Per cluster Key Management System

On the VMware Cloud Provider Platform

A Natural Partnership

For Cloud and Service Providers

Introduction

VM Encryption is one of the critical data security functions providers can offer their tenants through VMware Cloud Director(VCD). Provider administrator configures Storage policies and Key Management system on vCenter Server for all infrastructure. This link provides a complete list of supported KMS with vCenter. vSphere 7 introduces support for unique KMS Server configuration per cluster on vCenter Server. Also, vSphere 7u2 introduces a native Key provider on the vCenter Server. Also, Starting from VCD release 10.1, the provider admin can publish Storage policies capable of VM encryption to the tenants. The tenant users can encrypt and decrypt VM Applications through the VCD tenant portal.

The latest enhancement on the vCenter Server enables provider admins to offer independent VM encryption to each tenant when the provider associates each cluster on vCenter as Provider Virtual Data Center(PVDC) and Organization Virtual Data Center (OVDC) on the VCD. This document guides the configuration and concludes with a use case of elastic VDC for tenant/tenant organization on VCD.

Setup KMS on the vCenter Server:

The provider can configure KMS service and storage policies on the vCenter Server. These policies are then reflected on VCD while creating the PVDC. The compatibility matrix is updated autonomously of the KMS guide and can be found here for the complete product compatibility matrix. The detailed instructions of the KMS configuration can be found on official documentation here. Figure 1 shows an example KMS configuration on the vCenter Server.

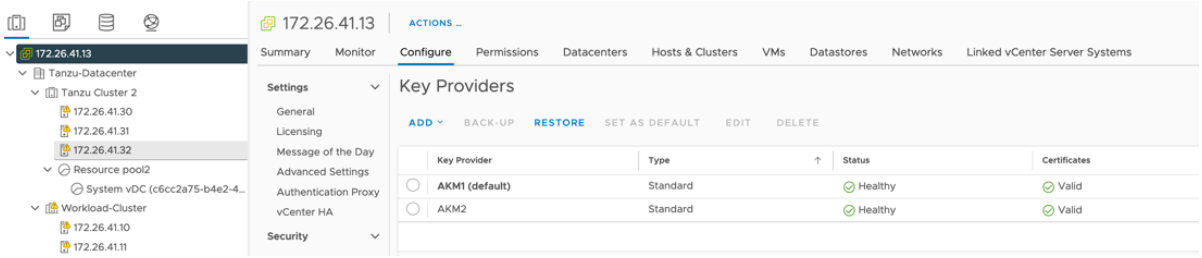

Figure 1 Setup KMS cluster on the vCenter Server for Datacenter

KMS for cloud providers

Starting with VMware Cloud Director 10.2.2, Provider admin can set the VM encryption policies to the following entity types individually:

- Virtual Machines – Used for VMs and vApps and their disks
- vApp/VM Templates – Used for vApp Templates
- Catalog Media – Used for Media inside catalogs
- Named Disks – Used for Named disks
- TKC – Used for TKG clusters
- Edge Gateways – Used for Edge Gateways

This ability gives an option to select storage policy per entity like Workload VMs or Catalog Media to the provider. The provider admin can accomplish this configuration by two simple steps on VCD UI in the Provider portal. Figures 2 and 3 showcases steps to configure the VM encryption entities through the VCD provider portal.

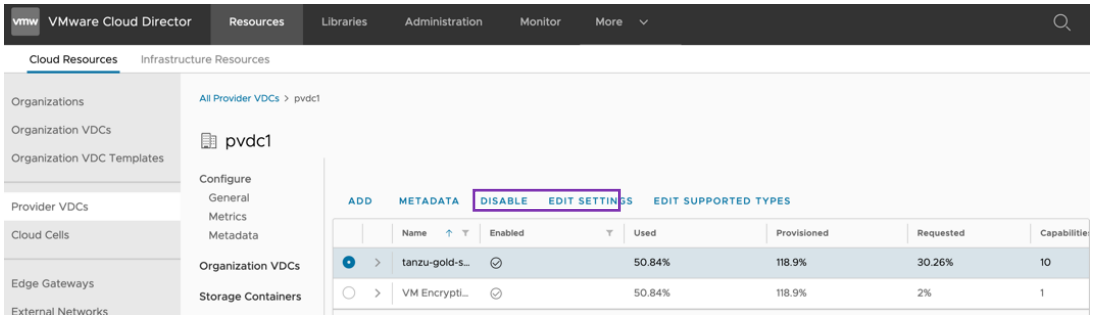

Figure 2 Configure supported Entities for Storage policies

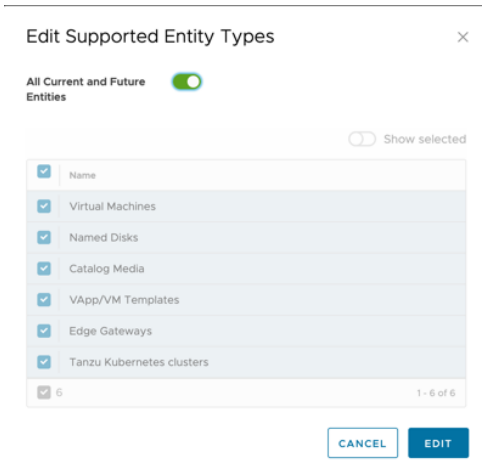

Figure 3Configure supported Entities for Storage policies

Use case: Provider to offer Unique Key Provider and Encryption per tenant

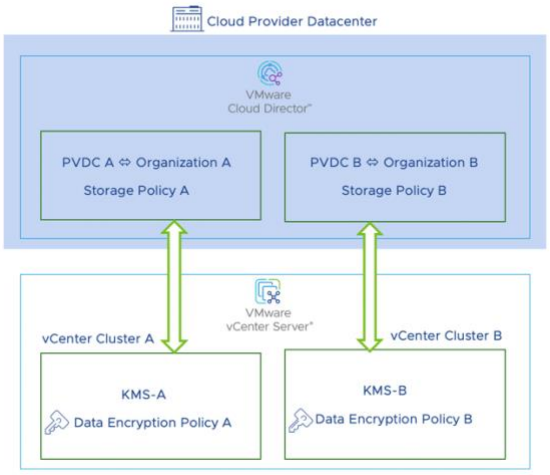

Figure 4 Per vCenter cluster KMS and Per tenant VM Encryption offering

Starting with vSphere 7.0 VI admin can now configure KMS per cluster on the vCenter Server. Table 1 showcases the supported Bill of Materials(BOM) for this use case.

vCenter Version	VCD Version	KMS
vSphere 7.0	VCD 10.2.2	AKM (Todo Hyperlink)

This setting is possible by configuring the custom entity of the cluster, as shown in Figure 4. Here 'domain-c24' is the vCenter cluster associated with PVDC on VCD. This 'domain-c24' uses AKM2 (Alliance Key Manager) KMS Server (Refer to Figure1 for all configured KMS Servers). Similarly, the provider can change the default key provider for the cluster on the vCenter server.

A few useful commands to configure default and per cluster KMS are as follows:

Set Default KMS for a vCenter cluster: *{vCenter URL}/mob/?moid=CryptoManager&method=setDefaultKmscluster (Use administrator@domain.com login to use the URL)*

Confirm Default KMS for the vCenter cluster: *{vCenter URL}//mob/?moid=CryptoManager&method=getDefaultKmscluster*

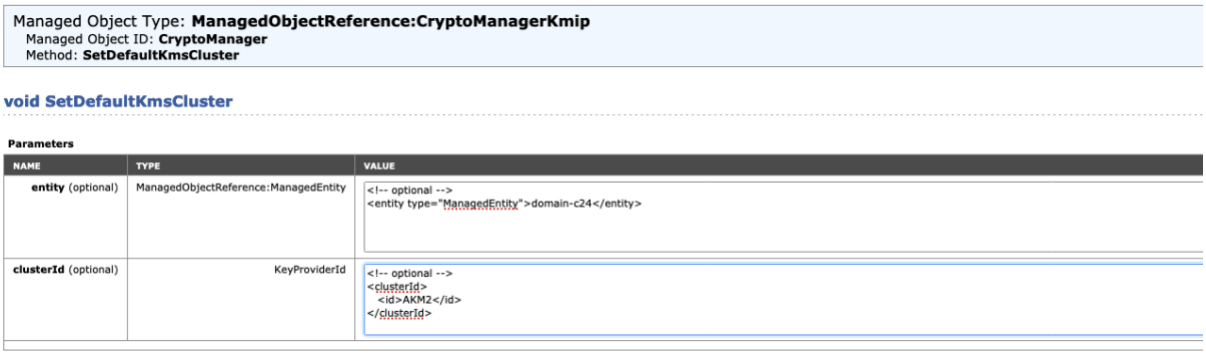

Figure 5 Unique Standard Key Provider Setting per cluster

On vCenter UI, we can also confirm the settings by navigating to each cluster on the vCenter Server.

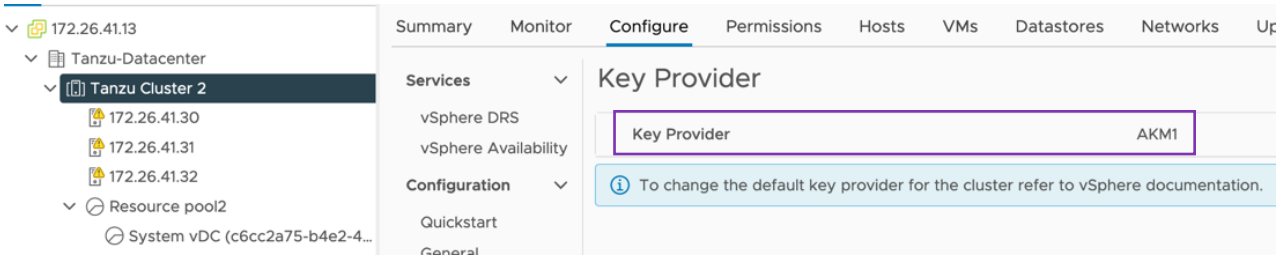

Figure 6 Default KMS on a cluster on the vCenter Server

With this configuration on the vCenter server, the provider is now ready to configure the Storage policy on VCD. The provider can publish the storage policies to the tenant. For this use case, it is required that the provider associates a single PVDC with a single tenant organization. Figure 4 explains this scenario. The significance of a unique Key Provider for the tenant is that each tenant can use independent encryption for all supported entity types.

Design Consideration:

When the Key Provider is unreachable for any reason, the tenant user can still decrypt the VMs for the configured storage policies successfully. However the re-encryption for a new workload from VCD fails, as the KMS is unreachable for the action. Figure 6 showcases how to edit the disks of a VM. The tenant user can decrypt the Workload needs to do the following:

1. Ensure that the disks are all either already using a non-VM-encryption storage policy or are using the VM Default Policy
2. Go to General -> Edit on the Virtual Machine, and click Edit on that screen.

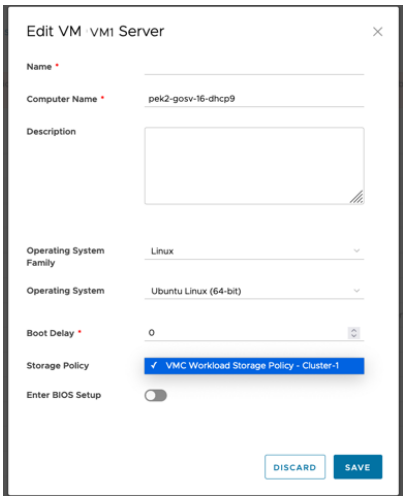

Figure 7 Encrypt/Decrypt a VM from the tenant portal

Use case: KMS Failure scenario with Elastic Org VDC

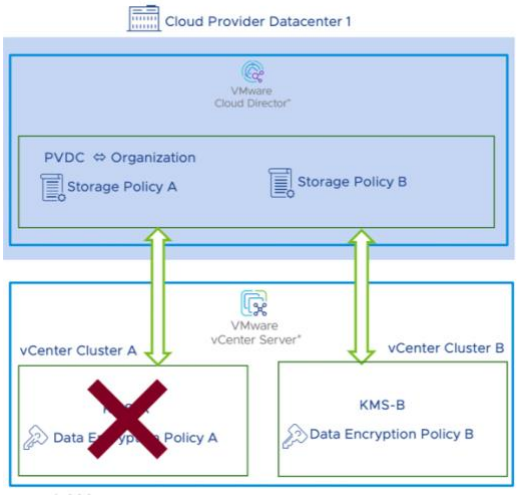

Figure 8 KMS Failure scenario with Elastic Org VDC

In the previous use case, we noticed that when a KMS is unreachable, VM encryption service can be interrupted for the tenant user. To maneuver this limitation, we can leverage Elastic VDC on VCD for the tenant OVDS(in this case, dedicated PVDC). The Elastic VDC allows tenant organizations to consume resources from multiple DRS clusters. The configuration is possible when PVDC spans across two or more clusters on the vCenter server. The official documentation explains the steps to create elastic VDC. The provider can leverage Elastic PVDC on VCD to provide redundancy for Storage encryption. Figure 7 showcases a scenario where the tenant consumes Elastic PVDC and has workloads with VM encryption with 'Storage policy A' and 'Storage Policy B'. In case of Failure of any KMS(in this example, KMS A/Storage Policy A), the tenant can still decrypt the VMs. The provider can migrate VM workloads from cluster A to cluster B. the tenant user then can continue to use 'Storage Policy B' to encrypt the workload VM and other entities.

Summary

To summarize, we reviewed two enhancements for the providers about Storage Policies. The provider can efficiently manage storage policy based on VM, vApp, Catalog, TKG, etc. With a dedicated Key Provider per cluster, the cloud provider can offer dedicated Encryption per tenant when tenant has dedicated PVDC on VCD. The Failure scenario with elastic cluster also provides backup for Encryption for existing and new tenant workloads of any entity type.

List of Figures

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com.

vmware®