CHAPTER 13

vSphere Storage Policies and Encryption

Storage policies and encryption are components in maintaining performance and strong security for virtual machines (VMs). In this chapter we will explore vSphere Storage Policies, which can be customized to meet I/O requirements and improve VM performance. We will also delve into the importance of storage encryption, a feature that ensures data integrity and confidentiality in today's security environment.

Understanding and effectively implementing these policies and encryption techniques is vital. They not only establish a foundation for efficient storage management but also serve as the backbone of a secure and resilient virtual infrastructure. This chapter will guide you through the process of optimizing your storage environment, from creating Storage I/O Controls to configuring VM storage policies for host-based data services. Additionally, we will cover the application of these policies to VMs. To round out the chapter, we'll examine how to set up encryption key providers, providing a comprehensive understanding of both the practical aspects and security considerations in vSphere storage management.

L. Patrão, *VMware vSphere Essentials*, https://doi.org/10.1007/979-8-8688-0208-9_13

A VM storage policy in VMware vSphere is a collection of rules that define the storage requirements for a VM. These rules can be used to control the following:

- The type of storage that is provided for the VM, such as block, NFS, vSAN, or vVols.
- How the VM is placed within the storage, such as on a specific datastore or RAID group.
- Which data services are offered for the VM, such as deduplication, compression, encryption, or replication.

VM storage policies can be used to improve the performance, availability, and security of your VMs. For example, you can create a policy that specifies that all VMs storing sensitive data must be placed on a datastore protected by replication. This will help to ensure that your data is protected in the event of a disaster.

13.1 Understanding vSphere Storage Policies

A set of regulations known as vSphere Storage Policies specify how VMs can store data. These policies may be used to guarantee that virtual machines are installed on datastores that satisfy their unique storage needs.

Storage policies can be used to define the following:

- **The type of storage on which VMs should be located:** You may, for instance, devise a policy that stipulates that VMs must be stored on a datastore that employs a certain storage protocol, such as iSCSI or Fibre Channel. In this case, the policy would specify the protocol.

The operational qualities of the storage medium that VMs should be located on: For instance, you may draft a policy that dictates VMs must be stored on a datastore that meets a certain threshold for the number of input/output operations per second (IOPS) or throughput. For example, you may have large application VMs with large databases that require a certain datastore because they have a lot of IOPS and you are looking for improved performance.

- **The accessibility of the storage medium in which VMs should be installed:** For instance, you may develop a policy that dictates that VMs must be stored on a datastore that replicates its data or is configured for high availability (HA).

Before we create our VM Storage Policy, we will create two Storage Policies, one for encryption and one for Storge I/O Control. This will enable you to understand how Storage Policies work and how they can be used in your VM Storage Policy.

13.2 Storage Policy - Storage I/O

Storage I/O Control (SPBM-SIOC) is a feature in VMware vSphere that allows you to control the I/O performance of your VMs. SIOC works by monitoring the I/O latency of datastores and throttling the I/O of VMs causing the latency. This can help to improve the performance of all VMs on the datastore by preventing a few VMs from hogging all the resources.

SIOC works by allocating shares and limits to VMs. *Shares* are a relative measure of importance, while *limits* are a hard cap on the amount of I/O a VM can consume. When SIOC detects that a datastore is experiencing I/O latency, it throttles the I/O of VMs with a lower share than the VMs that are causing the latency. This ensures that the VMs causing the latency do not get all the resources and that the other VMs on the datastore can still perform well.

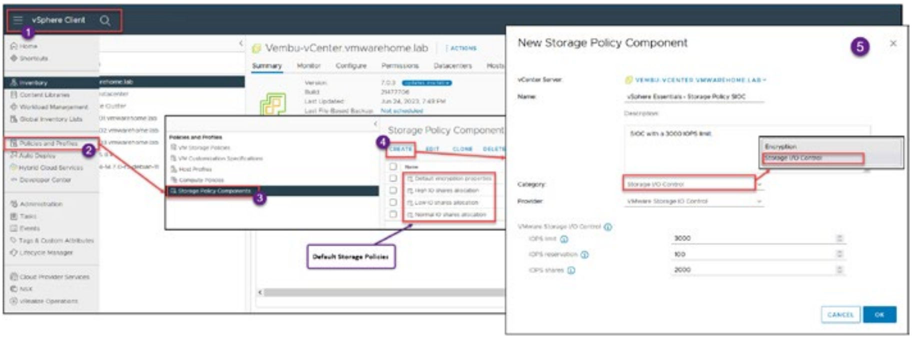
SIOC can be configured on a per-datastore basis. You can specify the following settings for each datastore:

- **I/O throttling threshold:** The I/O latency threshold that SIOC will use to throttle I/O.
- **I/O throttling ratio:** The ratio by which SIOC will throttle I/O. For example, if the I/O throttling threshold is 50ms and the I/O throttling ratio is 2, then SIOC will throttle the I/O of VMs causing latency by 200%.
- **I/O throttling delay:** The delay before SIOC starts throttling I/O. This is useful to prevent SIOC from throttling I/O for transient spikes in latency.

SIOC can be a valuable tool for improving the performance of your VMs. However, it is vital to use it carefully. If you throttle the I/O of VMs too much, you may impact the performance of the VMs. You should also consider the I/O requirements of your VMs when configuring SIOC. For example, if you have a VM running a database, you may want to give it a higher share than a VM running a web server.

13.3 Create a Storage I/O Control

In your vCenter, select the main menu, select **Policies and Profiles**, select **Storage Policy Components**, and click **Create**, as shown in Figure 13-1. In the *Name* field of the New Storage Policy Component dialog box, name your Storage Policy. For purposes of the test lab, use the name **vSphere Essentials - Storage Policy SIOC**. Then, in the *Category* drop-down list, select **Storage I/O Control**. As you can see in Figure 13-1, the other option is to create an Encryption Storage Policy, discussed in the next section.



New Storage Policy Component

vCenter Server: VEMBU-VCENTER.VMWAREHOME.LAB

Name: vSphere Essentials - Storage Policy SIOC

Description: SIOC with a 3000 IOPS limit

Category: Storage I/O Control

Provider: VMware Storage IO Control

VMware Storage I/O Control

IOPS limit: 3000

IOPS reservation: 100

IOPS shares: 2000

Figure 13-1. *(vSphere Storage Policies 1 of 14)*

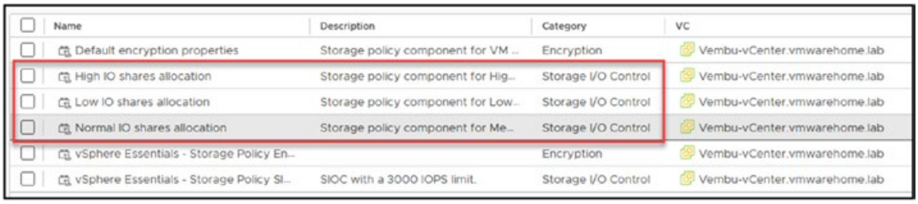
In the VMware Storage I/O Control section, set the *IOPS shares* field to **2000**. This indicates that the datastore that we'll use for this Storage Policy will have reserved shares and won't be used in conjunction with any other datastores.

We also have an IOPS cap. The maximum IOPS for every VM kept in this datastore is 3000, so set the *IOPS limit* field to **3000**. With this cap, we ensure that the VMs kept in this datastore won't consume all of the storage's IOPS.

Caution Use extreme caution when setting the *IOPS limit* option. Be sure the number corresponds to the kind of virtual machines you are keeping in this datastore.

Take into account that the I/O size for *IOPS limit* is normalized to 32KB. This means that if you set *IOPS limit* to 10,000 and the typical I/O size from the VM was 64KB, then you could do only 5000 IOPS. If your block size is 4KB/8KB/16KB or 32KB, you would be able to achieve the 10,000 IOPS limit.

Figure 13-2 shows that you have some default Storage Policies for SIOC, with High, Low, and Normal IOPS. You can use the default SIOC in your VM Storage Policy if it fits your needs.



□	Name	Description	Category	VC
□	Default encryption properties	Storage policy component for VM ...	Encryption	Vembu-vCenter.vmwarehome.lab
□	High IO shares allocation	Storage policy component for Hig...	Storage I/O Control	Vembu-vCenter.vmwarehome.lab
□	Low IO shares allocation	Storage policy component for Low...	Storage I/O Control	Vembu-vCenter.vmwarehome.lab
□	Normal IO shares allocation	Storage policy component for Me...	Storage I/O Control	Vembu-vCenter.vmwarehome.lab
□	vSphere Essentials - Storage Policy En...		Encryption	Vembu-vCenter.vmwarehome.lab
□	vSphere Essentials - Storage Policy SI...	SIOC with a 3000 IOPS limit.	Storage I/O Control	Vembu-vCenter.vmwarehome.lab

Figure 13-2. *(vSphere Storage Policies 2 of 14)*

13.4 Storage Policy - Encryption

Storage Policy - Encryption (SPBM-Encryption) is a feature in VMware vSphere that allows you to encrypt the data on your VMs. Encryption can help to protect your data from unauthorized access.

SPBM-Encryption encrypts the data on the VM's disks before it is written to the datastore. vCenter Server or a third-party key manager manages the encryption key. When the VM boots, it decrypts the data on its disks and uses it as usual.

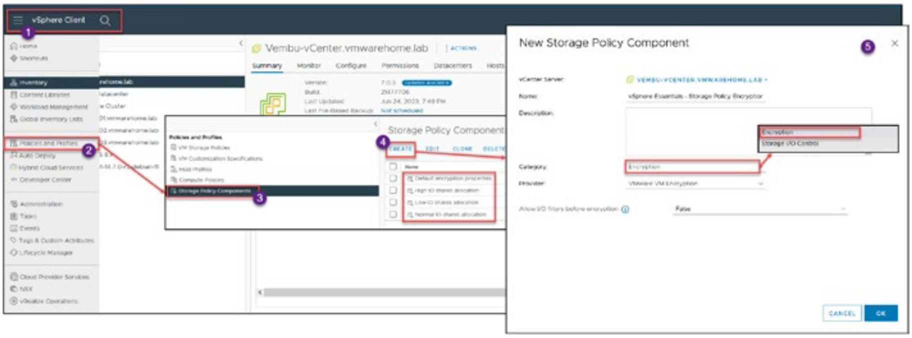
SPBM-Encryption can be configured on a per-VM basis. You can specify the following settings for each VM:

- **Encryption algorithm:** The encryption algorithm that will be used to encrypt the data
- **Key provider:** The key provider that will be used to manage the encryption keys
- **Key rotation:** Whether or not the encryption keys will be rotated on a regular basis
- **Key management:** Whether you will manage the encryption keys yourself or have vCenter Server manage them for you

SPBM encryption can be a valuable tool for protecting your data from unauthorized access. However, using it carefully is essential. If you encrypt the data on your VMs, you cannot access the data without the encryption key. It would be best to consider the performance impact of encryption before enabling it for your VMs.

13.5 Create a Storage Policy - Encryption

Creating a custom Storage Policy Encryption is the same process as shown previously in Figure 13-1, but in the final step you select the *Category* setting **Encryption** instead of Storage I/O Control. You then see the option *Allow I/O filters before encryption*, as shown in Figure 13-3. This option in a VM storage policy in vSphere determines whether I/O filters can be applied to the VM before the data is encrypted. This can improve the performance of the VM, but it can also reduce the security of the data.



vCenter Server: VEMBU-VCENTER.VMWAREHOME.LAB

Name: vSphere Essentials - Storage Policy Encryption

Description:

Category: Encryption

Provider: VMware VM Encryption

Allow I/O filters before encryption: False

Figure 13-3. *(vSphere Storage Policies 3 of 14)*

I/O filters are software components that can be used to modify the data that is being transferred between a VM and its datastore. For example, I/O filters can be used to deduplicate, compress, or encrypt data.

When the *Allow I/O filters before the encryption* option is enabled (set to True), I/O filters will be applied to the VM before the data is encrypted.

This can improve the performance of the VM because the I/O filters will not have to process encrypted data. However, it can also reduce the security of the data because the I/O filters will be able to access the data in clear text before it is encrypted.

Whether or not to enable the *Allow I/O filters before the encryption* option depends on your specific requirements. If you are concerned about the performance of your VMs, you may want to enable this option. However, if you are concerned about the security of your data, you may want to disable this option. In our test lab configuration, will not allow I/O filters before the encryption, so make sure this option is set to **False**.

13.6 VM Storage Policy for Host-Based Data Services

Host-based services options in VMware vSphere allow you to enable and configure the ESXi host's data services. These services can improve the performance, availability, and security of your VMs. This is the default policy for your VM Storage Encryption, but you can create a custom policy.

The Create VM Storage Policy wizard in the vSphere Client enables you to define VM storage policy. This wizard creates data service rules for ESXi hosts. These VM storage policy rules activate virtual machine data services.

Caching, I/O control, and encryption are data services. VMware offers data encryption. Host-installed third-party I/O filters provide other services. Data services are general and independent of datastores. Datastore-specific storage policy rules are optional.

If your policy includes rules specific to datastores, it can enforce encryption through both the host and storage I/O filters, resulting in the virtual machine data being encrypted twice by the I/O filter and the storage system. vSphere Virtual Volumes (vVols) and I/O filter replication cannot coexist in a storage policy.

Once you have enabled host-based services for a VM, the services will be available to the VM when it is powered on. The services will be used to improve the performance, availability, and security of the VM.

It is important to note that not all host-based services are supported on all ESXi hosts. You should check the compatibility matrix for your ESXi host to see which services are supported.

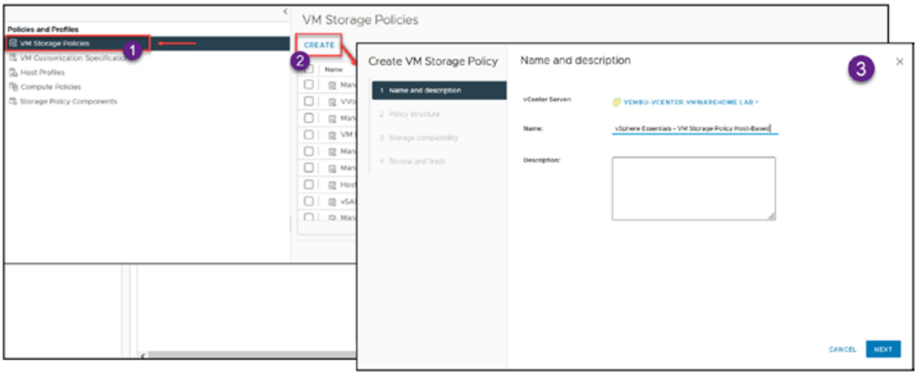
Here are some additional things to keep in mind about host-based services:

- Host-based services can have a performance impact on your VMs. You should carefully evaluate the performance impact before enabling host-based services for your VMs.
- Host-based services can increase the complexity of your vSphere environment. You should carefully plan your host-based services configuration to ensure it is manageable.
- Host-based services can be a security risk. You should carefully configure your host-based services to protect your data from unauthorized access.

13.7 Create VM Storage Policy for Host-Based Data Services

In the vSphere Client, select **Policies and Profiles**, then **VM Storage Policies**, and click **Create** to open the Create VM Storage Policy wizard and start creating your VM storage policy for host-based data services.

In step 1, shown in Figure 13-4, name your Storage Policy. For purposes of the test lab, use the name **vSphere Essentials - VM Storage Policy Host-Based**. Then, if you prefer, add a description (it is not mandatory). Click **Next**.



vCenter Server: VEMBU-VCENTER.VMWAREHOME.LAB

Name: vSphere Essentials - VM Storage Policy Host-Based

Description:

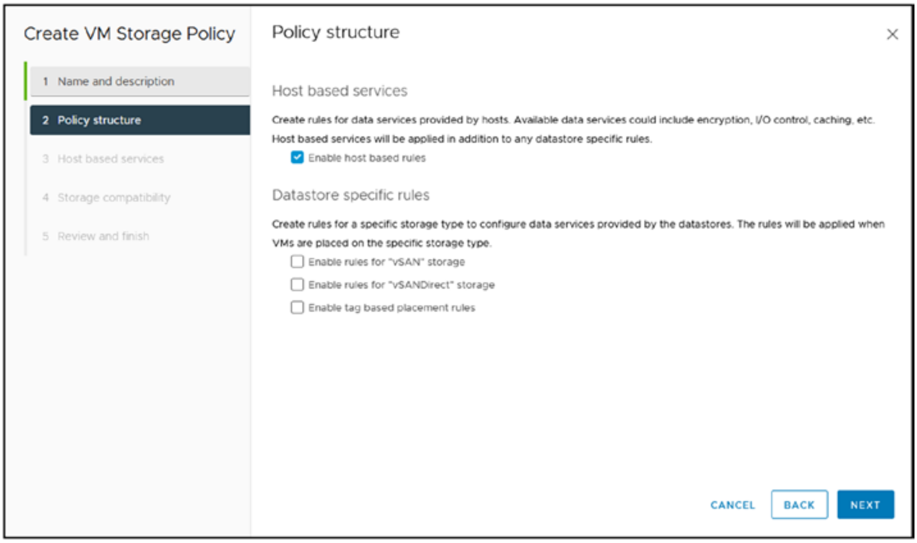
Figure 13-4. *(vSphere Storage Policies 4 of 14)*

In step 2, *Policy structure* (see Figure 13-5), click **Enable host based rules** to enable host-based rules in this VM Storage Policy. Next in step 2, in the *Datastore specific rules* section, you can select datastore-specific rules, allowing you to create rules specific to a particular datastore type. For example, you could create a rule specifying that all VMs placed on a vSAN datastore must be encrypted. This will help to protect your data from unauthorized access. The options are as follows:

- **Enable rules for "vSAN" storage:** This option enables datastore-specific rules for vSAN datastores. This is useful to configure data services for vSAN datastores, such as deduplication, compression, or encryption.
- **Enable rules for "vSANDirect" storage:** This feature, introduced in version vSphere 7 Update 3, is specifically tailored for containerized applications. It works well in conjunction with VMware Tanzu Kubernetes Grid. By attaching datastores to ESXi hosts, vSANDirect offers optimized storage performance. It's important to note that vSANDirect is meant for containerized

environments and is not suitable for VM workloads. Leveraging vSANDirect can greatly improve storage efficiency and performance for applications running in containers.

Note The preceding two rules are used only if you use vSAN in your environment.



Create VM Storage Policy

1 Name and description
2 Policy structure
3 Host based services
4 Storage compatibility
5 Review and finish

Policy structure

Host based services

Create rules for data services provided by hosts. Available data services could include encryption, I/O control, caching, etc. Host based services will be applied in addition to any datastore specific rules.

☑ Enable host based rules

Datastore specific rules

Create rules for a specific storage type to configure data services provided by the datastores. The rules will be applied when VMs are placed on the specific storage type.

□ Enable rules for "vSAN" storage
□ Enable rules for "vSANDirect" storage
□ Enable tag based placement rules

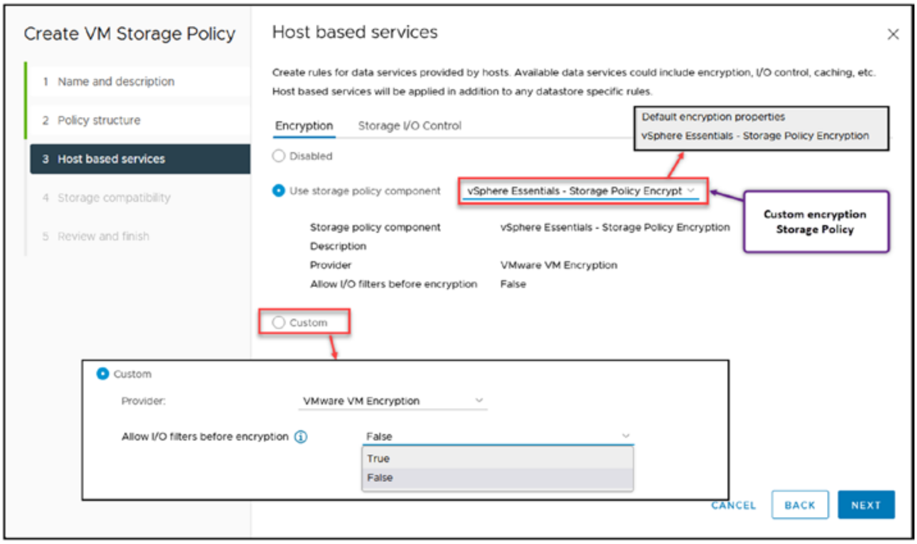
Figure 13-5. *(vSphere Storage Policies 5 of 14)*

Enable tag based placement rules: This option allows you to create rules based on tags. You can assign labels to datastores, VMs, and other objects in vSphere. For example, you could assign a “high performance” tag to all datastores dedicated to running high-performance VMs. You could then create a rule that specifies that all VMs tagged with “high performance” must be placed on a datastore tagged with “high performance.” This will help ensure that your high-performance VMs are always on the best possible storage.

In the test lab environment, we won't be using tags or vSAN; therefore, leave these settings deactivated. Click **Next**.

In step 3 of the wizard, *Host based services*, you configure the Encryption and Storage I/O Control settings on their respective tabs, described here:

- **Encryption:** This tab, shown in Figure 13-6, includes the following options:
- **Disabled:** This option disables host-based services for the VM. This means that no data services will be provided to the VM by the ESXi host.
- **Use storage policy component:** This option uses the data services defined in the storage policy component associated with the VM. This is the default option.



Create VM Storage Policy

1 Name and description
2 Policy structure
3 Host based services
4 Storage compatibility
5 Review and finish

Host based services

Create rules for data services provided by hosts. Available data services could include encryption, I/O control, caching, etc. Host based services will be applied in addition to any datastore specific rules.

Encryption | Storage I/O Control

Default encryption properties
vSphere Essentials - Storage Policy Encryption

○ Disabled

● Use storage policy component: vSphere Essentials - Storage Policy Encrypt

Custom encryption Storage Policy

Storage policy component	vSphere Essentials - Storage Policy Encryption
Description	
Provider	VMware VM Encryption
Allow I/O filters before encryption	False

○ Custom

● Custom

Provider: VMware VM Encryption

Allow I/O filters before encryption: False (True / False)

Figure 13-6. *(vSphere Storage Policies 6 of 14)*

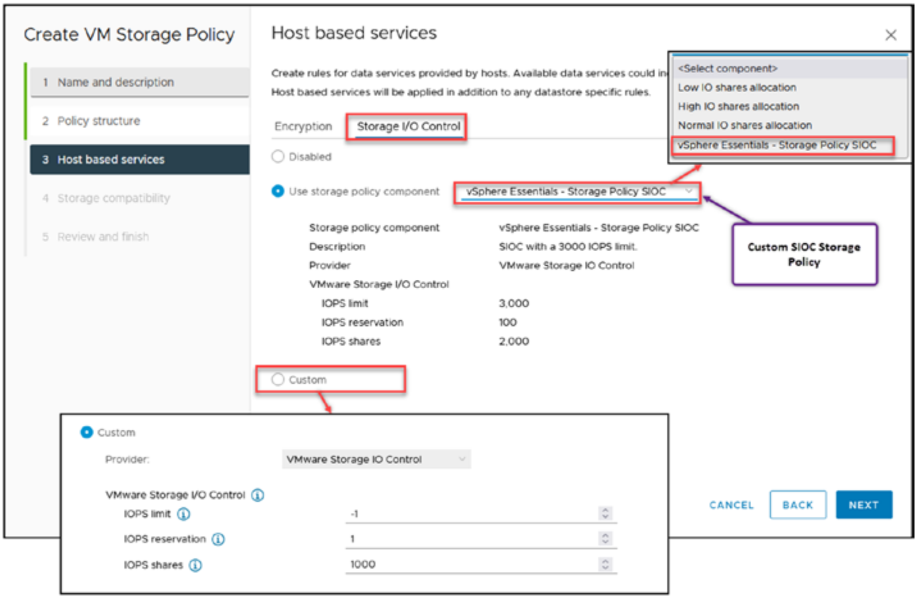
Note We previously created some custom Storage Policies (encryption or Storage I/O Control). We can now use this option in our host-based services. In our case, we previously created one Storage I/O Control.

- **Custom:** This option allows you to specify custom data services for the VM. You can choose from the following data services: Deduplication, Compression, Encryption, and Replication. Figure 13-6 shows that you can use the default VMware VM Encryption provider in the *Custom* option and turn the I/O filters on or off before encryption.
- **Storage I/O Control:** This tab, shown in Figure 13-7, includes options to configure SIOC (previously discussed). In VM Storage Policy SIOC we will disable or add our policy created before, or don't use any default/custom and create a custom SIOC just for this VM Storage Policy. This tab includes the following options:
- **Disabled:** This option disables host-based services for the VM. This means that no data services will be provided to the VM by the ESXi host. This option is useful if you do not want any data services to be provided to the VM. This may be useful for VMs that do not need any data services, such as small VMs or VMs that are not used often.
- **Use storage policy component:** This option uses the data services defined in the storage policy component associated with the VM. This is the default option. This

is the most common option, as it ensures that the VM always uses the most appropriate data services for its needs. We will use the **vSphere Essentials - Storage Policy SIOC** Storage Policy SIOC created in the previous section.

- **Custom:** This option allows you to specify custom data services for the VM. You set limits for your environment. This option is useful if you have specific requirements for the data services that are provided to the VM. For example, you may want to specify that the VM should be encrypted, or that it should be replicated to a remote location. Figure 13-7 shows the VMware Storage IO Control provider selected. The remainder of this list describes the other fields in the *Custom* option.
- **IOPS limit:** Sets an upper boundary on the number of IOPS a VM or VMDK can perform. It ensures that the VM or its disks do not consume I/O beyond this limit, regardless of available I/O resources on the datastore.
- **IOPS reservation:** Defines a guaranteed minimum number of IOPS that will be reserved for the VM or its VMDKs. With this setting, you're ensuring that even under storage contention, the VM or disk will always have this minimum level of performance.
- **IOPS shares:** Represents the relative priority or weight of a VM's I/O allocation when there is contention. VMs with more shares will be allocated more I/O resources during contention than VMs with fewer shares.

It is essential to carefully consider your requirements before choosing the option for host-based services in a VM storage policy. You should also monitor the performance of your VMs to ensure that the provided data services are meeting your needs. Click **Next** to proceed to step 4 of the Create VM Storage Policy wizard.



Create VM Storage Policy

1 Name and description

2 Policy structure

3 Host based services

4 Storage compatibility

5 Review and finish

Host based services

Create rules for data services provided by hosts. Available data services could in Host based services will be applied in addition to any datastore specific rules.

Encryption | Storage I/O Control

○ Disabled

● Use storage policy component: vSphere Essentials - Storage Policy SIOC

Storage policy component	vSphere Essentials - Storage Policy SIOC
Description	SIOC with a 3000 IOPS limit.
Provider	VMware Storage IO Control
VMware Storage I/O Control	
IOPS limit	3,000
IOPS reservation	100
IOPS shares	2,000

○ Custom

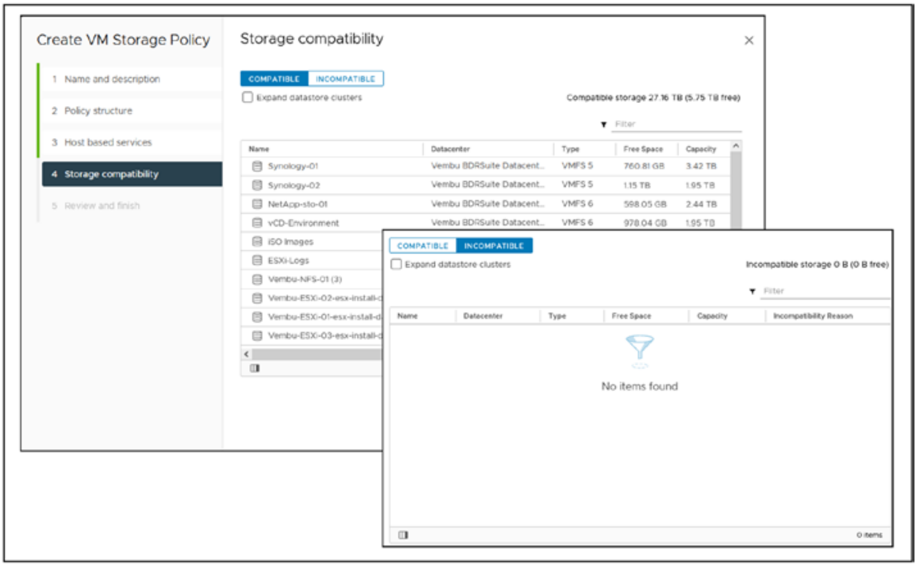
● Custom

Provider:	VMware Storage IO Control
VMware Storage I/O Control	
IOPS limit	-1
IOPS reservation	1
IOPS shares	1000

<Select component>
Low IO shares allocation
High IO shares allocation
Normal IO shares allocation
vSphere Essentials - Storage Policy SIOC
Custom SIOC Storage Policy
CANCEL
BACK
NEXT

Figure 13-7. *(vSphere Storage Policies 7 of 14)*

Step 4, shown in Figure 13-8, lists all existing datastores compatible with the VM Storage Policy we created. You can also click the **Incompatible** tab to check the ones that are not compatible, shown in the lower-right image.



Create VM Storage Policy

1 Name and description

2 Policy structure

3 Host based services

4 Storage compatibility

5 Review and finish

Storage compatibility

COMPATIBLE INCOMPATIBLE

□ Expand datastore clusters

Compatible storage 27.16 TB (5.75 TB free)

Name	Datacenter	Type	Free Space	Capacity
Synology-01	Vembu BDRSuite Datacent...	VMFS 5	760.81 GB	3.42 TB
Synology-02	Vembu BDRSuite Datacent...	VMFS 5	1.15 TB	1.95 TB
NetApp-sto-01	Vembu BDRSuite Datacent...	VMFS 6	598.05 GB	2.44 TB
vCD-Environment	Vembu BDRSuite Datacent...	VMFS 6	978.04 GB	1.95 TB
ISO Images				
ESXi-Logs				
Vembu-NFS-01 (3)				
Vembu-ESXi-02-esx-install-d				
Vembu-ESXi-01-esx-install-d				
Vembu-ESXi-03-esx-install-d				

COMPATIBLE INCOMPATIBLE

□ Expand datastore clusters

Incompatible storage 0 B (0 B free)

Name	Datacenter	Type	Free Space	Capacity	Incompatibility Reason

No items found

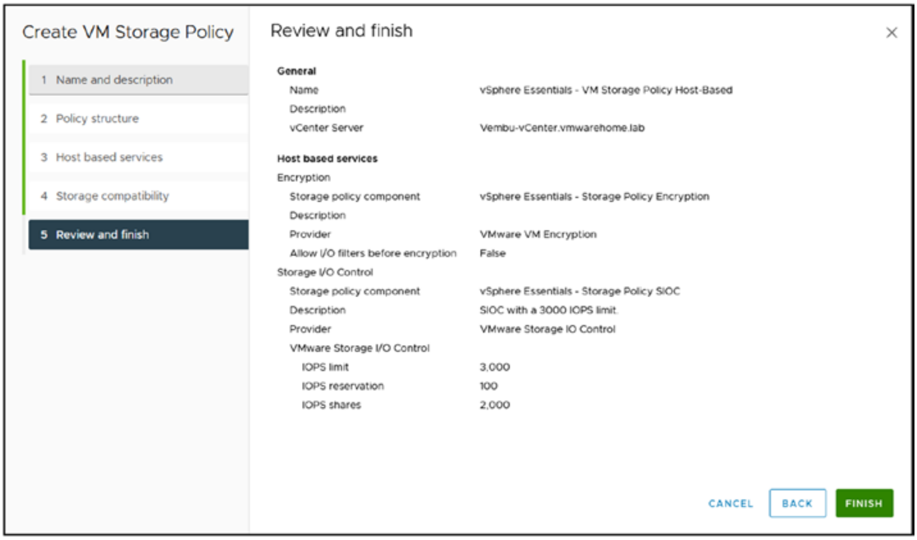
0 items

Figure 13-8. *(vSphere Storage Policies 8 of 14)*

The compatibility status of datastores is important to know so that you can create or move your VMs to the correct datastore and have your VM Storage Policy applied.

Figure 13-8 shows that all datastores are compatible with the VM Storage Policy created. The *Incompatible* tab is empty. Click **Next**.

Finally, review all the settings you have configured in the previous wizard steps (see Figure 13-9) and finish creating your VM Storage Policy by clicking **Finish**.



Create VM Storage Policy

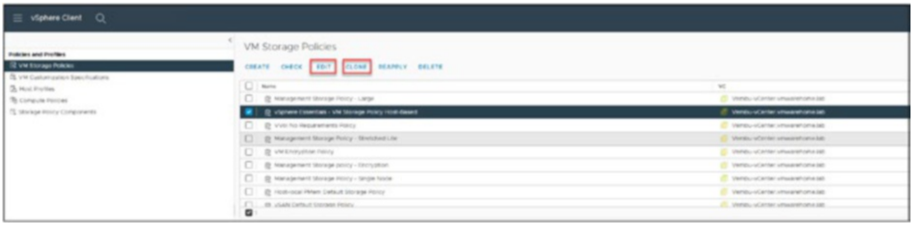
1 Name and description
2 Policy structure
3 Host based services
4 Storage compatibility
5 Review and finish

Review and finish

General	
Name	vSphere Essentials - VM Storage Policy Host-Based
Description	
vCenter Server	Vembu-vCenter.vmwarehome.lab
Host based services	
Encryption	
Storage policy component	vSphere Essentials - Storage Policy Encryption
Description	
Provider	VMware VM Encryption
Allow I/O filters before encryption	False
Storage I/O Control	
Storage policy component	vSphere Essentials - Storage Policy SIOC
Description	SIOC with a 3000 IOPS limit.
Provider	VMware Storage IO Control
VMware Storage I/O Control	
IOPS limit	3,000
IOPS reservation	100
IOPS shares	2,000

Figure 13-9. *(vSphere Storage Policies 9 of 14)*

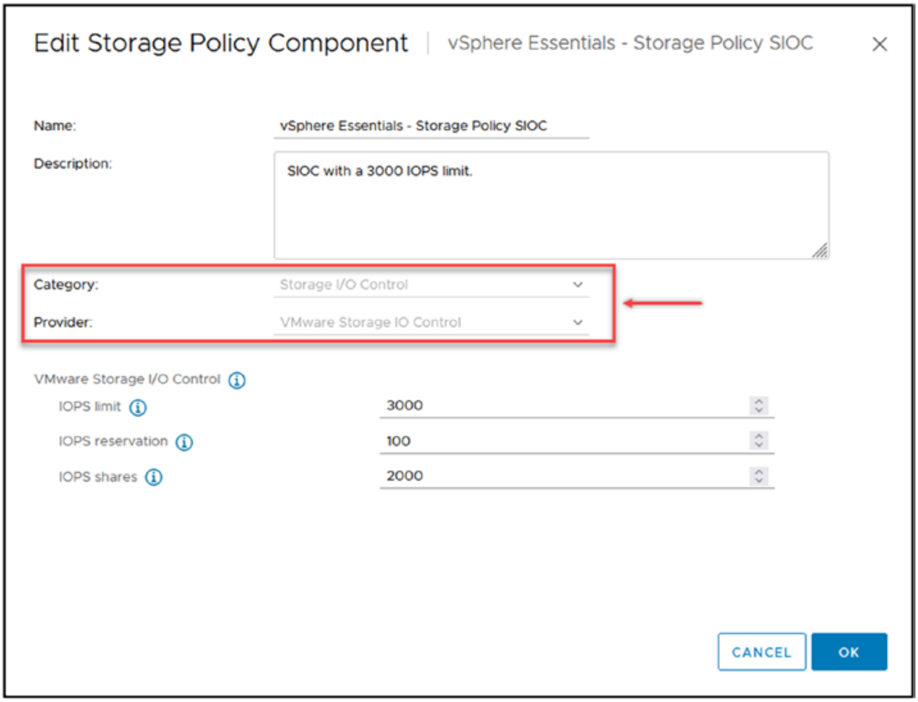
After your VM Storage Policy is finished, you can edit or clone it (or any existing Storage Policy or VM Storage Policy in the list of existing Policies) by selecting it and clicking **Edit** or **Clone**. See Figure 13-10.



□	Name	VC
□	Management Storage Policy - Large	Vembu-vCenter.vmwarehome.lab
☑	vSphere Essentials - VM Storage Policy Host-Based	Vembu-vCenter.vmwarehome.lab
□	VVol No Requirements Policy	Vembu-vCenter.vmwarehome.lab
□	Management Storage Policy - Stretched Lite	Vembu-vCenter.vmwarehome.lab
□	VM Encryption Policy	Vembu-vCenter.vmwarehome.lab
□	Management Storage policy - Encryption	Vembu-vCenter.vmwarehome.lab
□	Management Storage Policy - Single Node	Vembu-vCenter.vmwarehome.lab
□	Host-local PMem Default Storage Policy	Vembu-vCenter.vmwarehome.lab
□	vSAN Default Storage Policy	Vembu-vCenter.vmwarehome.lab

Figure 13-10. *(vSphere Storage Policies 10 of 14)*

You can change any settings in the VM Storage Policy and Storage Policy **Clone** option. However, as shown in Figure 13-11, you cannot change the Category and Provider settings with the **Edit** option in SIOC or and Encryption policy serve distinct purposes and operate differently.



Edit Storage Policy Component | vSphere Essentials - Storage Policy SIOC

Name: vSphere Essentials - Storage Policy SIOC

Description: SIOC with a 3000 IOPS limit.

Category: Storage I/O Control

Provider: VMware Storage IO Control

VMware Storage I/O Control

IOPS limit: 3000

IOPS reservation: 100

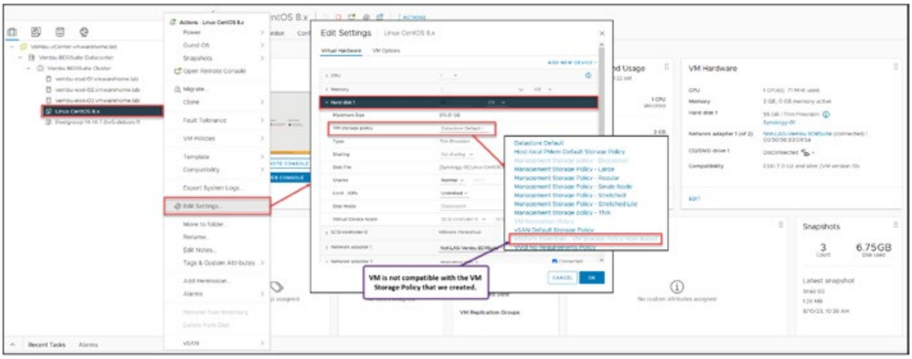
IOPS shares: 2000

Figure 13-11. *(vSphere Storage Policies 11 of 14)*

13.8 Apply VM Storage Policy to VMs

After creating all our Storage Policies and VM Storage Policies, we need to apply them to the existing VMs or use them when creating a new VM.

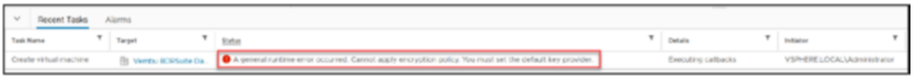
You need to ***Edit VM setting***s, select the Hard Disk, and change the *VM Storage policy* option for the existing VM. However, as shown in Figure 13-12, although this VM was created, it is incompatible with the VM Storage Policy we previously created.



VM is not compatible with the VM Storage Policy that we created.

Figure 13-12. *(vSphere Storage Policies 12 of 14)*

If we try to create a VM with the new encrypted VM Storage Policy, we get the error shown in Figure 13-13: *A general runtime error occurred. Cannot apply encryption policy. You must set the default key provider.*



Task Name	Target	Status	Details	Initiator
Create virtual machine	Vembu BCRSuite Da...	A general runtime error occurred. Cannot apply encryption policy. You must set the default key provider.	Executing callbacks	VSPHERE.LOCAL\Administrator

Figure 13-13. *(vSphere Storage Policies 13 of 14)*

This error occurs because we are trying to encrypt our datastore and VMs but haven't created a key provider. We select the ESXi host, configure tab and in Security and Key Providers option we that is empty. As shown in the Figure 13-14.

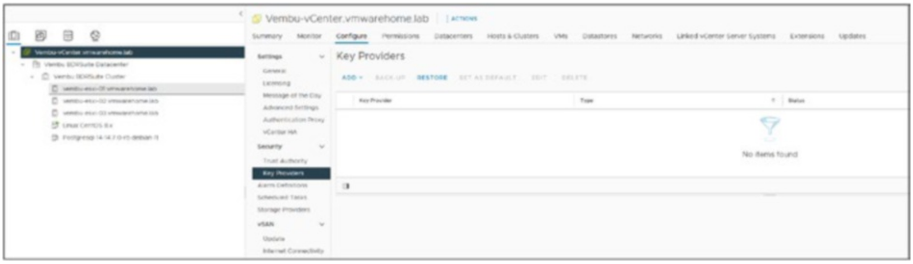


Figure 13-14. *(vSphere Storage Policies 14 of 14)*

So, we need to add a key provider in our vCenter. But before we add a key provider, let's examine what exactly is a key provider.

13.8.1 What Is a Key Provider?

A *security key provider* is a software component responsible for managing the encryption keys used to protect your data. Storage vendors typically implement security key providers.

When you create a VM storage policy specifying that encryption should be enabled, you can specify the security key provider you want to use. The security key provider will then manage the encryption keys used to encrypt the data on the VM's disks.

There are two types of security key providers:

- **Local security key providers:** Store the encryption keys on the ESXi host. This is the most common type of security key provider.
- **Remote security key providers:** Store the encryption keys on a remote server. This type of security key provider is more secure than local security key providers, but it is also more complex to configure.

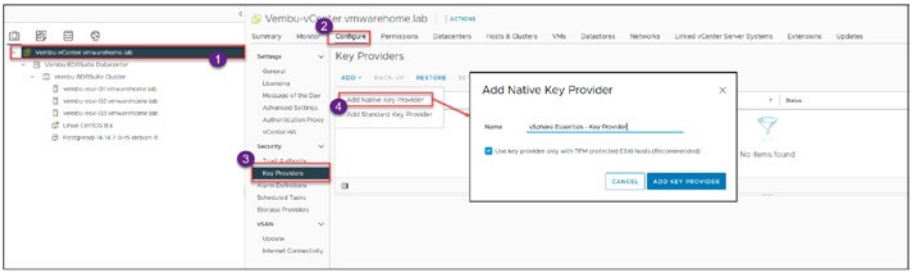
The decision of whether to use a local or remote security key provider depends on your specific requirements. If you need a high level of security, you should use a remote security key provider. You should use a local security key provider for a more straightforward configuration.

Without a key provider, vCenter cannot handle the encryption.

13.9 Add an Encryption Key Provider

To add a key provider, go to vCenter, click the **Configure** tab, select **Key Providers** in the *Security* section, and select either of the following options (see Figure 13-15):

- **Add Native Key Provider:** This option adds the vCenter Server Native Key Provider to the VM storage policy. The vCenter Server Native Key Provider is a local security key provider that stores the encryption keys on the ESXi host. This is the most common option to use.
- **Add Standard Key Provider:** This option adds a third-party security key provider to the VM storage policy. Third-party security key providers can offer more features and security than the vCenter Server Native Key Provider. However, they are also more complex to configure.


Add Native Key Provider

Name: vSphere Essentials - Key Provider

☑ Use key provider only with TPM protected ESXi hosts (Recommended)

Figure 13-15. *(Key Provider 1 of 4)*

The decision of whether to use the vCenter Server Native Key Provider or a third-party security key provider depends on your specific requirements. If you need a simple and secure solution, use the vCenter

Server Native Key Provider. If you need more features and security, you should use a third-party security key provider.

Here are some of the benefits of using the vCenter Server Native Key Provider:

- **Simple to configure:** The vCenter Server Native Key Provider is easy to configure and manage.
- **Secure:** The vCenter Server Native Key Provider uses strong encryption algorithms to protect your data.
- **Consistent:** The vCenter Server Native Key Provider is available on all supported ESXi hosts.

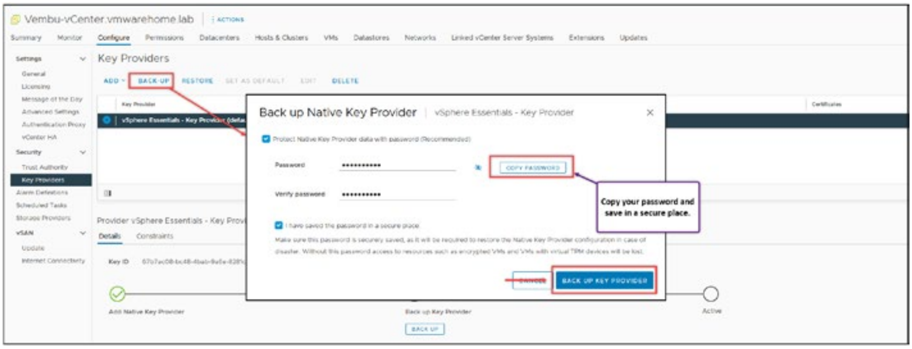
Here are some of the benefits of using a third-party security key provider:

- **More features:** Third-party security key providers can offer more features than the vCenter Server Native Key Provider, such as centralized key management and auditing.
- **More secure:** Third-party security key providers can offer more security than the vCenter Server Native Key Provider, such as hardware security modules and multifactor authentication.
- **Scalable:** Third-party security key providers can be scaled to meet the needs of your environment. For example, you can use multiple third-party security key providers to store the encryption keys for your VMs. This option adds the vCenter Server Native Key Provider to the VM storage policy.

For our test lab environment, add the default Native Key Provider managed by vCenter, which is free, by using the option **Add Native Key Provider** and then clicking **Add Key Provider** in the dialog box (see Figure 13-15). If you use the option **Add Standard Key Provider**, this requires a third-party service that usually has a service cost. For production, you should always use the latter option.

Caution Enable the option *Use key provider only with TPM protected ESXi hosts* (shown in Figure 13-15) only if you have hardware TPM.

Next, to finalize your key provider, you need to back it up. As shown in Figure 13-16, select **Key Providers**, click the **Back-Up** option, check the option **Protect Native Key Provider data with password**, and provide a password for your key provider. Click **Copy Password** to copy and save your password in a secure place. Check the check box to confirm your action. Finally, click **Back Up Key Provider**.



Back up Native Key Provider | vSphere Essentials - Key Provider

☑ Protect Native Key Provider data with password (Recommended)

Password ••••••••••• COPY PASSWORD

Verify password •••••••••••

☑ I have saved the password in a secure place

Make sure this password is securely saved, as it will be required to restore the Native Key Provider configuration in case of disaster. Without this password access to resources such as encrypted VMs and VMs with virtual TPM devices will be lost.

CANCEL BACK UP KEY PROVIDER

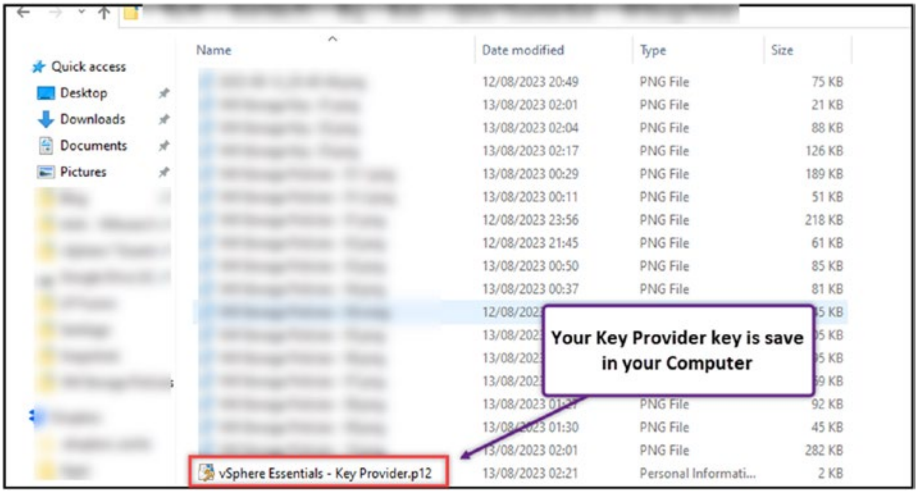
Copy your password and save in a secure place.

Figure 13-16. *(Key Provider 2 of 4)*

Caution If you lose your password, you cannot unencrypt any data.

Note Always select the option to protect the Native Key Provider data with a password. Backing up the Native Key Provider without password protection exposes its configuration data and the virtual machines encrypted with key providers to potential security threats.

After you click Back Up Key Provider, the Key Provider file is downloaded to your computer, as shown in Figure 13-17. Store the file in a secure place.

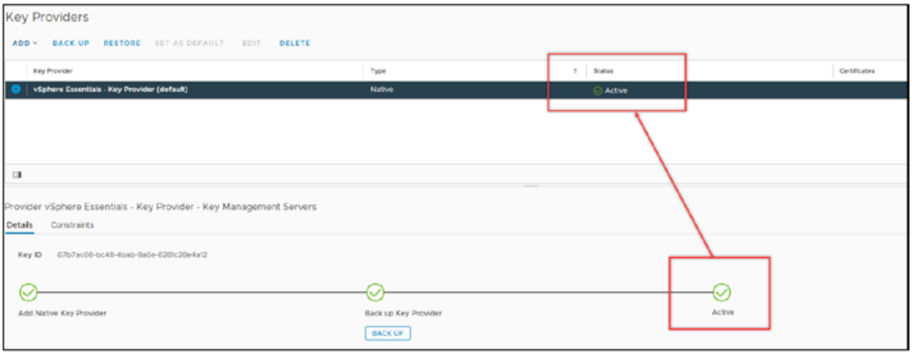


Name	Date modified	Type	Size
[redacted]	12/08/2023 20:49	PNG File	75 KB
[redacted]	13/08/2023 02:01	PNG File	21 KB
[redacted]	13/08/2023 02:04	PNG File	88 KB
[redacted]	13/08/2023 02:17	PNG File	126 KB
[redacted]	13/08/2023 00:29	PNG File	189 KB
[redacted]	13/08/2023 00:11	PNG File	51 KB
[redacted]	12/08/2023 23:56	PNG File	218 KB
[redacted]	12/08/2023 21:45	PNG File	61 KB
[redacted]	13/08/2023 00:50	PNG File	85 KB
[redacted]	13/08/2023 00:37	PNG File	81 KB
[redacted]	12/08/202		5 KB
[redacted]	13/08/202		5 KB
[redacted]	13/08/202		5 KB
[redacted]	13/08/202		9 KB
[redacted]	13/08/2023 01:27	PNG File	92 KB
[redacted]	13/08/2023 01:30	PNG File	45 KB
[redacted]	13/08/2023 02:01	PNG File	282 KB
vSphere Essentials - Key Provider.p12	13/08/2023 02:21	Personal Informati...	2 KB

Your Key Provider key is save in your Computer

Figure 13-17. *(Key Provider 3 of 4)*

Now your key provider is active (see Figure 13-18), and you can use any of the Storage or VM Encryption policies you have previously created.



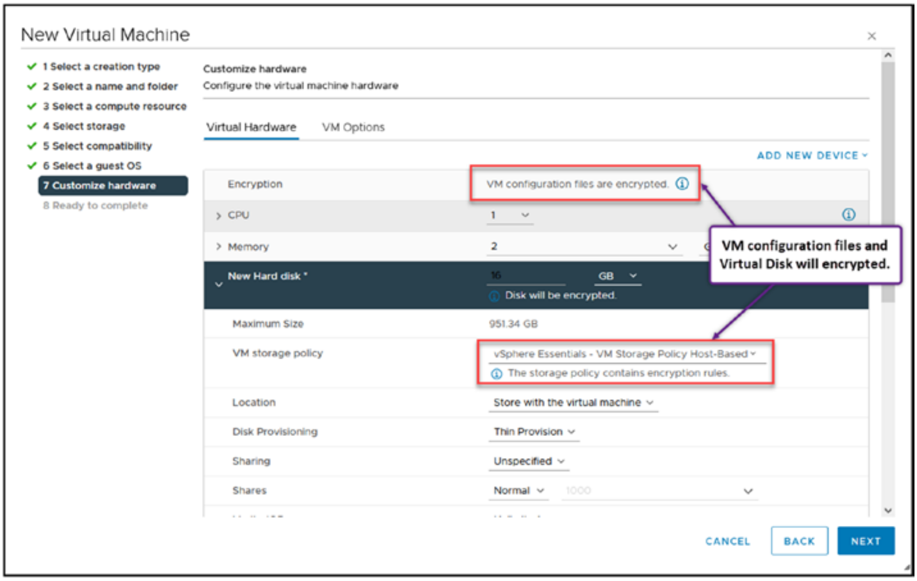
Key Provider	Type	Status	Certificates
vSphere Essentials - Key Provider (default)	Native	Active	

Provider vSphere Essentials - Key Provider - Key Management Servers

Key ID 67b7ac08-bc48-4bab-9a5e-0281c28e4a12

Figure 13-18. *(Key Provider 4 of 4)*

As Figure 13-19 shows, the VM and virtual disk are now encrypted when we create a new VM and select our VM Storage Policy.



Customize hardware
Configure the virtual machine hardware

Encryption: VM configuration files are encrypted.

CPU: 1

Memory: 2

New Hard disk *: 16 GB
Disk will be encrypted.

Maximum Size: 951.34 GB

VM storage policy: vSphere Essentials - VM Storage Policy Host-Based
The storage policy contains encryption rules.

Location: Store with the virtual machine

Disk Provisioning: Thin Provision

Sharing: Unspecified

Shares: Normal 1000

VM configuration files and Virtual Disk will encrypted.

Figure 13-19. *(vSphere Storage Policies 14 of 15)*

To encrypt VMs that already exist, we need to encrypt the VM configuration files first and then the VM virtual disk.

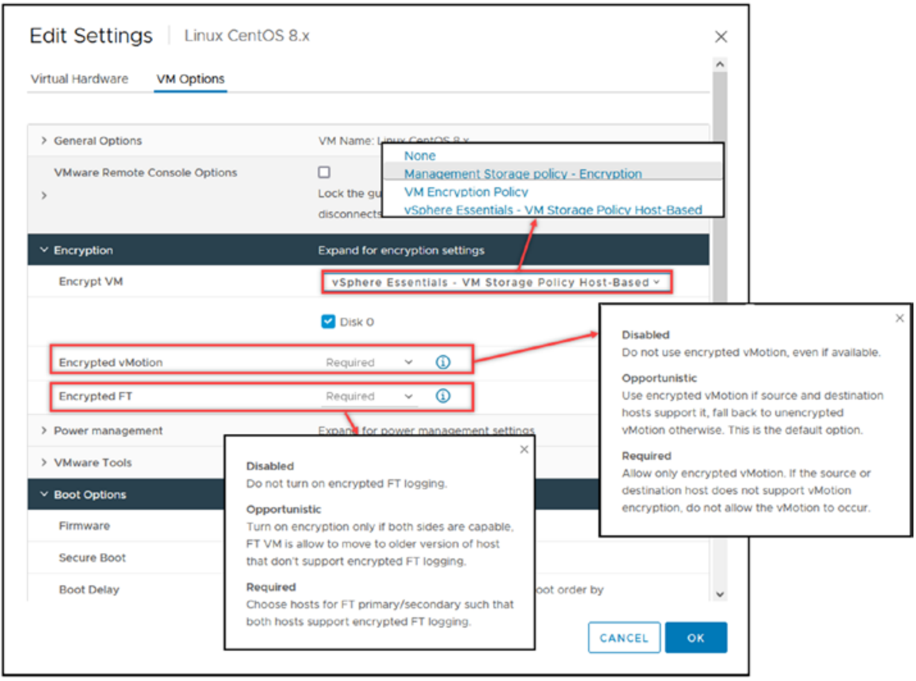
The VM needs to be powered off to encrypt the VM configuration files. Go to **VM settings**, click the **VM Options** tab, expand the **Encryption** section, and then ***VM Encryption*** and use change to your VM Storage Policy.

By selecting the option **Disk**, it also encrypts the virtual disk. Then you don’t need to return to the VM Settings and change the virtual disk VM Storage Policy.

The VM configuration files and virtual disk will both be encrypted.

Note If the VM has any snapshots, it is not possible to encrypt the virtual disks. If you want to encrypt the virtual disks, delete all snapshots from the VM.

When you encrypt your VM, you can also choose to encrypt vMotion and vSphere Fault Tolerance (FT) for the VM. Check Figure 13-20 for the options you have to encrypt those two vSphere features.



Edit Settings | Linux CentOS 8.x

Virtual Hardware | VM Options

General Options — VM Name: Linux CentOS 8.x

VMware Remote Console Options — □ Lock the gu… disconnects

- None
- Management Storage policy - Encryption
- VM Encryption Policy
- vSphere Essentials - VM Storage Policy Host-Based

Encryption — Expand for encryption settings

Encrypt VM — vSphere Essentials - VM Storage Policy Host-Based

☑ Disk 0

Encrypted vMotion — Required

Encrypted FT — Required

Power management — Expand for power management settings

VMware Tools

Boot Options

Firmware

Secure Boot

Boot Delay — …oot order by

Disabled
Do not use encrypted vMotion, even if available.

Opportunistic
Use encrypted vMotion if source and destination hosts support it, fall back to unencrypted vMotion otherwise. This is the default option.

Required
Allow only encrypted vMotion. If the source or destination host does not support vMotion encryption, do not allow the vMotion to occur.

Disabled
Do not turn on encrypted FT logging.

Opportunistic
Turn on encryption only if both sides are capable. FT VM is allow to move to older version of host that don't support encrypted FT logging.

Required
Choose hosts for FT primary/secondary such that both hosts support encrypted FT logging.

Figure 13-20. *(vSphere Storage Policies 15 of 15)*

13.10 Summary

This chapterfocuses on enhancing performance and security for virtual machines (VMs). It covers how custom storage policies can meet specific I/O requirements to boost VM performance and details the significance of storage encryption for protecting data integrity and confidentiality.

The discussion includes optimizing storage through Storage I/O Controls (SIOC) and configuring VM policies for host-based data services, alongside their application to VMs. The setup of encryption providers is also addressed, providing a rounded understanding of the practicalities and security considerations in managing vSphere storage.

Key points include the importance of tailoring storage configurations to improve performance and offer essential data services like deduplication, compression, and encryption. The guidance offered helps establish efficient storage management and a secure virtual infrastructure, emphasizing encryption for data protection and the strategic use of SIOC for performance enhancement.