK).

This solution guarantees complete confidentiality of data hosted in the virtual machines, as each tenant exclusively owns the keys required to decrypt the data within their own VMs.

In this document we'll explore how Veeam Backup and Replication will behave in such environments, to guarantee the highest confidentiality of data.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

1. vSphere VM Encryption with KMS



Let's start with the theory: how VMware handles encryption.

When using an external Key Management Server (KMS), vSphere employs a dual-layer "Envelope Encryption" model.

vCenter acts as a broker, requesting a Key Encryption Key (KEK) from the KMS via the KMIP protocol.

This KEK is sent to the ESXi host, which then generates a unique Data Encryption Key (DEK) to actually encrypt the VM's files (VMDK, VMX, etc.). The host "wraps" the DEK with the KEK and stores only the encrypted DEK on disk. This ensures that even if the physical storage is stolen, the data cannot be decrypted without the KEK, which resides safely in the KMS or the host's volatile RAM.

Both vSphere and Veeam Backup & Replication use two different encryption algorithms in this model, each chosen for a specific reason.

The actual data — whether VM disk blocks encrypted by vSphere or backup blocks encrypted by Veeam — is always encrypted using **AES-256**, a symmetric algorithm where the same key is used to both encrypt and decrypt. Symmetric encryption is extremely fast and efficient, making it practical for encrypting large volumes of data without impacting performance.

The data encryption key (DEK) however cannot be stored in plaintext on disk — if it were, anyone with access to the storage would have everything they need to decrypt

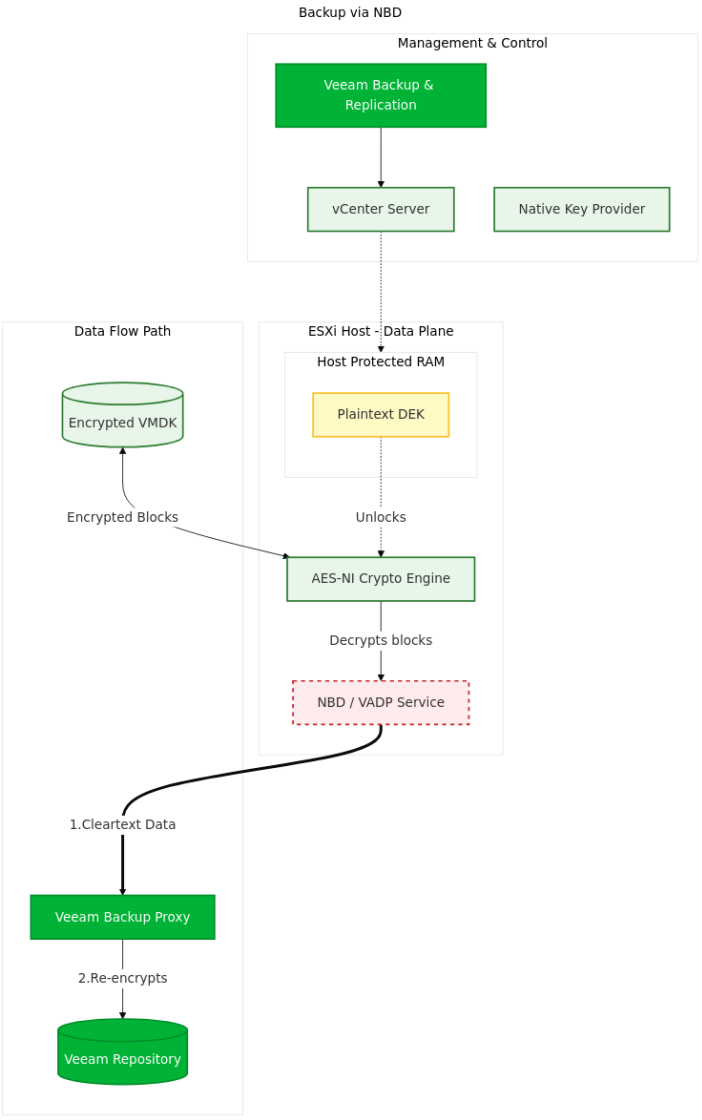
© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

the data. This is where asymmetric encryption comes in: an external key (the KEK in vSphere, or the KMS key in Veeam) is used to **wrap** (encrypt) the DEK using an asymmetric algorithm. Asymmetric encryption uses a key pair — a public key to encrypt and a private key to decrypt — so the KMS can protect the DEK without ever exposing the private key to the host or the backup server. The unwrapped DEK is only ever held in volatile RAM during operation, and is never persisted to disk in plaintext.

This combination — fast symmetric encryption for data, secure asymmetric encryption for key protection — is known as **envelope encryption** and is a widely adopted pattern in enterprise security architectures.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

2. Veeam Backup: The NBD Scenario

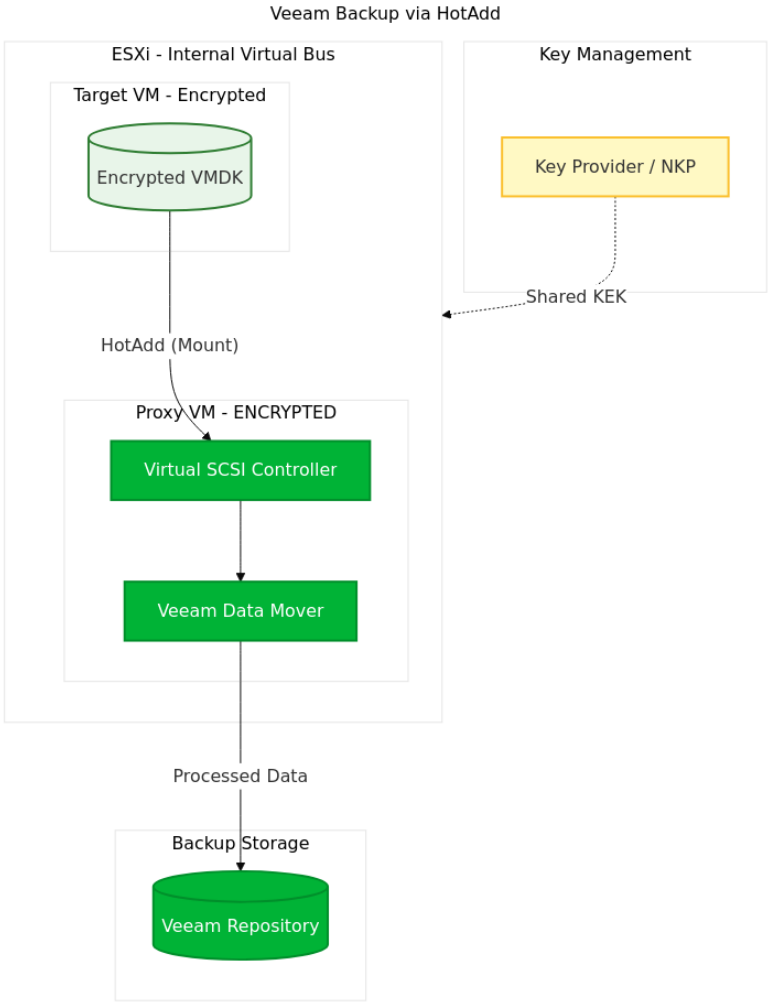


In the Network Block Device (NBD) transport mode, the ESXi host is responsible for the heavy lifting of decryption during the backup process. When Veeam requests VM data through the vSphere Storage APIs (VADP), the ESXi host retrieves the encrypted blocks from storage, uses the DEK in its RAM to decrypt them, and then streams the data over the management network.

By default, this data travels in cleartext across the network to the Veeam Proxy. To maintain security, administrators must ensure that Veeam is configured to re-encrypt the data before it is written to the backup repository and use encrypted NBD (SSL) if supported.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

3. Veeam Backup: The HotAdd Scenario



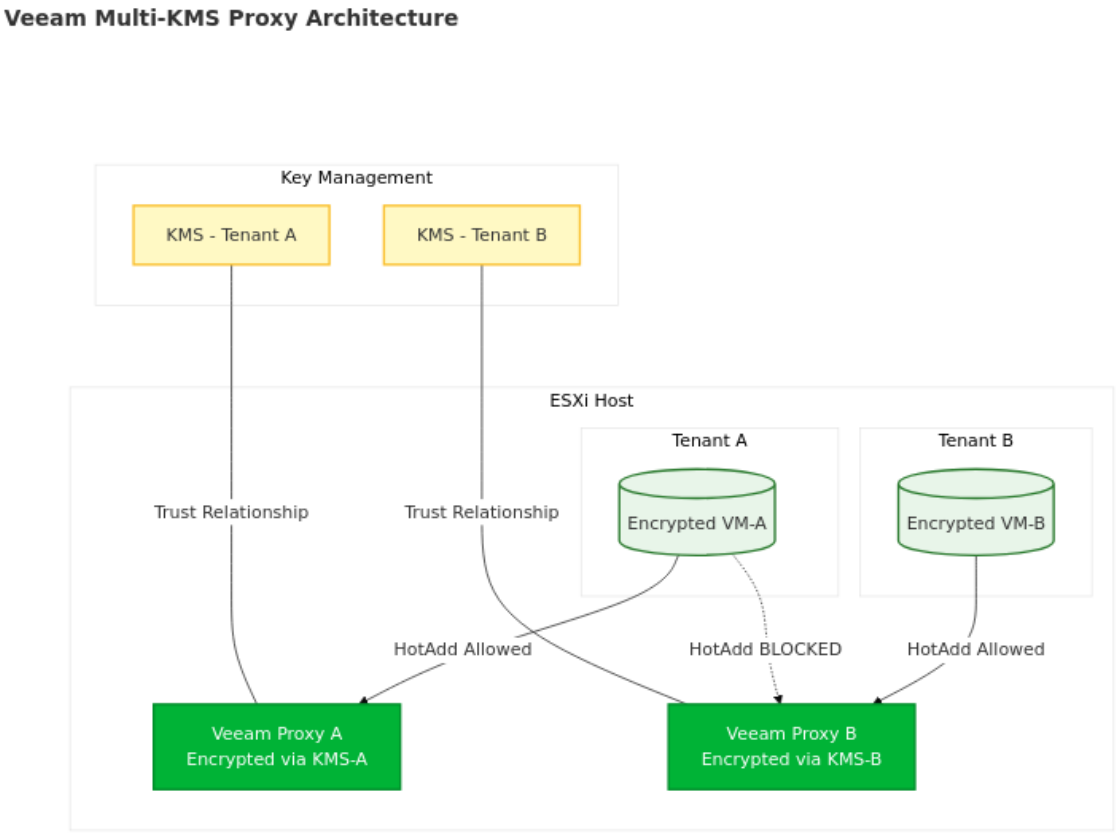
The HotAdd scenario is more restrictive but offers an inherently more secure data path.

In this mode, the Veeam Proxy (which must be a Virtual Machine) "mounts" the encrypted disks of the target VM directly to its own virtual SCSI controller. For this to work, the Veeam Proxy VM itself must be encrypted using the same Key Provider as the target VM. The ESXi host treats the Proxy as an authorized entity, allowing it to "see" the decrypted data blocks across the internal virtual bus.

Because the data is processed locally within the host's I/O stack and never leaves the host in an unencrypted state over the network, HotAdd avoids the "cleartext-on-the-wire" risk associated with standard NBD.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

4. Veeam with Multi-KMS



In a multi-tenant environment where different tenants use different Key Providers, vSphere maintains a strict security boundary: a VM encrypted by KMS-A can only be "touched" or "mounted" by another server (like an ESXi or a Veeam Proxy) that is also trusted by KMS-A.

If there are 10 VMs encrypted via KMS-A and 10 VMs encrypted via KMS-B, a single Veeam Proxy cannot HotAdd all of them unless that Proxy is somehow authorized for both.

Since a VM can typically only have one encryption policy, a Veeam Proxy encrypted via KMS-A will trigger a "Permission Denied" or "Cryptographic Error" when it tries to HotAdd a disk belonging to a KMS-B VM.

To use HotAdd, Veeam will need at least one Veeam Proxy encrypted under each specific KMS. Veeam's "Proxy Selection" logic selects the best proxy based on the connection method, from the most to the least efficient:

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

- Direct Storage
- HotAdd
- NBD

However, a proxy is selected because it's capable of doing hotadd, but KMS compatibility with the protected VM is not checked in advance. So, a proxy with the "wrong" KMS configuration may still be selected; in this case, the proxy will still be used, but it will fail over to NBD. If failover to NDB is disabled, the proxy will fail to process the disk.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

5. Considerations and Best Practices

Because of the described behavior, we can identify 2 scenarios:

- **Distributed NBD:** to avoid any mixed configuration and have one uniform setup, providers should use all proxies in NBD mode. This is a "no brainer" design, even if maybe slower. Please enable NBD-SSL to guarantee end-to-end encryption in flight of the data;
- **Dedicated HotAdd:** in situations where a single tenant may have a significant amount of VM, a provider can deploy dedicated virtual proxies, encrypted with the specific KMS of the tenant to protect. This group of proxies will only be used to perform operations for the specific tenant, and thanks to this setup a full HotAdd mode will be possible.

  In both cases, avoid automatic selection of HotAdd proxies, as proxies encrypted with the wrong kms may be selected, thus slowing down the process (and even failing if failover to NBD has been unselected).

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

6. Key management in Veeam Backup and Replication

To better understand the behavior, we added here the answers to some of the most common questions.

Does Veeam rotate keys?

No.
Veeam does not rotate keys, it's the duty of KMS administrator. Key policies are set by higher level security, not backup admins. They are consumers of the managed key services and thus should have no power to decide the rotation policies.

Veeam has a built-in support for rotated keys – when a job starts, Veeam Backup & Replication checks the key from KMS and verifies the key version (key version is KMIP API property). If a new key is available, VBR will retrieve it from KMS and the job will use it and encrypt the new backup with the new key.

This operation is 100% transparent to the backup administrators.

Does Veeam delete the keys?

No.
Veeam does not remove keys no longer in use, since it doesn't even store them. Rather, Veeam keeps the KMS_ID + keyIDs and re-encrypts backup metadata with the latest key version, and stores all this information – in an encrypted format – inside the **.vbm** file.

When Veeam receives a new encryption key, it doesn't matter if it comes from a KMS or is manually created by a user: a new backup is created, and backup metadata is re-encrypted using the new key as well inside the vbm file. In this way the user doesn't need to provide any previous key to decrypt the chain, as long as the vbm file is available. If vbm is not available and the backup needs to be read directly from the vbk file (for example when importing the backup into a new system without a vbm file) then the whole set of KMS keys and passwords that were used to encrypt data encryption keys are needed.

So, the best practice is to take extra caution in protecting the vbm files, since they allow easier data decryption.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Does Veeam supports multi-key-encrypted-chains?

Yes.

Veeam tracks keyID for every restore point and knows which keys have to be used for the decryption.

How does Veeam handle a Disaster Recovery scenario?

Let's assume the complete loss of the Veeam Backup server.
A backup administrator installs a new Veeam Backup server without a configuration backup, and only the encrypted backups are mounted from the repositories.

- if the administrators reconfigure the connection to the KMS, so that this is present by the time of backup decryption, Veeam will simply decrypt all points using respective keys automatically;
- if KMS is not present or Keys are missing, Veeam will show users a list of encrypted backups with a list of respective keyID's to be provided. This is a "last resort" operation, since those keys have to be exported manually from the KMS server.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

7. Resources

VMware / Broadcom Resources

- vSphere Virtual Machine Encryption Overview

  Broadcom TechDocs – Virtual Machine Encryption (vSphere 8.0)

  The main entry point for vSphere 8.0 VM encryption. Covers key provider types (Standard KMS, Native Key Provider, Trusted Authority) and the relationship between vCenter, ESXi hosts, and external KMS servers.

- How vSphere VM Encryption Protects Your Environment

  Broadcom TechDocs – How VM Encryption Protects Your Environment (vSphere 8.0)

  Explains the Envelope Encryption model, the role of the KEK and DEK, and how the ESXi host handles keys in volatile RAM.

- Virtual Machine Encryption Best Practices

  Broadcom TechDocs – VM Encryption Best Practices (vSphere 8.0)

  Covers AES-NI requirements, KMS availability policies, key persistence on ESXi hosts (introduced in vSphere 7.0 U2), and core dump handling for encrypted VMs.

- Virtual Machine Encryption Interoperability

  Broadcom TechDocs – VM Encryption Interoperability (vSphere 8.0)

  Explicitly documents the backup software requirement to use VADP with either HotAdd or NBD-SSL for encrypted VMs. Also details cloning, vTPM, and Native Key Provider limitations.

Veeam Resources

- Transport Modes – Veeam Backup & Replication User Guide for VMware vSphere

  Veeam Help Center – Transport Modes

  Primary reference for NBD, NBD-SSL, and HotAdd (Virtual Appliance) transport modes, including the encrypted VM requirement that the proxy itself must be encrypted to use HotAdd.

- Key Management System Keys – Veeam Backup & Replication User Guide

  Veeam Help Center – KMS Keys

  Documents how Veeam integrates with an external KMS for backup encryption, including key rotation handling, the role of the .vbm file, and behavior during disaster recovery scenarios.

- How KMS Works – Veeam Backup & Replication User Guide

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Veeam Help Center – How KMS Works

Details the asymmetric key model used by Veeam (RSA 4096-bit), how Veeam stores only the public key locally while the private key remains on the KMS, and the automatic key rotation sync job.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.