vSphere Native Key Provider (NKP) Questions & Answers

Table of contents

vSphere Native Key Provider (NKP) Questions & Answers

Questions & Answers

Is Native Key Provider suitable for production environments?

Yes, Native Key Provider is fully supported and ready to be used in all types of environments, including production.

Is Native Key Provider a KMS?

Native Key Provider is designed specifically for encryption in vSphere and is not a Key Management System (KMS), therefore it doesn't support KMIP or other protocols for key interchange.

Can I use Native Key Provider with my external devices, like my tape library or storage array?

Native Key Provider is for use only within vSphere and does not support traditional KMS connectivity.

What version of vSphere do I need to use Native Key Provider?

Both vCenter Server and ESXi need to be at vSphere 7 Update 2 or newer.

Can I use Native Key Provider with vSphere 6.7 if I update vCenter Server to version 7 or 8?

Both vCenter Server and ESXi need to be at vCenter Server 7 Update 2 or later. We strongly recommend running the latest versions of supported products.

Are there more requirements to use Native Key Provider?

You must log into the vSphere Client using the FQDN of the vCenter Server, you must back the Native Key Provider instance up before it will let you use it, and you must set a default key provider. Please review the documentation for more information about requirements.

I’m having trouble enabling Native Key Provider. What should I look at?

Native Key Provider is easy to use, but there are some things to check if you are having difficulties:

- Did you back the Native Key Provider instance up before trying to use it? It will not let you use it until you have exported/backed up the primary key.
- Is there a key provider set as default?
- Is the host in a cluster? Standalone hosts cannot participate in Native Key Provider unless they are inside a cluster. However, you can create a cluster with just one host in it.
- Are you accessing the vSphere Client via a FQDN? You will not be able to export the Native Key Provider backup if you are accessing the vSphere Client via IP address.
- Did you indicate that only hosts with a TPM should participate in Native Key Provider, but you have hosts without a TPM?
- Do you have multiple vCenter Servers configured with independent Native Key Provider instances, but they are all named identically?

Can I move from Native Key Provider to another key provider, or vice-versa?

Yes. Define a new key provider, set it as the new default provider for the cluster, and then use the UI or PowerCLI to shallow rekey/re-encrypt to the new provider (instructions for rekeying are below). This will cause vSphere to re-encrypt the DEKs with a new KEK from the new key provider. A similar process is available for vSAN, too (also below).

Can I use Native Key Provider with a standalone host?

Organizations must use vCenter Server to manage Native Key Provider, and hosts must be inside a vSphere cluster object. However, you can put a single host inside a vCenter Server cluster object.

Can I use Native Key Provider with vSAN?

Yes! Configure Native Key Provider as the default before you enable data-at-rest encryption on the vSAN datastore & cluster or use the rekeying process to change between a standard key provider and Native Key Provider. For more information visit the vSAN Frequently Asked Questions page.

Can I use Native Key Provider with vSphere Trust Authority?

No; vSphere Trust Authority requires a Standard Key Provider (KMS).

How many hosts can use Native Key Provider? Are there scalability limits?

Native Key Provider has the same virtual machine scalability maximums as vSphere. See the VMware Configuration Maximum tool.

Do I need a Trusted Platform Module 2.0 (TPM) for my ESXi hosts?

While we recommend a TPM, one is not required to use Native Key Provider. If a TPM 2.0 is available and configured on the host it will be used to store the Native Key Provider keys. If one is not configured, the Native Key Provider keys will be stored as part of the encrypted ESXi configuration data.

Can I use TPM 1.2 for Native Key Provider?

No. Support for TPM 1.2 is deprecated in vSphere 7 and removed in vSphere 8.

What happens if check “Use key provider only with TPM protected ESXi hosts” and I do not have a TPM on my host?

If you leave the default “Use key provider only with TPM protected ESXi hosts” option selected, hosts without TPMs will not participate in Native Key Provider. When you attempt cryptographic operations on a virtual machine on those hosts they will fail.

If I have a cluster where some hosts have TPMs and some don’t, what happens if I only deploy to the TPM-enabled hosts?

If you only deploy to TPM-enabled hosts in a non-homogenous cluster there may be availability concerns, as part of the cluster will not be able to run those workloads. For best results on non-homogenous clusters please uncheck the TPM option when creating a Native Key Provider.

If I have a cluster where some hosts have TPMs and some don’t, will the TPM-enabled hosts use the TPM by default?

Yes, if a host has a TPM installed and configured it will be used to store ESXi secrets such as the Native Key Provider KDK.

Are there situations where Native Key Provider might not be suitable for use?

Threats and risks are something that organizations must assess for themselves when designing systems and organizational processes. However, one area of consideration is often around physical security of hosts. Since Native Key Provider stores decryption keys locally on ESXi hosts, an attacker that steals a host may still be able to unlock encrypted VMs and vSAN datastores. If physical security is a concern then Standard Key Providers configured to access a remote KMS may be a better solution, depending on your threat models, risks, and such.

What vSphere license do I need for Native Key Provider?

All vSphere editions include VMware vSphere Native Key Provider (NKP), which enables the use of vTPMs for workloads.

VM Encryption and vSAN Data-at-Rest Encryption can also use Native Key Provider, but require additional licensing (vSphere Enterprise Plus, for example).

Please consult with your account team for specifics.

What encryption technologies work with Native Key Provider?

VM Encryption, vTPM, and vSAN Encryption work with Native Key Provider.

vSphere Trust Authority, the feature that lets you create a trusted computing base with a separate vSphere cluster, currently requires the standard key provider.

Does ESXi Configuration Encryption require Native Key Provider?

ESXi Configuration Encryption does not use Native Key Provider. It uses the same encryption libraries present in vSphere but handles encryption operations itself, in order to manage and avoid dependencies at cluster startup.

Is the ESXi configuration encryption key stored in Native Key Provider?

No. It’s the opposite – the Native Key Provider KDK is stored in the encrypted configuration. If a TPM is present and configured it will be used to help protect the encrypted configurations.

Do the VMware Certificate Authority (VMCA) functions use Native Key Provider?

No, the VMCA and its certificate operations do not use Native Key Provider, though they all use the same shared encryption libraries present in vSphere.

Does Encrypted vSphere vMotion require Native Key Provider?

No. It uses the same underlying encryption libraries in vSphere, but it handles encryption operations itself. The keys used for vMotion Encryption are one-time use keys known as “nonces.” The vMotion encryption keys are ephemeral and not stored anywhere except temporarily in memory of vCenter Server and the two ESXi hosts involved.

Does vMotion work for virtual machines that are encrypted?

Yes, all vSphere features continue to work when you use virtual machine Encryption, vSAN Encryption, or vTPM with Native Key Provider.

Can I use Cross-vCenter vMotion to migrate encrypted virtual machines?

Yes. Encrypted virtual machines need to find their key provider configured at the destination. Simply import the backup of the key provider.

Does DRS work for virtual machines that are encrypted?

Yes, all vSphere features continue to work when you use virtual machine Encryption, vSAN Encryption, or vTPM with Native Key Provider.

Does vSphere HA work for virtual machines that are encrypted?

Yes, all vSphere features continue to work when you use virtual machine Encryption, vSAN Encryption, or vTPM with Native Key Provider.

What is a KEK?

KEK stands for Key Encryption Key and is a key used to encrypt other encryption keys.

What is a DEK?

DEK stands for Data Encryption Key and is the key that is used to encrypt individual virtual machine objects, like the NVRAM file where vTPM data is stored, VMDKs, etc. In vSphere, the DEK is encrypted with a KEK and written into the virtual machine configuration file for portability (replication, backups, etc.).

What is a KDK? What is the difference between a KDK and a KEK?

KDK stands for Key Derivation Key. Native Key Provider uses a key derivation function to generate the equivalent of a KEK for each virtual machine, with the KDK as the seed for that function. From a functional perspective it’s the same as a KEK stored in a standard key provider/KMS, but the underlying technology is different.

Where do hosts keep the KDK?

The Native Key Provider KDK is stored in a TPM, if the host has one, or as part of the ESXi encrypted configuration if the host does not have a TPM. When you configure the Native Key Provider, you can choose if you want to permit hosts without TPMs to participate.

Do I need to back up the Native Key Provider instance?

Yes, a backup of the Native Key Provider instance must be made before the key provider can be used.

Can the backups of key providers be automated?

Yes, you can use the vSphere APIs to trigger the backup, or use the vCenter Server File-Based Backup & Restore function, which also backs up key provider data as part of the overall vCenter Server backup.

Are key provider backups secure?

Native Key Provider backups allow for a password to be set on the exported file. Beyond that, security and availability of the backup files and/or the vCenter Server File-Based Backups are a design exercise for customers.

What keys are contained in the vCenter Server backups?

The Native Key Provider KDK is in the vCenter Server backup, as is authentication information for standard key providers, and all

sorts of other authentication information for vSphere SSO and such. It has always been important that you write this backup to a secure location.

Can I have more than one Native Key Provider?

Yes, you can have more than one Native Key Provider instance. However, only one key provider can be set as default.

How does Native Key Provider work with Enhanced Linked Mode (ELM)?

Key providers only serve hosts that are directly attached to a vCenter Server, and are not automatically replicated between the vCenter Servers that participate in Enhanced Linked Mode. Configure the individual vCenter Server key providers separately.

I have many vCenter Servers. Should I configure them all with different Native Key Provider instances, or should I export one and import it everywhere else?

This is a design decision on your part, but both options are supported. If you want to use Cross-vCenter vMotion to migrate encrypted workloads between clusters you will need the same key provider configured on both the source and the destination. If you choose to configure separate Native Key Provider instances ensure that their names are unique, so that future name collisions do not occur if you restore a backup of an Native Key Provider instance.

Are there problems with using the same Native Key Provider instance on all vCenter Servers?

This is supported. All environments are different, and any potential risks involved in using the same cryptographic keys in all locations should be modeled with the help of your own information security experts. It is worth noting that, if a Native Key Provider KDK is compromised, it is straightforward to create a new Native Key Provider instance, import it elsewhere, set as the default, and have all the virtual machines rekeyed to the new instance using PowerCLI, while the workloads are running.

Does the virtual machine have to be off to rekey/re-encrypt it?

A re-encrypt or “shallow rekey” can be done with the virtual machine powered on and operational. It only changes the KEK/KDK. A “deep rekey” changes the Data Encryption Key (DEK), which is what protects the virtual machine configuration files and VMDKs. A deep rekey requires the virtual machine to be powered off. To change the key provider you only need to do a shallow rekey or “re-encrypt” from the vSphere Client.

How do I do a “shallow rekey” of a VM?

A shallow rekey changes the KEK/KDK on a VM and can be done in several ways. In the vSphere Client, select the VM or VMs, right-click or “Actions,” select “VM Policies” and then “Re-encrypt.”

Alternately, use PowerCLI to automate the task:

```
$keyprovider = Get-KeyProvider -Name $keyprovidername -ErrorAction Stop
Set-VM -VM $vm -KeyProvider $keyprovider -SkipHardDisks
```

You can also put this action in a loop, which is helpful when changing between key providers:

```
foreach ($vm in Get-VM) {
    $vmview = Get-View $vm
    if ($vmview.Config.KeyId) {
        Set-VM -VM $vm -KeyProvider $keyprovider -SkipHardDisks -Confirm:$false -ErrorAction Stop
    }
}
```

You can use the vSphere API directly from a variety of languages. For more information visit https://developer.vmware.com.

Shallow rekeys can be done while the VM is powered on. The guest OS will never know!

How do I do a “deep rekey” of a VM?

A deep rekey changes the DEK for a VM and can be done in several ways. You can decrypt and then encrypt the VM again, or use PowerCLI to automate the task:

```
$keyprovider = Get-KeyProvider -Name $keyprovidername -ErrorAction Stop
Set-VM -VM $vm -KeyProvider $keyprovider -SkipHardDisks
```

You can use the vSphere API directly from a variety of languages. For more information visit https://developer.vmware.com.

Deep rekeys must be done with the VM powered off.

How can I rekey vSAN datastores?

You can configure a new key provider for vSAN in the vSphere Client, and then trigger a rekey operation from the UI. Or you can use PowerCLI:

```
$keyprovider = Get-KeyProvider -Name $keyprovidername
foreach ($cluster in Get-Cluster) {
    $clusterinfo = Get-VsanClusterConfiguration -Cluster $cluster
    if ($clusterinfo.EncryptionEnabled) {
        Write-Host "[REKEY] Rekeying vSAN datastores in $cluster to $keyprovider ($date)" -ForegroundColor Green
        Start-VsanEncryptionConfiguration -Cluster $cluster -KeyProvider $keyprovider -Confirm:$false -ErrorAction
Stop | Out-Null
        Start-VsanEncryptionConfiguration -Cluster $cluster -ShallowRekey -Confirm:$false -ErrorAction Stop | Out-Null
    } else {
        Write-Host "[SKIP]  $cluster does not have an encrypted vSAN datastore ($date)" -ForegroundColor White
    }
}
```

How can I tell if a VM is using Native Key Provider?

You cannot tell directly if a VM is using Native Key Provider, but you can find VMs that are encrypted by using the $VM.ExtensionData.Config.KeyID objects in PowerCLI, like:

```
foreach ($VM in Get-VM) {
    if ($vm.ExtensionData.Config.KeyId) {
        echo $vm.name
    }
}
```

If I move a host with encrypted virtual machines on it to another vCenter Server, what will happen?

vCenter Server synchronizes and remediates key provider configurations every five minutes by default, controlled by the vpxd.KMS.remediationInterval vCenter Server advanced option. This means there is a short time where everything may appear to continue to work, but that may be deceptive.

If the same Native Key Provider instance is configured in both locations everything will continue to work. If not, and the virtual machines are running, they will continue running, but once those virtual machines are powered off, they will be unable to power on again until the correct key provider is imported.

If encrypted virtual machines are not running, they will become locked, and alarms will be displayed. Once the correct key provider is imported a vSphere administrator can re-enable encryption mode on the host. This will unlock all encrypted virtual machines and allow them to be powered on.

After this move, we suggest re-encrypting/re-keying virtual machines to your preferred key provider to ensure consistency.

I use Site Recovery Manager. What considerations are there to ensure encrypted virtual machines can run on the DR site?

When using Site Recovery Manager, you must configure both vCenter instances with the same vSphere Native Key Provider key encryption key (KEK). This requires you to export the vSphere Native Key Provider from one vCenter instance and import it into the DR vCenter instance. For more see Site Recovery Manager and Virtual Machine Encryption.

Does VMware vCenter Server HA support Native Key Provider?

Yes. vCenter Server HA is not considered a backup strategy, so please back up the Key Derivation Key as instructed when you created the Native Key Provider instance.

Can I have both a Native Key Provider and a Standard Key Provider?

Yes. This is also a technique to set cross-vCenter vMotion up between sites if there isn't a common key provider between them. Create a "migration" Native Key Provider instance on the source, import it on the destination, rekey the virtual machine to the "migration" Native Key Provider instance, and vMotion it. At the destination you can rekey the virtual machine using the desired key provider.

Can I rename the Native Key Provider?

Not directly. Choose the name wisely if you plan to import it elsewhere, so that you do not have name collisions. You can create a new key provider, set it as the default, and do a shallow rekey/re-encrypt to move virtual machines to the new provider. See instructions in this FAQ for more information on rekeying VMs.

How often does Native Key Provider rotate its keys?

Native Key Provider does not rotate its keys automatically, as that could endanger other environments where that key is used. To change the Native Key Provider key you can create another Native Key Provider instance, set it as the default key provider, and do a shallow rekey/re-encrypt to move virtual machines to the new provider. See instructions in this FAQ for more information on rekeying VMs.

What is in the backup .p12 file?

The Key Derivation Key is exported in the backup file.

Where should I keep the backup .p12 file?

This is a design decision organizations need to make for themselves. Somewhere safe but also accessible in case of emergency. Large organizations usually have a solution for this. Smaller organizations might consider something like a safety deposit box for offsite copies. Ensure the media is reliable.

Should I set a password on the .p12 file?

This is a design decision customers must make. On one hand, it seems like a good idea to protect the key in that manner. On the other hand, if someone needs to restore it from backup during an incident, how will the person doing that work know the password? Some organizations have chosen to omit the password when the storage location is secure, but it's up to you. Do what works and is secure for YOUR organization.

Can I delete a Native Key Provider instance? What problems might I experience?

Yes. However, due to the way Native Key Provider works it is impossible to tell if a key provider is in use by a virtual machine. Encrypted virtual machines may be backed up and/or replicated, and if you delete the key provider you may lose access to those copies. We recommend re-keying all virtual machines to the desired Native Key Provider instance as a preventative step prior to deleting the key provider. Ensure that you have a backup of the key provider stored so that, if there is an issue, the key provider can be imported again.

If I delete a Native Key Provider should I delete the .p12 files I've stored?

Whether you should delete them or not is up to you. The backup key files (.p12 files) might be necessary to decrypt replica or backed-up copies of virtual machines.

How do I tell which virtual machines are using a key provider?

There is currently no method to tell which virtual machines are using a key provider except by examining the .vmx file for each virtual machine. To work around this we suggest setting the default key provider as you desire, then doing a re-encrypt on the virtual machines to ensure they're using the key provider you want.

What FIPS 140-2 levels does Native Key Provider support?

FIPS 140-2 defines different "levels" of requirements. Levels 2 through 4 require tamper-evident physical devices. As shipped by VMware, Native Key Provider is a completely software-based solution and does not involve devices. Therefore, it meets Level 1 requirements, as vSphere does.

Is Native Key Provider certified for use with PCI DSS, HIPAA, NIST 800-53, ISO 27001, etc.?

Native Key Provider is often used to meet data-at-rest requirements found in a variety of regulatory compliance frameworks. Compliance certification happens against implementations of software, not the software itself, and will depend on the design and implementation decisions you make when building your environment. Please consult your compliance auditors for more information about how system design choices may affect your compliance goals.

I replicate to a DR site; how will I decrypt my replicated virtual machines?

You can import the Native Key Provider backup into the DR site vCenter Server. That will allow that cluster to decrypt and run the encrypted virtual machines. We recommend testing it prior to an incident, of course. Ensure that a copy of the key provider backup is also available to the DR site.

Is Native Key Provider available in VMware Cloud on AWS SDDCs?

Yes, but not completely like the on-premises version. Native Key Provider is enabled in VMware Cloud on AWS 1.19 and later in order to enable vTPM. However, the Native Key Provider instance is not configurable by customers beyond that. Individual virtual machine Encryption and configurable Native Key Provider are roadmap items. Need these features? Submit a feature request

through your account team so our product managers know that there is interest and that you have a use case for it.

Is the SDDC Native Key Provider backed up in VMware Cloud on AWS?

Yes. The VMware Cloud on AWS service automatically backs up and stores the recovery key (Key Derivation Key) for customers. VMware Cloud on AWS Support can restore the backup key if needed.

Can I import a Native Key Provider key into VMware Cloud on AWS?

Key provider configurations in an SDDC are not currently available for customer configuration.

Do I need to set the Native Key Provider to be the default before I remove the old provider?

If you delete the key provider that was the default, you will not have a new default until you assign one (we do not have enough information to safely assign a new default so we leave it to an administrator to do). There should always be a default key provider configured.

Are encryption keys persisted across ESXi reboots?

Functionally yes. Because the ESXi host has the Key Derivation Key stored as part of its configuration it can operate independently.

Do I need to enable ESXi Key Persistence to use Native Key Provider?

No – ESXi Key Persistence is a separate feature that, in effect, caches encryption keys from a standard key provider (not a Native Key Provider) on a host using the host's Trusted Platform Module. While Native Key Provider does something similar, it does not use the Key Persistence feature, and does not require the feature to be enabled.

Key Persistence is disabled by default, and the use cases for the feature are limited. Most organizations should not enable Key Persistence without thoroughly examining their threat models and risks.

What algorithms are used for generating keys in Native Key Provider?

AES.

What is the length of a key in Native Key Provider?

256 bits (AES).

Does Native Key Provider use SHA1?

No.

Can I customize the length of the keys that are used for the KDK, KEK, or DEK?

No, they are a fixed length and cannot be altered.

What impact is there to encrypted virtual machines if vCenter Server is offline?

There is no immediate impact to encrypted virtual machines while vCenter Server is offline. When using a properly configured Native Key Provider, each ESXi host in a cluster has a copy of the KDK stored and can operate independently.

How are Native Key Provider keys protected in transit?

All management communications between vCenter Server and ESXi are protected with TLS.

How are Native Key Provider keys protected at rest?

The Native Key Provider KDK is stored in the ESXi encrypted configuration. If a TPM is present and configured it will be used to help protect the encrypted configuration.

In theory, could an attacker get the Key Derivation Key from the VCSA VMDK, then be able to decrypt all the VMs that are on the same cluster?

The Native Key Provider key derivation key is stored in the VCSA. It is also stored on the hosts, in a TPM If available, or on the boot disk there, too. For someone to retrieve it from the VCSA VMDK on disk they will need administrative access to the vSphere cluster it resides in, which would also mean they could just log into vCenter to do whatever nefarious acts they were planning.

They could also retrieve it from image or file-based backups of the VCSA, too.

Eventually something needs to know that key so that decryption can happen, but because of dependencies NKP has to put the key in places that also make it susceptible to theft. Standard Key Providers (using an external KMS) use a different model and don't

cache the keys locally like that, though someone who has access to the VCSA VMDK could retrieve the KMS login credentials, too. Tough problem to solve because someone eventually needs to know how to get the keys. This is why VMware recommends isolation of the infrastructure management interfaces, such that access is controlled, and unauthorized access can be detected quickly.

Disclaimer

This document is intended to provide general guidance for organizations that are considering VMware solutions. The information contained in this document is for educational and informational purposes only. This document is not intended to provide advice and is provided “AS IS.” VMware makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of requirements and effectiveness of implementations.

Additional Resources

Please visit the vSphere security resources at https://core.vmware.com/security.

Feedback

The purpose of this document is to answer questions that may fall outside the scope of product documentation and system design guidance. Your feedback is valuable. To comment on this document please use the feedback mechanisms on this page. Thank you.